**How does CPM manage Windows accounts / passwords?**

The CPM uses Microsoft API commands to connect to, verify, change and reconcile passwords for Windows accounts. The best way to simulate the CPM's actions are as follows:

Note: All commands must be run from the CPM machine.

* Connect / Verify
From the Command Line:
**"net use \\<address>\IPC$ /user:<domain>\<username>"**Note:
	+ When using a local account, <address> and <domain> are identical and are taken from the "address" property of the password object
	+ When using a domain account, <domain> is taken from the "address" property of the password object and for the <address>, run the following to find the server name or IP address to be used: **"nslookup <domain>"**. CPM should be in the same domain as the target domain or have a trust with it.
* Change password
	+ Press Ctrl+Alt+Del. and then press "Change Password". Make sure you type the address in the "Log on to:" field and the user name as specified in the password object.
* Reconcile password
	+ Make sure you are able to Connect (see above method) using the reconcile account credentials.
	+ For a local account, logon to the remote machine with the reconcile account credentials and type the following command from the Command Line: **"net user <username> <password>"**
	+ For a domain account, logon to the CPM machine using the reconcile account credentials and type the following command from the Command Line: **"net user <username> <password> /domain"**

**Note:** For Windows 2008, "User Account Control: Run all administrators in Admin Approval Mode" (located in Security Policy of the target machine) must be disabled (disabling this, requires restart of the machine).

The following Windows settings control the ability to connect to remote machines:

* From the Properties of Local Area Connection:
1. "File and Print Sharing For Microsoft Networks" is enabled.
2. "Client for Microsoft Networks" is enabled.
* "Network security: LAN Manager authentication level:" in the security policy of the CPM matches the remote machine's requirements setting.
Default is "Send LM & NTLM responses".
For managing remote accounts with various requirements (LM, NTLM and NTLMv2) set "Send LM & NTLM - use NTLMv2 session security if negotiated".
* NETBIOS name, Primary DNS Suffix and WINS server setup allows resolving the remote machine name.

Make sure the "Workstation" service is running on the local computer while "Server" service is running on the remote computer

For password management the CPM uses the Microsoft API to communicate with the target devices using SMB to connect to the IPC share. In previous versions of windows 139 was used over NetBIOS however 445 is used for modern windows operating systems to access the IPC share (SMB direct over TCP/IP). In current systems if port 445 is not available then port 139 would be used although 445 is used as a preference but this is down to the operating system and not the CyberArk components.