



# Exercise Guide

## Contents

<b>INTRODUCTION .....</b>	<b>4</b>
USING SKYTAP .....	4
INTERNATIONAL USERS .....	6
<b>SCENARIO .....</b>	<b>10</b>
<b>EPV INSTRUCTIONS.....</b>	<b>11</b>
<b>VAULT INSTALLATION.....</b>	<b>12</b>
BEFORE INSTALLATION .....	12
VAULT SERVER INSTALLATION.....	15
PRIVATEARK CLIENT INSTALLATION .....	26
<b>INSTALL CPM (DISTRIBUTED).....</b>	<b>30</b>
INSTALL 1 <sup>ST</sup> CPM.....	30
INSTALL THE PRIVATEARK CLIENT ON THE COMPONENT SERVER .....	35
FOLLOWING THE CPM INSTALLATION .....	35
INSTALL 2 <sup>ND</sup> CPM.....	35
INSTALL THE PRIVATEARK CLIENT ON THE COMP01B SERVER.....	37
RENAME 1 <sup>ST</sup> CPM .....	37
<b>INSTALL PVWA (LOAD BALANCED).....</b>	<b>40</b>
PVWA PRE-REQUISITES.....	40
USE HTTP OVER SSL (PVWA) .....	41
INSTALL 1ST PVWA.....	50
INSTALL 2 <sup>ND</sup> PVWA .....	56
HARDENING THE CYBERARK CPM AND PVWA SERVERS.....	59
CONFIGURE THE EXTERNAL LOAD BALANCER FOR THE PVWA SERVERS .....	60
<b>INTEGRATIONS .....</b>	<b>64</b>
LDAP AUTHENTICATION (OVER SSL).....	64
SMTP INTEGRATION .....	70
SIEM INTEGRATION .....	72
<b>AUTHENTICATION TYPES .....</b>	<b>76</b>
RADIUS AUTHENTICATION .....	76
WINDOWS AUTHENTICATION.....	83
PKI AUTHENTICATION .....	85
TWO FACTOR AUTHENTICATION (2FA) .....	90
<b>EPV IMPLEMENTATIONS.....</b>	<b>92</b>
WINDOWS REQUIREMENTS .....	92
UNIX REQUIREMENTS.....	92
DATABASE REQUIREMENTS.....	92
<b>INSTALL PSM/PSMP.....</b>	<b>94</b>
<b>STANDALONE PSM INSTALLATION.....</b>	<b>95</b>
PSM INSTALLATION .....	95
PSM POST INSTALLATION AND HARDENING TASKS.....	99



PSM TESTING AND VALIDATION .....	102
<b>LOAD BALANCED PSM INSTALLATION.....</b>	<b>105</b>
INSTALL 2ND PSM.....	105
CONFIGURE PSM LOAD BALANCING .....	107
<b>PSMP INSTALLATION .....</b>	<b>111</b>
INSTALL PSMP .....	111
(OPTIONAL) ADVANCED PSMP IMPLEMENTATIONS .....	116
<b>SECURING CYBERARK .....</b>	<b>122</b>
USE RDP OVER SSL .....	122
MANAGE LDAP BINDACCOUNT .....	128
MANAGE PSMCONNECT/PSMADMINCONNECT USING THE CPM .....	129
MANAGE CYBERARK ADMIN ACCOUNTS USING THE CPM .....	133
CONNECT WITH PSM-PRIVATEARK CLIENT.....	135
CONNECT WITH PSM-PVWA.....	139
REMOVE UNNECESSARY CYBERARK ADMINISTRATIVE PRIVILEGES.....	143
<b>BACKUP .....</b>	<b>147</b>
ENABLE THE BACKUP AND USERS .....	147
INSTALL THE PRIVATEARK REPLICATOR.....	150
TESTING THE BACKUP/RESTORE PROCESS.....	157
<b>DISASTER RECOVERY .....</b>	<b>160</b>
INSTALL THE DISASTER RECOVERY MODULE .....	160
VALIDATE THE REPLICATION WAS SUCCESSFUL .....	163
EXECUTE AUTOMATIC FAILOVER TEST .....	164
EXECUTE FAILBACK PROCEDURE USING MANUAL FAILOVER .....	166
<b>EPV IMPLEMENTATIONS (PROPOSED SOLUTION) .....</b>	<b>171</b>
WINDOWS .....	171
UNIX.....	173
DATABASE.....	174



## Important Notice

### Conditions and Restrictions

This Guide is delivered subject to the following conditions and restrictions:

This guide contains proprietary information belonging to Cyber-Ark® Software Ltd. Such information is supplied solely for the purpose of assisting explicitly and properly authorized users of the Cyber-Ark Vault.

No part of its contents may be used for any other purpose, disclosed to any person or firm or reproduced by any means, electronic and mechanical, without the express prior written permission of Cyber-Ark® Software Ltd.

The software described in this document is furnished under a license. The software may be used or copied only in accordance with the terms of that agreement.

The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.

Information in this document is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.

Third party components used in the Cyber-Ark Vault may be subject to terms and conditions listed on [www.cyberark.com/privateark/acknowledgement.htm](http://www.cyberark.com/privateark/acknowledgement.htm).

### Acknowledgements

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes software written by Ian F. Darwin.

This product includes software developed by the ICU Project (<http://site.icu-project.org/>) Copyright © 1995-2009 International Business Machines Corporation and other. All rights reserved.

This product includes software developed by the Python Software Foundation. Copyright © 2001-2010 Python Software Foundation; All Rights Reserved.

This product includes software developed by Infrae. Copyright (c) 2004 Infrae. All rights reserved.

This product includes software developed by Michael Foord. Copyright (c) 2003-2010, Michael Foord. All rights reserved.

### Copyright

© 2000-2012 Cyber-Ark Software, Ltd. All rights reserved. US Patent No 6,356,941.

Cyber-Ark®, the Cyber-Ark logo, the Cyber-Ark slogan, PrivateArk™, Network Vault®, Password Vault®, Inter-Business Vault®, Vaulting Technology®, Geographical Security™ and Visual Security™ are trademarks of Cyber-Ark Software Ltd.

All other product names mentioned herein are trademarks of their respective owners.

Information in this document is subject to change without notice.



## Introduction

### Using Skytap

Before beginning exercises here are a few tips to help you navigate the labs more effectively.

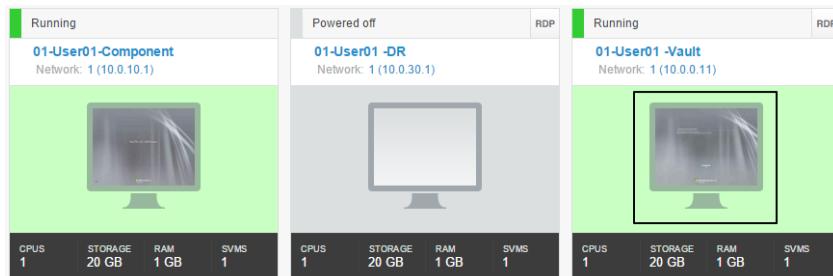
There are two ways to access the virtual machines: directly via the browser or through RDP.

- Click directly on the screen icon to access the virtual machine directly in your browser
- Click on the **RDP** button in the upper right-hand corner of the VM box.

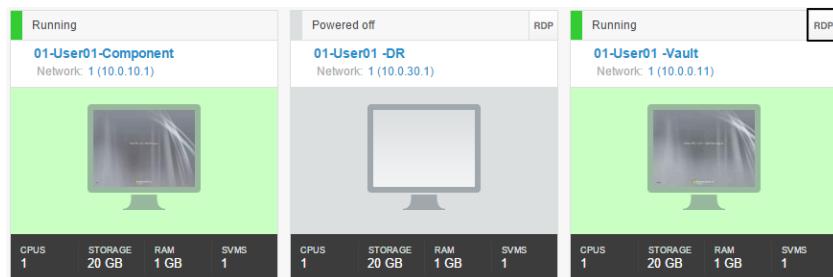
If you are using any keyboard other than a standard US, then it is strongly recommended that you use an RDP connection rather than the HTML 5 client directly in the browser. When using RDP, all you need to do is set the keyboard language in Windows and everything should work fine.

Go to the section for ***International Users*** for instructions on changing the keyboard.

