CYBERARK®

CYBERARK UNIVERSITY

Securing CyberArk

CyberArk Training

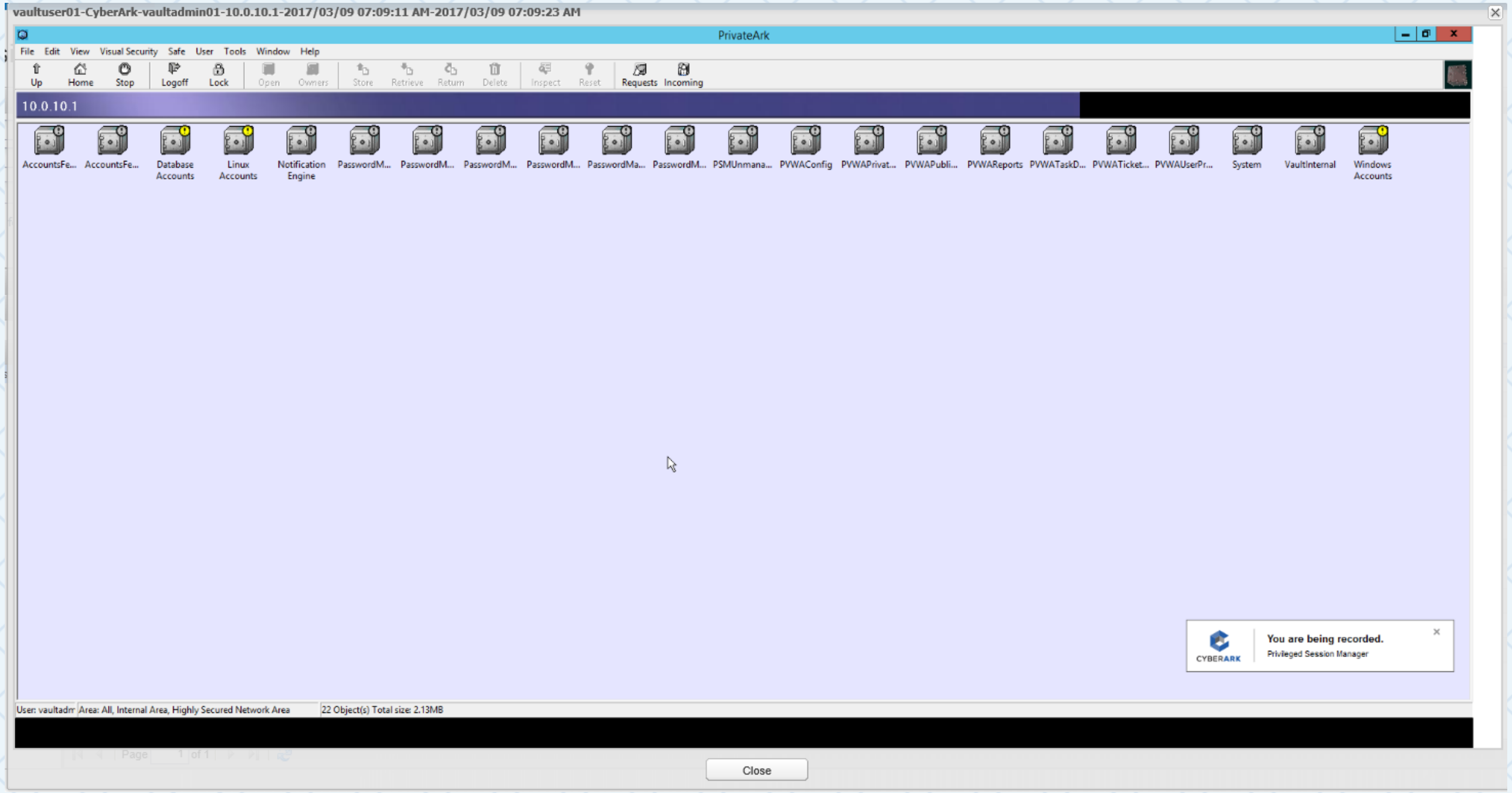
OBJECTIVES

- By the end of this session, you will be able to:
  - Use the Enterprise Password Vault to secure and manage CyberArk Administrative Accounts
  - Use Privileged Session Manager to isolate and monitor access to CyberArk administrative interfaces

OVERVIEW

CONNECTING TO CYBERARK ADMINISTRATIVE INTERFACES

- It is highly recommended that CyberArk administrative accounts are added to the Digital Vault and managed by the CPM
- CyberArk built-in administrative accounts should be stored in a safe with automatic password management enabled
- User access to built-in account should be enabled via PSM



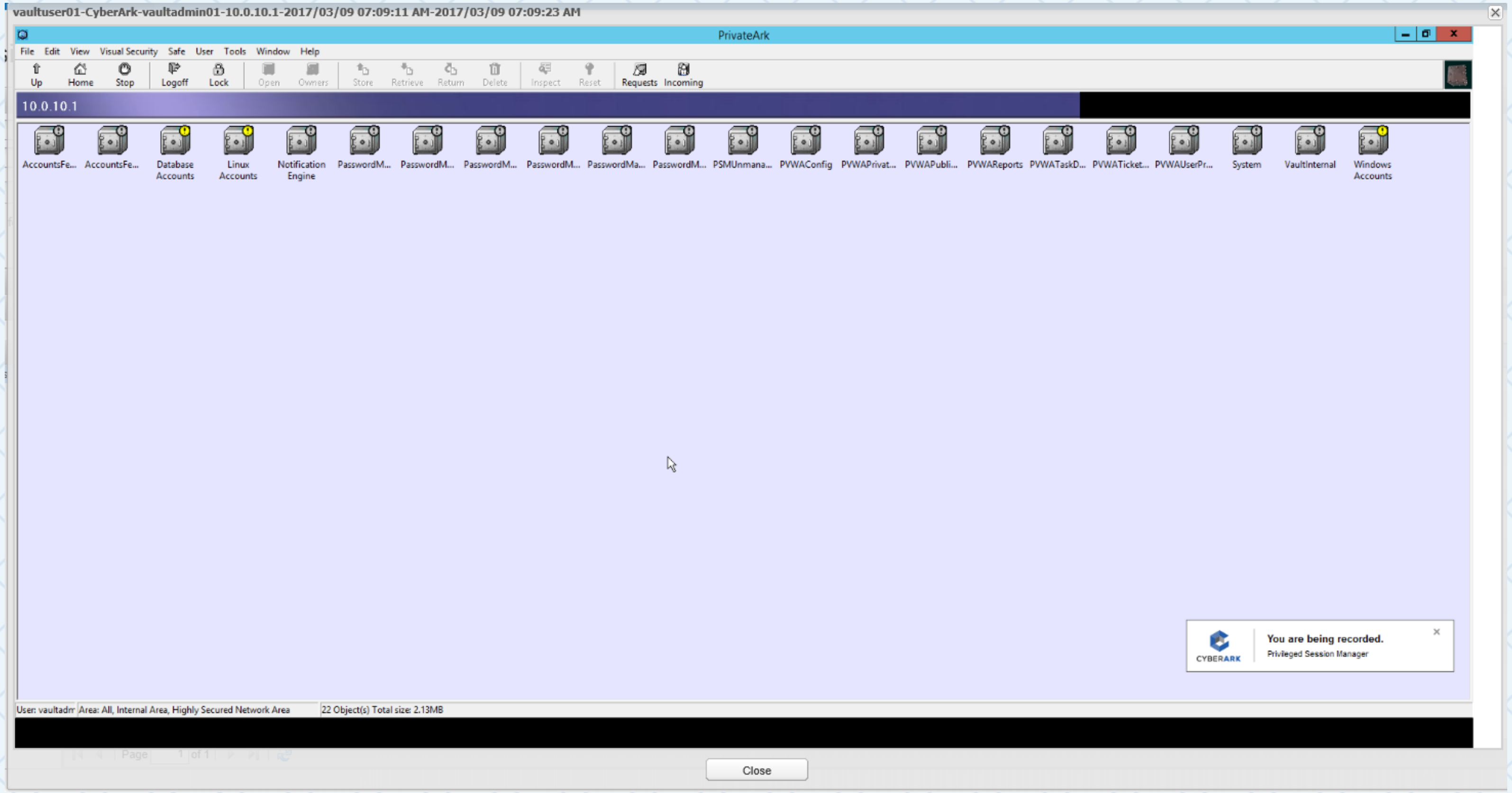
vaultuser01-CyberArk-vaultadmin01-10.0.10.1-2017/03/09 07:09:11 AM-2017/03/09 07:09:23 AM

User: vaultadm Area: All, Internal Area, Highly Secured Network Area 22 Object(s) Total size: 2.13MB

You are being recorded.
Privileged Session Manager

CYBERARK SERVICE ACCOUNTS

- Accounts created to support CyberArk PAS operations should be stored in the vault and managed by the CPM
- Examples of CyberArk Service Accounts
    - LDAP Bind Account
    - PSMConnect
    - PSMAdminConnect
- PasswordManagerUser



vaultuser01-CyberArk-vaultadmin01-10.0.10.1-2017/03/09 07:09:11 AM-2017/03/09 07:09:23 AM

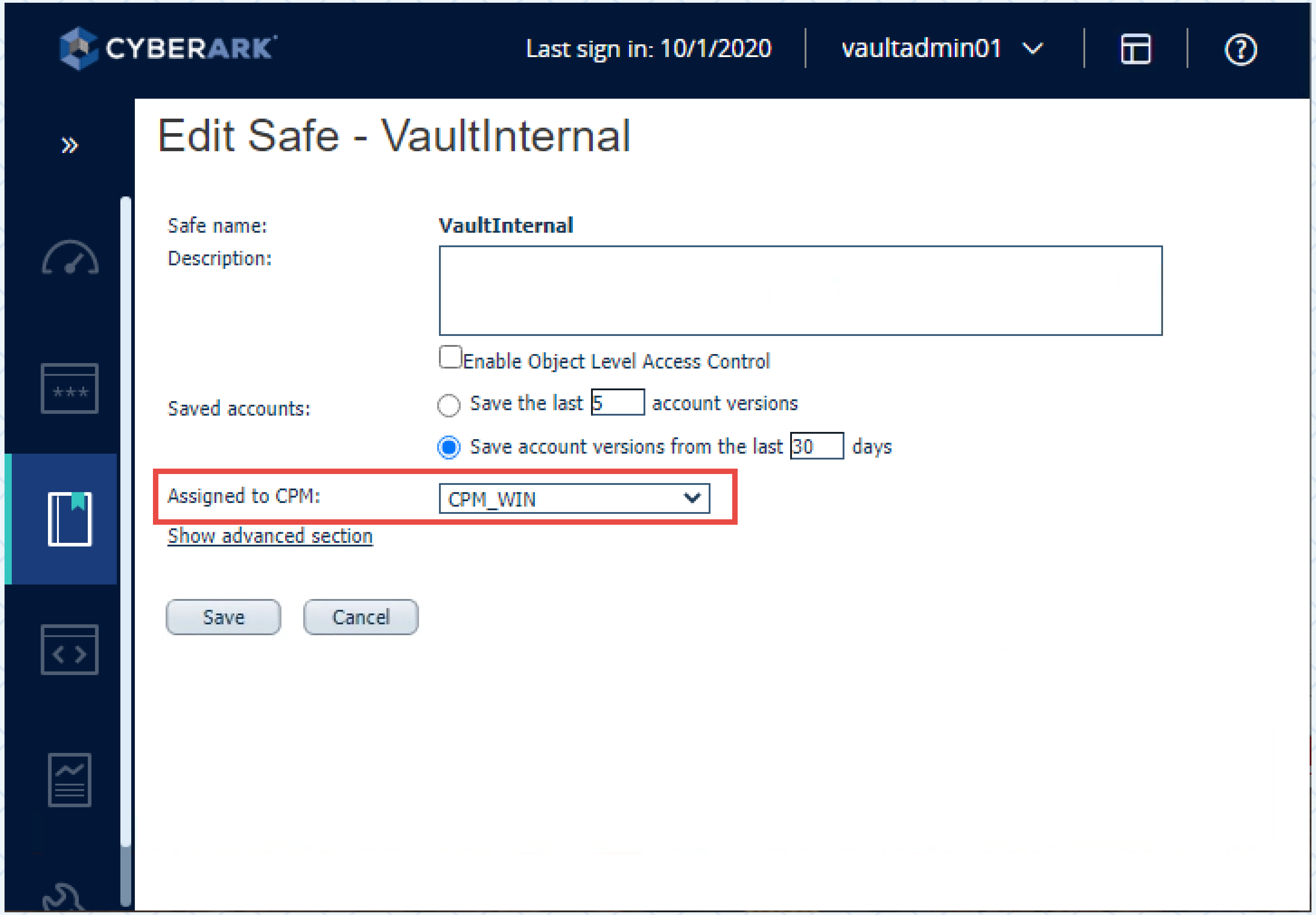
You are being recorded.
Privileged Session Manager

User: vaultadm Area: All, Internal Area, Highly Secured Network Area 22 Object(s) Total size: 2.13MB

