

14.6 CYBERARK

CyberArk is a complete cybersecurity solution designed to protect and manage sensitive accounts and credentials (Privileged Access Management).

It includes several components like password vaulting, session monitoring, and automatic access control.

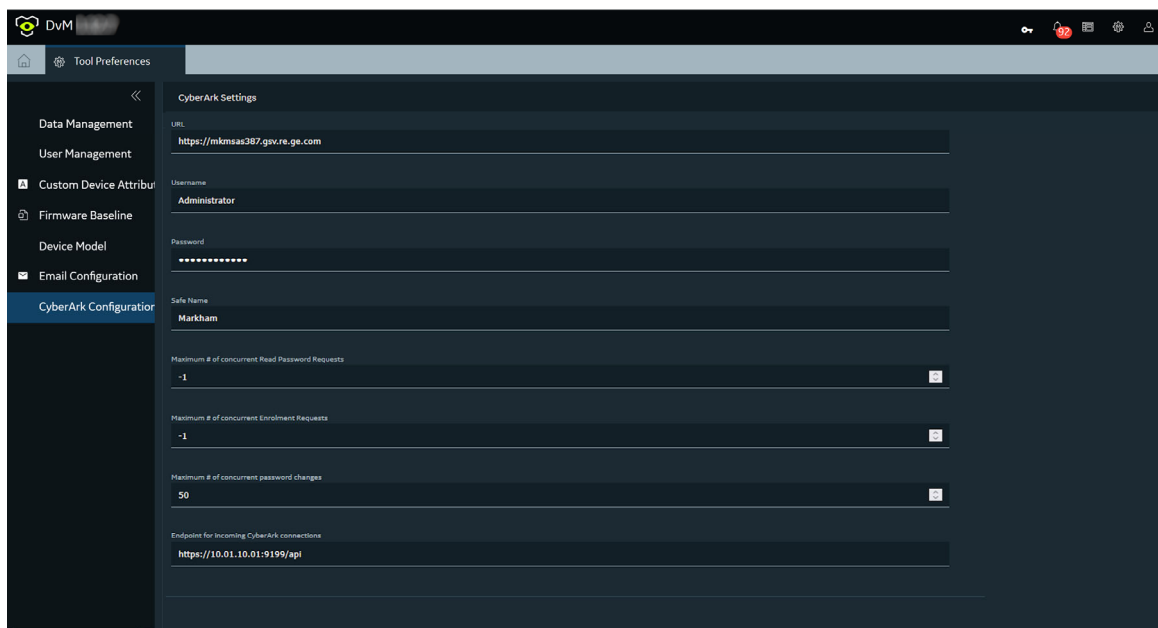
CEPA (CyberArk Enterprise Password Automation) is one of these components. It focuses on automating the creation, rotation and removal of privileged passwords. It automatically controls access and keeps audit logs to reduce the risks linked to privileged access.

14.6.1 CONFIGURE INTEGRATION WITH CYBERARK PVWA

To configure integration with CyberArk PVWA (Password Vault Web Access):

- Log in to DvM.
- Click on the **Settings** icon  and select **Tool Preferences**.
- In the left menu, select **CyberArk Configuration**.

The **CyberArk Settings** view is displayed. This is where the user can set up the CyberArk parameters:



The screenshot shows the 'CyberArk Settings' configuration page within the DvM interface. The left sidebar contains a menu with options: Data Management, User Management, Custom Device Attribution, Firmware Baseline, Device Model, Email Configuration, and CyberArk Configuration (which is highlighted). The main content area is titled 'CyberArk Settings' and contains the following fields:

- URL:** `https://mkmsac387.gvx.re.ge.com`
- Username:** `Administrator`
- Password:** `*****`
- Safe Name:** `Markham`
- Maximum # of concurrent Read Password Requests:** `-1`
- Maximum # of concurrent Enrollment Requests:** `-1`
- Maximum # of concurrent password changes:** `50`
- Endpoint for incoming CyberArk connections:** `https://10.01.10.01:9199/api`

CyberArk Settings section

- **URL:** URL of your CyberArk PVWA server. This allows CEPA to communicate with CyberArk to read, enroll and rotate credentials.
- **Username:** username to log in to the CyberArk web console.
- **Password:** corresponding password for the above username (hidden for security).
- **Safe Name:** you may optionally specify a CyberArk safe where credentials are stored and managed.

- **Maximum number of concurrent Read Password Requests:** defines how many simultaneous password retrievals are allowed.
- **Maximum number of concurrent Enrollment Requests:** sets the number of account enrollment operations.
- **Maximum number of concurrent password changes:** Limits how many password rotation actions can happen at the same time.
- **Endpoint for incoming CyberArk connections:** Internal API endpoint used between CEPA and CyberArk services to verify password operations.