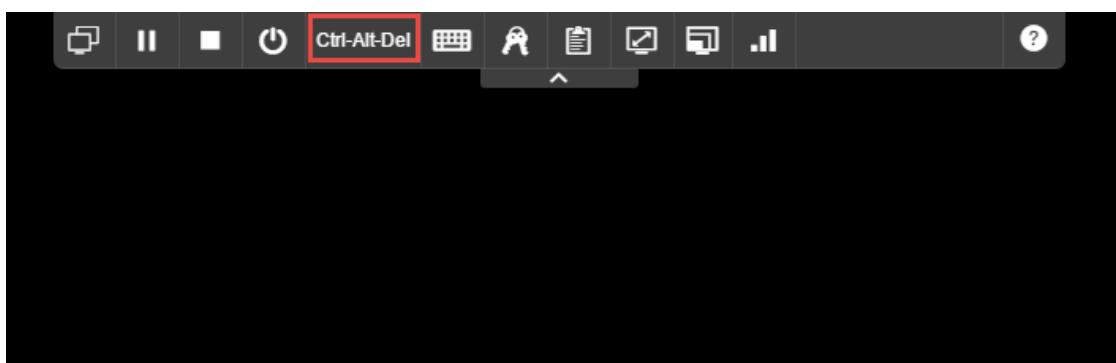
1. Click the large monitor icon to connect with the HTML 5 client.



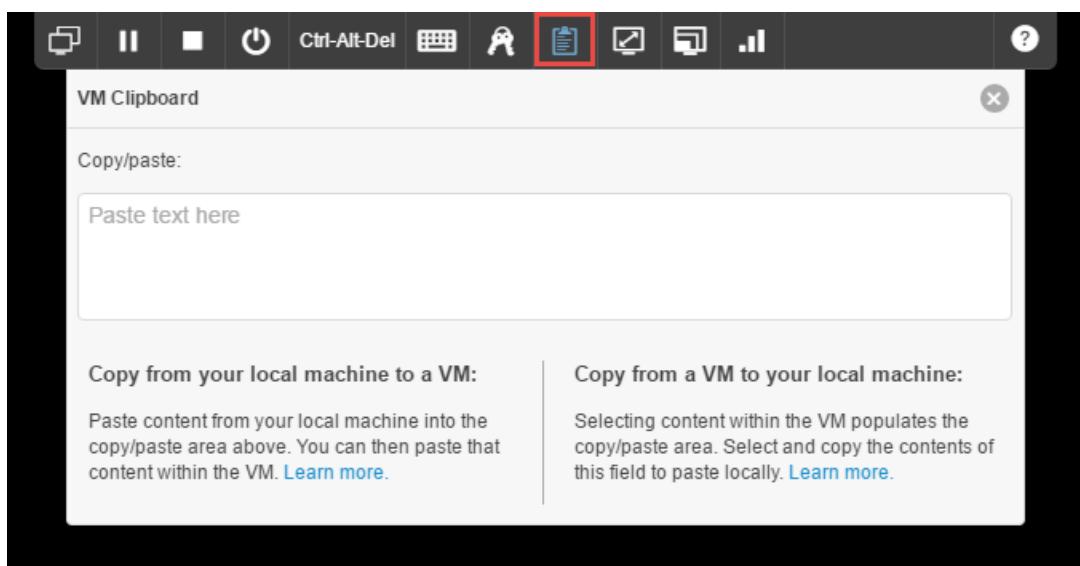
2. If HTML does not work try direct RDP. Inform your instructor if you do this, because some actions will not work as shown in the book.



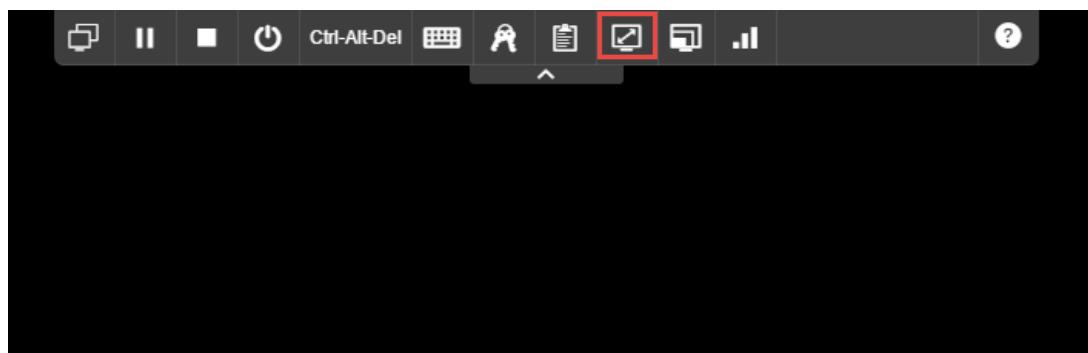
3. Use the **Ctrl-Alt-Del** button on the tool bar to send a Ctrl-Alt-Del to the machine.



4. The clipboard icon will allow you to copy and paste text between your computer and your lab machine.

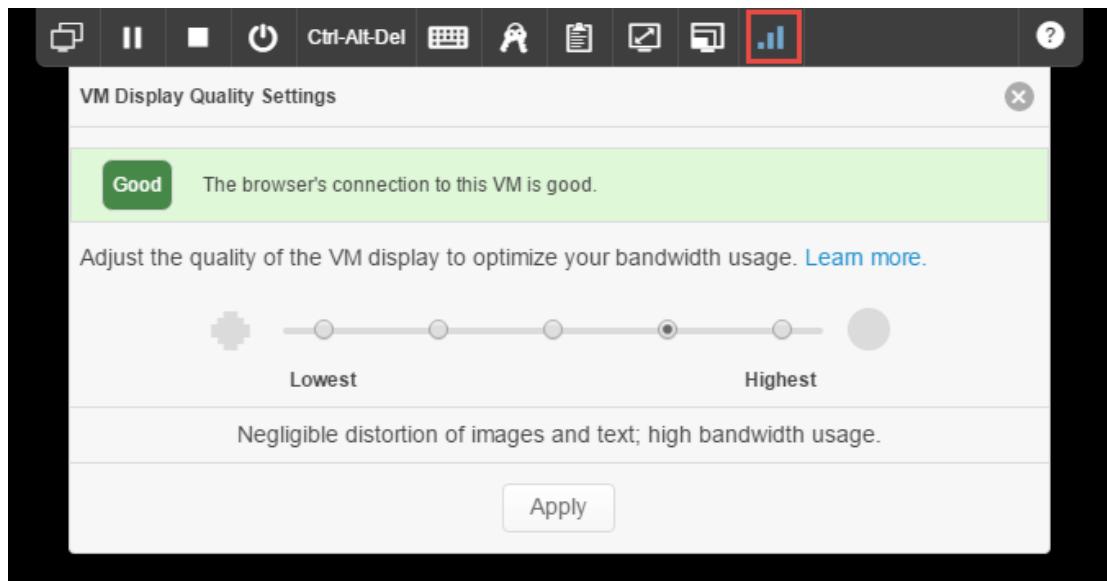


5. The full screen icon will resize your lab machine to match your computer's screen settings to avoid scrolling.





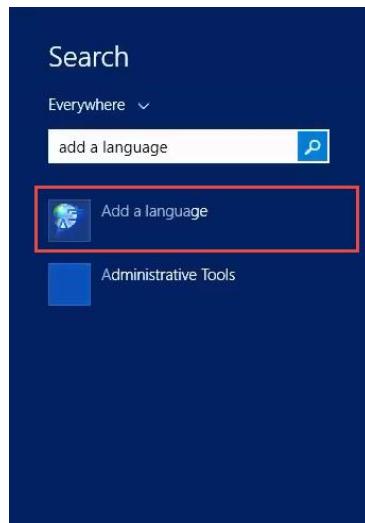
6. You may need to adjust your bandwidth setting on slower connections.



### International Users

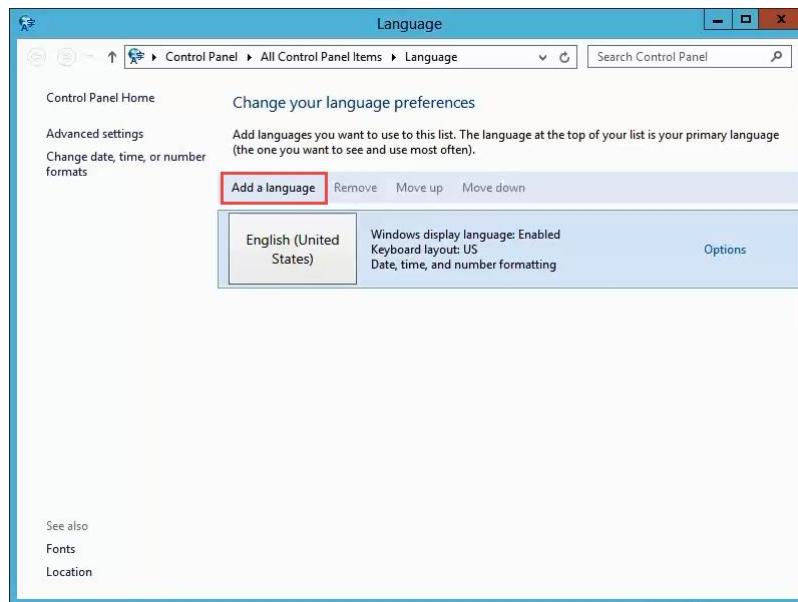
By default, the lab machines are configured to use a US English keyboard layout. If you use a machine from a country other than the US, you may experience odd behavior from your lab machines. The solution is to install the keyboard layout for your keyboard on our lab machines. Follow the process below to find and configure the correct keyboard layout for your keyboard.