MANAGING LDAP BIND ACCOUNT WITH CPM

MANAGE THE LDAP BIND ACCOUNT

- The Bind Account is automatically created in the VaultInternal safe
- A CPM must be assigned to the VaultInternal safe to enable CPM operations



Edit Safe - VaultInternal

Safe name: **VaultInternal**

Description:

□ Enable Object Level Access Control

Saved accounts: ○ Save the last 5 account versions

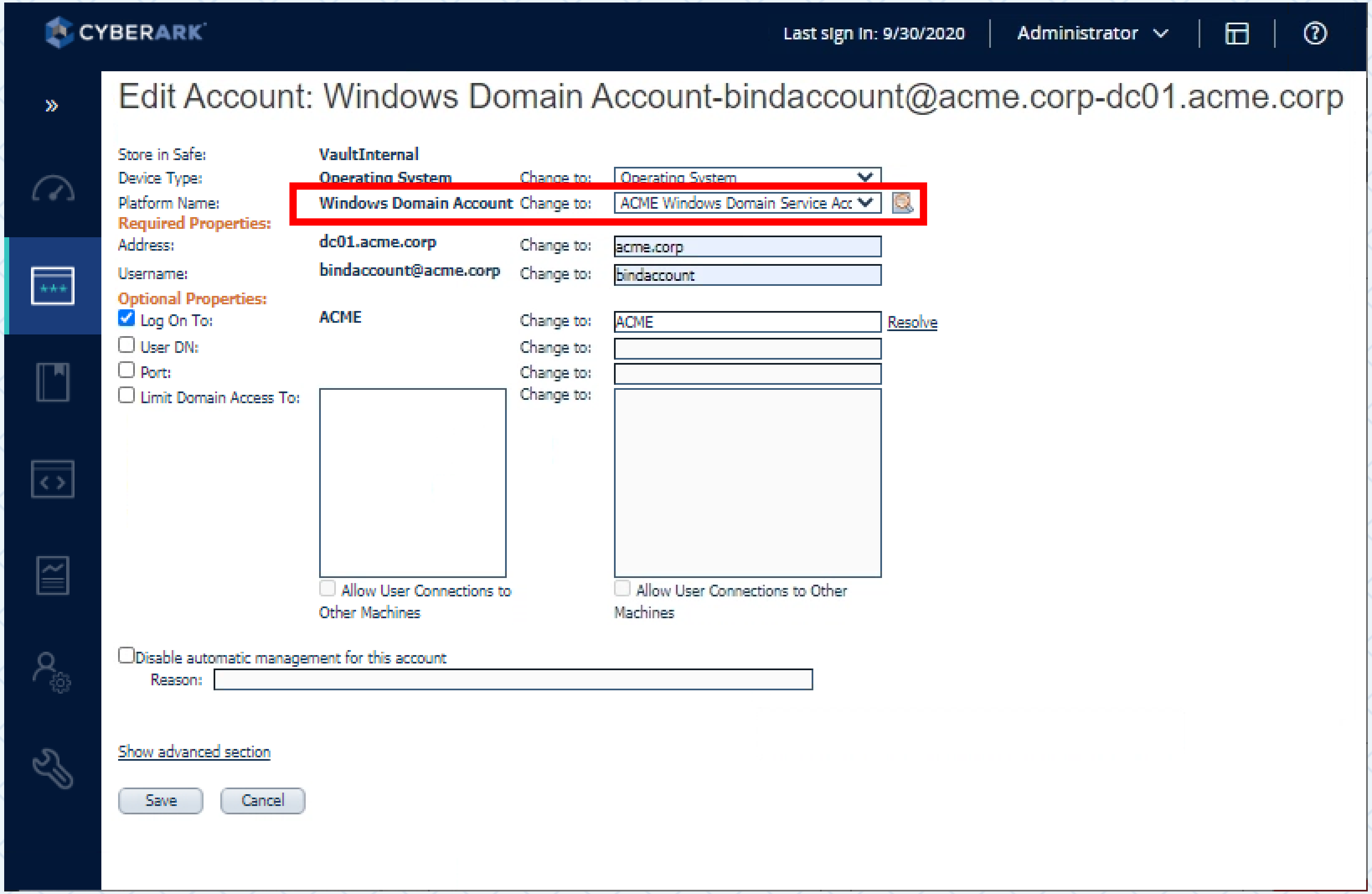
● Save account versions from the last 30 days

Assigned to CPM: CPM_WIN

Show advanced section

MANAGE LDAP BIND ACCOUNT

- Assign the LDAP Bind Account to a customized platform for CyberArk service accounts
- Creating a platform specifically for the Bind Account provides flexibility for scheduling Password Management operations



Edit Account: Windows Domain Account-bindaccount@acme.corp-dc01.acme.corp

Store in Safe:	VaultInternal			
Device Type:	Operating System	Change to:	Operating System	
Platform Name:	Windows Domain Account	Change to:	ACME Windows Domain Service Acc	
Required Properties:				
Address:	dc01.acme.corp	Change to:	acme.corp	
Username:	bindaccount@acme.corp	Change to:	bindaccount	
Optional Properties:				
☑ Log On To:	ACME	Change to:	ACME	Resolve
□ User DN:		Change to:		
□ Port:		Change to:		
□ Limit Domain Access To:	□ Allow User Connections to Other Machines	Change to:	□ Allow User Connections to Other Machines	

□ Disable automatic management for this account

Reason:

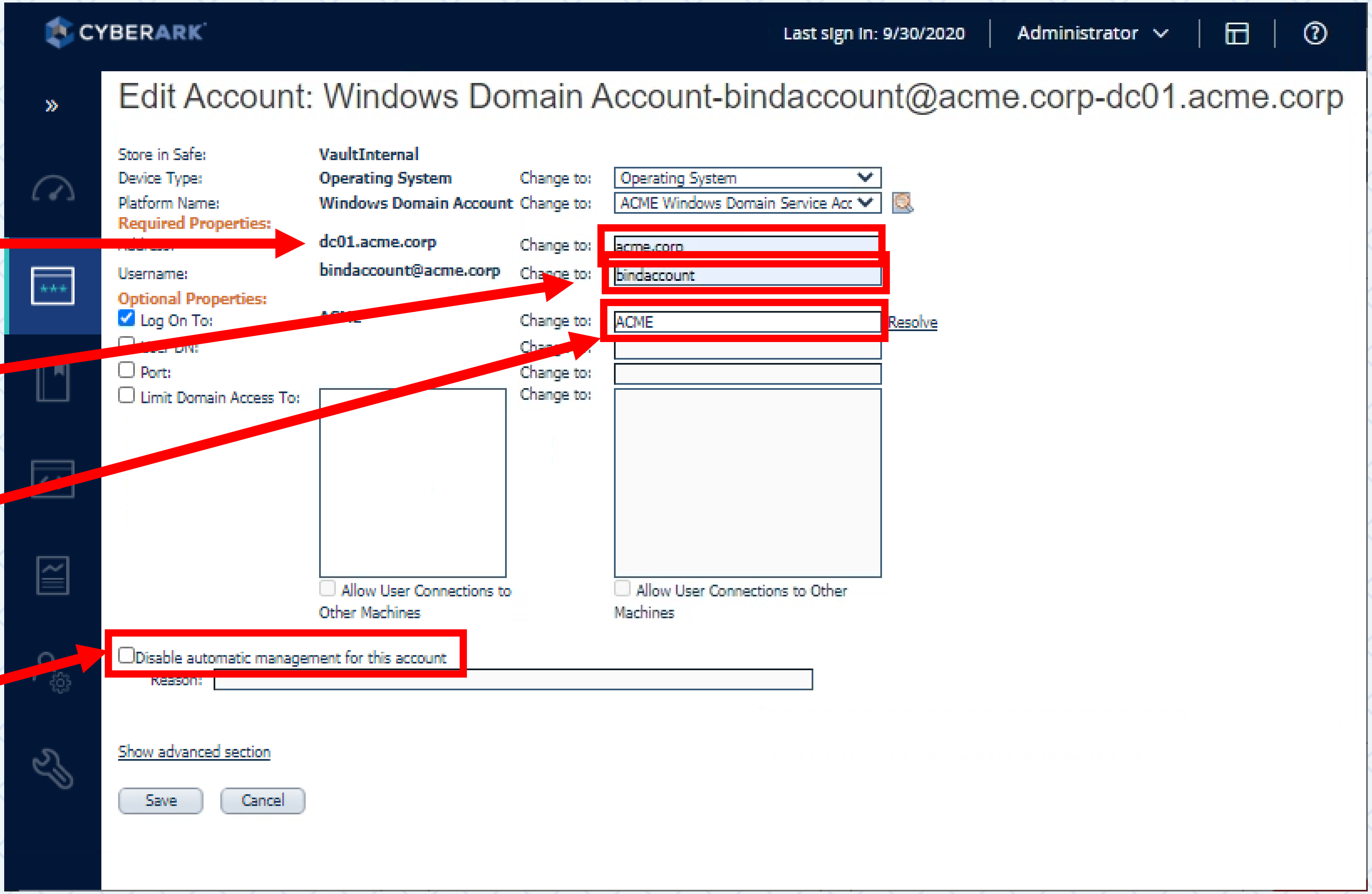
Show advanced section

Save Cancel

MANAGE LDAP BIND ACCOUNT

Update the Required Properties

- Address should be the domain name, not a specific Domain Controller
- Username should not include the domain suffix
- Log On To:, select “Resolve” to populate the NetBIOS name
- Deselect “Disable automatic management for this account”



Edit Account: Windows Domain Account-bindaccount@acme.corp-dc01.acme.corp

Store in Safe:	VaultInternal		
Device Type:	Operating System	Change to:	Operating System
Platform Name:	Windows Domain Account	Change to:	ACME Windows Domain Service Acc
Required Properties:			
Address:	dc01.acme.corp	Change to:	acme.corp
Username:	bindaccount@acme.corp	Change to:	bindaccount
Optional Properties:			
☑ Log On To:	ACME	Change to:	ACME Resolve
□ User DN:		Change to:	
□ Port:		Change to:	
□ Limit Domain Access To:		Change to:	
	□ Allow User Connections to Other Machines		□ Allow User Connections to Other Machines

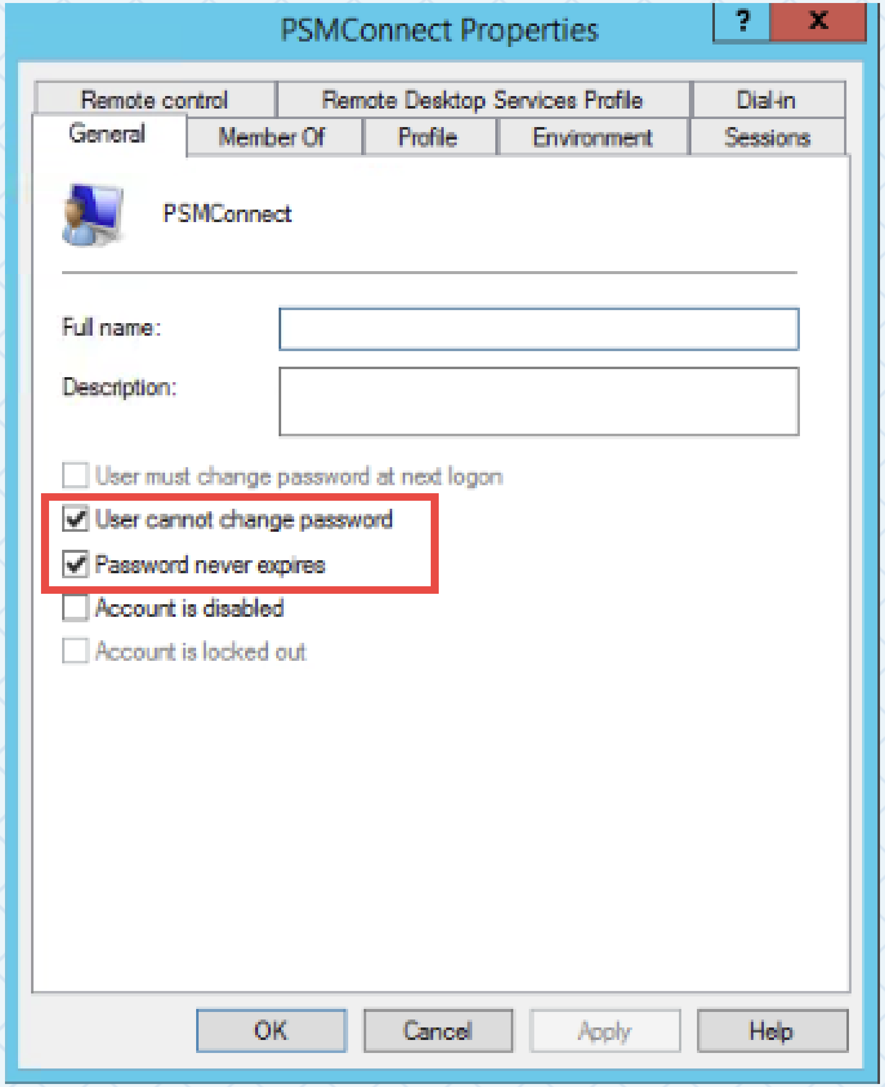
□ Disable automatic management for this account

