



# PAM Administration

## Troubleshooting Common Issues



# Agenda

By the end of this session, you will be able to perform basic troubleshooting tasks to resolve common issues related to:

- User authentication
- Component connectivity to the **Vault**
- Automatic password management by **CPM**
- Launching privileged sessions via **PSM**



# User Authentication Issues



# User Receives an Authentication Failure

Bill is unable to log in.  
He changed his network password recently and tried to log in to the **PVWA** with his old password.  
Now he is trying with his new password and it does not work.  
He contacts his Vault administrator.



✖ Authentication failure for User [bill].

Specify your **Idap** authentication details

Username

Password

Sign In

< Change authentication method

Activate Windows  
Go to Settings to activate Windows.

# Identifying the Error in the ITAlog

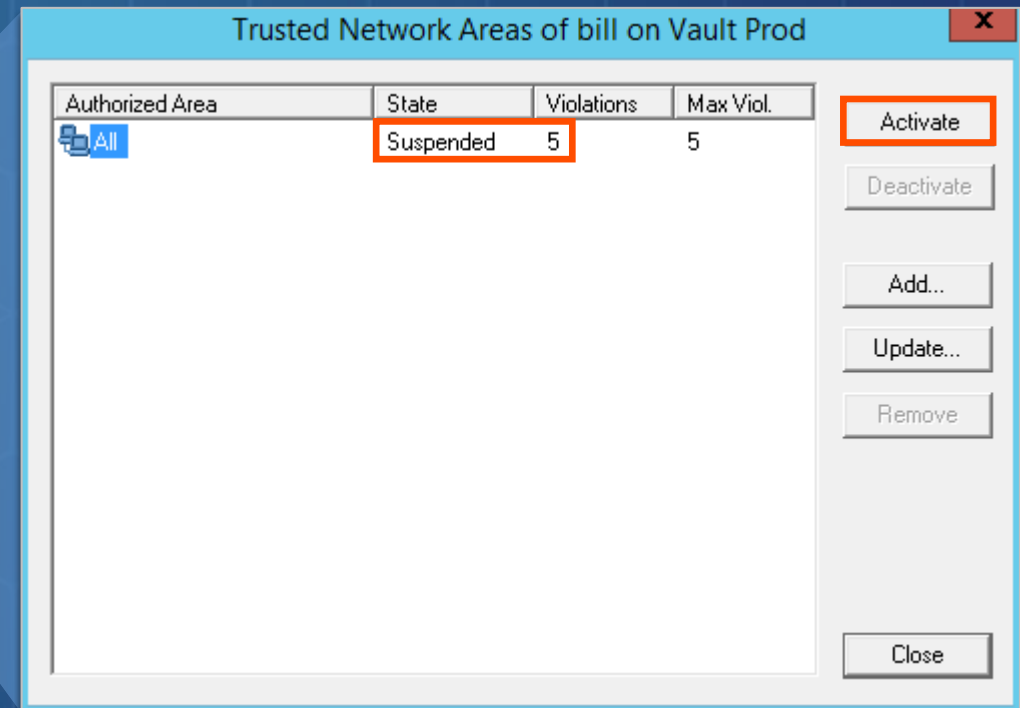
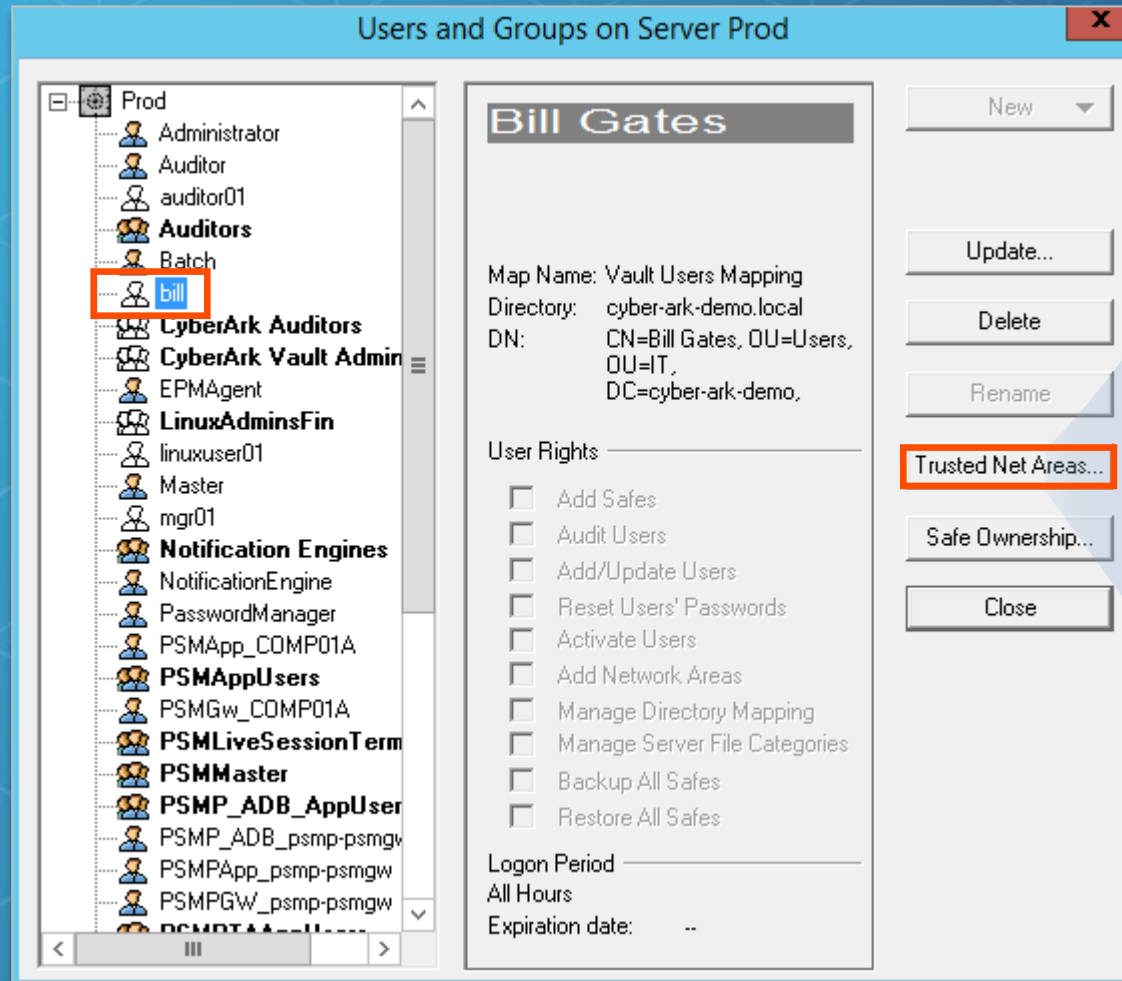
The Vault administrator can see in the ITAlog on the Vault that the user Bill failed to log in 5 times and then was suspended.

```
itaalog.log
5 04/02/2019 14:25:42 ITATS319W Firewall contains external rules.
6 04/02/2019 14:40:44 ITATS319W Firewall contains external rules.
7 04/02/2019 14:55:47 ITATS319W Firewall contains external rules.
8 04/02/2019 15:10:50 ITATS319W Firewall contains external rules.
9 04/02/2019 15:22:36 ITATS528E Authentication failure for user bill from station: 10.0.20.1 (code: -108).
10 04/02/2019 15:22:41 ITATS528E Authentication failure for user bill from station: 10.0.20.1 (code: -108).
11 04/02/2019 15:22:44 ITATS528E Authentication failure for user bill from station: 10.0.20.1 (code: -108).
12 04/02/2019 15:22:48 ITATS528E Authentication failure for user bill from station: 10.0.20.1 (code: -108).
13 04/02/2019 15:22:52 ITATS528E Authentication failure for user bill from station: 10.0.20.1 (code: -108).
14 04/02/2019 15:22:58 ITATS433E IP Address 10.0.20.1 is suspended for User bill.
15 04/02/2019 15:23:26 ITATS433E IP Address 10.0.20.1 is suspended for User bill.
16 04/02/2019 15:24:13 ITATS433E IP Address 10.0.20.1 is suspended for User bill.
17 04/02/2019 15:25:52 ITATS319W Firewall contains external rules.
18 04/02/2019 15:40:56 ITATS319W Firewall contains external rules.
19 04/02/2019 15:55:58 ITATS319W Firewall contains external rules.
20 04/02/2019 16:11:01 ITATS319W Firewall contains external rules.
21 04/02/2019 16:26:04 ITATS319W Firewall contains external rules.
```

Normal text file      length: 1 550 lines: 21      Ln: 14 Col: 79 Sel: 78 | 1      Windows (CR LF) UTF-8      INS