7. From the *Start Menu* launch “Add a language.”

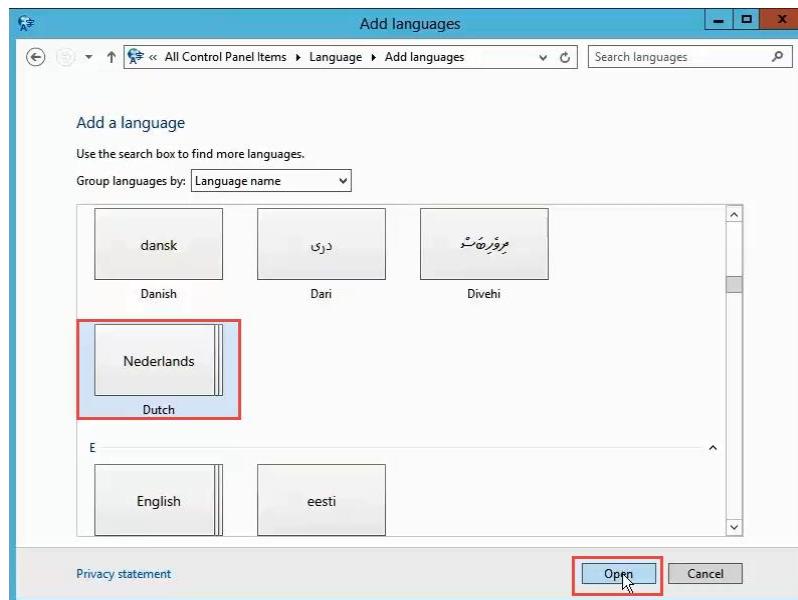




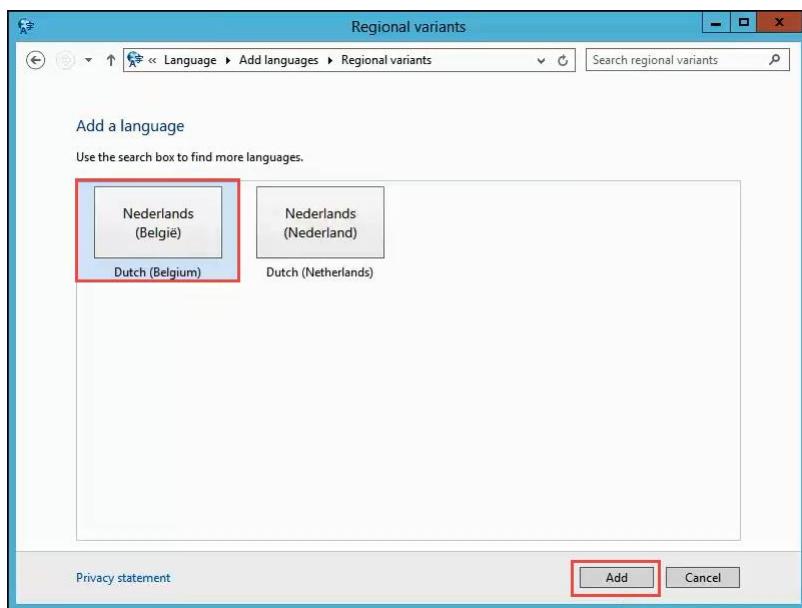
8. Click “Add a language.”



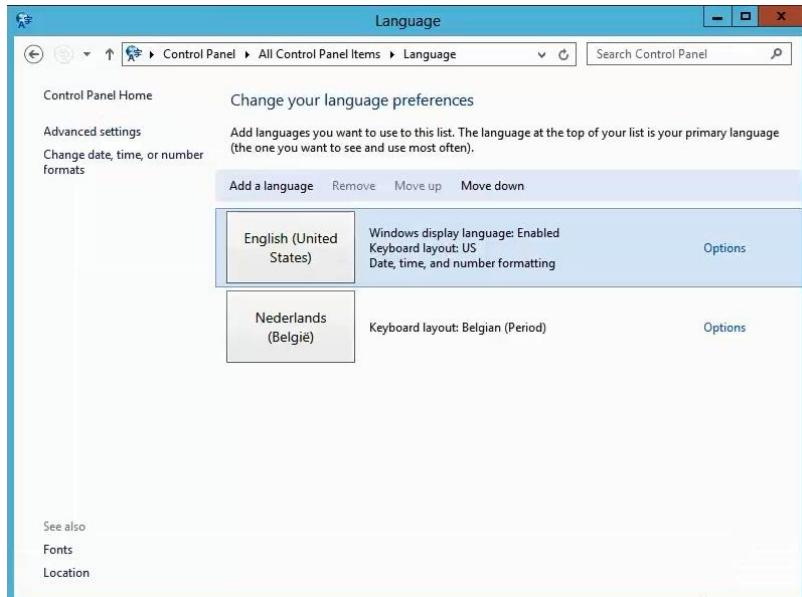
9. Select your language. Click Open.



10. Select your specific locality or dialect. Click Add.



11. With the option *English (United States)* selected, click the **Move down** button. This will make your language the default. Don't remove US English altogether as your instructor may need it if he/she connects to your machine.



**Note:** If you use an alternate keyboard layout (e.g. AZERTY, Dvorak) you can click options next to your language to install that. Otherwise, close the **Language** window.



12. In the system tray, click **ENG**, then choose your keyboard layout. You may switch back and forth between keyboard layouts. Your instructor may need to switch back to ENG to help you with exercises, occasionally.





## Scenario

CyberArk Demo Inc. (“the Customer”) has just purchased CyberArk’s **Privileged Account Security** (PAS). This document details the Customer’s specific requirements regarding the use of PAS in their environment:

Network	Server Name	IP Address
Windows <i>Domain: cyber-ark-demo.local</i>	DC01	10.0.0.2
	DomainMember	10.0.10.50
Unix / Linux	CentOS-target	10.0.0.20
	Load Balancer	10.0.0.5
	RADIUS	10.0.0.6
CyberArk PAS	Vault01A	10.0.10.1
	Comp01a	10.0.20.1
	Comp01b	10.0.21.1
	DR	10.0.14.1
	PSMP	10.0.1.16

You are required to install and implement the PAS solution to support the customer’s specific requirements. You will be given access to CyberArk’s documentation in order to complete your task. You may use the detailed installation guide provided by the trainer or the formal CyberArk installation guide. The Installation guide provided by the trainer should be used in the training environment only. In real-life deployments you must always use CyberArk formal documentation.

Unless specified otherwise, the default password for all privileged accounts and servers in the customer’s network is **Cyberark1**



## EPV Instructions

The Customer has purchased CyberArk's EPV solution to protect and manage their privileged accounts. End users are required to authenticate to CyberArk using two factor authentication.

**In the following sections you will be required to:**

1. Install a standalone Vault
2. Install 2 CPMs (one for managing Windows accounts and one for managing Unix and Oracle)
3. Install 2 PVWAs in a load balanced environment
4. Integrate CyberArk with the Customer's LDAP, SMTP and SIEM solutions
5. Implement 2FA based on LDAP, RADIUS, Windows and PKI methods
6. Vault and manage the Customer's privileged accounts



## Vault Installation

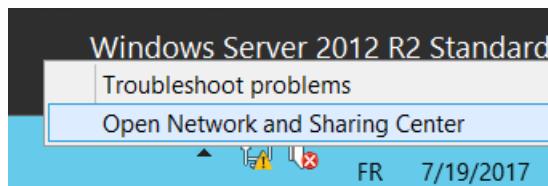
This exercise provides detailed instructions on installing the **CyberArk Digital Vault** server and client software and is broken down into three sections:

- Before Installation
- Vault Server Installation
- PrivateArk Client Installation

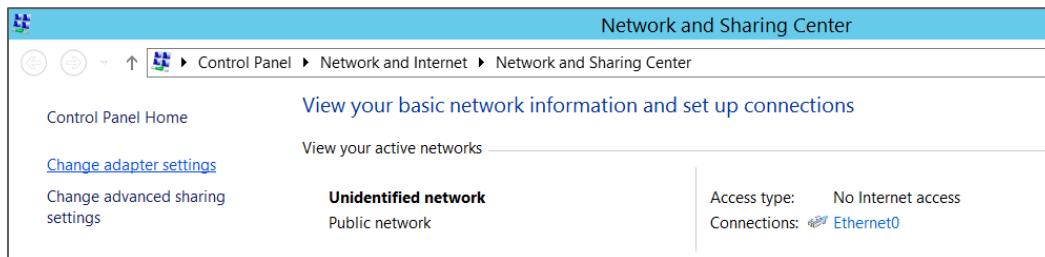
### Before Installation

**Objective:** A stand-alone **Vault** server only requires TCP/IPv4 for network communication. In preparation to install the **Vault** server software, we will first remove all networking protocols not required for **Vault** functionality

1. Connect to your **Vault01A** server as *Administrator*. Initially, this should not require a password.
2. Right click the **Network** icon in the system tray and select *Open Network and Sharing Center*.