Reason:

MANAGING PSM USERS WITH CPM

MANAGE THE PSM ACCOUNTS

- Select “User cannot change password”
- This prevents an end user the ability to change the password of the PSMConnect account



PSMConnect Properties

PSMConnect

Full name:

Description:

☐ User must change password at next logon

☑ User cannot change password

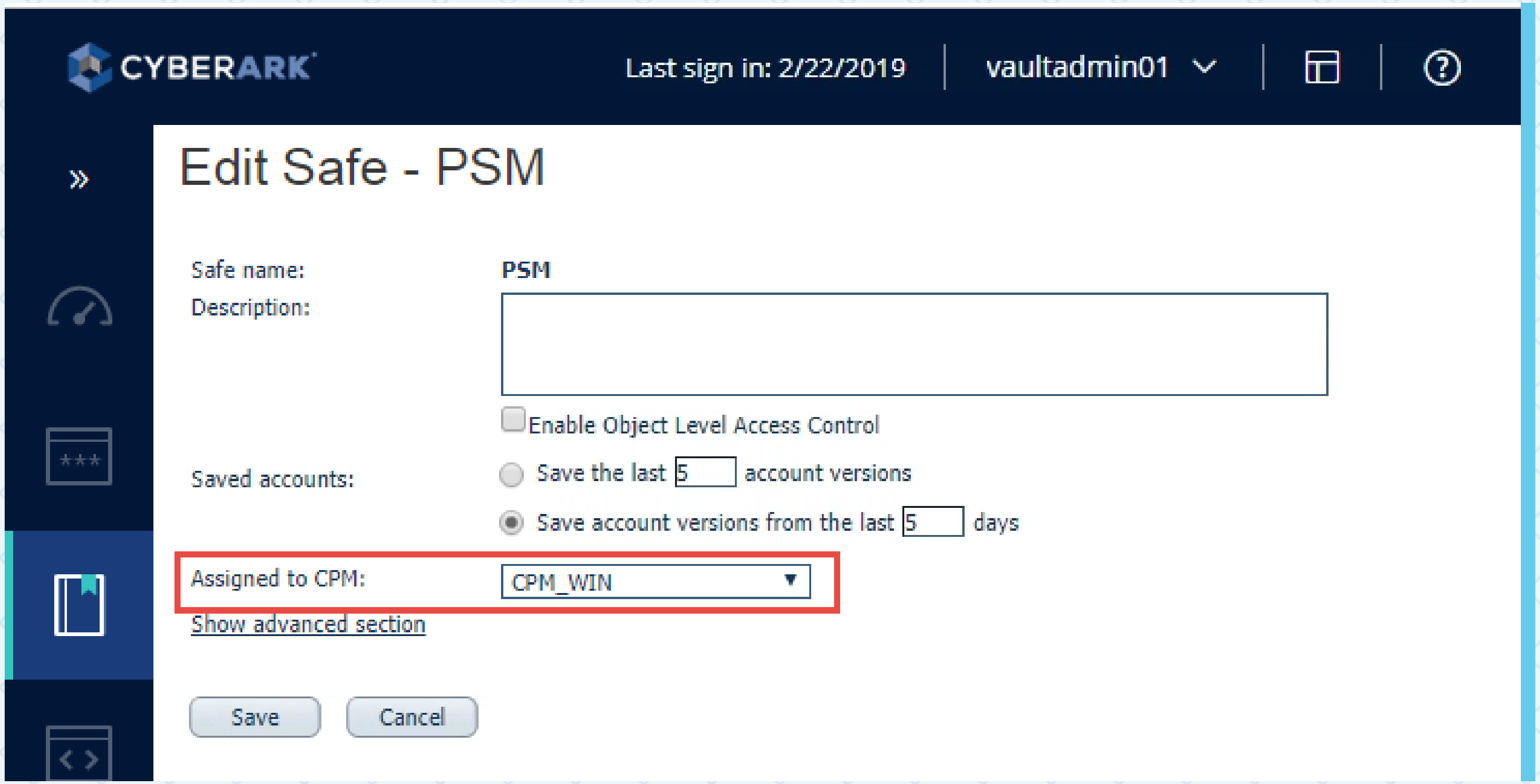
☑ Password never expires

☐ Account is disabled

☐ Account is locked out

MANAGE THE PSM ACCOUNTS

- An appropriate CPM must be assigned to the PSM safe, to enable Password Management operations



Edit Safe - PSM

Safe name: **PSM**

Description:

□ Enable Object Level Access Control

Saved accounts:

○ Save the last 5 account versions

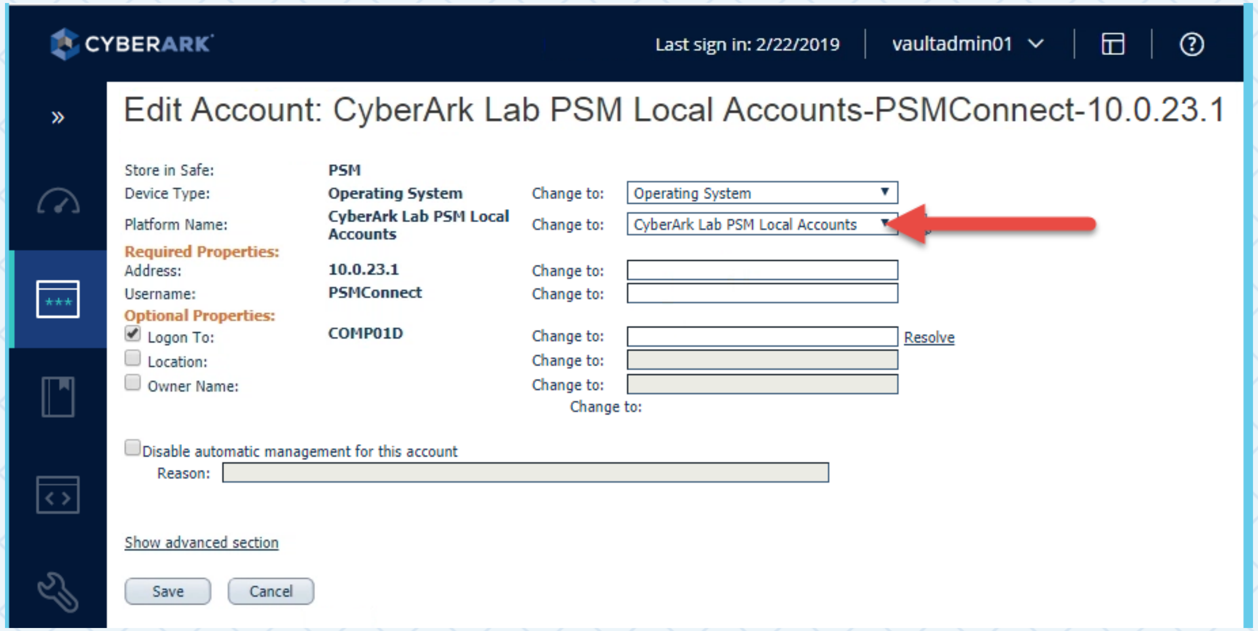
● Save account versions from the last 5 days

Assigned to CPM: CPM_WIN ▾

Show advanced section

MANAGE THE PSM ACCOUNTS

- Assign the PSM accounts to a Windows Target account platform dedicated to PSM service accounts
- Creating a platform specifically for the PSM accounts provides flexibility for scheduling Password Management operations



Edit Account: CyberArk Lab PSM Local Accounts-PSMConnect-10.0.23.1

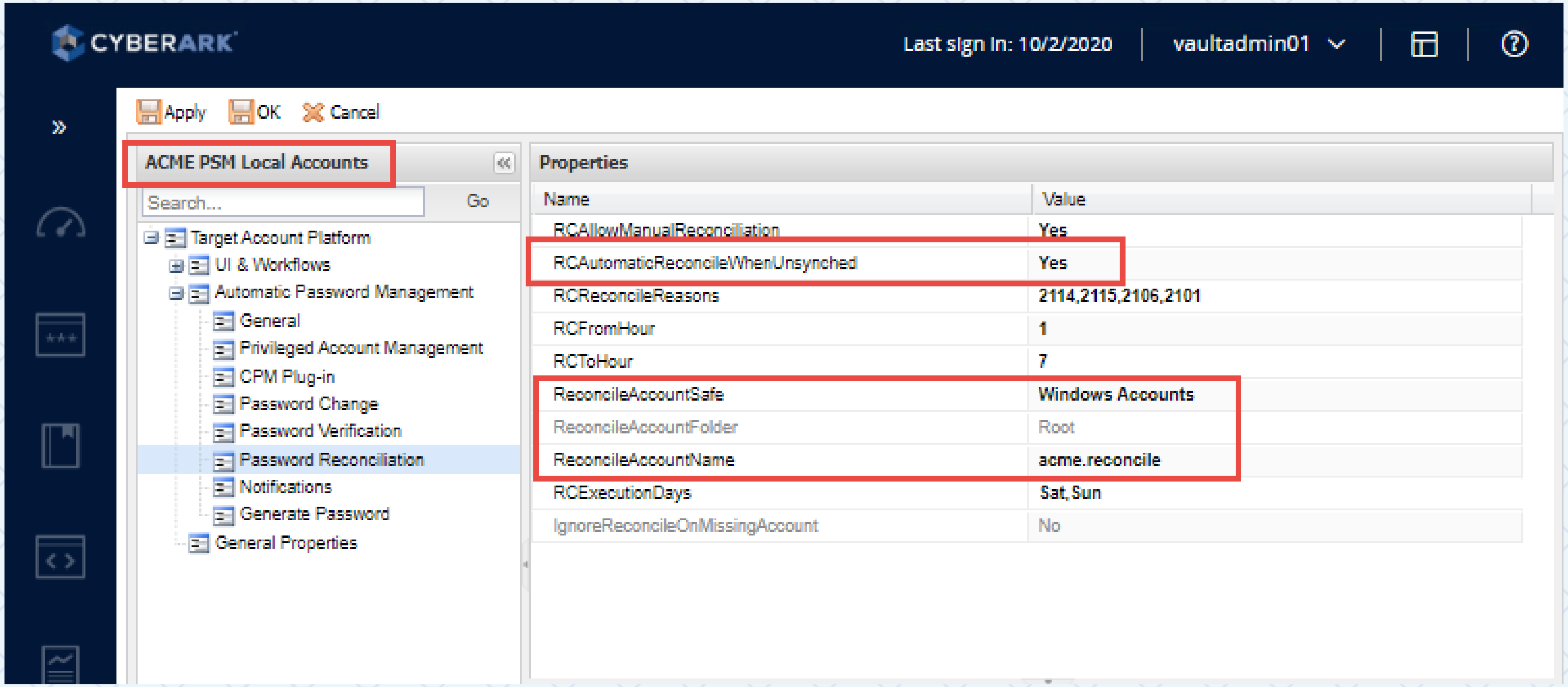
Store in Safe:	PSM			
Device Type:	Operating System	Change to:	Operating System ▼	
Platform Name:	CyberArk Lab PSM Local Accounts	Change to:	CyberArk Lab PSM Local Accounts ▼	
Required Properties:				
Address:	10.0.23.1	Change to:		
Username:	PSMConnect	Change to:		
Optional Properties:				
☑ Logon To:	COMP01D	Change to:		Resolve
□ Location:		Change to:		
□ Owner Name:		Change to:		
		Change to:		

□ Disable automatic management for this account

Reason:

MANAGE PSM ACCOUNTS

- Associate a Reconcile Account to the PSMConnect and PSMAdminConnect accounts
- Recommended to define the reconcile account at the platform
- Ensure “RCAutomaticReconcileWhenUnsynched” is set to **Yes** in the platform



