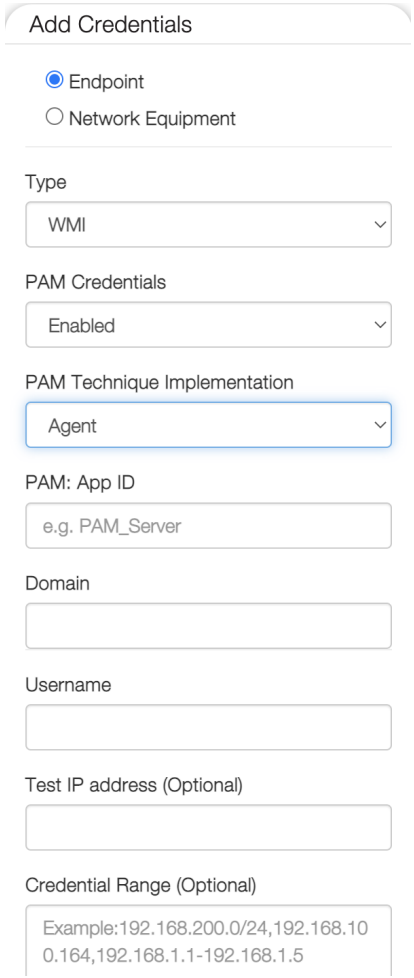
Orchestra Group

Perform secure Orchestra Purple vulnerability scans using the CyberArk Privileged Access Manager

Simple Setup

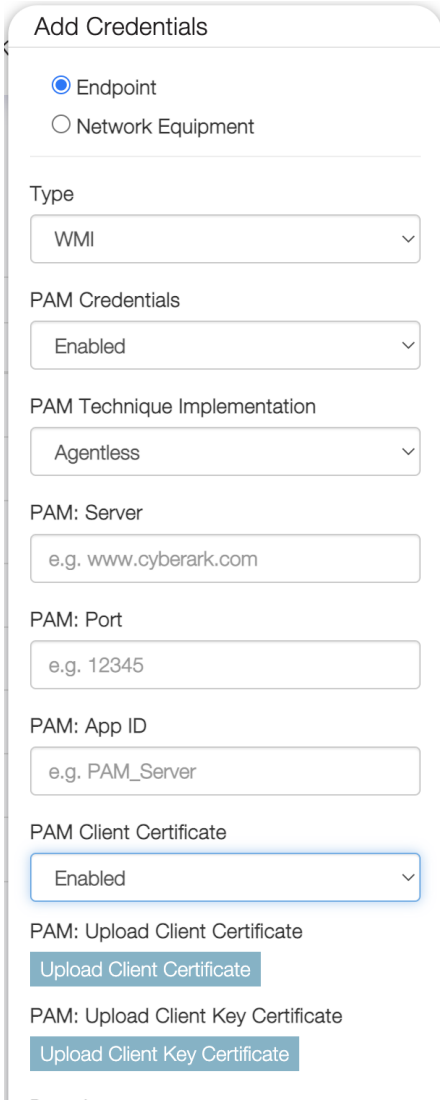
1. User configures the CyberArk solution in the desired default and creates an application for Purple
2. User configures the Purple-CyberArk authentication details using the Purple System Credentials section
3. Choose an Endpoint scan
4. Choose the scan type (WMI or SSH, both use PAM)
5. Enable “PAM Credentials” (Highlighted below)
6. In addition to the standard scan fields, populate the PAM related fields:
    a. For the agent solution:

i.



ii. **Please note:** CyberArk server and port should be predefined when deploying Purple
iii. Application ID - the ID provided when creating the Purple application using the CyberArk portal

b. For the agentless solution:
i. Server - the URL for the PAM server
ii. Port - the port used to access the PAM server
iii. Application ID - the ID provided when creating the Purple application using the CyberArk portal
iv. Certificate (Optional) - make sure you upload a .crt file



How does the scan work?

1. Launch a scan
2. The Harmony Purple service queries CyberArk's Privileged Access Manager for secure credentials retrieval from the CyberArk Digital Vault
3. Purple scans the server using the provided credentials (Works on both Windows and Unix)
4. The server validates the credentials provided by both Purple's scanner against the one provided by CyberArk