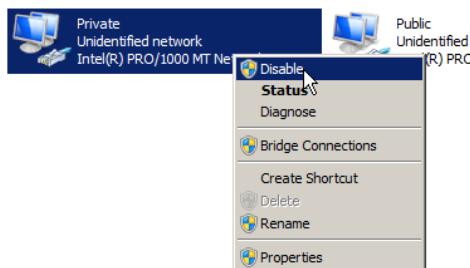


3. Click **Change adapter settings**.





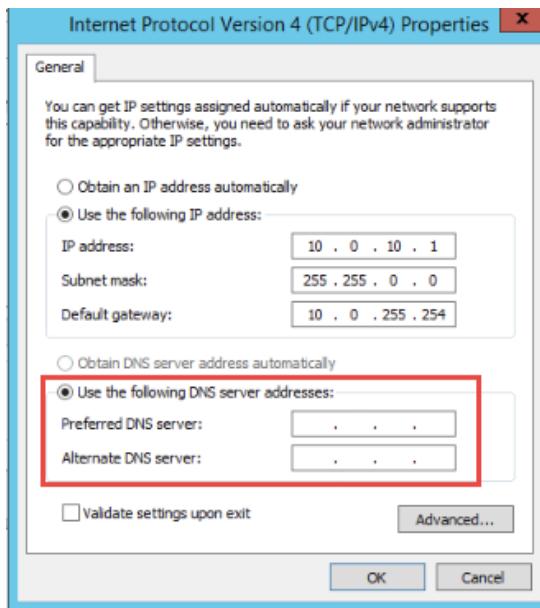
4. If there are two network adapters, right-click the one labeled **Private** and click **Disable**. This adapter isn't needed for this class and we should always disable unnecessary interfaces.



5. Double-click the **Public** network adapter.

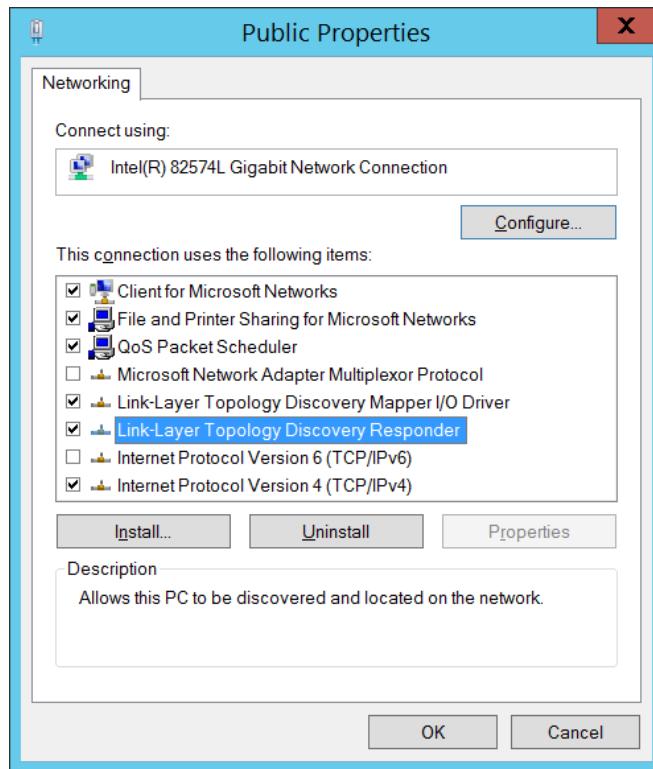


6. Select the **Properties** button and de-select the check box for Internet Protocol Version 6 (TCP/IPv6).
7. Select Internet Protocol Version 4 (TCP/IPv4) and select Properties. Confirm that no DNS server addresses are defined. Select OK and return to Public Properties.

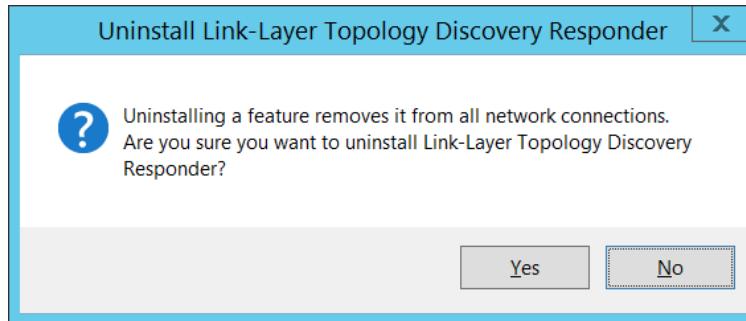




8. Select the *Link-Layer Topology Discovery Responder* and press the **Uninstall** button.



9. Press **Yes** to confirm.





10. Working from the bottom up, uninstall all of the remaining items, except for Internet Protocol Version 4 (TCP/IPv4). *Internet Protocol Version 6 (TCP/IPv6)* cannot be removed, so uncheck its box instead.

11. Uninstall the *Client for Microsoft Networks* **last**.

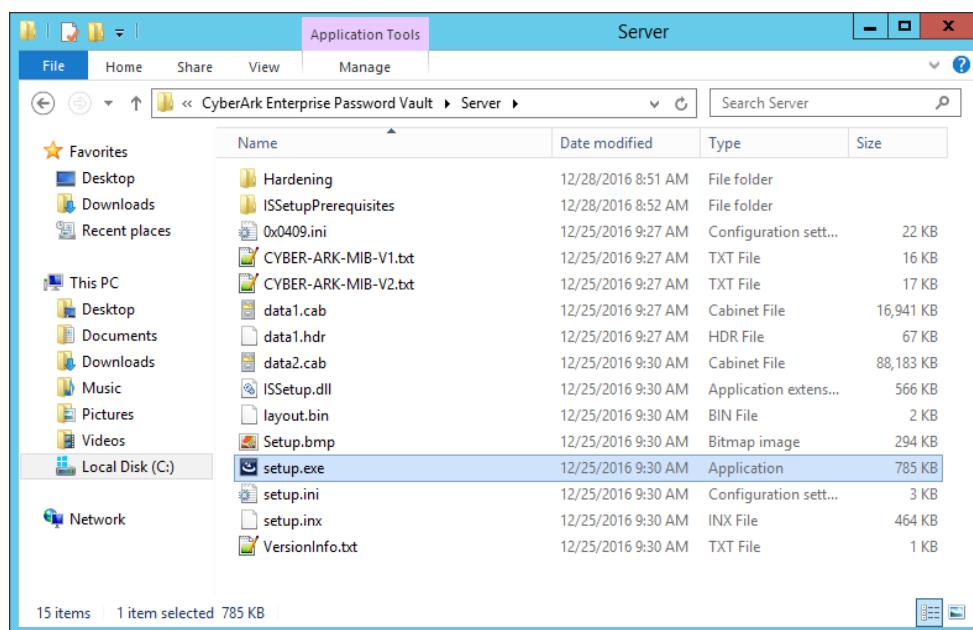
12. After uninstalling *Client for Microsoft Networks*, press **Yes** to allow the server to reboot.