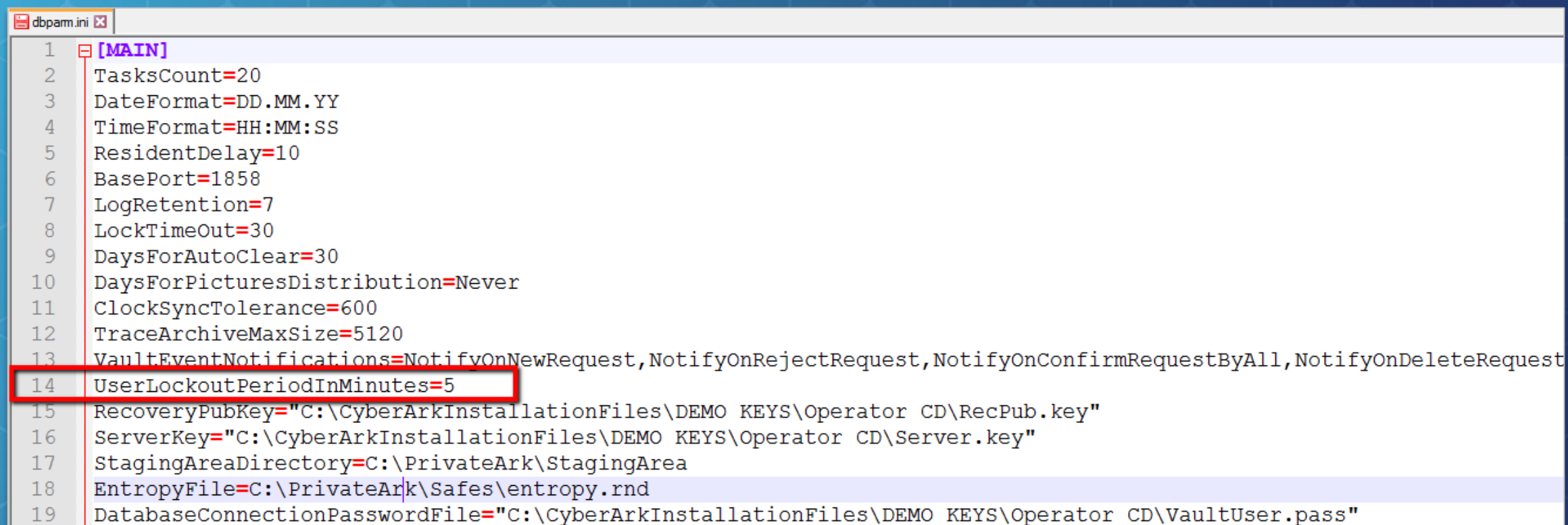
# Unsuspend the User





# Automatic Unsuspend

The **Vault** can be configured to unsuspend users automatically after a predefined time period, using the **UserLockoutPeriodInMinutes** parameter in *dbparm.ini*.



```
dbparm.ini
1 [MAIN]
2 TasksCount=20
3 DateFormat=DD.MM.YY
4 TimeFormat=HH:MM:SS
5 ResidentDelay=10
6 BasePort=1858
7 LogRetention=7
8 LockTimeOut=30
9 DaysForAutoClear=30
10 DaysForPicturesDistribution=Never
11 ClockSyncTolerance=600
12 TraceArchiveMaxSize=5120
13 VaultEventNotifications=NotifyOnNewRequest,NotifyOnRejectRequest,NotifyOnConfirmRequestByAll,NotifyOnDeleteRequest
14 UserLockoutPeriodInMinutes=5
15 RecoveryPubKey="C:\CyberArkInstallationFiles\DEMO KEYS\Operator CD\RecPub.key"
16 ServerKey="C:\CyberArkInstallationFiles\DEMO KEYS\Operator CD\Server.key"
17 StagingAreaDirectory=C:\PrivateArk\StagingArea
18 EntropyFile=C:\PrivateArk\Safes\entropy.rnd
19 DatabaseConnectionPasswordFile="C:\CyberArkInstallationFiles\DEMO KEYS\Operator CD\VaultUser.pass"
```

# Component Connectivity Issues





# Identifying a Suspended Component

The screenshot displays the 'System Health' dashboard of the PVWA (Privileged Vault Web Administration) interface. The dashboard is organized into several sections:

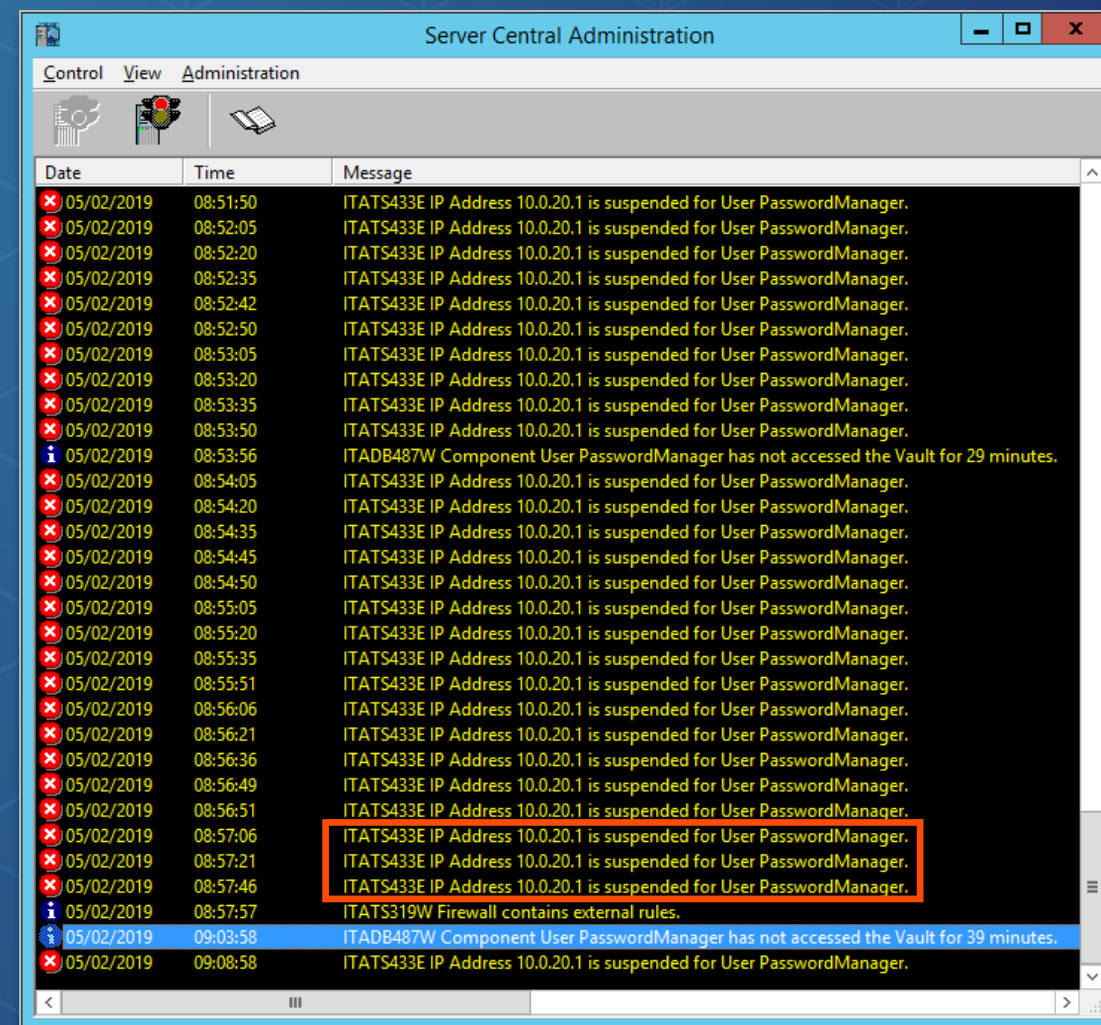
- Vaults:** Shows two vaults: 'PRIMARY' (10.0.10.1) and 'DR' (10.0.14.1). The 'PRIMARY' vault is marked with a green up arrow and a yellow crown icon, while the 'DR' vault is marked with a green up arrow.
- Web Portal:** Contains two sub-sections:
  - App User Instances (1):** A green progress bar indicates 1 connected instance.
  - Active Users:** Shows 1 active user.
- CPM and Accounts Discovery:** This section is highlighted with a red box. It contains two sub-sections:
  - App User Instances (1):** A red progress bar indicates 1 disconnected instance.
  - Managed Accounts:** Shows 37 managed accounts.
- PSM and PSM for SSH:** Contains two sub-sections:
  - App User Instances (2):** A green progress bar indicates 2 connected instances.
  - Concurrent Sessions:** Shows 0 concurrent sessions.
- PTA:** Contains two sub-sections:
  - App User Instances (1):** A green progress bar indicates 1 connected instance.
  - Monitored Targets:** Shows 2 monitored targets.

A callout box points to the 'CPM and Accounts Discovery' section, stating: "In the **PVWA System Health**, we can see that the **CPM** user is disconnected".