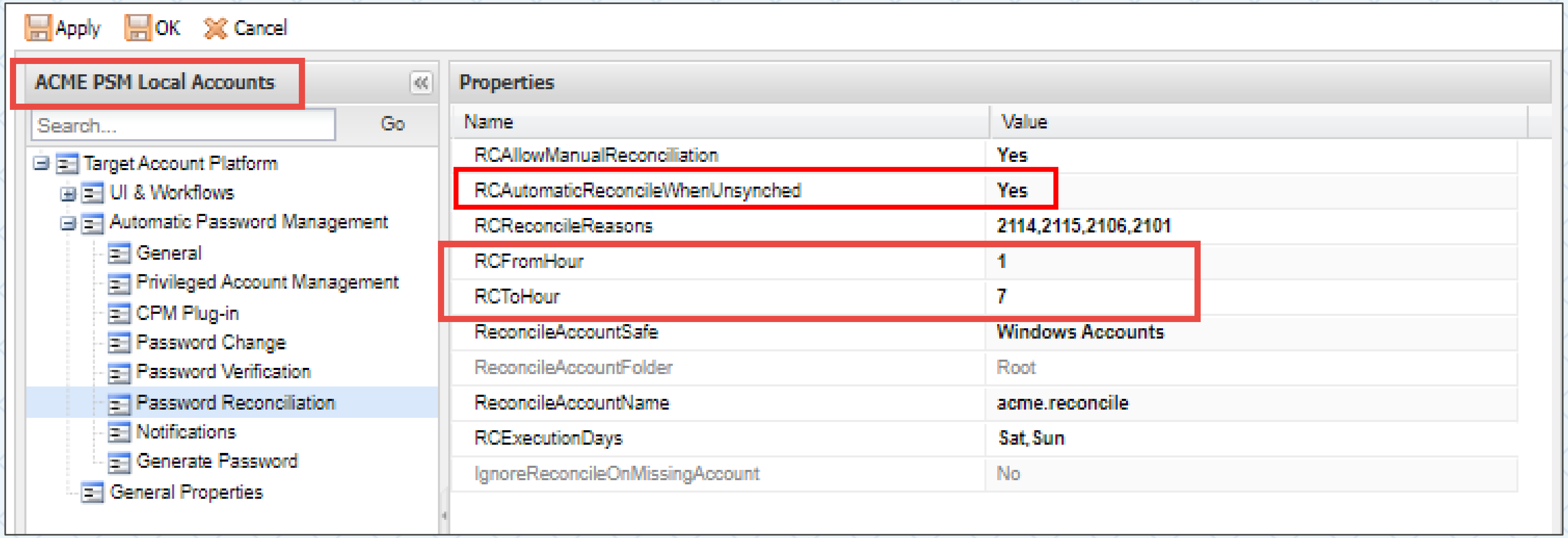
Name	Value
RCAllowManualReconciliation	Yes
RCAutomaticReconcileWhenUnsynched	Yes
RCReconcileReasons	2114,2115,2106,2101
RCFromHour	1
RCToHour	7
ReconcileAccountSafe	Windows Accounts
ReconcileAccountFolder	Root
ReconcileAccountName	acme.reconcile
RCExecutionDays	Sat, Sun
IgnoreReconcileOnMissingAccount	No

MANAGE PSM ACCOUNTS

Configure FromHour and ToHour parameters in the target platform

Account management operations can be scheduled for certain days of the week and time of day.

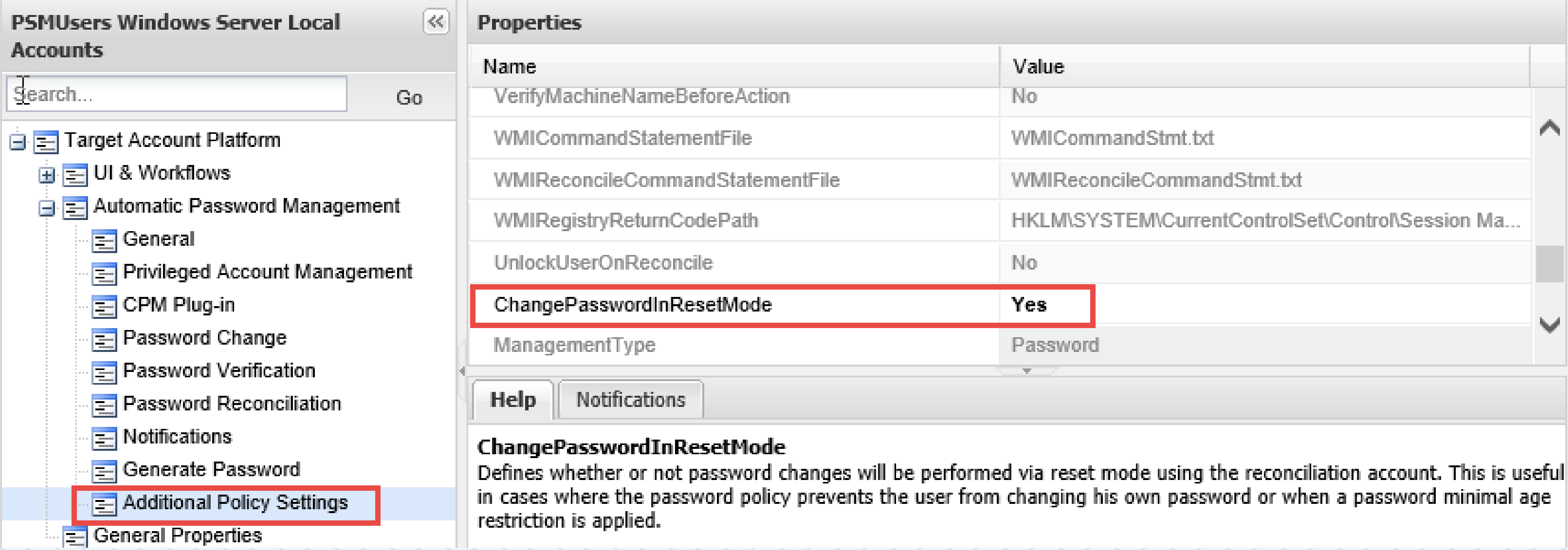
Enable RCAutomaticReconciliationWhenUnsynched. Passwords will never be reset automatically if not enabled



Name	Value
RCAllowManualReconciliation	Yes
RCAutomaticReconcileWhenUnsynched	Yes
RCReconcileReasons	2114,2115,2106,2101
RCFromHour	1
RCToHour	7
ReconcileAccountSafe	Windows Accounts
ReconcileAccountFolder	Root
ReconcileAccountName	acme.reconcile
RCExecutionDays	Sat,Sun
IgnoreReconcileOnMissingAccount	No

MANAGE THE PSM ACCOUNTS

Enable parameter **ChangePasswordInResetMode** in Additional Policy Settings Automatic Password Management.



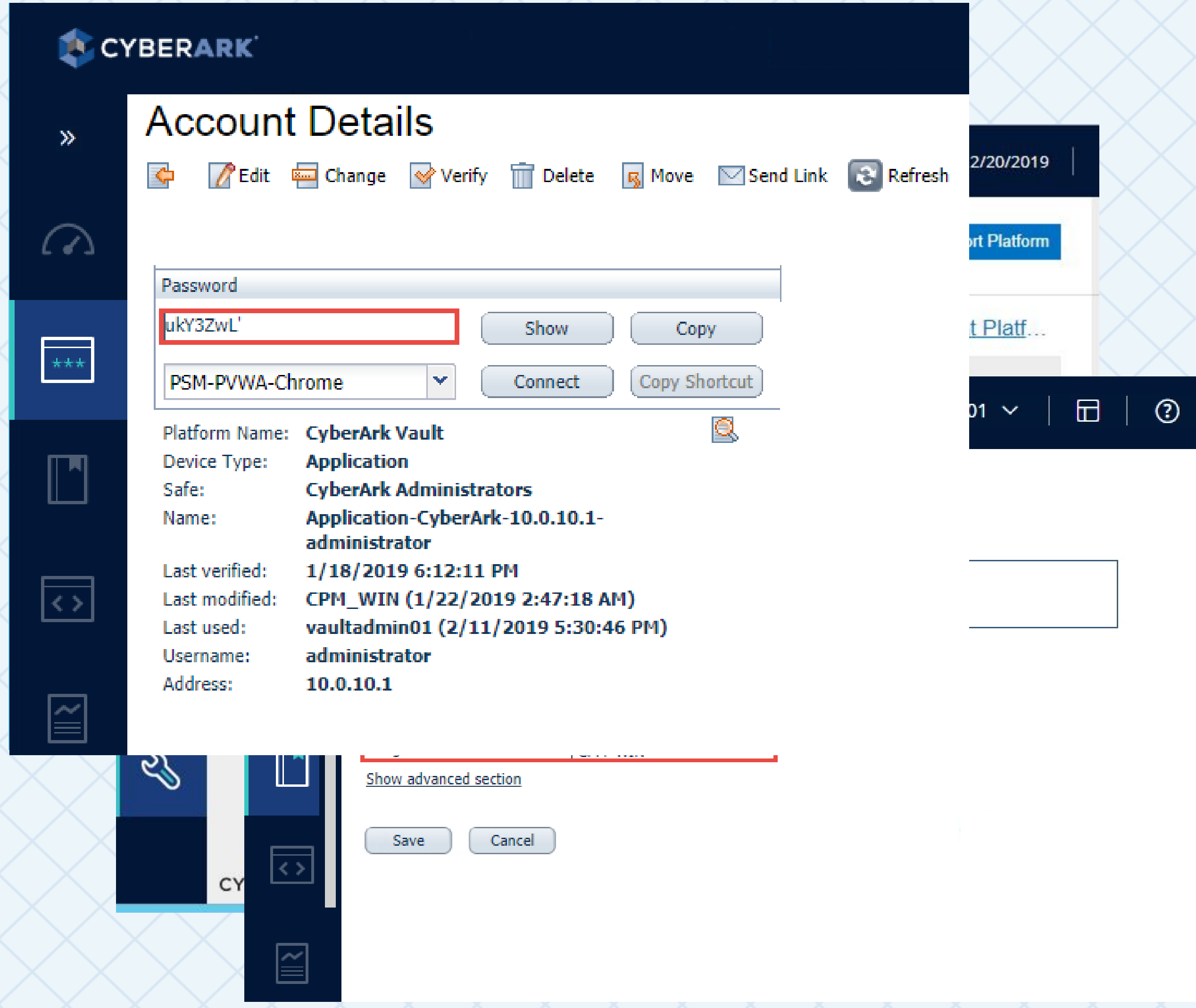
Name	Value
VerifyMachineNameBeforeAction	No
WMICommandStatementFile	WMICommandStmt.txt
WMIReconcileCommandStatementFile	WMIReconcileCommandStmt.txt
WMIRegistryReturnCodePath	HKLM\SYSTEM\CurrentControlSet\Control\Session Ma...
UnlockUserOnReconcile	No
ChangePasswordInResetMode	Yes
ManagementType	Password

ChangePasswordInResetMode
Defines whether or not password changes will be performed via reset mode using the reconciliation account. This is useful in cases where the password policy prevents the user from changing his own password or when a password minimal age restriction is applied.

MANAGING CYBERARK ADMINISTRATIVE ACCOUNTS

MANAGE CYBERARK ADMINISTRATIVE ACCOUNTS

- The CPM can change and verify internal CyberArk users' passwords and store the password in the Vault
- To manage internal CyberArk administrative accounts, enable the “CyberArk Vault” platform and consider scheduling changes during a specific timeframe
- Create a safe to store the account, assign permissions and an appropriate CPM
- Create the accounts



Password: ukY3ZwL'

PSM-PVWA-Chrome

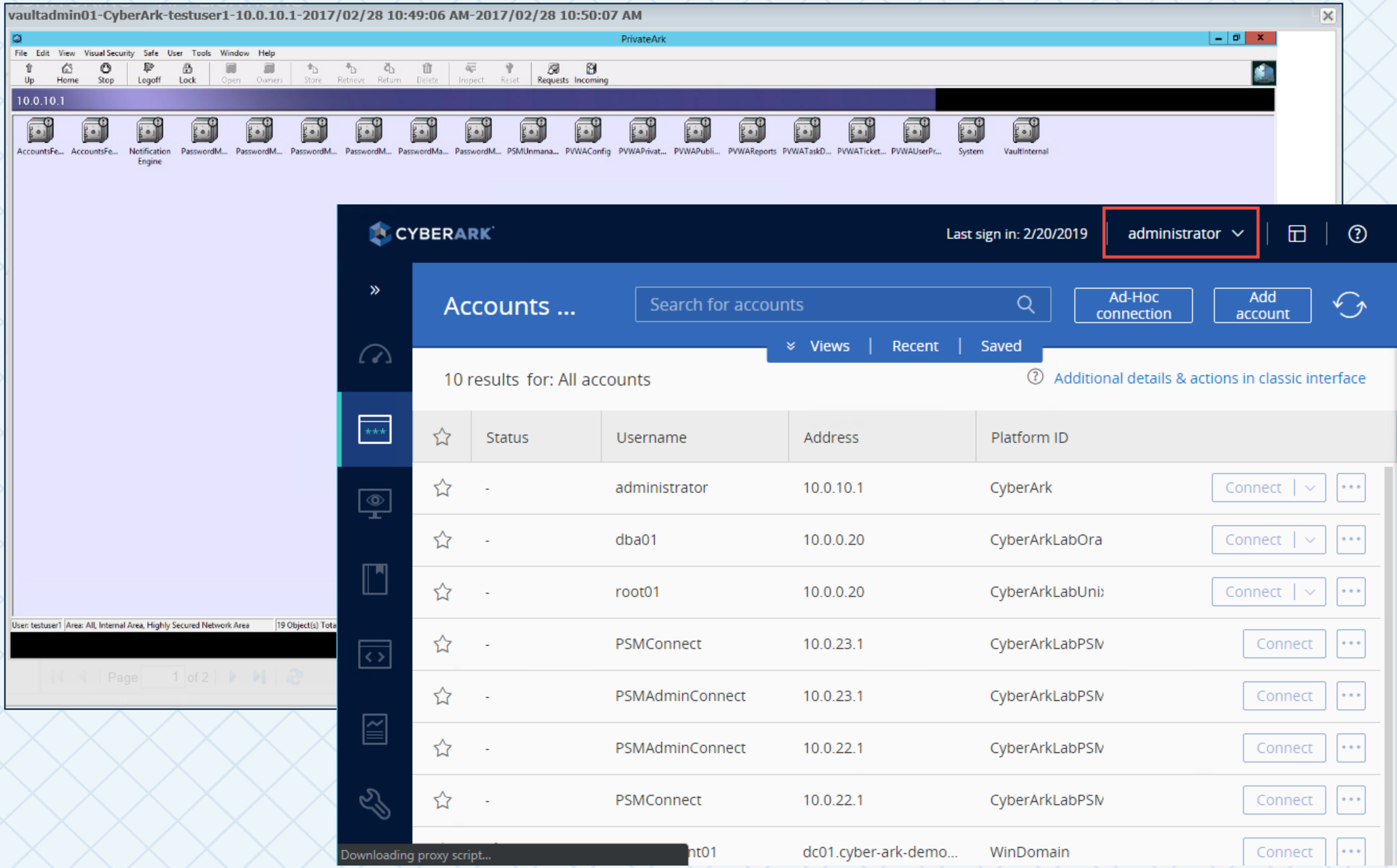
Platform Name: CyberArk Vault
Device Type: Application
Safe: CyberArk Administrators
Name: Application-CyberArk-10.0.10.1-administrator
Last verified: 1/18/2019 6:12:11 PM
Last modified: CPM_WIN (1/22/2019 2:47:18 AM)
Last used: vaultadmin01 (2/11/2019 5:30:46 PM)
Username: administrator
Address: 10.0.10.1