## Vault Server Installation

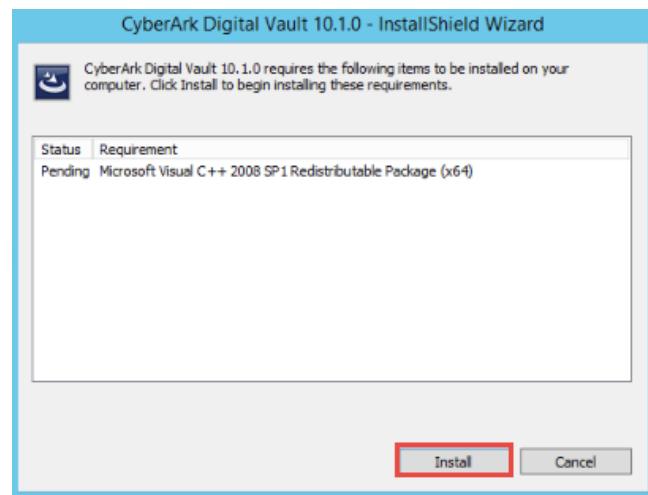
**Objective:** This exercise provides detailed, step-by-step instructions on installing the **CyberArk Digital Vault** server and **Private Ark Client** software. On the lab server, the following directories contain the required files to complete the installation:

- Installation files --> C:\CyberArk Installation Files
- License --> C:\CyberArk Installation Files\License
- Operator CD contents --> C:\PrivateArk\Keys

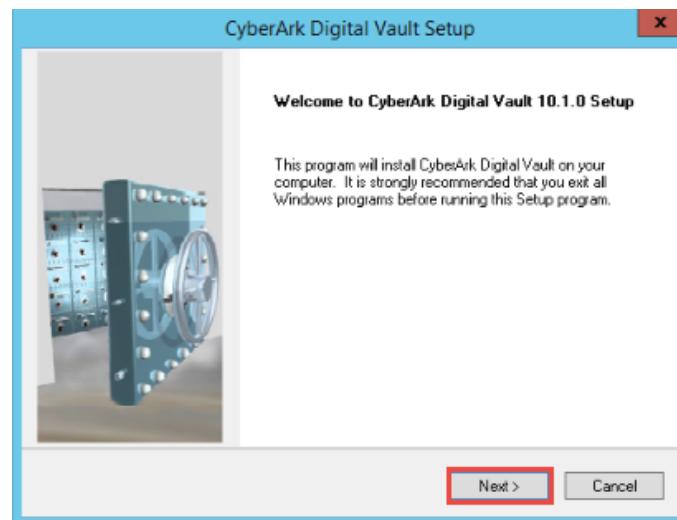
1. After the reboot, go to C:\CyberArk Installation Files\CyberArk Enterprise Password Vault\Server.
2. Double-click the **setup** icon.



3. The *CyberArk Digital Vault InstallShield Wizard* will open with a message regarding C++ SP1 Redistributable Package. Click **Install**.