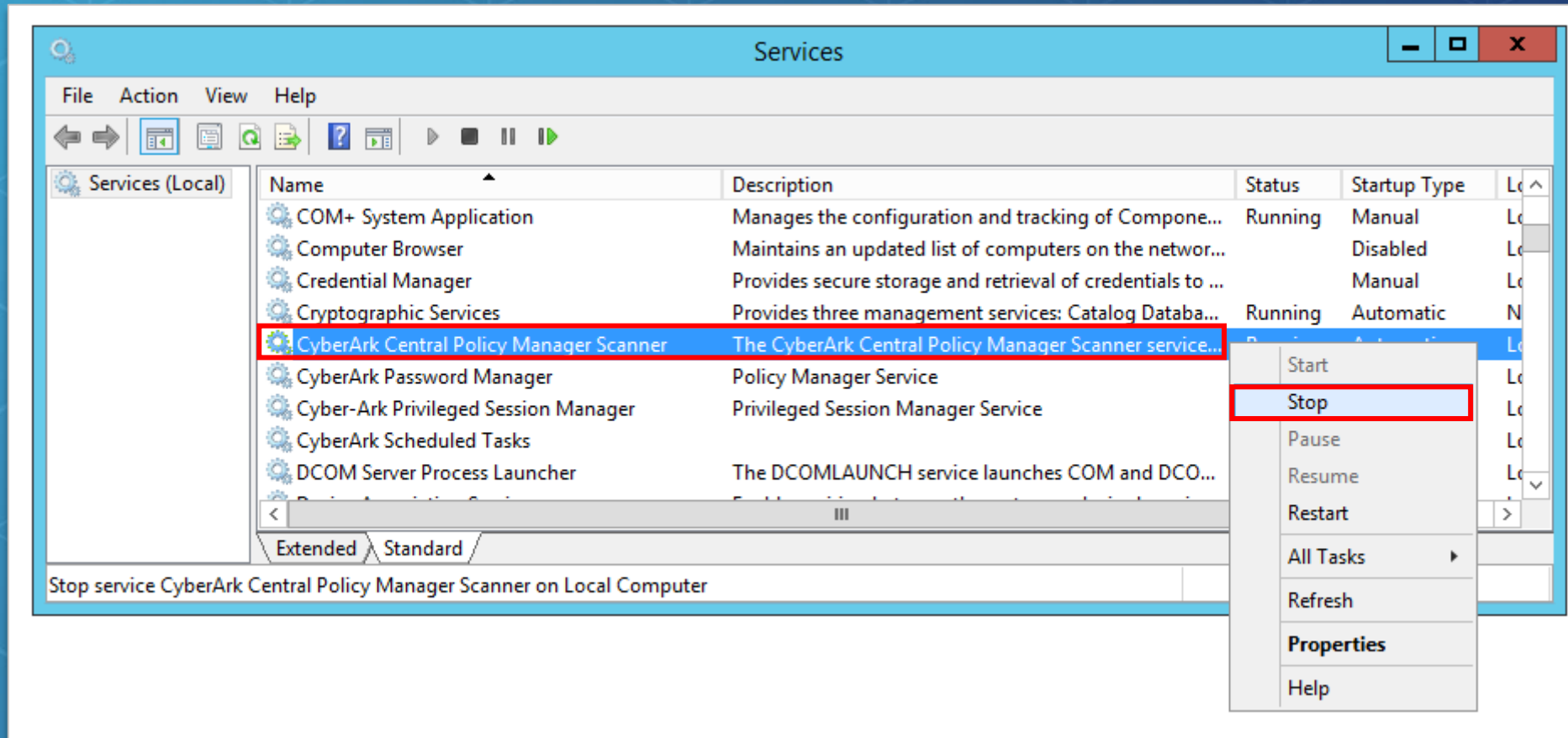
At the bottom right, there is a watermark that says "Activate Windows Go to Settings to activate Windows."

# Component Authentication Error

- Occasionally, the passwords for a component user can get out of sync: the password stored in the **Vault** no longer matches the password stored in the credential file.
- There is a tool available in the **CyberArk Support Vault** that can be used to unsuspend component users (Solution 3643).
- These next few slides will show you how to do it manually for the default **CPM** component user *PasswordManager*.



# 1 Stop the CPM Services



## 2 Reset the Password in the Vault

Update User: PasswordManager

Time Limitations | Personal details | Phone/Notes | Business/Internet  
General | Authentication | Authorizations | Member Of

Change Password

Authentication method: Password

☐ Require RSA SecurID authentication

Distinguished Name:

Select

Password: xxxxxx

Confirm: xxxxxx

☐ User Must Change Password at Next Logon

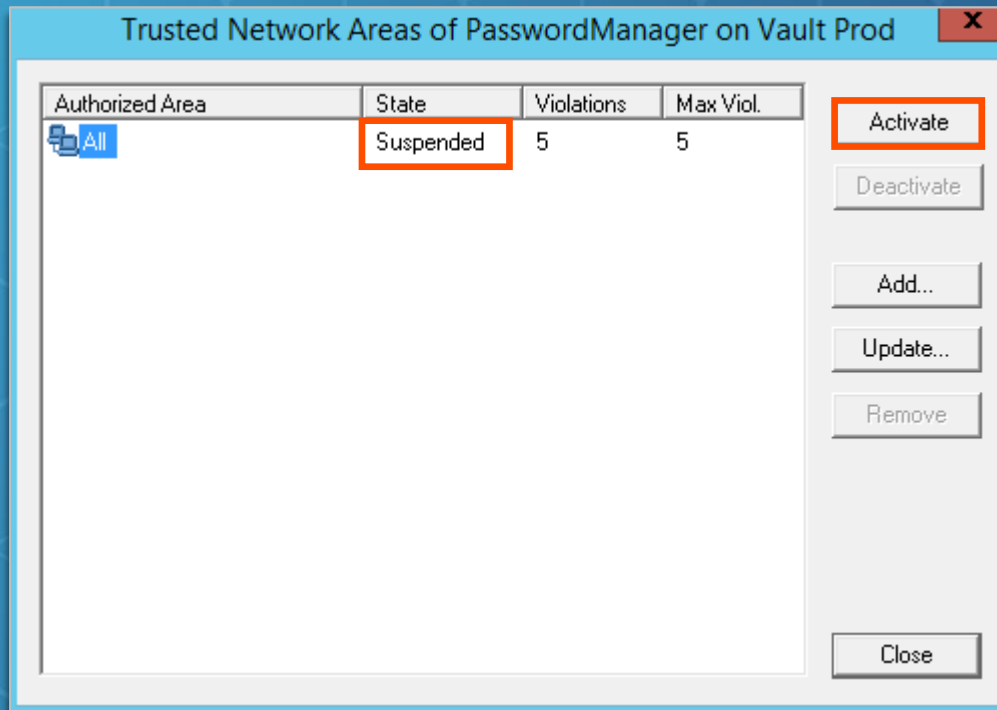
☐ Password Never Expires

OK Cancel

Set the **PasswordManager** user's password to a known value.