USING PSM CONNECTION COMPONENTS WITH THE BUILT-IN ADMINISTRATOR

PSM-PRIVATEARK CLIENT
PSM-PVWA

CONNECTING TO CYBERARK ADMINISTRATIVE INTERFACES

- CyberArk administrative access should be protected, monitored and fully audited by the PSM
- PSM includes preconfigured PrivateArk client and PVWA connection components
- Allows Vault users to administer the Vault via PSM



vaultadmin01-CyberArk-testuser1-10.0.10.1-2017/02/28 10:49:06 AM-2017/02/28 10:50:07 AM

PrivateArk
File Edit View Visual Security Safe User Tools Window Help
Up Home Stop Logoff Lock Open Owners Store Retrieve Return Delete Inspect Reset Requests Incoming
10.0.10.1
AccountsFe... AccountsFe... Notification Engine PasswordM... PasswordM... PasswordM... PasswordM... PasswordMa... PasswordM... PSMUnmana... PVWAConfig PVWAPrivat... PVWAPubli... PVWAReports PVWATaskD... PVWATicket... PVWAUserPr... System VaultInternal
User: testuser1 Area: All, Internal Area, Highly Secured Network Area 19 Object(s) Tota
Page 1 of 2
CYBERARK
Last sign in: 2/20/2019
administrator
Accounts ...
Search for accounts
Ad-Hoc connection
Add account
Views Recent Saved
Additional details & actions in classic interface
Downloading proxy script...

10 results for: All accounts

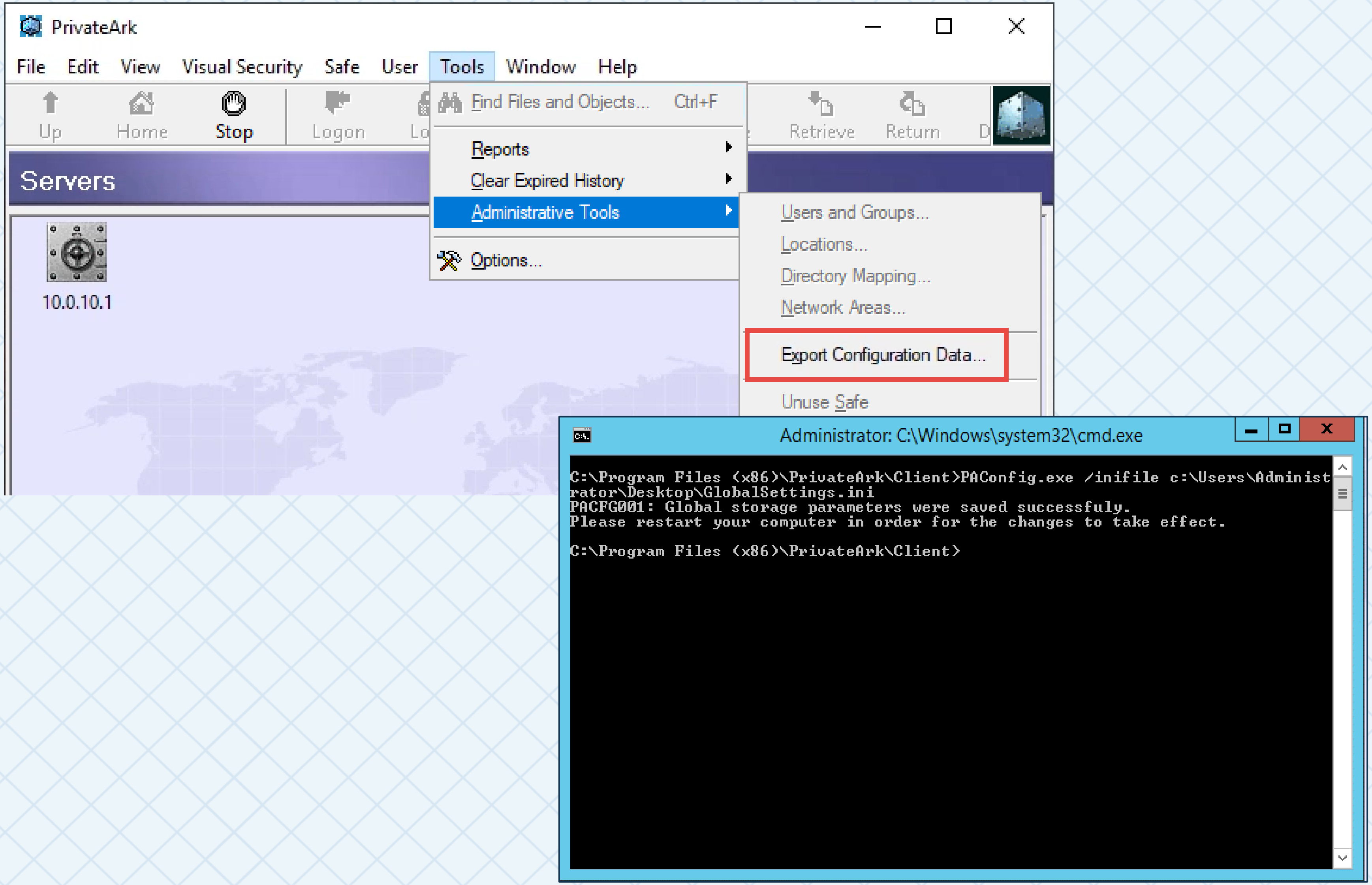
Status	Username	Address	Platform ID	
-	administrator	10.0.10.1	CyberArk	Connect
-	dba01	10.0.0.20	CyberArkLabOra	Connect
-	root01	10.0.0.20	CyberArkLabUni:	Connect
-	PSMConnect	10.0.23.1	CyberArkLabPSM	Connect
-	PSMAdminConnect	10.0.23.1	CyberArkLabPSM	Connect
-	PSMAdminConnect	10.0.22.1	CyberArkLabPSM	Connect
-	PSMConnect	10.0.22.1	CyberArkLabPSM	Connect
	nt01	dc01.cyber-ark-demo...	WinDomain	Connect

PSM-PRIVATEARK CLIENT

PSM-PRIVATEARK CLIENT PREREQUISITES

Configure the PrivateArk Administrative Client installed on the PSM server in Global Configuration mode

- Define at least one Vault definition in the PrivateArk Client
- Export Configuration Data to a local file
- Run the PAConfig.exe utility

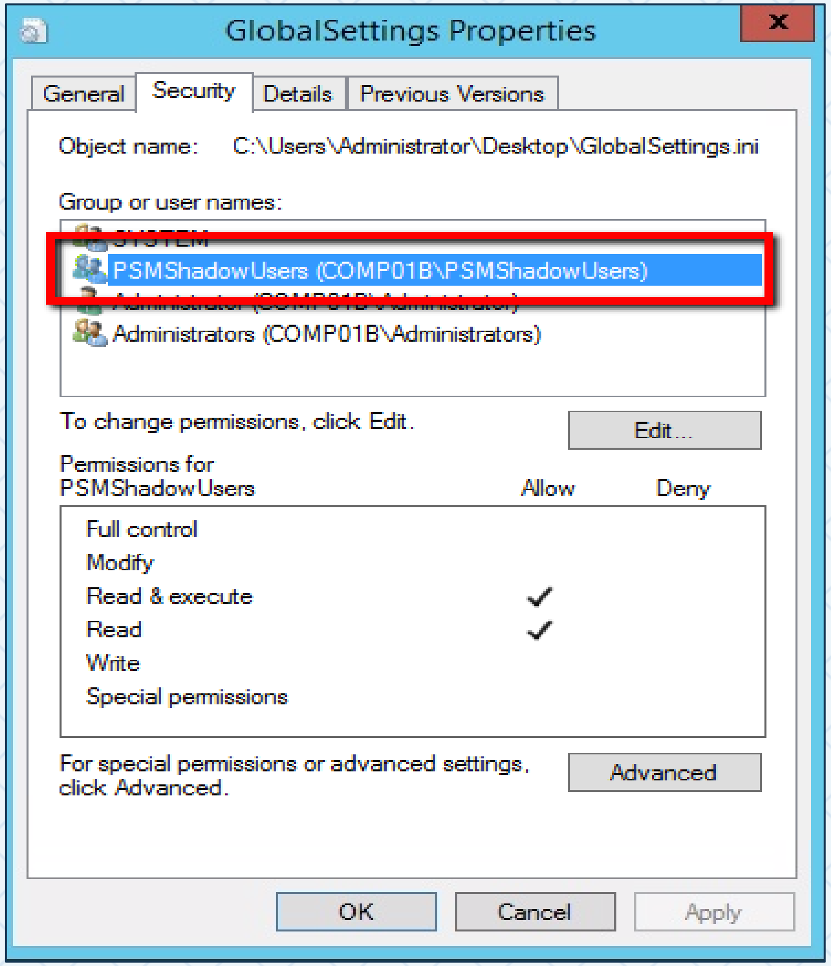


```
C:\Program Files (x86)\PrivateArk\Client>PAConfig.exe /infile c:\Users\Administ
rator\Desktop\GlobalSettings.ini
PACFG001: Global storage parameters were saved successfuly.
Please restart your computer in order for the changes to take effect.

C:\Program Files (x86)\PrivateArk\Client>
```

CONNECTING WITH PSM-PRIVATEARK CLIENT

- The **PSMShadowUsers group** must have Read and Execute permissions on the Global Settings configuration file used by the PrivateArk Client



GlobalSettings Properties

Object name: C:\Users\Administrator\Desktop\GlobalSettings.ini

Group or user names:

SYSTEM
PSMShadowUsers (COMP01B\PSMShadowUsers)
Administrator (COMP01B\Administrator)
Administrators (COMP01B\Administrators)

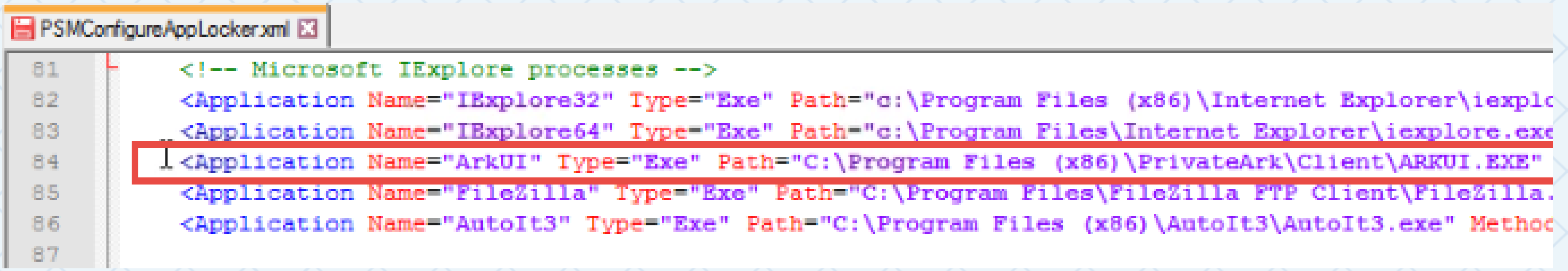
To change permissions, click Edit.