4. Press **Next** to continue.

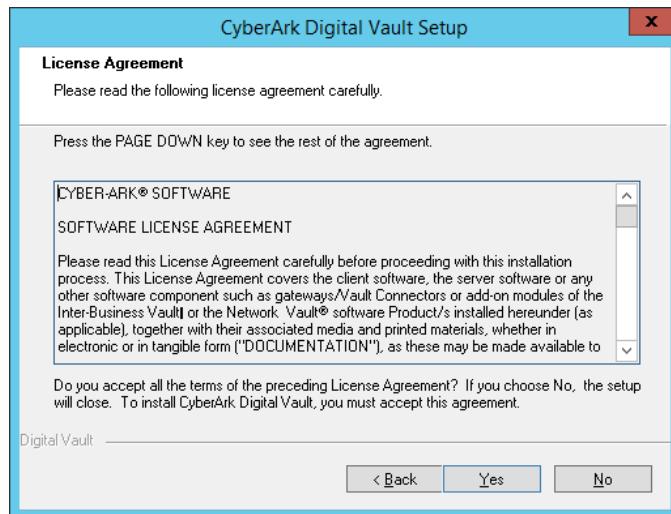




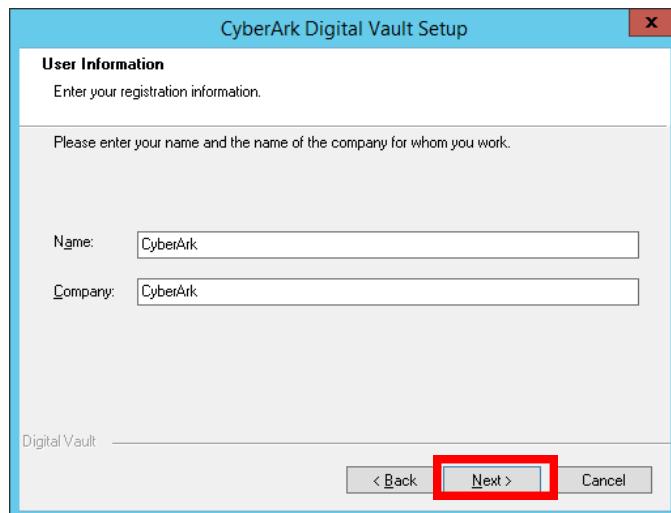
CYBERARK®

## Privileged Account Security Install & Configure, v10.x

5. Press **Yes** to accept the license agreement.

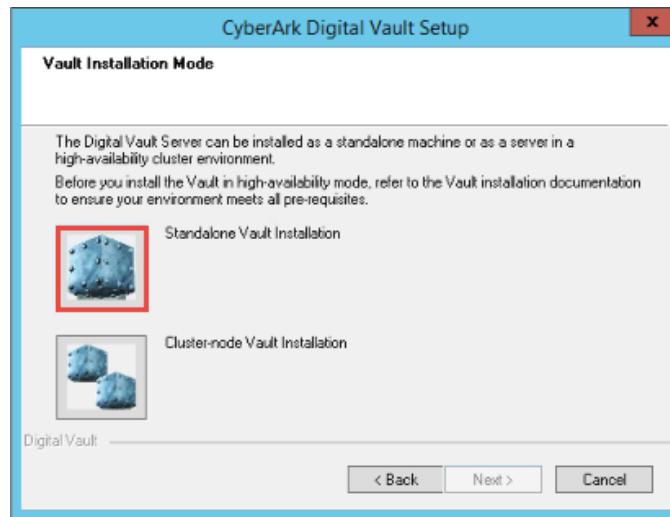


6. Enter *CyberArk* in the **Name** and **Company** fields.

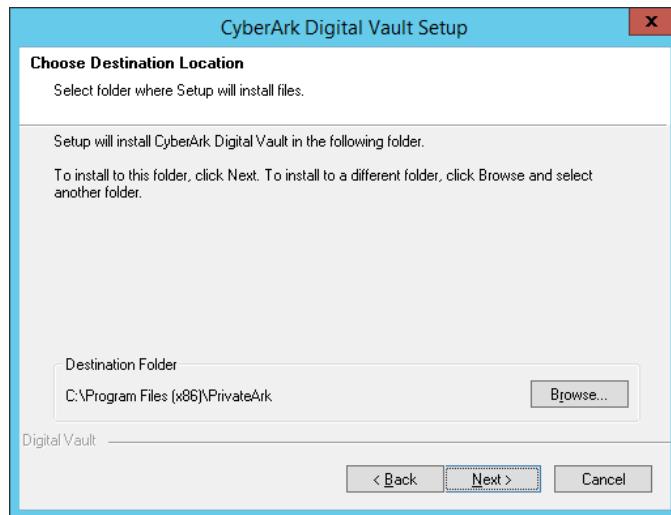




7. Press the **Standalone Vault Installation** button to install the **Vault** on a standard, stand-alone server.

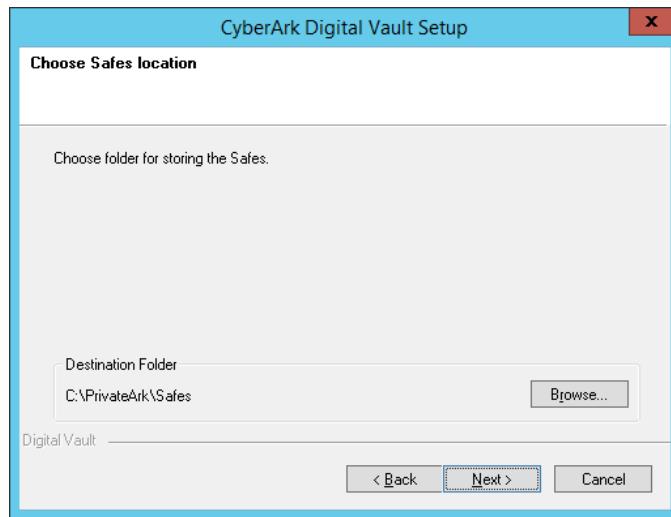


8. Press **Next** to accept the default installation location.

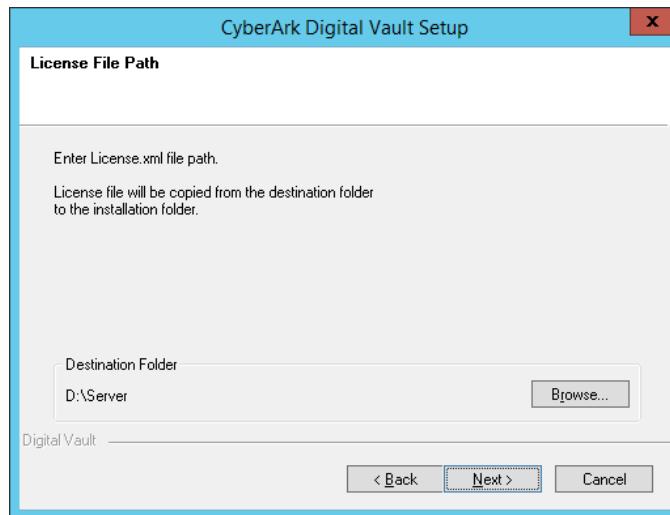




9. Press **Next** to accept the default **Safes** location, which is where the password data will be stored.

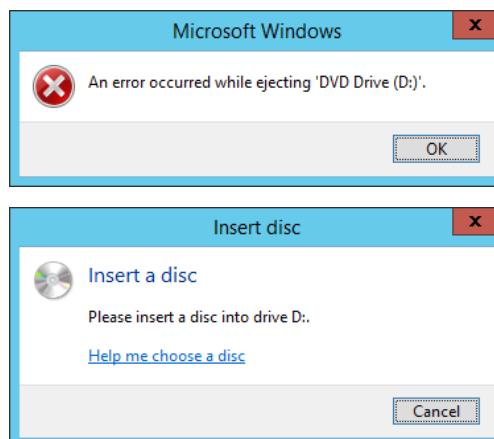


10. Press **Browse** to select a custom license file path.

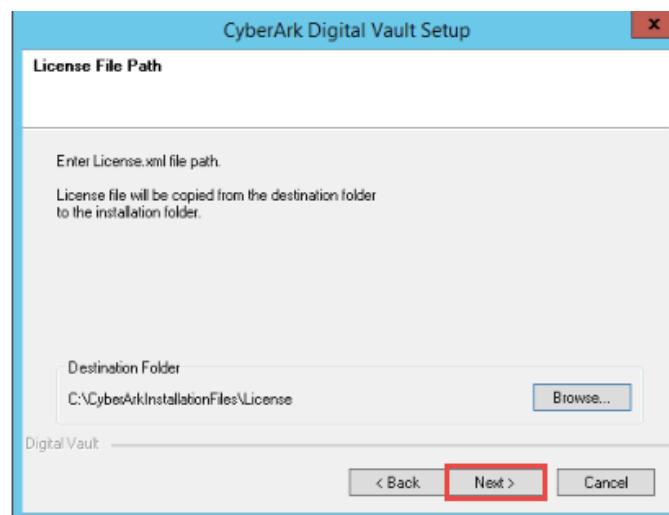
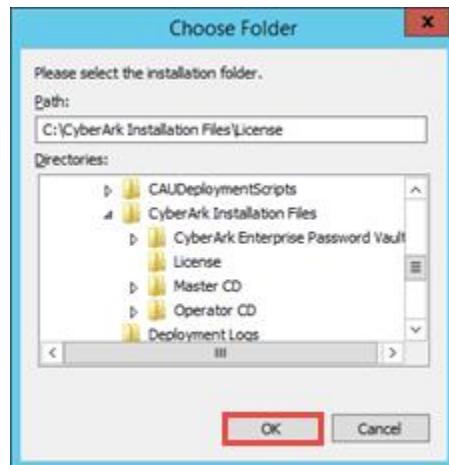


11. Click **OK** and then **Cancel** on the **Insert disc** pop-up to browse to the correct location.

**Note:** Because the software is configured to look for the license file on the DVD drive by default, you will probably receive an error message regarding the *D:* drive.

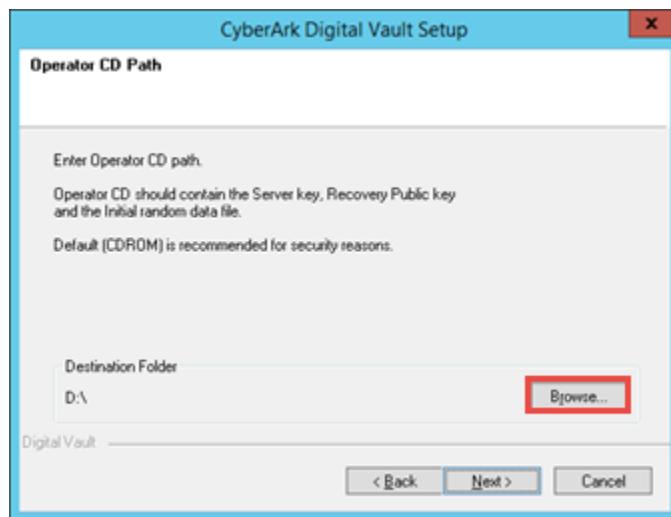


12. In the **Choose folder** pop-up, browse to *C:\CyberArk Installation Files\License*, press **OK** and then press **Next**.

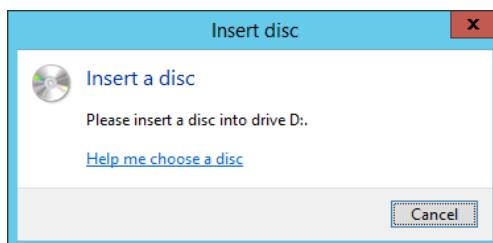
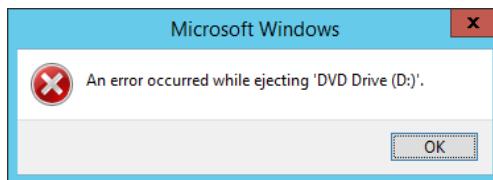




13. The same procedure is required for the Operator CD. Press **Browse** to select a custom Operator CD path.



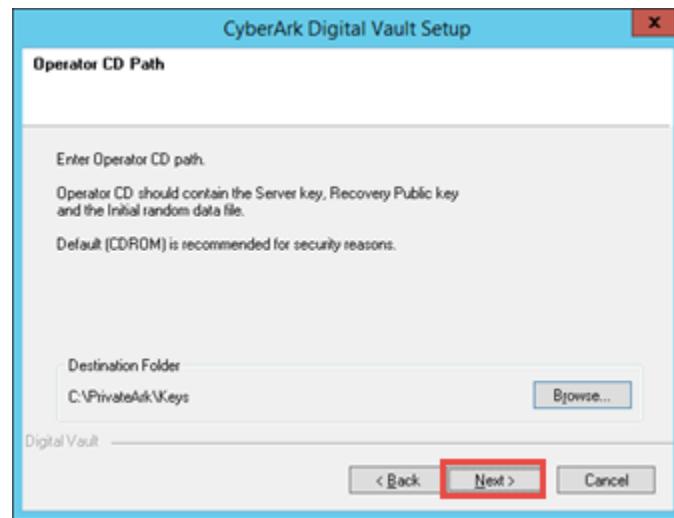
14. You will receive the same error message regarding the *D:* drive. Click **OK** and then **Cancel** on the **Insert disc** pop-up to browse to the correct location.



15. Browse to the *C:\PrivateArk\Keys* directory and click **OK** and then and press **Next**.

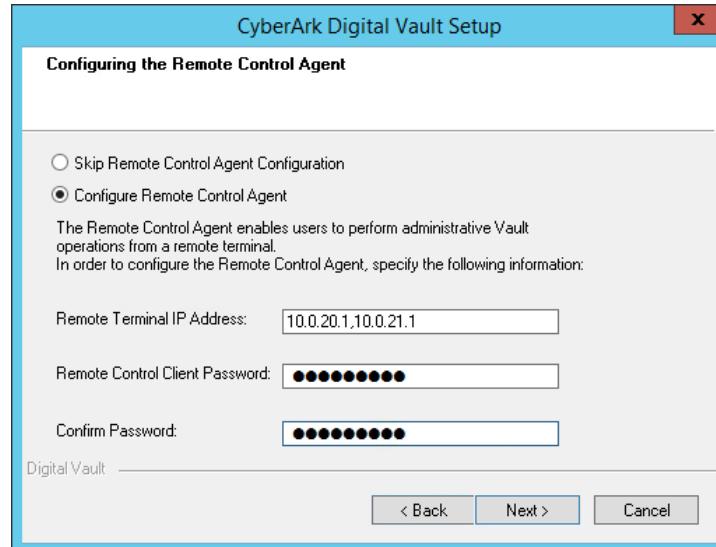
**Note:**

The contents of the Operator CD have already been copied here. These files must be accessible to the **PrivateArk Server** service in order to start the **Vault**. A Hardware Security Module (HSM) is the recommended method for key storage. If these files are to be stored on the file system, it is highly recommended that the keys and encrypted files be stored on separate media. Also, the keys should be stored in a folder on an NTFS drive which is protected by OS Access Control.