### 3 Unsuspend the Component User

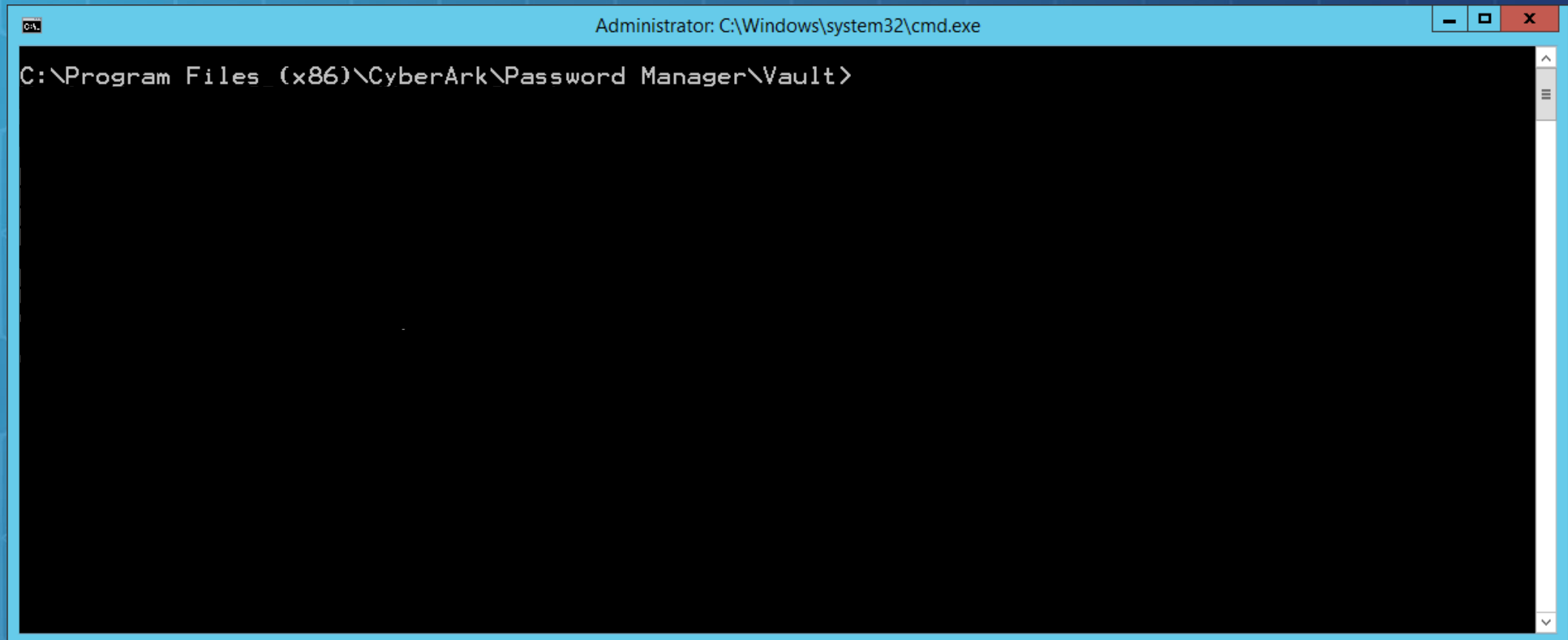


In **Trusted Net** Areas, click **Activate** to unsuspend the user



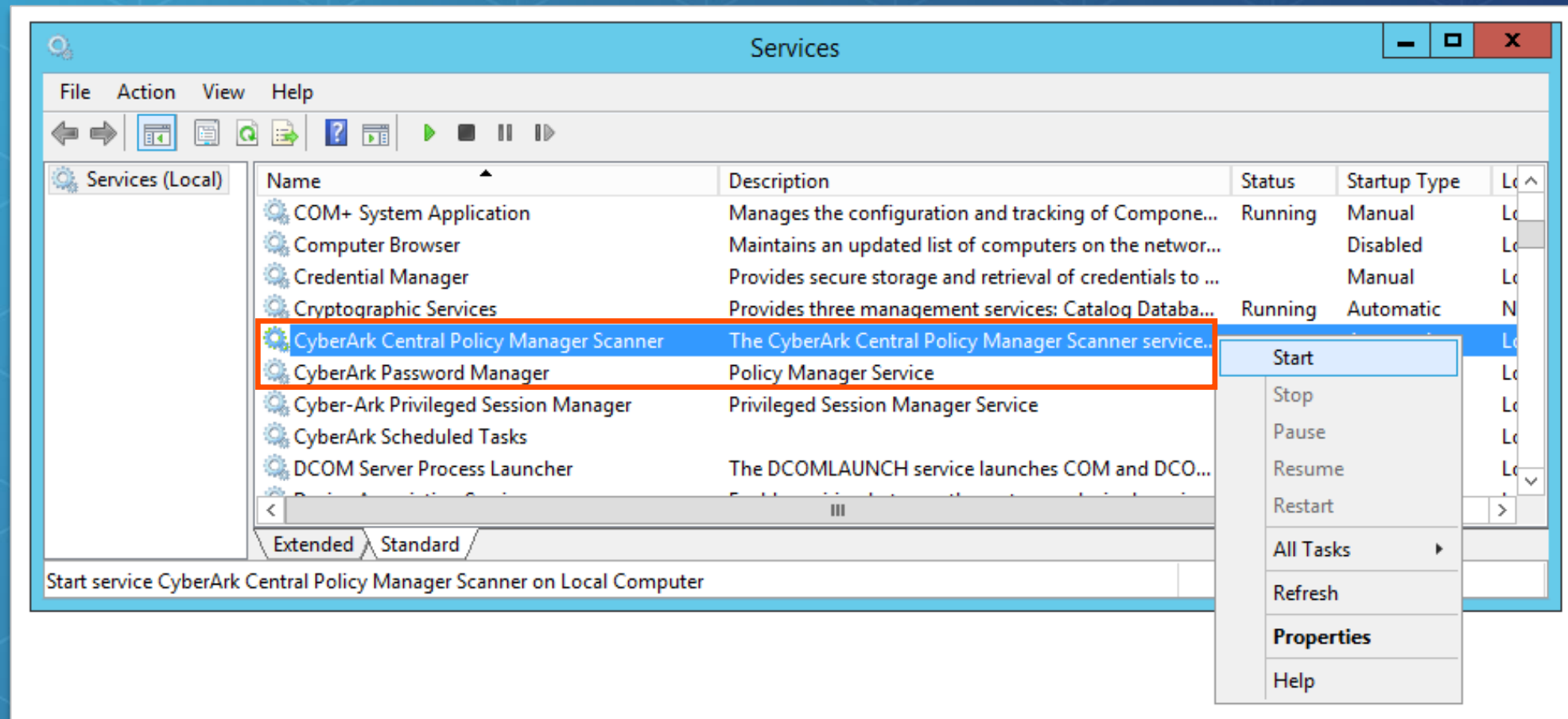
## 4 Generate a New Credential File

In the ***Vault*** folder under ***Password Manager***, run the command: `CreateCredFile.exe user.ini`





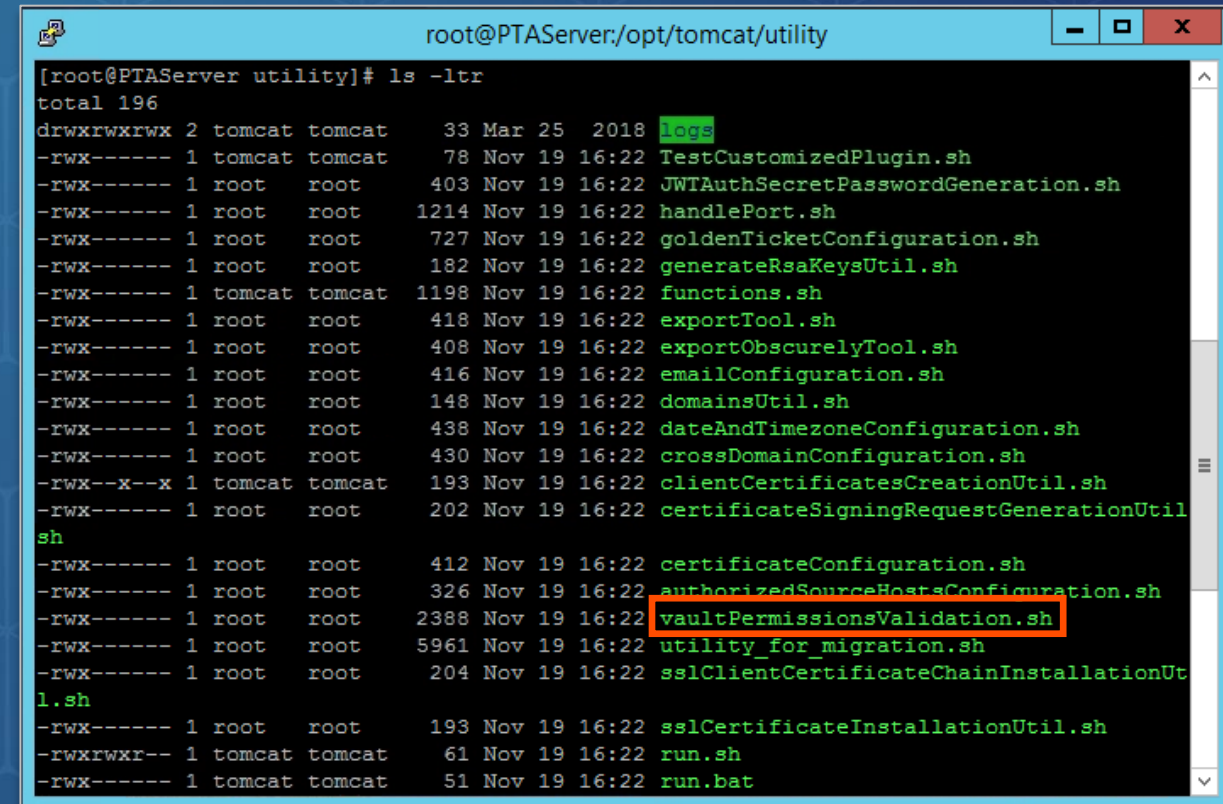
## 5 Restart the CPM Services



# Resynch PTA Credentials

- In the event the **PTA** connectivity is not working, we may need to resynch the credentials for the PTA Vault users, as well as the credentials stored in the **PTA\_PAS\_Gateway** account (used for REST calls between **PVWA** and **PTA**).
- This can be done easily by running the ***VaultPermissionsValidation.sh*** script located in the utility folder on the **PTA** server.
- You can navigate to the utility folder by entering the following alias:

**UTILITYDIR**



A terminal window titled 'root@PTAServer:/opt/tomcat/utility' showing the output of the command 'ls -ltr'. The output lists various shell scripts in the directory, including 'logs', 'TestCustomizedPlugin.sh', 'JWTAuthSecretPasswordGeneration.sh', 'handlePort.sh', 'goldenTicketConfiguration.sh', 'generateRsaKeysUtil.sh', 'functions.sh', 'exportTool.sh', 'exportObscurelyTool.sh', 'emailConfiguration.sh', 'domainsUtil.sh', 'dateAndTimezoneConfiguration.sh', 'crossDomainConfiguration.sh', 'clientCertificatesCreationUtil.sh', 'certificateSigningRequestGenerationUtil.sh', 'certificateConfiguration.sh', 'authorizedSourceHostsConfiguration.sh', 'vaultPermissionsValidation.sh' (highlighted with a red box), 'utility\_for\_migration.sh', 'sslClientCertificateChainInstallationUtil.sh', 'sslCertificateInstallationUtil.sh', 'run.sh', and 'run.bat'.

```
root@PTAServer:/opt/tomcat/utility
[root@PTAServer utility]# ls -ltr
total 196
drwxrwxrwx 2 tomcat tomcat   33 Mar 25  2018 logs
-rwx----- 1 tomcat tomcat   78 Nov 19 16:22 TestCustomizedPlugin.sh
-rwx----- 1 root   root   403 Nov 19 16:22 JWTAuthSecretPasswordGeneration.sh
-rwx----- 1 root   root  1214 Nov 19 16:22 handlePort.sh
-rwx----- 1 root   root   727 Nov 19 16:22 goldenTicketConfiguration.sh
-rwx----- 1 root   root   182 Nov 19 16:22 generateRsaKeysUtil.sh
-rwx----- 1 tomcat tomcat 1198 Nov 19 16:22 functions.sh
-rwx----- 1 root   root   418 Nov 19 16:22 exportTool.sh
-rwx----- 1 root   root   408 Nov 19 16:22 exportObscurelyTool.sh
-rwx----- 1 root   root   416 Nov 19 16:22 emailConfiguration.sh
-rwx----- 1 root   root   148 Nov 19 16:22 domainsUtil.sh
-rwx----- 1 root   root   438 Nov 19 16:22 dateAndTimezoneConfiguration.sh
-rwx----- 1 root   root   430 Nov 19 16:22 crossDomainConfiguration.sh
-rwx--x--x 1 tomcat tomcat  193 Nov 19 16:22 clientCertificatesCreationUtil.sh
-rwx----- 1 root   root   202 Nov 19 16:22 certificateSigningRequestGenerationUtil
sh
-rwx----- 1 root   root   412 Nov 19 16:22 certificateConfiguration.sh
-rwx----- 1 root   root   326 Nov 19 16:22 authorizedSourceHostsConfiguration.sh
-rwx----- 1 root   root  2388 Nov 19 16:22 vaultPermissionsValidation.sh
-rwx----- 1 root   root  5961 Nov 19 16:22 utility_for_migration.sh
-rwx----- 1 root   root   204 Nov 19 16:22 sslClientCertificateChainInstallationUt
l.sh
-rwx----- 1 root   root   193 Nov 19 16:22 sslCertificateInstallationUtil.sh
-rwxrwxr-- 1 tomcat tomcat   61 Nov 19 16:22 run.sh
-rwx----- 1 tomcat tomcat   51 Nov 19 16:22 run.bat
```



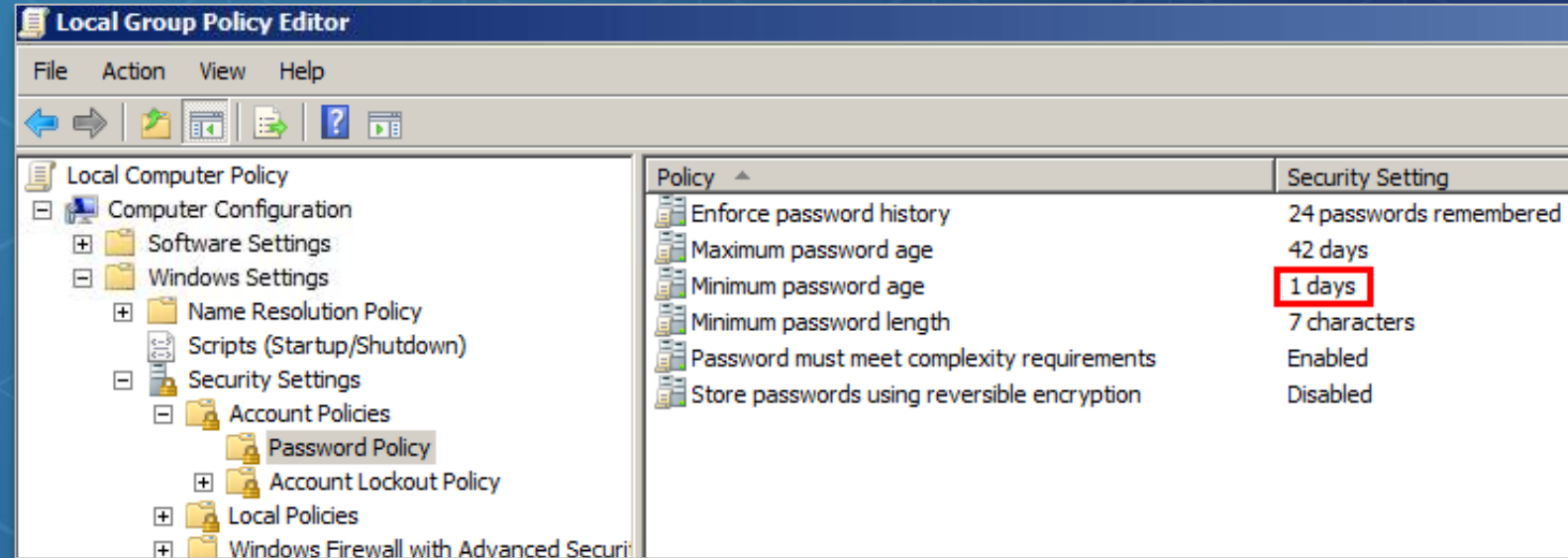
# Common Issues Related to CPM



# What Can Interfere With the CPM?

## *Local Computer Policy*

- The **Platform** and **Master Policy** settings must not conflict with the password policy on the target device



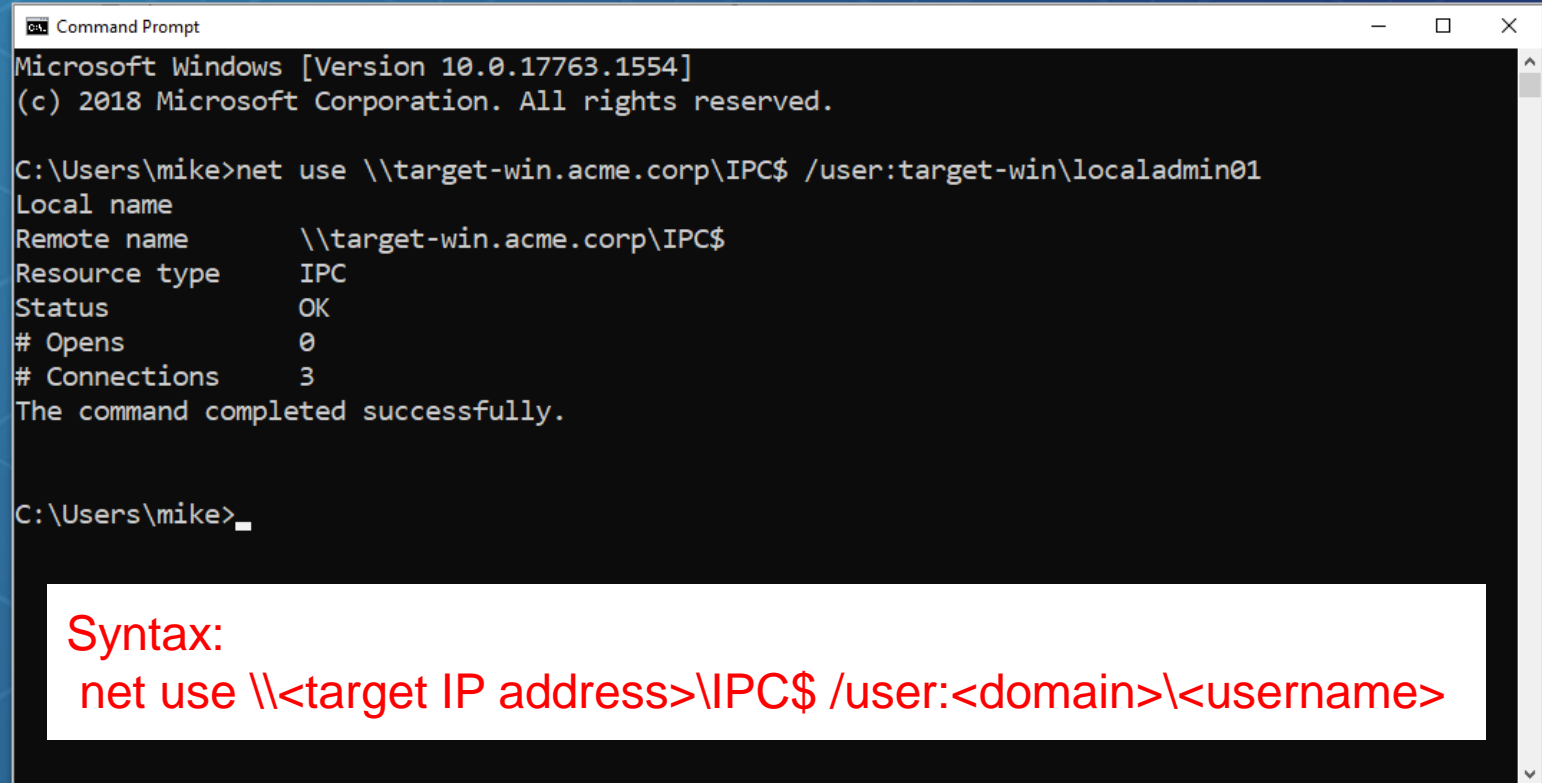
# Target Windows Accounts

## Understanding the problem:

- Verify / Change / Reconcile
- API and “net use” command
- Alternative plugins: WMI plugin / PowerShell plugin