Permissions for PSMShadowUsers	Allow	Deny
Full control		
Modify		
Read & execute	✓	
Read	✓	
Write		
Special permissions		

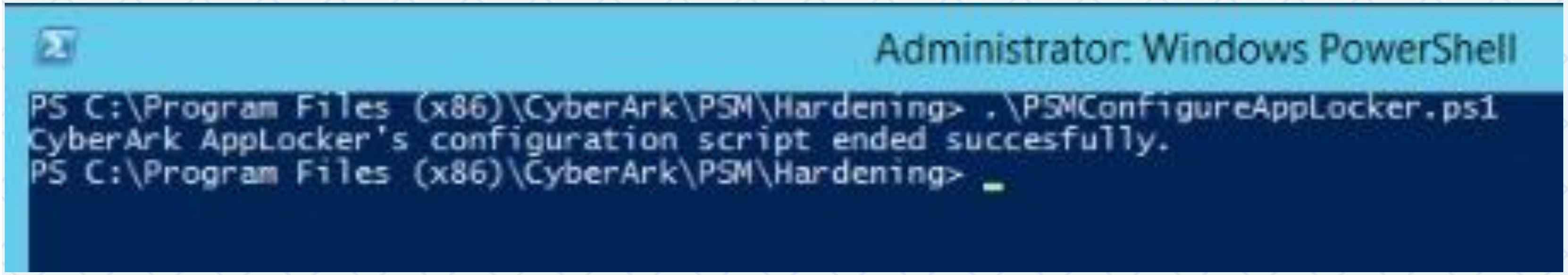
For special permissions or advanced settings, click Advanced.

PSM-PRIVATEARK CLIENT PREREQUISITES

- The PrivateArk Client is no different than any other client software used for a PSM connection
- An AppLocker rule must be configured to enable the PrivateArk client to launch in the context of a PSM connection
- Run the AppLocker script to add the rule to the Local Security Policy



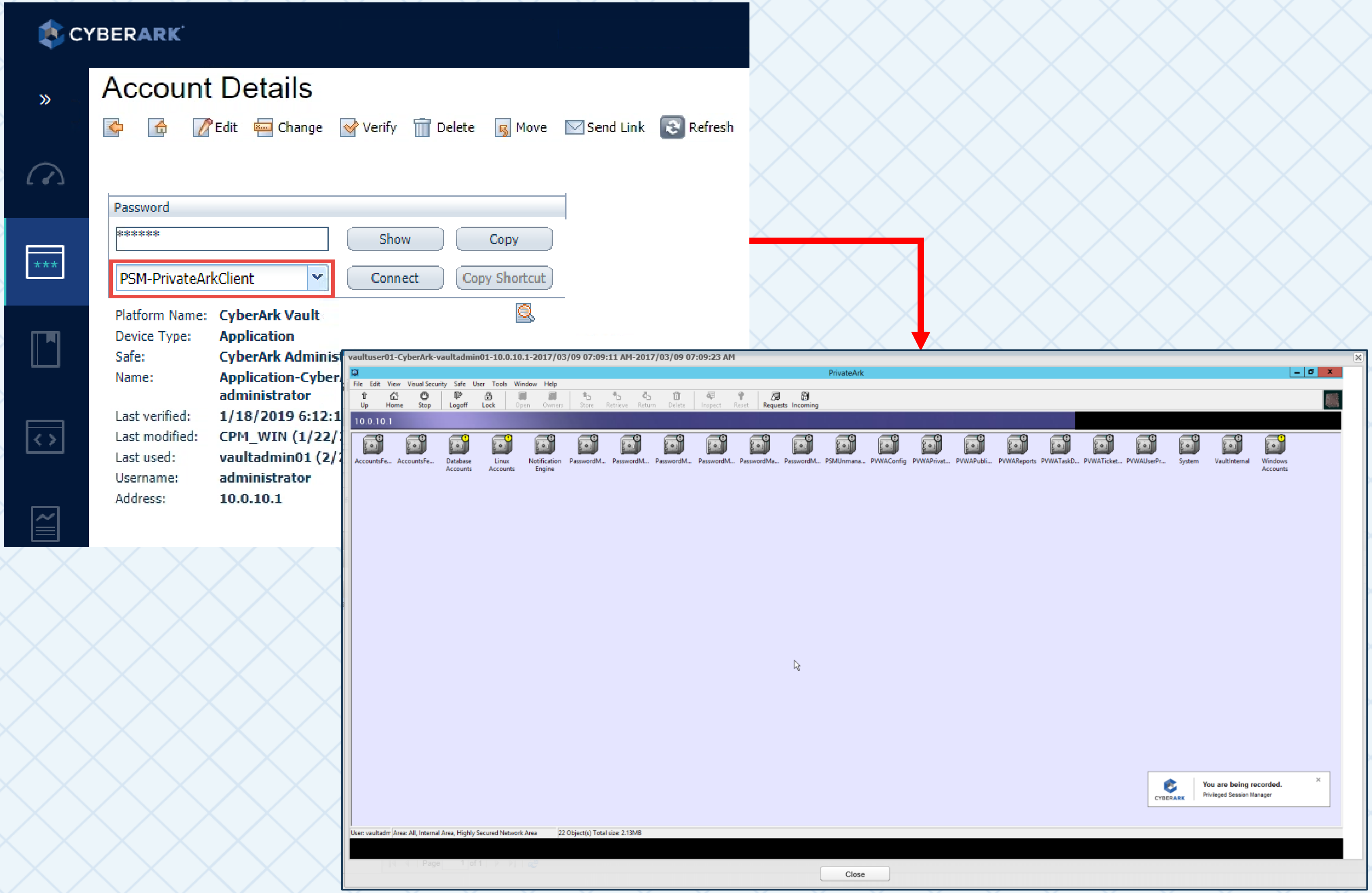
```
    <!-- Microsoft IExplore processes -->
    <Application Name="IExplore32" Type="Exe" Path="c:\Program Files (x86)\Internet Explorer\iexplc
    <Application Name="IExplore64" Type="Exe" Path="c:\Program Files\Internet Explorer\iexplore.exe
    <Application Name="ArkUI" Type="Exe" Path="C:\Program Files (x86)\PrivateArk\Client\ARKUI.EXE"
    <Application Name="FileZilla" Type="Exe" Path="C:\Program Files\FileZilla FTP Client\FileZilla.
    <Application Name="AutoIt3" Type="Exe" Path="C:\Program Files (x86)\AutoIt3\AutoIt3.exe" Methoc
```



```
PS C:\Program Files (x86)\CyberArk\PSM\Hardening> .\PSMConfigureAppLocker.ps1
CyberArk AppLocker's configuration script ended succesfully.
PS C:\Program Files (x86)\CyberArk\PSM\Hardening> _
```

CONNECTING WITH PSM-PRIVATEARK CLIENT

- In the PVWA find the built-in Administrator
- Select “PSM-PrivateArkClient”
- Additional information on Connection component parameters for the PSM-PrivateArkClient connection component can be found online at docs.cyberark.com



Account Details

Password: *******

PSM-PrivateArkClient

Platform Name: CyberArk Vault
Device Type: Application
Safe: CyberArk Adminis
Name: Application-Cyber administrator
Last verified: 1/18/2019 6:12:1
Last modified: CPM_WIN (1/22/
Last used: vaultadmin01 (2/
Username: administrator
Address: 10.0.10.1

vaultuser01-CyberArk-vaultadmin01-10.0.10.1-2017/03/09 07:09:11 AM-2017/03/09 07:09:23 AM

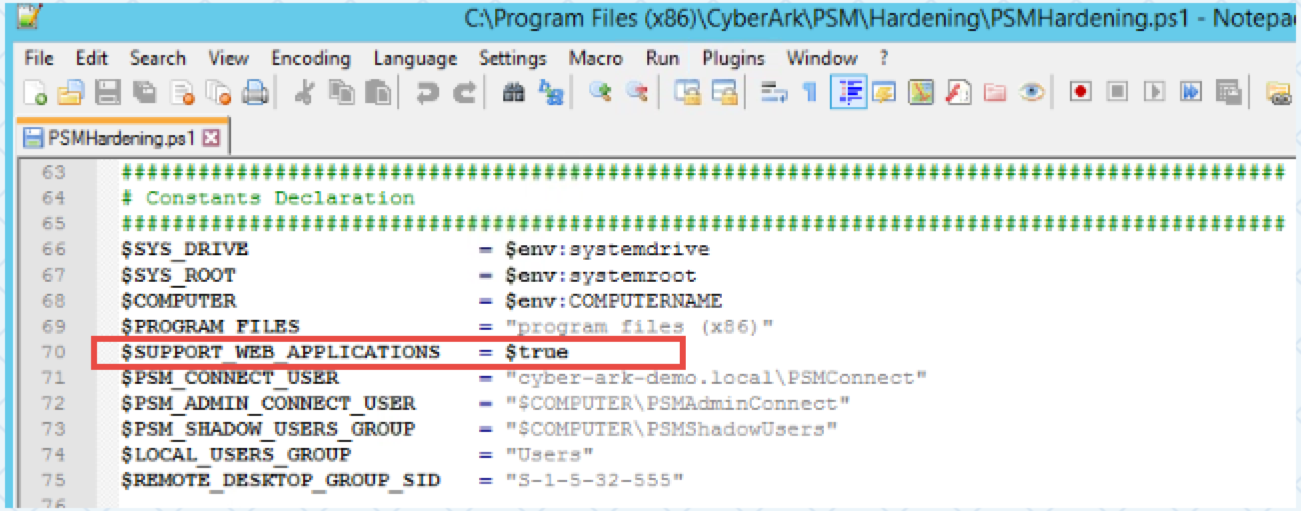
User: vaultadm Area: All, Internal Area, Highly Secured Network Area 22 Object(s) Total size: 2.13MB

You are being recorded. Privileged Session Manager

PSM-PVWA

PSM-PVWA PREREQUISITES

- Enable support for Web Applications on all PSM servers in a Load Balanced configuration
- Configure the PSM Hardening Script to enable PSM to connect to Web applications
- Run the Hardening script

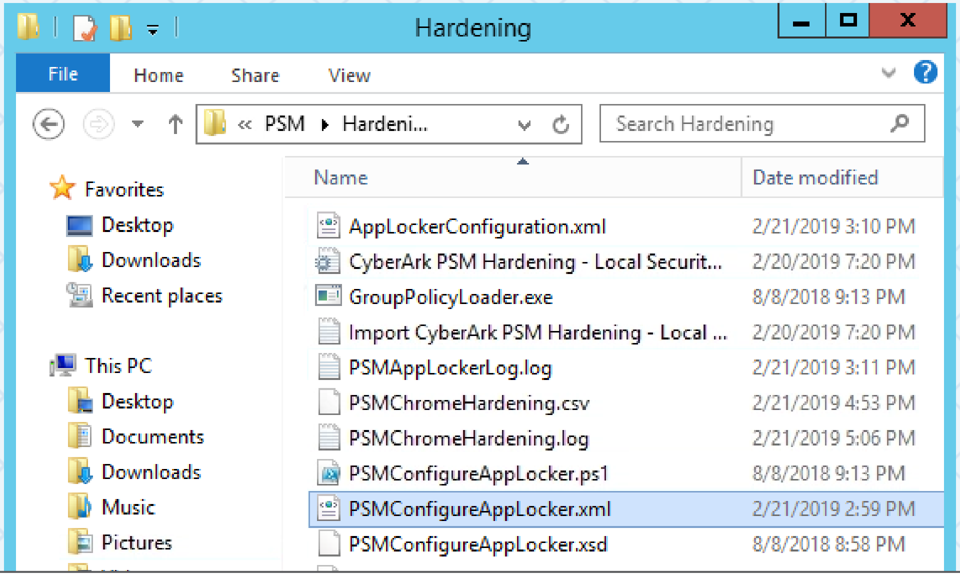

C:\Program Files (x86)\CyberArk\PSM\Hardening\PSMHardening.ps1 - Notepa
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
PSMHardening.ps1

```
###########################################################################################
# Constants Declaration
###########################################################################################
$SYS_DRIVE                  = $env:systemdrive
$SYS_ROOT                   = $env:systemroot
$COMPUTER                   = $env:COMPUTERNAME
$PROGRAM_FILES              = "program files (x86)"
$SUPPORT_WEB_APPLICATIONS   = $true
$PSM_CONNECT_USER           = "cyber-ark-demo.local\PSMConnect"
$PSM_ADMIN_CONNECT_USER     = "$COMPUTER\PSMAdminConnect"
$PSM_SHADOW_USERS_GROUP     = "$COMPUTER\PSMShadowUsers"
$LOCAL_USERS_GROUP          = "Users"
$REMOTE_DESKTOP_GROUP_SID   = "S-1-5-32-555"
```

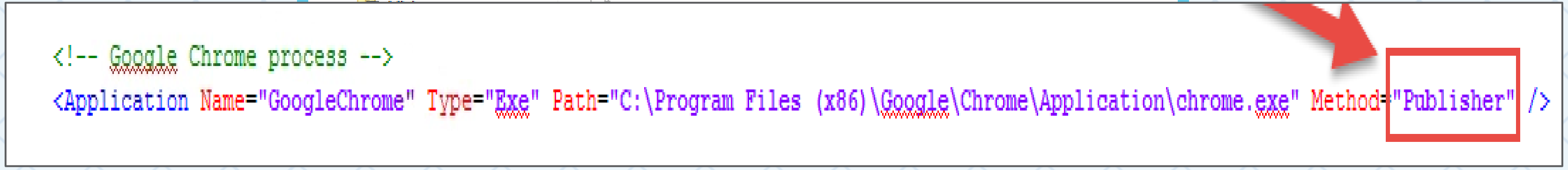
PSM-PVWA-CHROME PREREQUISITES

Configure Applocker to enable Google Chrome

- In the PSM\Hardening subfolder, edit the PSMConfigureApplocker.xml
- Remove comments from “Google Chrome process” section and change Method to “Publisher”