**Note:** If the **Vault** is installed on a virtual machine, storing Operator CD files on the file system is not recommended due to the lack of physical security.

16. Enter the IP address(es) of your **Component** servers in the **Remote Terminal IP Address** field – **10.0.20.1,10.0.21.1** and **Cyberark1** – in the password fields and press **Next**.



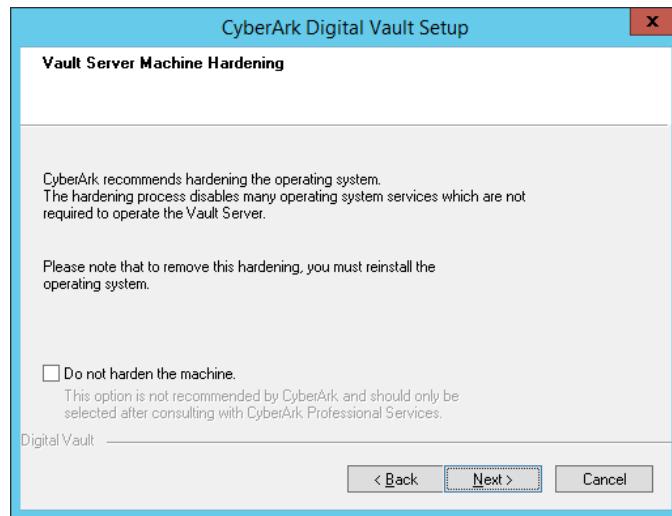
**NOTE:** The **Remote Control Agent** allows you to perform administrative functions on the **Vault** server from the specified remote machine. This is useful when you do not have console access to the **Vault** server. It is also required if you would like to enable the **Vault** to send SNMP traps.



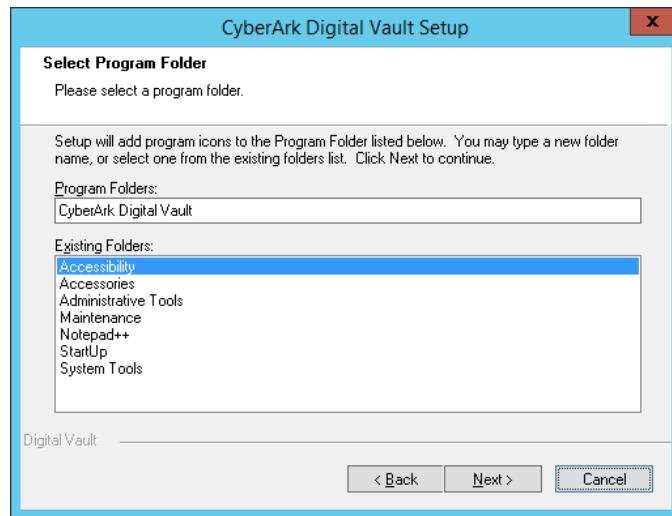
CYBERARK®

## Privileged Account Security Install & Configure, v10.x

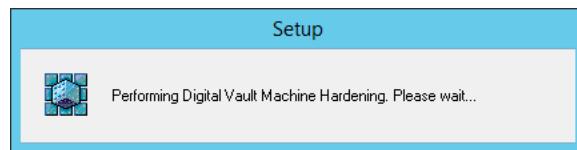
17. Press **Next** to allow **CyberArk** to harden the CyberArk Digital Vault machine.



18. Press **Next** to accept the default *Program Folder*.

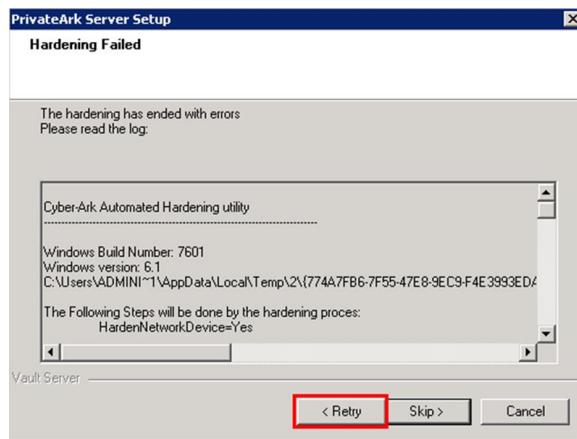


The **Performing Vault Server Machine Hardening** window will appear. This will take a few minutes.



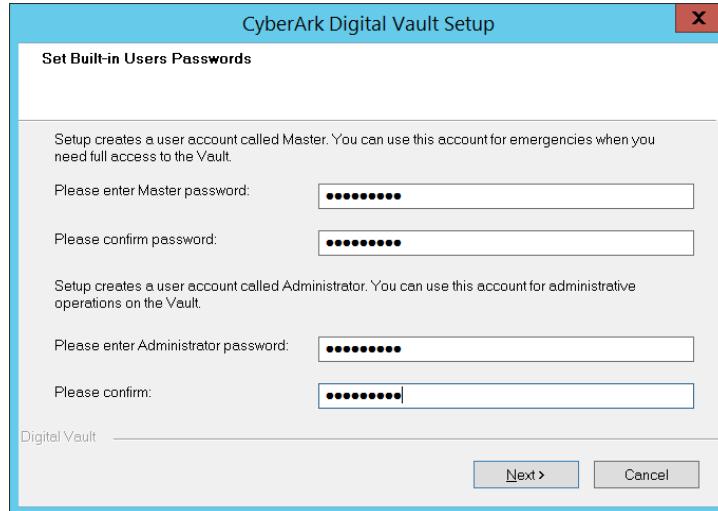


19. In the **SkyTap** environment, you may receive a message that the hardening failed. If so, press the **Retry** button. In training, a failure is usually caused by a timeout in stopping services because we are using virtual machines with limited resources.



20. Enter *Cyberark1* in all of the password fields and press **Next**.

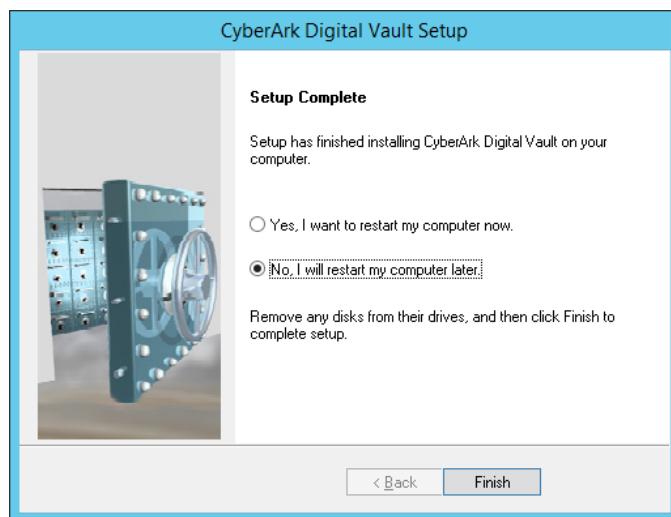
**Note:** We will use the password '*Cyberark1*' everywhere in the training. It is not recommended that you do this in a production environment.





**Reminder:** The **Master** user should only be used in emergency situations, has all **Vault** Authorizations, and access to all data within the **Vault**. The Master private key must be accessible to the **Vault** server for a user to login to the **Vault** using the Master password. The Master password and CD should be stored in a physical Safe with limited access. The **Administrator** user has all **Vault** authorizations but no access to data by default.