## Suggested Troubleshooting:

- Check **Windows Event Viewer**
- Check for unusual Local Security Settings
- Run “net use” manually from the CPM server to verify the connection



```
Command Prompt
Microsoft Windows [Version 10.0.17763.1554]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\mike>net use \\target-win.acme.corp\IPC$ /user:target-win\localadmin01
Local name
Remote name      \\target-win.acme.corp\IPC$
Resource type    IPC
Status           OK
# Opens          0
# Connections    3
The command completed successfully.

C:\Users\mike>
```

**Syntax:**  
`net use \\<target IP address>\IPC$ /user:<domain>\<username>`





# Target Unix Accounts

## Understanding the problem:

- Which operations are affected: **Verify / Change / Reconcile / All**

## Suggested Troubleshooting:

- Running plink manually
- Disable **DEP** / add exceptions for **DEP** on the **CPM** server
- **Prompts** and **Process** files – add a basic prompt

```
Command Prompt - "C:\Program Files (x86)\CyberArk\Password Manager\bin\plink.exe" 10.0.0.20 -ssh -P 22
Microsoft Windows [Version 10.0.17763.1554]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\mike>"C:\Program Files (x86)\CyberArk\Password Manager\bin\plink.exe" 10.0.0.20 -ssh -P 22
login as: login as: logon01

logon01@10.0.0.20's password: logon01@10.0.0.20's password:

Last login: Tue Mar 1 08:58:07 2022 from components.acme.corp
Last login: Tue Mar 1 08:58:07 2022 from components.acme.corp
[?]0;logon01@target-lin:~[?]1034h[logon01@target-lin ~]$ [?]0;logon01@target-lin:~[?]1034h[logon01@target-lin ~]$ ppwwdd
/home/logon01
[?]0;logon01@target-lin:~[logon01@target-lin ~]$
/home/logon01
[?]0;logon01@target-lin:~[logon01@target-lin ~]$
```

### Syntax:

```
C:\Program Files (x86)\CyberArk\Password
Manager\bin\plink.exe <target IP address> -ssh -P <port>
```





# Common Issues Related to PSM



# PSM-RDP Connection Troubleshooting

## Understanding the problem

- ▶ At what stage does the problem occur? PVWA / PSM / Target
- ▶ One account? Multiple accounts? Same type?
- ▶ Is the PSM hardened?
- ▶ Is the PSM in a domain?
- ▶ Which connection type is being used? RDP file / RemoteApp
- ▶ If there are multiple PSM servers, are they distributed or load balanced?

# PSM-RDP Connection Troubleshooting

## Suggested Troubleshooting:

- ▶ Check the PSM service – is it off/hanging?
- ▶ Logs and events on PSM server (System and Application)
- ▶ Disable NLA on PSM and target
- ▶ Initiate a manual connection with PSMConnect and run MSTSC to the target
- ▶ Check safe permissions (compare with other safes)
- ▶ Disable recording and auditing
- ▶ Check PSM Protocol version
- ▶ Increase Time-out values

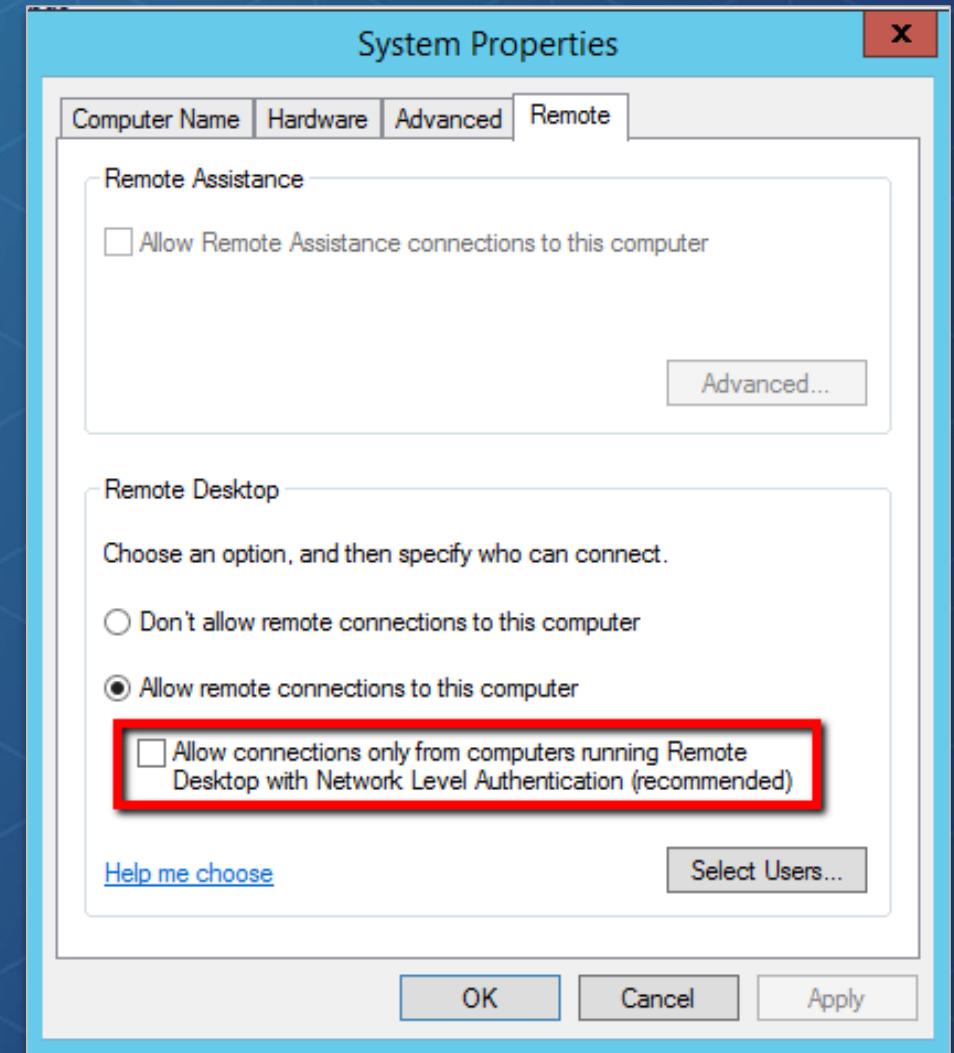
# Disable NLA

## Network Level Authentication (NLA)

requires the connecting user to authenticate themselves before a session is established with the server.

You can disable NLA in order to determine if that is causing the problem.

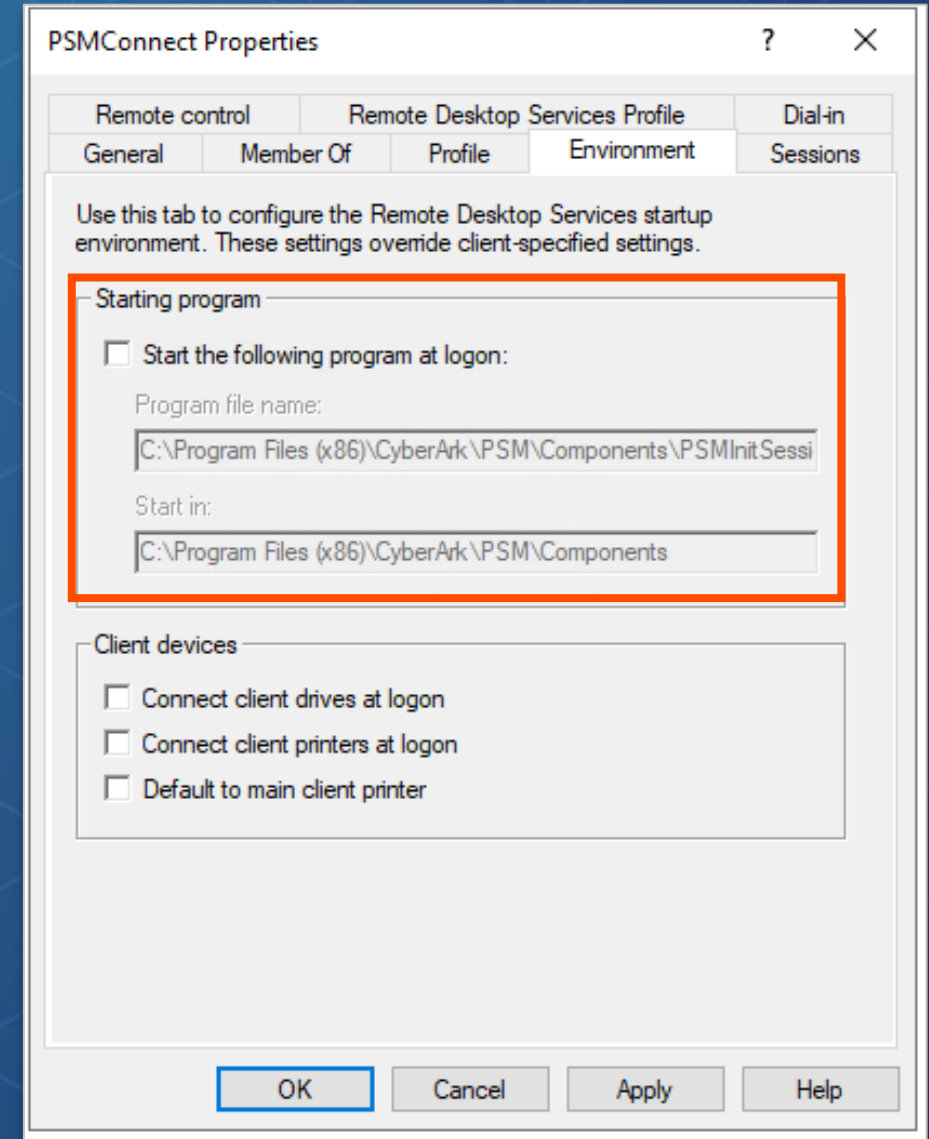
- On the PSM Machine or Target Machine:  
Go to **Control Panel → System and Security → System → Remote Settings**