Click **Save** to apply and active these settings.

14.6.2 ENROLL DEVICES AND APPLICABLE ACCOUNTS

DvM natively supports integration with CyberArk.

When the user imports or adds a device to DvM, the device and applicable accounts are automatically enrolled for password rotation in CyberArk.

To ensure a new device is enrolled, log in to the **CyberArk Password Vault Web Access (PVAM)** interface. After signing in, authorized users can access the vault to retrieve/rotate credentials and manage accounts.

In CyberArk, go to the **Accounts View**. It shows the list of all accounts according to their status.

Note: To filter accounts for a particular device, enter (or copy/paste) the CyberArk ID of this device (GUID/UUID format). The corresponding CyberArk ID can be seen in the **Device view** > [Device Identification](#) panel.

In the **Accounts view** page, the device name matches the device name in DvM. All accounts associated with the current device are displayed in the **Username** column.

Device CyberArk ID

Accounts View

Filter: 844c3ccd-c58a-4a50-ad5b-dfb533a43699

Views: Recent Saved

My accounts: All accounts (default), Recently used, Favorites, Checked-out

Status: Disabled by CPM, Failed, Newly added, Deleted

Operational state: Scheduled for Change, Scheduled for Verification, Scheduled for Reconciliation, Successfully Reconciled

4 results for: 844c3ccd-c58a-4a50-ad5b-dfb533a43699

Status	Username	Platform ID	Safe	Device Name	Access Request	
☆ ⚡	ZAC	GE_SEL_MODERN	Markham	SEL_651R_HTC_New88	-	Show ...
☆ ⚡	ACC	GE_SEL_MODERN	Markham	SEL_651R_HTC_New88	-	Show ...
☆ ⚡	BAC	GE_SEL_MODERN	Markham	SEL_651R_HTC_New88	-	Show ...
☆ ⚡	CAL	GE_SEL_MODERN	Markham	SEL_651R_HTC_New88	-	Show ...

Device accounts

Device name as in DvM

S000ENa

To view and manage a specific privileged account on the device, select the account row in the results grid.

The details panel opens on the right. Click **Additional details & actions in classic interface** in the right panel.

Accounts View

Filter: 844c3ccd-c58a-4a50-ad5b-dfb533a43699

4 results for: 844c3ccd-c58a-4a50-ad5b-dfb533a43699

Status	Username	Platform ID
★ ⚡	ZAC	GE_SEL_MODERN
★ ⚡	ACC	GE_SEL_MODERN
★ ⚡	BAC	GE_SEL_MODERN
★ ⚡	CAL	GE_SEL_MODERN

ACC On 10.14.25.28:9199

Platform: GE_SEL_MODERN Safe: Markham

Additional details & actions in classic interface

Overview Details Activities Versions

Compliance Status **Compliant**

0 Days ago

Changed by lakeran Jan 30, 2024 8:57 AM

Reconcile Change

Last Verified

Never Verified Created 5 hours ago

Verify

Activities (Last 5)

- Jan 30 8:58:09 AM lakeran Add File Category
- Jan 30 8:58:09 AM lakeran Add File Category
- Jan 30 8:58:09 AM lakeran Add File Category
- Jan 30 8:58:07 AM lakeran Add File Category
- Jan 30 8:58:07 AM lakeran Add File Category

Last Access

by lakeran Today

The **Account Details** view is displayed. In the **Password** area, click **Show**.

Account Details

Edit Change Reconcile Verify Send Link Refresh

Password

Show

Platform Name: GE_SEL_MODERN

Device Type: Imported Platforms

Safe: Markham

Name: ACC-844c3ccd-c58a-4a50-ad5b-dfb533a43699

Last verified: N/A

Last modified: lakeran (1/30/2024 10:57:59 AH)

Last used: lakeran (1/30/2024 10:57:59 AH)

Username: ACC

Vendor ID: 2

Device Name: SEL_651R_HTC_New88

Customer Device: Sel_651R_HTC_New88

ID: 10.14.25.28:9199

Address: 10.14.25.28:9199

Device ID: 844c3ccd-c58a-4a50-ad5b-dfb533a43699

Device Type: SEL-651R

Device Firmware: RA

Version: 1.0.0

CPN

Account	Platform	Clear	Associate	Create New
Account 1:	GE_SEL_MODERN-ACC-10.14.25.28:91			
Account 2:	GE_SEL_MODERN-ZAC-10.14.25.28:91			
Account 3:				

Account Group

Group: [Name]

Modify Create New

If prompted, enter the reason for showing the password and click **OK**.