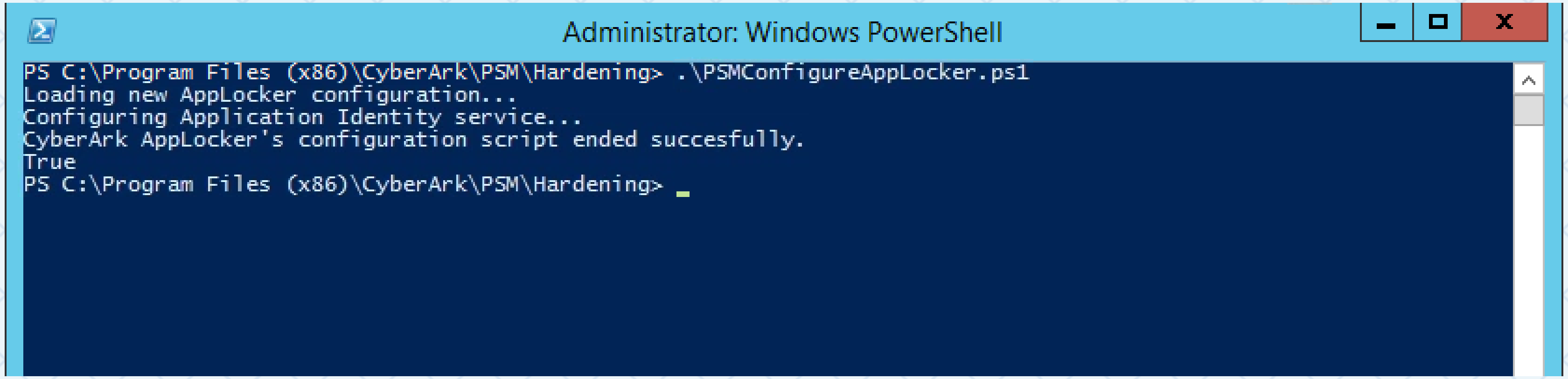
Name	Date modified
AppLockerConfiguration.xml	2/21/2019 3:10 PM
CyberArk PSM Hardening - Local Securit...	2/20/2019 7:20 PM
GroupPolicyLoader.exe	8/8/2018 9:13 PM
Import CyberArk PSM Hardening - Local ...	2/20/2019 7:20 PM
PSMAppLockerLog.log	2/21/2019 3:11 PM
PSMChromeHardening.csv	2/21/2019 4:53 PM
PSMChromeHardening.log	2/21/2019 5:06 PM
PSMConfigureAppLocker.ps1	8/8/2018 9:13 PM
PSMConfigureAppLocker.xml	2/21/2019 2:59 PM
PSMConfigureAppLocker.xsd	8/8/2018 8:58 PM



```
<!-- Google Chrome process -->
<Application Name="GoogleChrome" Type="Exe" Path="C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" Method="Publisher" />
```

PSM-PVWA-CHROME PREREQUISITES

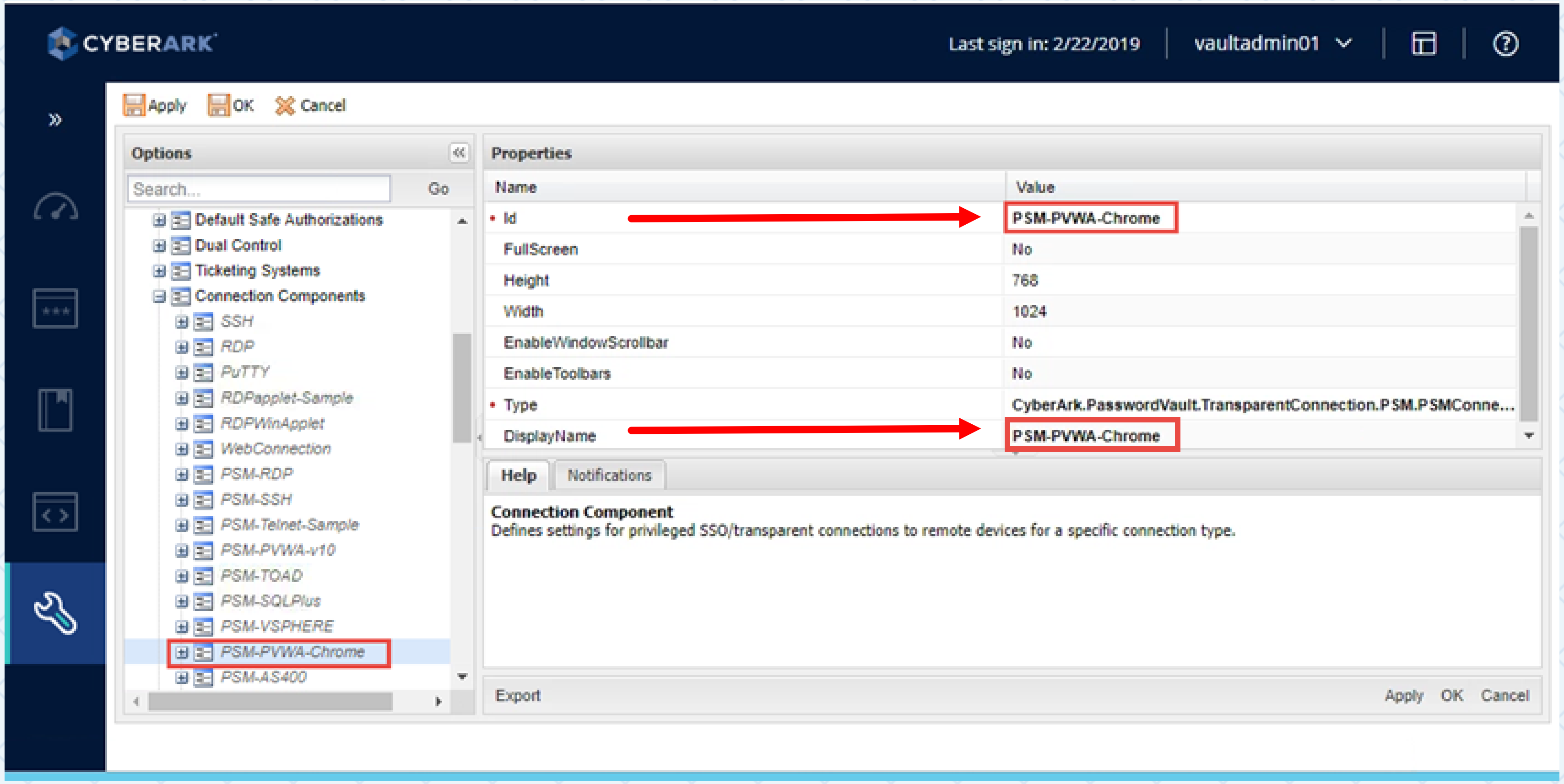
- Open PowerShell as Administrator and execute the PSMConfigureApplocker.ps1 script, applying the Applocker rules defined in PSMConfigureApplocker.xml



```
PS C:\Program Files (x86)\CyberArk\PSM\Hardening> .\PSMConfigureAppLocker.ps1
Loading new AppLocker configuration...
Configuring Application Identity service...
CyberArk AppLocker's configuration script ended succesfully.
True
PS C:\Program Files (x86)\CyberArk\PSM\Hardening> _
```

CONNECTING WITH PSM-PVWA-CHROME

- In PVWA Options > Connection Components > Select and copy **PSM-PVWA-v10** and paste it
- Rename the copy to **PSM-PVWA-Chrome**
- Update the DisplayName

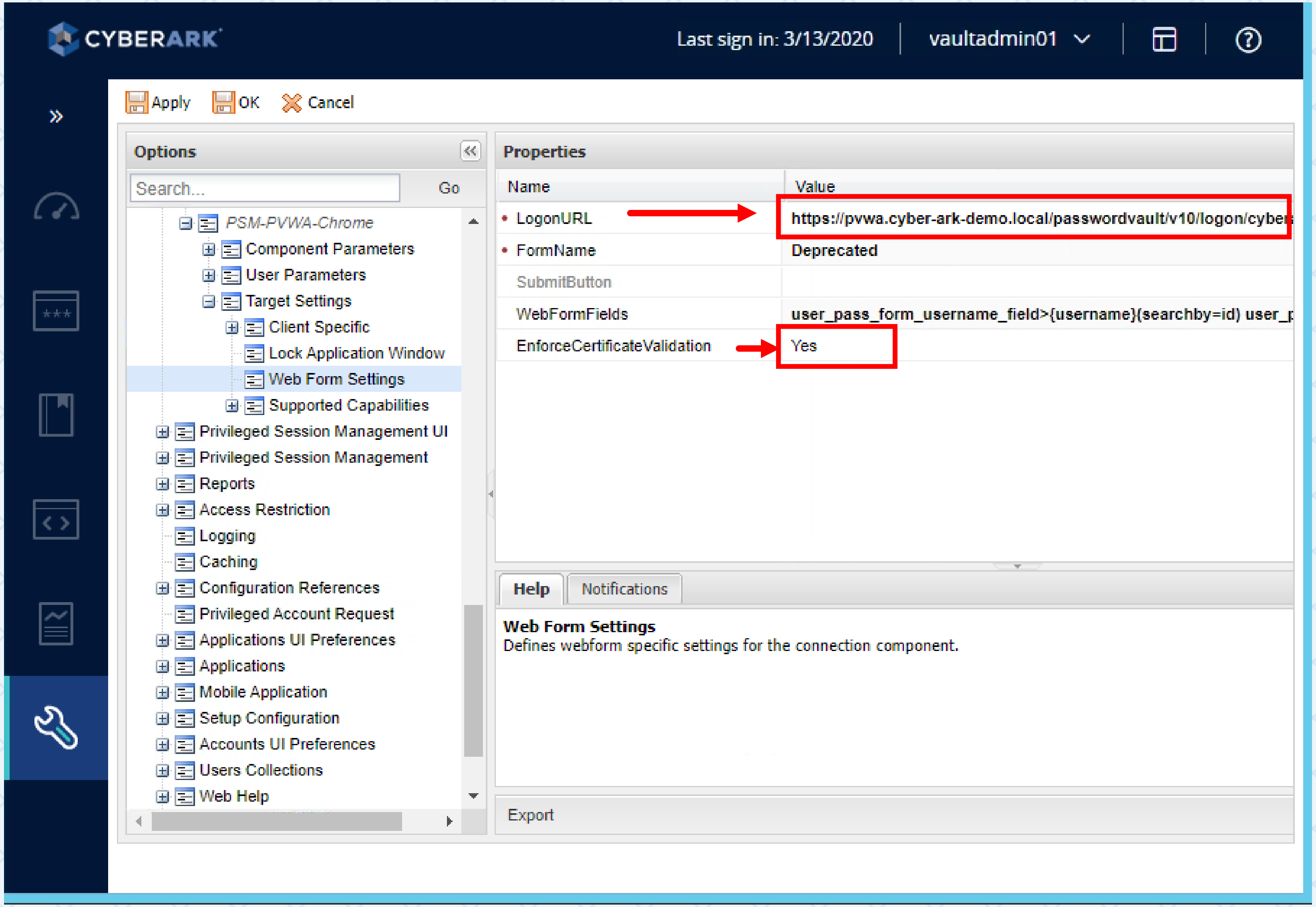


Name	Value
• Id	PSM-PVWA-Chrome
FullScreen	No
Height	768
Width	1024
EnableWindowScrollbar	No
EnableToolbars	No
• Type	CyberArk.PasswordVault.TransparentConnection.PSM.PSMConne...
DisplayName	PSM-PVWA-Chrome

Connection Component
Defines settings for privileged SSO/transparent connections to remote devices for a specific connection type.