# Connect Manually with PSMConnect

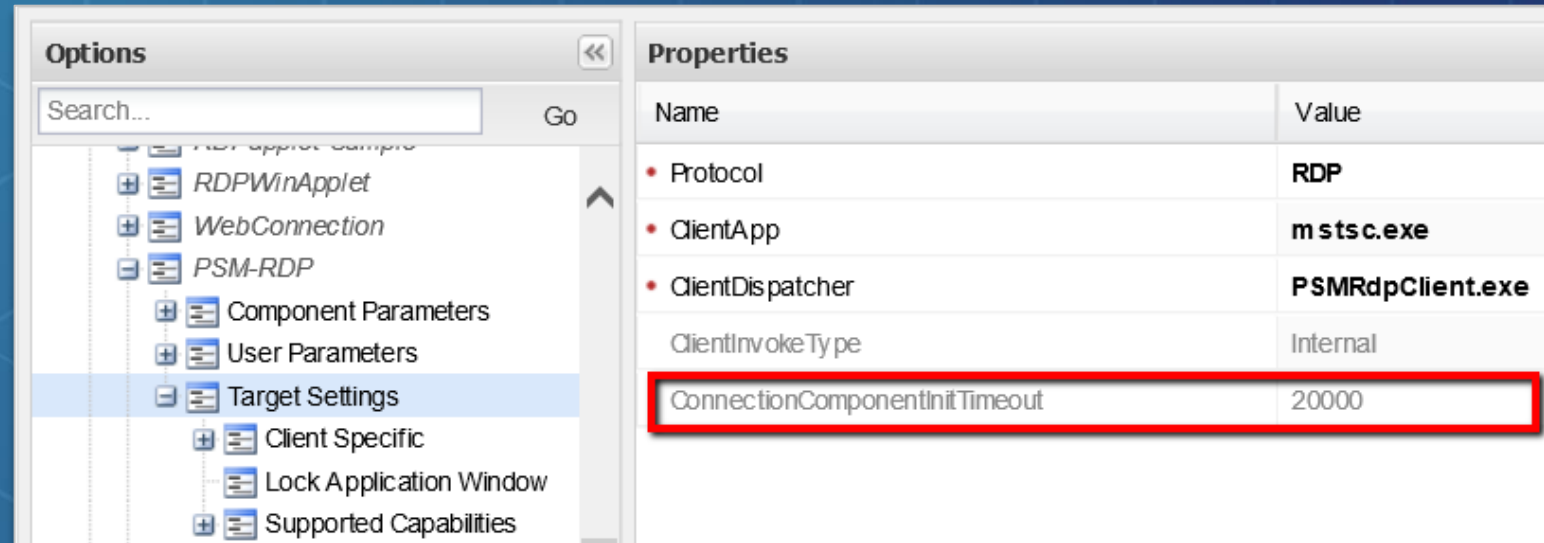
To manually test the **PSMConnect** user

1. Go to the local **Computer Management** (or **Active Directory**) and disable the **Start Program** in the **Environment** tab.
2. Get the **PSMConnect** account password (using the PVWA or PrivateArk Client).
3. Connect to the PSM with **PSMConnect** and run **MSTSC** to the target.



# Increase Timeouts

- Timeout parameters determine how long the **PSM** will wait for certain components to work before considering them as 'failed' and ending the session.
- Overloaded environments may suffer from longer times for certain components to begin working, so it is recommended to **double their timeout values.**



(e.g.) ConnectionComponentTimeout: 20000





# PSM-[Component]

## Understanding the problem:

- PSM users (PSMConnect / Shadow users)
- Is it supported?
- Is Mapping drives enabled?

## Suggested Troubleshooting:

- Same recommendations as for PSM-RDP
- Run component manually using shadow user
- Delete Shadow users (from PSM computer management)
- Adjust AppLocker (or remove it manually in Windows for isolation)



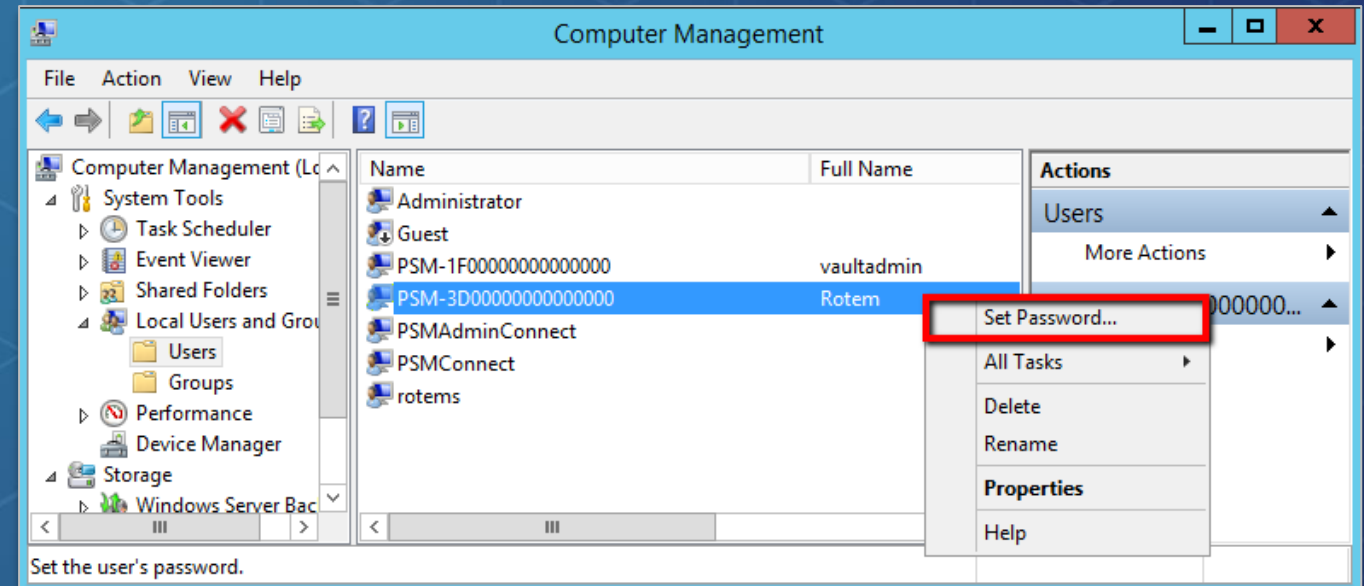
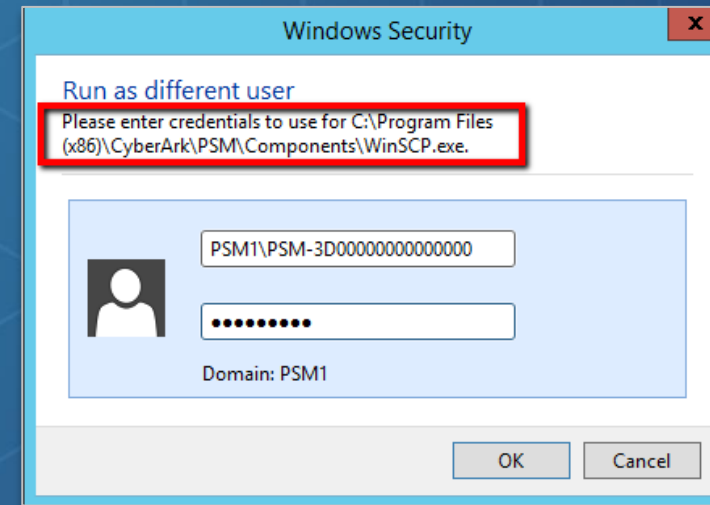
# PSM

## Shadow Users

Shadow users are created by the **PSM** upon first connection. Shadow users are used to run connection components and store user preferences.