The password for the selected account is displayed so you can verify that it has been enrolled correctly.

14.6.3 MANAGE DEVICE ACCOUNTS

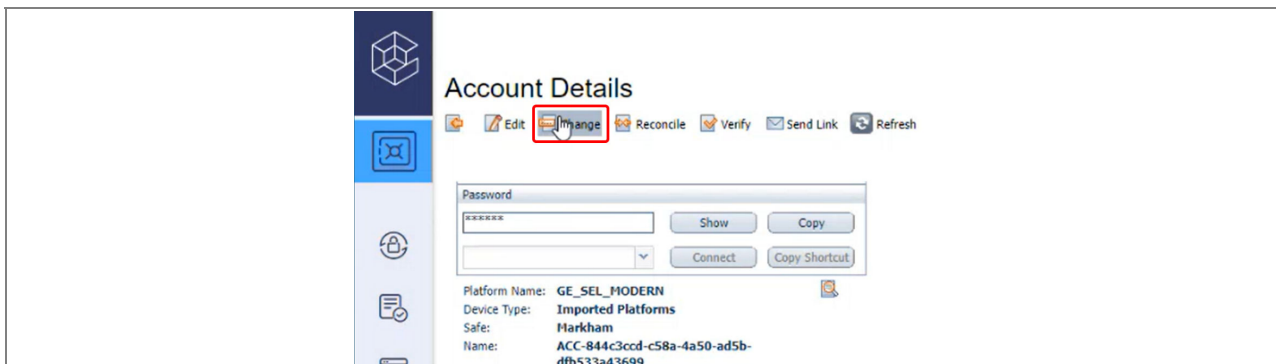
14.6.3.1 CHANGE PASSWORDS IN CYBERARK

When an account is added to CyberArk, a specific user-defined policy is assigned to it (*automatic password rotation, checkout requirements...*).

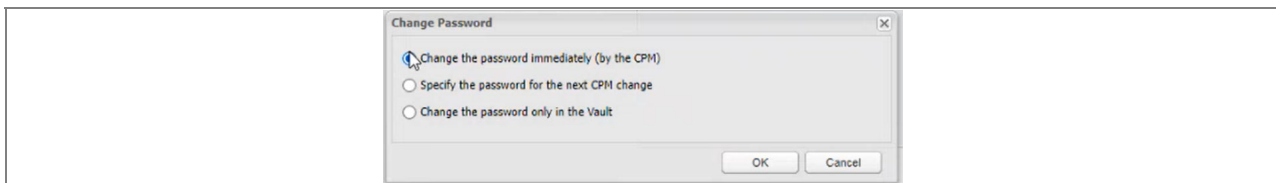
But authorized users can initiate an immediate password change in which the **Central Policy Manager (CPM)** will change the password to a new random password.

To change a password in CyberArk:

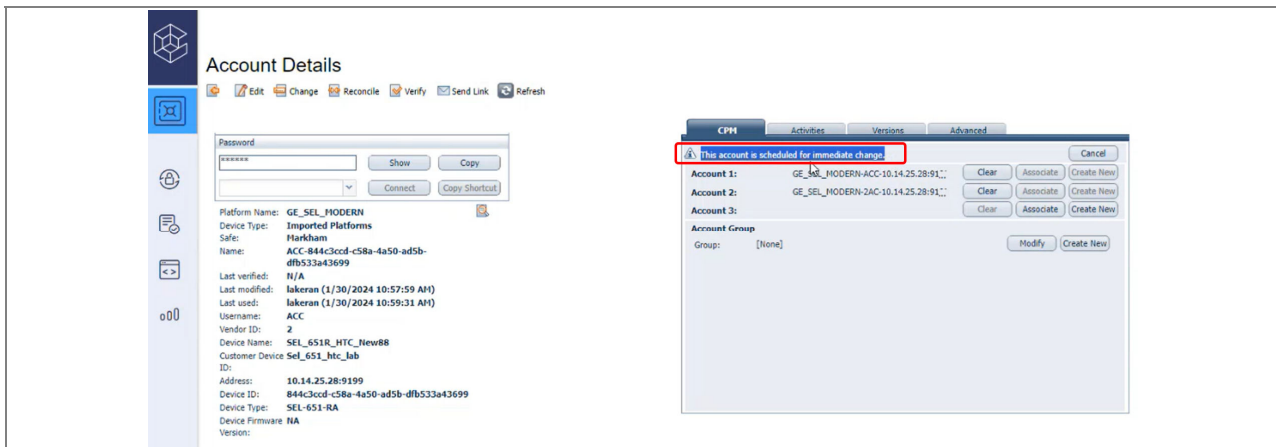
- Click the desired device account. The details panel is displayed on the right. Click **Additional details & actions in classic interface** in the right panel.
- In the **Account Details** view, click **Change**:



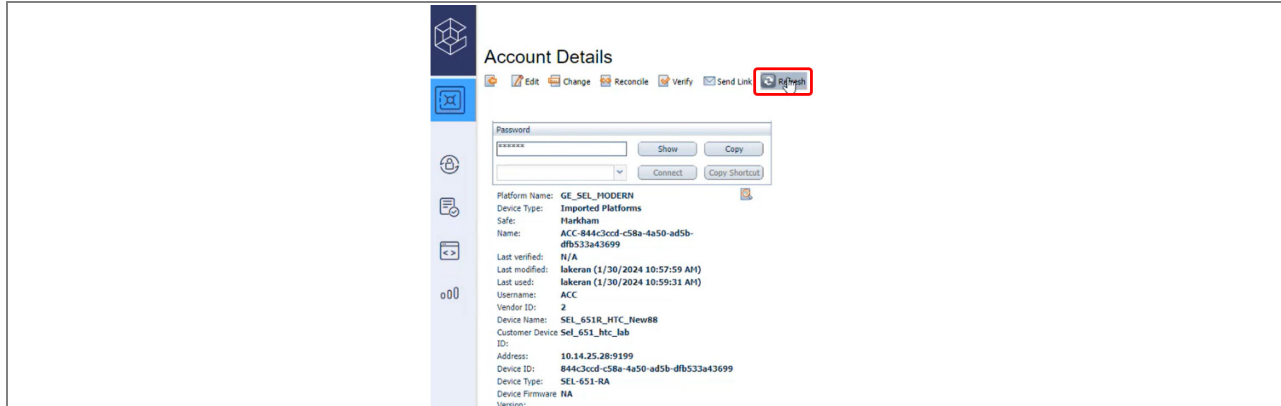
- In the **Change password** popup, select **Change the password immediately (by the CPM)** and click **OK**.



- A warning message that the account is scheduled for immediate change is highlighted:

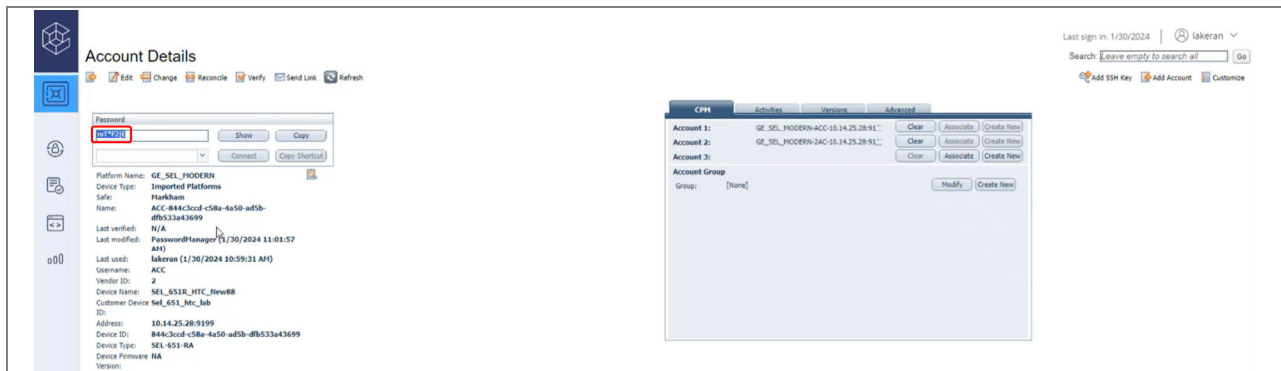


- Click **Refresh** to make sure that there is no error message:



- If there is no error message, the user can assume that the password change was successful. To verify it, open the device logs in DvM. The states for the actual operation are listed. A validation message indicates that the password change for that device was successful.
- Go back to the **Account Details** in CyberArk and refresh the page. The warning has disappeared.
- Click **Show**. If prompted, enter a reason for showing the new random password and click **OK**.

The new password is displayed:



14.6.3.2 CONNECT TO THE DEVICE WITH THE NEW PASSWORD

To confirm the new password was updated on the device, connect to it using any supported access method (*i.e. Telnet, SSH...*) and enter the new password. The connection should be successful.

You can also open the IED configuration tool. If the communication credentials still use the default (old) passwords, the tool will fail to connect to the device. To read settings from the device, a valid user account is required. Because the previous password is no longer valid, the tool should prompt for credentials. Enter the new password for the account. The connection should succeed, and the tool should retrieve settings from the device.