

Purpose

This tool automates the process of migrating PSMConnect and PSMAdminConnect accounts from local to domain-based. By using this tool, you can ensure a seamless transition and better management of these accounts in your CyberArk environment.

Prerequisites

Before running the tool, you need to complete the following steps:

1. Environment Setup

Make sure that you have installed the following components:

- Vault
- PVWA (Password Vault Web Access)
- CPM (Central Password Manager)
- PSM (Privileged Session Manager)

Also, make sure that PSM is joined to the domain.

2. Domain Controller Configuration

You need to configure the following elements on the domain controller:

- Organizational Unit (OU):
 - Create an OU for PSM.
 - Add the PSM machines to this OU.
- Group Policy Object (GPO):
 - Create a new GPO object.
 - Import the In-Domain GPO from the hardening folder in the PSM installation package into this GPO object.
Use the standalone GPO, or the unified GPO if CPM is installed on the same machine as PSM.
 - Link the new GPO object to the OU.

3. Client (End-User) Machine

Ensure the following for the Client (End-User) Machine:

- The machine is joined to the same domain as the PSMs.
- .NET Framework 4.8 is installed on the machine.

Usage Instructions

1. Prepare the Configuration File

Create and edit the config.yaml file with the parameters shown below:

```
# =====  
# PSMDomainUsersTool Configuration File  
# =====  
  
# psmGPOName – Exact name of the Group Policy Object that hardens / configures  
# PSM.  
# psmHostnames – Comma-separated NetBIOS hostnames of every PSM server.  
#       Example: "PSM-01, PSM-02, PSM-DR"  
# cpmUsername – CPM service user that rotates the PSM applicative-user credentials.  
#       Leave it empty ("" ) if you are not integrating with CPM.  
  
psmGPOName: "PSM_Standalone_v14.6_Clean"  
psmHostnames: "PSM-01, PSM-02, PSM-DR"  
cpmUsername: ""
```

Field descriptions:

Field	Where to find / how to set
psmGPOName	Open Group Policy Management (gpmc.msc) and copy the exact name of the PSM-hardening GPO.
psmHostnames	1. RDP to each PSM server. 2. Open PowerShell and run: hostname 3. Copy each result and list them in one line, separated by commas.
cpmUsername	Enter the CPM service account if you use CPM. otherwise leave it as "".

2. Log in to the Client (End-User) Machine

Log in with domain admin privileges.

3. Run the Tool

Execute `PSMDomainUserTool.exe` using PowerShell as an administrator.

4. Input Credentials

Enter the following credentials when prompted:

- Domain Admin Credentials: For performing domain operations.
- Vault Admin Credentials: For interacting with the CyberArk vault.

5. Monitor the Process

The tool will perform the following tasks:

- Migrate PSMConnect and PSMAAdminConnect accounts to domain-based accounts.
- Update system settings and security configurations accordingly.

Post-Execution Verification

After the tool has finished its tasks, you can verify the success by:

- Checking PSM Sessions:
 - Log in to each PSM machine and open Task Manager.
 - Check that PSMConnect and PSMAAdminConnect sessions are using domain accounts instead of local accounts.
- Reviewing Security Policies:
 - Verify that the new domain users have the appropriate rules applied in the Local Security Policy under AppLocker.