You can isolate problems related to shadow users by:

- Running the component manually as the shadow user (after password reset)
- Deleting the user (this will allow the **PSM** to create the user again)

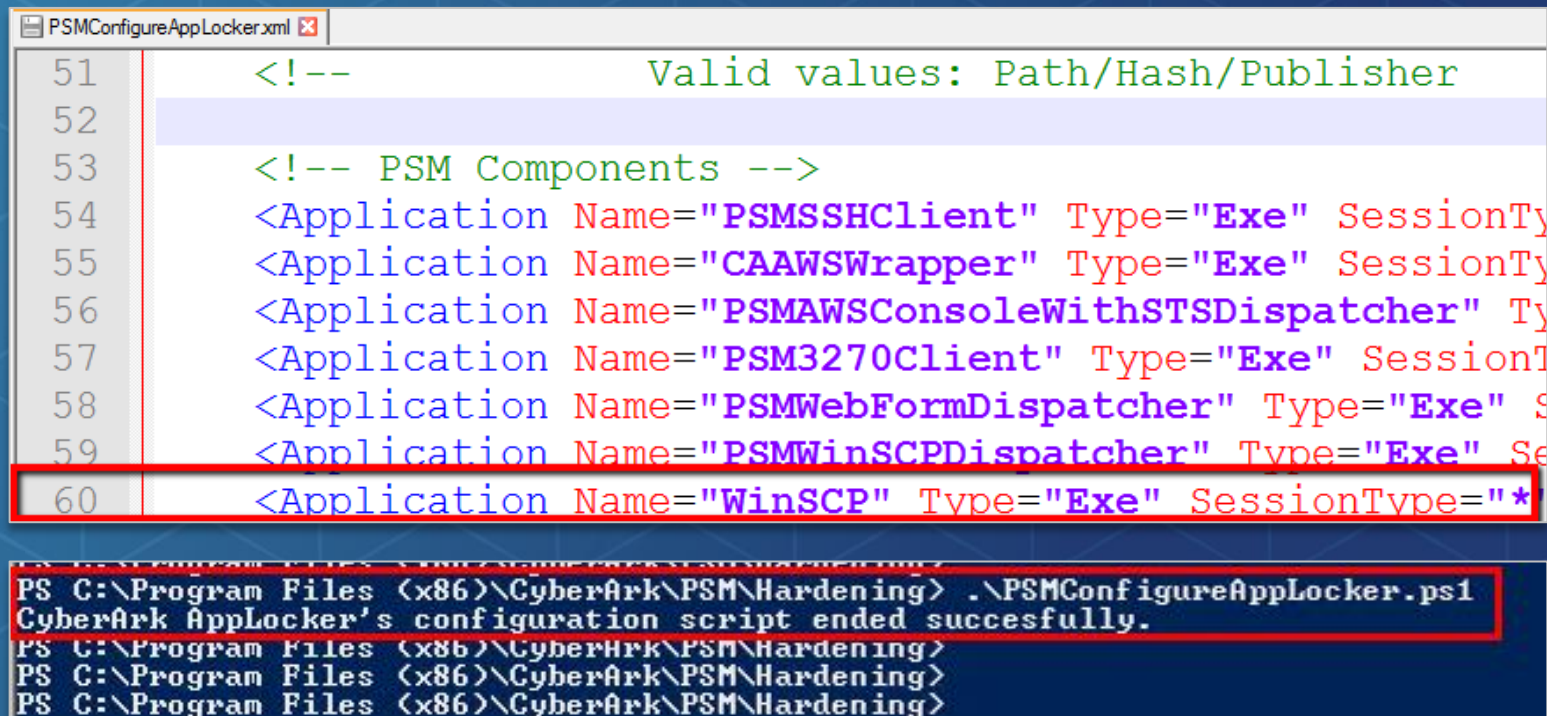


# Adjust AppLocker

The **PSM** uses the Windows AppLocker feature which defines a set of rules that allow or deny applications from running on the **PSM** machine.

When adding a new component, you must also adjust AppLocker by:

- Adding an exception to ***PSMConfigureApplocker.xml***
  - Uncomment the line relating to the new component
- Running the ***PSMConfigureApplocker.ps1*** script

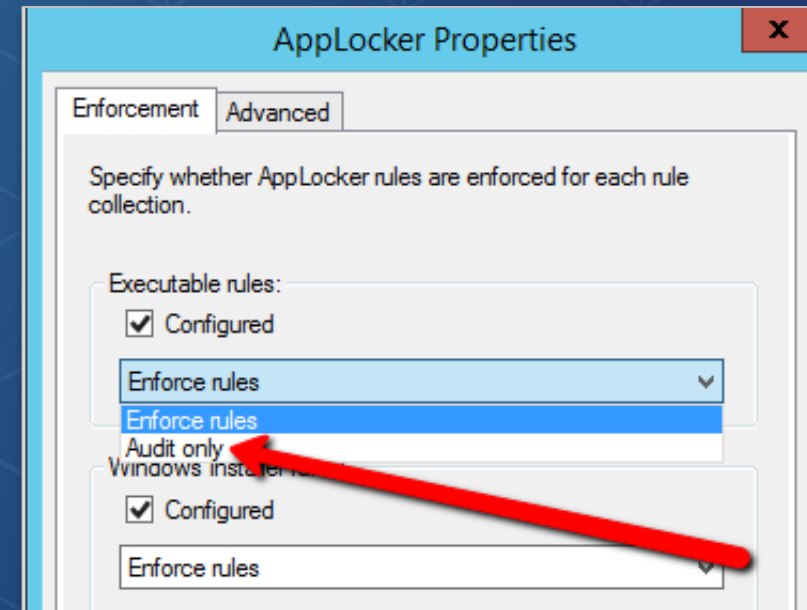
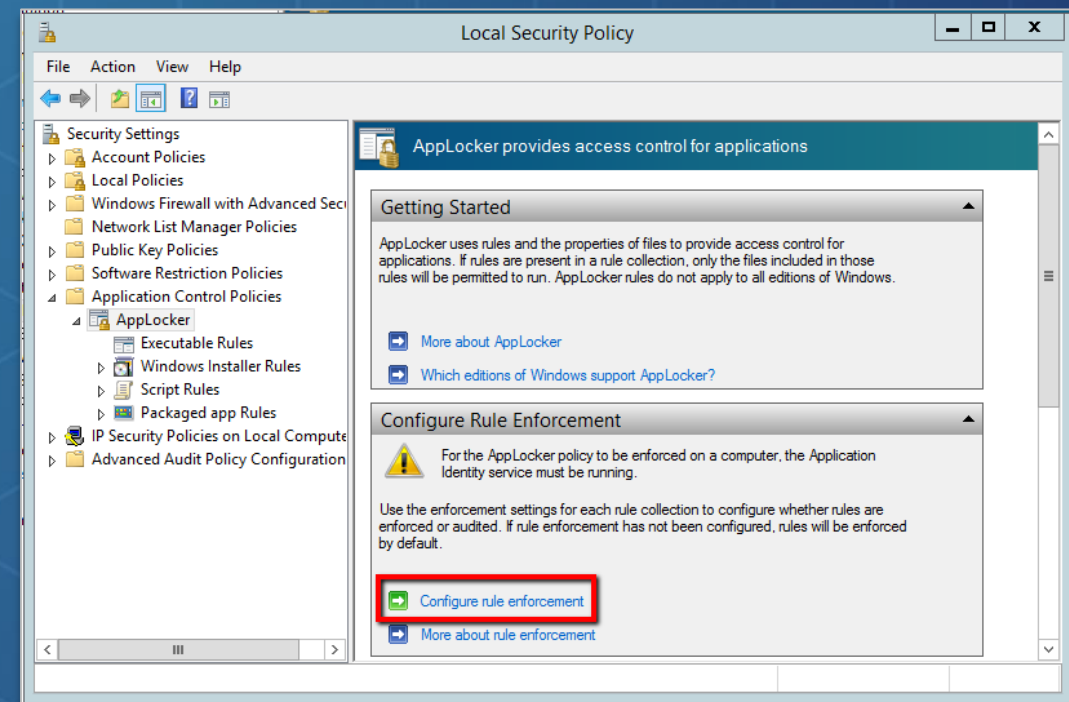


The image shows two screenshots. The top screenshot is a text editor window titled 'PSMConfigureAppLocker.xml'. It displays XML code with line numbers 51 through 60. Line 51 contains a comment: '

# Disable AppLocker

You can also disable AppLocker entirely (for isolating the problem only) using the MMC snap-ins:

1. On the **Start** screen, type **secpol.msc** or **gpedit.msc**
2. Go to **Computer Configuration → Windows Settings → Security Settings → Application Control Policies → AppLocker**
3. Click on **Configure rule enforcement** and set **Executable Rules** to **Audit Only**
4. **Turn Enforce rules back on after testing**





# Summary



# Summary

In this session we covered basic troubleshooting steps to resolve common issues related to:

- ✔ User authentication
- ✔ Component connectivity to the Vault
- ✔ Automatic password management by CPM
- ✔ Launching privileged sessions via PSM