CONNECTING WITH PSM-PVWA-CHROME

- In Target Settings > Web Form Settings, update LogonURL to match the fully qualified hostname of your PVWA server, including the authentication method
- EnforceCertificateValidation should be set to “Yes” when using a Web Certificate from a trusted Certificate Authority

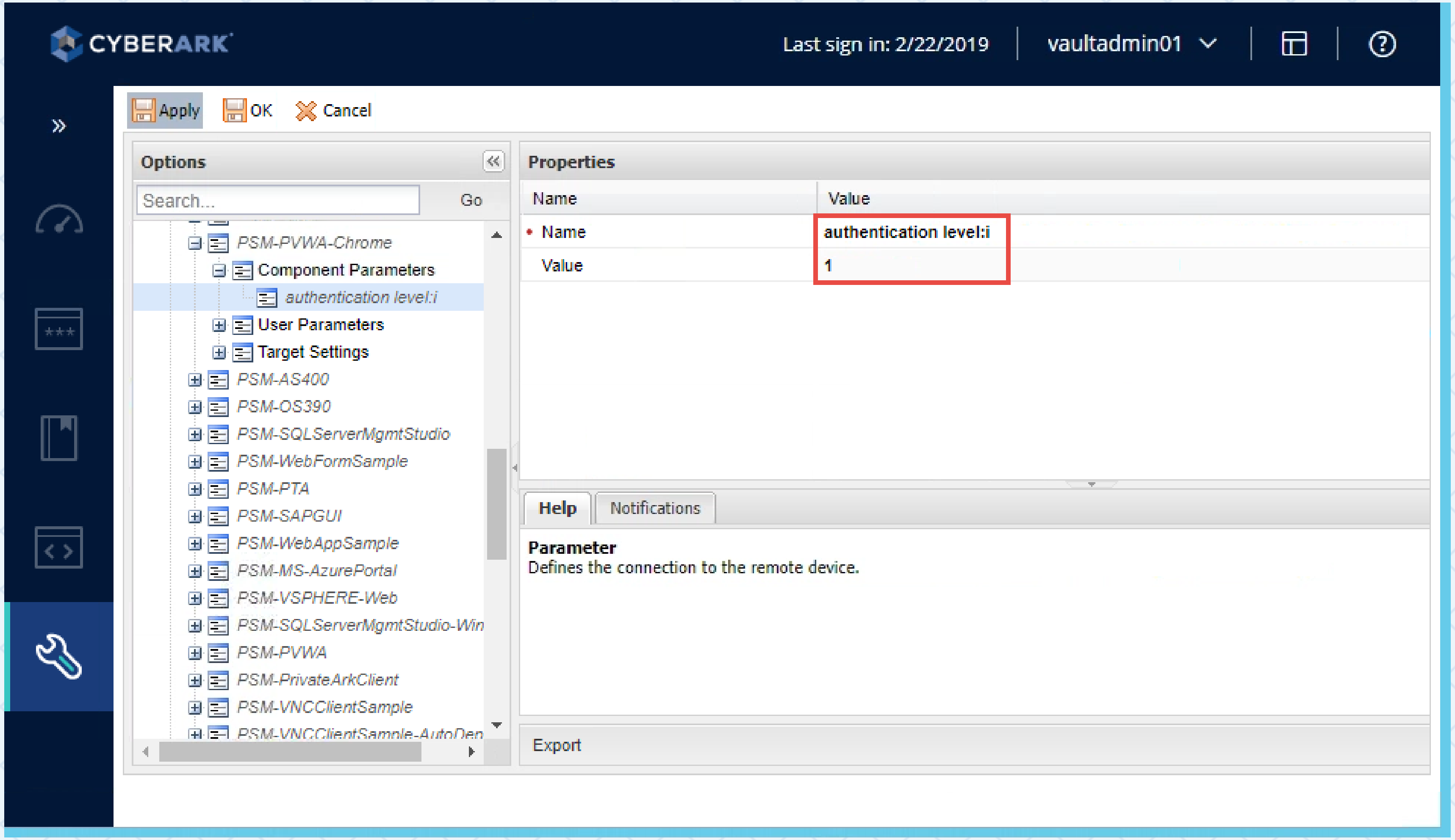


Name	Value
• LogonURL	https://pvwa.cyber-ark-demo.local/passwordvault/v10/logon/cyber
• FormName	Deprecated
SubmitButton	
WebFormFields	user_pass_form_username_field>{username}(searchby=id) user_p
EnforceCertificateValidation	Yes

Web Form Settings
Defines webform specific settings for the connection component.

CONNECTING WITH PSM-PVWA-CHROME

- Enable RDP over SSL for the **PSM-PVWA-Chrome** connection component by adding Component Parameter
  - Name: Authentication level:I
  - Value: 1



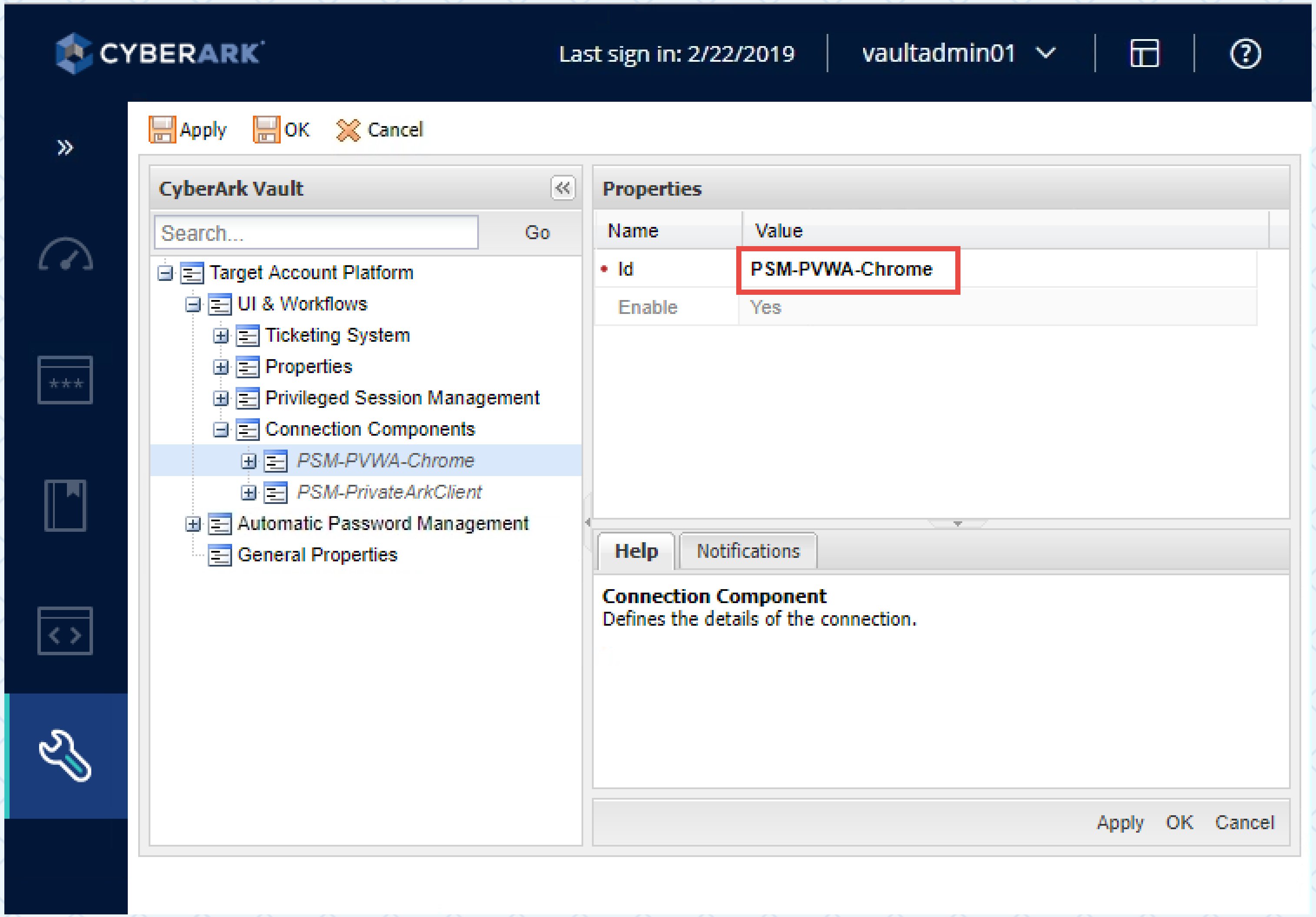
Name	Value
• Name	authentication level:i
Value	1

Parameter
Defines the connection to the remote device.

CONNECTING WITH PSM-PVWA-CHROME

Edit the CyberArk Vault platform.

- Rename **PSM-PVWA-v10** connection component to **PSM-PVWA-Chrome.**

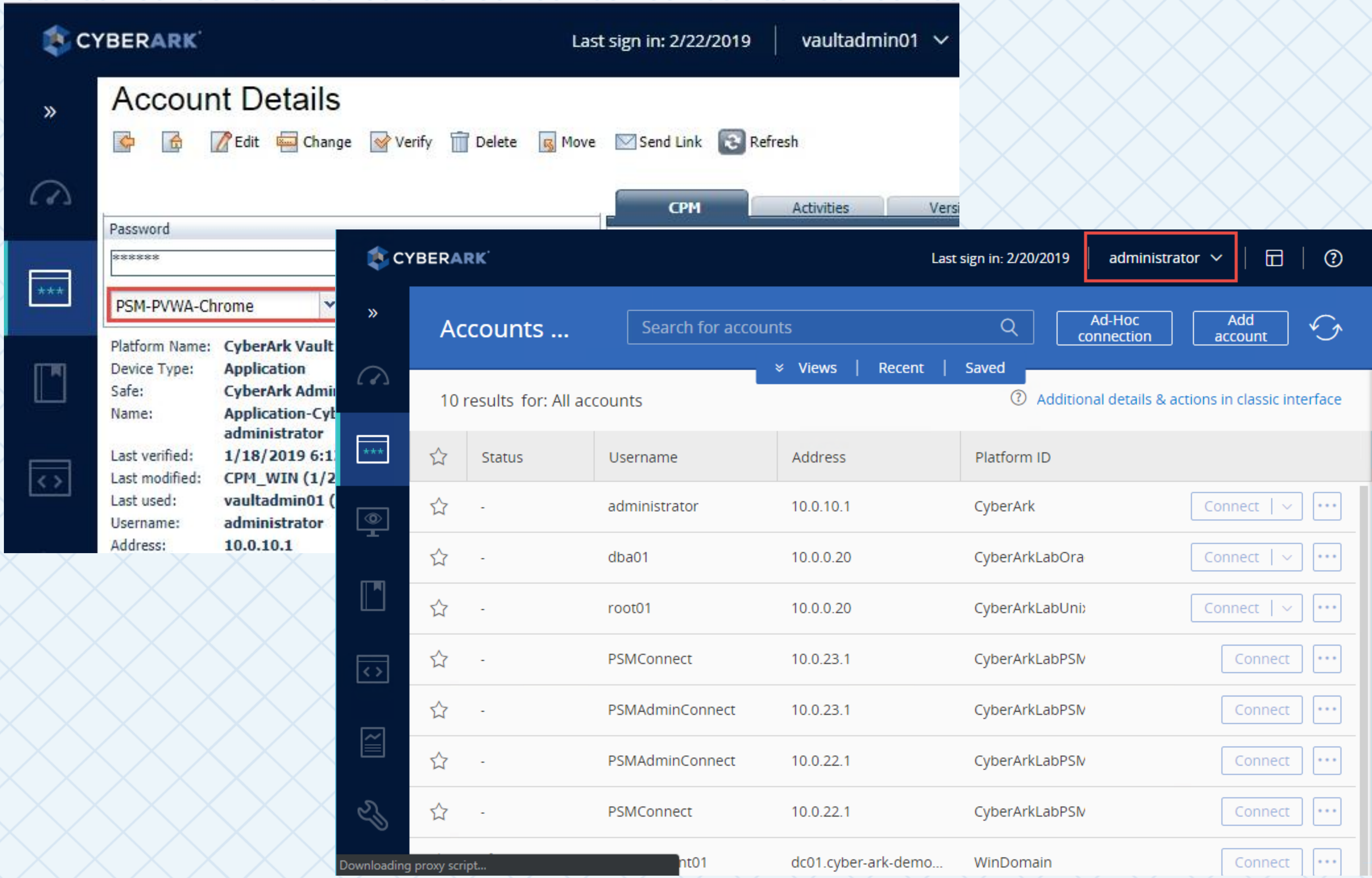


Name	Value
Id	PSM-PVWA-Chrome
Enable	Yes

Connection Component
Defines the details of the connection.

CONNECTING WITH PSM-PVWA-CHROME

- Test the PSM-PVWA-Chrome connection component
- Detailed information on Connection component parameters can be found online at CyberArk Docs



Account Details

Password: *******

PSM-PVWA-Chrome

Platform Name:	CyberArk Vault
Device Type:	Application
Safe:	CyberArk Admi
Name:	Application-Cyb administrator
Last verified:	1/18/2019 6:1
Last modified:	CPM_WIN (1/2
Last used:	vaultadmin01 (
Username:	administrator
Address:	10.0.10.1

10 results for: All accounts

Status	Username	Address	Platform ID	
-	administrator	10.0.10.1	CyberArk	Connect
-	dba01	10.0.0.20	CyberArkLabOra	Connect
-	root01	10.0.0.20	CyberArkLabUni:	Connect
-	PSMConnect	10.0.23.1	CyberArkLabPSN	Connect
-	PSMAdminConnect	10.0.23.1	CyberArkLabPSN	Connect
-	PSMAdminConnect	10.0.22.1	CyberArkLabPSN	Connect
-	PSMConnect	10.0.22.1	CyberArkLabPSN	Connect
	nt01	dc01.cyber-ark-demo...	WinDomain	Connect

SUMMARY

In this session we:

- Learned how to use the Enterprise Password Vault to secure and manage CyberArk Administrative and Service Accounts
- Learned how to use Privileged Session Manager to isolate and monitor access to CyberArk administrative interfaces using managed built-in CyberArk Administrative accounts

CYBERARK

THANK YOU