21. Choose *No, I will restart my computer later* and press **Finish**.

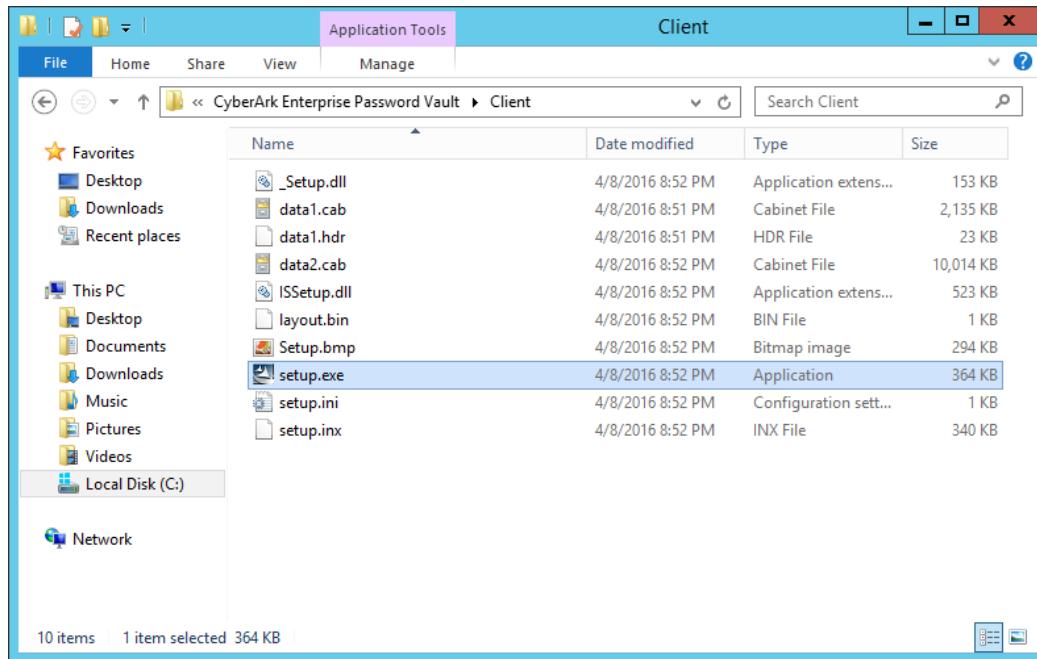




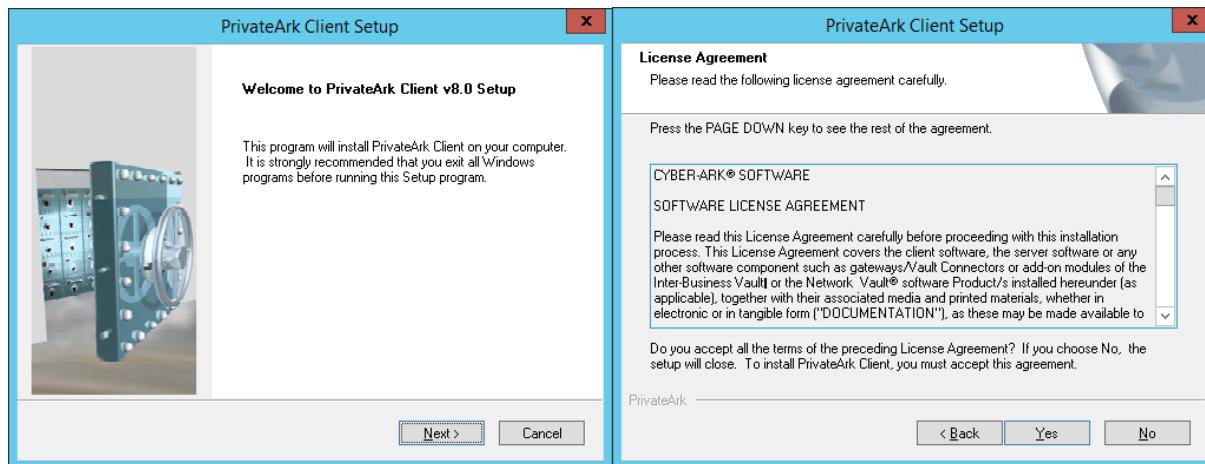
## PrivateArk Client Installation

Next, we will install the **PrivateArk Client** on the **Vault** server.

1. Go to *C:\CyberArk Install Files\CyberArk Enterprise Password Vault\Client* and double click *setup.exe*.



2. Accept the default options in each of the next six windows. If the **User Information** window is blank, enter **Name: CyberArk** and **Company: CyberArk**.





PrivateArk Client Setup

User Information  
Enter your registration information.

Please enter your name and the name of the company for whom you work.

Name: CyberArk

Company: CyberArk

PrivateArk

< Back Next > Cancel

PrivateArk Client Setup

Choose Destination Location  
Select folder where Setup will install files.

Setup will install PrivateArk Client in the following folder.  
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder: C:\Program Files (x86)\PrivateArk

PrivateArk

< Back Next > Cancel

PrivateArk Client Setup

Select Client setup type  
Click the type of Setup you prefer, then click Next.

Typical Program will be installed with the most common options. Recommended for most users.

Custom You may choose the options you want to install. Recommended for advanced users.

PrivateArk

< Back Next > Cancel

PrivateArk Client Setup

Select Program Folder  
Please select a program folder.

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing folders list. Click Next to continue.

Program Folders: PrivateArk

Existing Folders:  
Accessibility  
Accessories  
Administrative Tools  
Maintenance  
Notepad++  
PrivateArk  
StartUp  
System Tools

PrivateArk

< Back Next > Cancel

3. Press **OK** to define your first connection to the **PrivateArk Vault**. This will create a shortcut to your **Vault** within the **PrivateArk Client**.



4. Enter the following information:

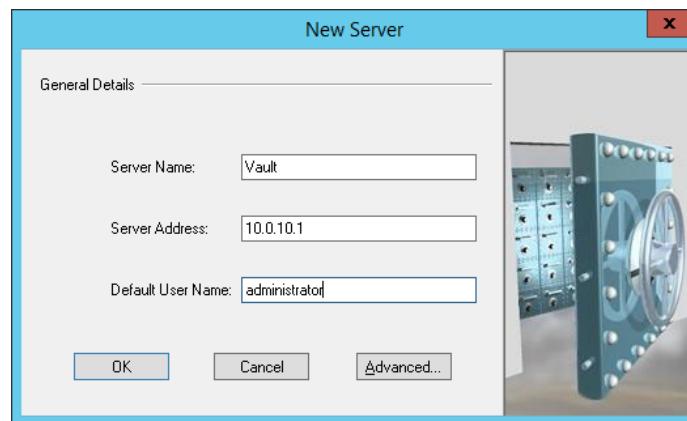
**Server Name**      *Vault*

**Server Address**      *10.0.10.1*

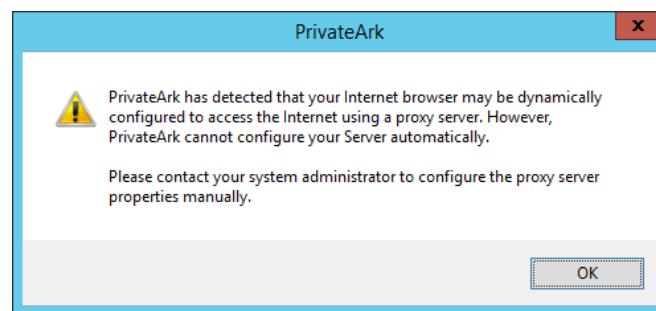
**Default User Name** *administrator or leave blank (leaving blank means the client will remember the last logged on user)*



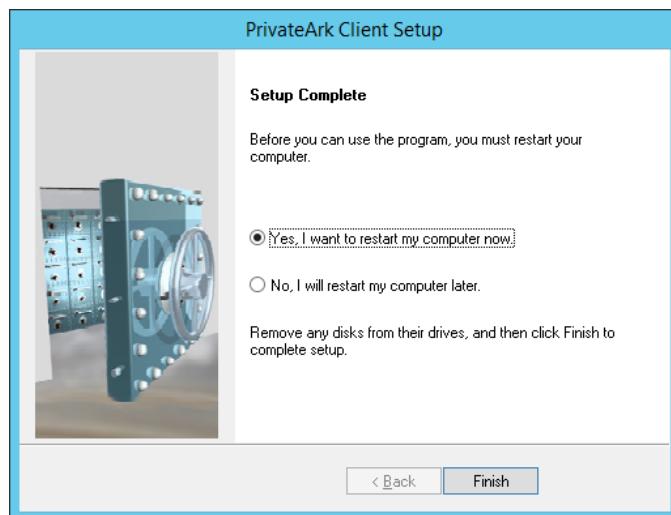
5. Press **OK**.



6. You **may** receive a message regarding your Internet proxy. This is normal for our lab environment. Press **OK** to acknowledge that message.



7. Select *Yes, I want to restart my computer now* and press **Finish**.



8. Login to the **Vault01A** server. The vault hardening process prevents auto-logon so you will be required to enter the Administrator credentials.
9. Double-click the **PrivateArk Server** shortcut on the desktop to open the Server Central Administration utility. Confirm there are no errors, and “ITAFW001I Firewall is open for client communication” message appears.
10. Open Windows Services and check that the following services have been installed and started.
  - a. PrivateArk Database
  - b. PrivateArk Remote Control Agent
  - c. PrivateArk Server
  - d. CyberArk Logic Container
  - e. Cyber-Ark Event Notification Engine.

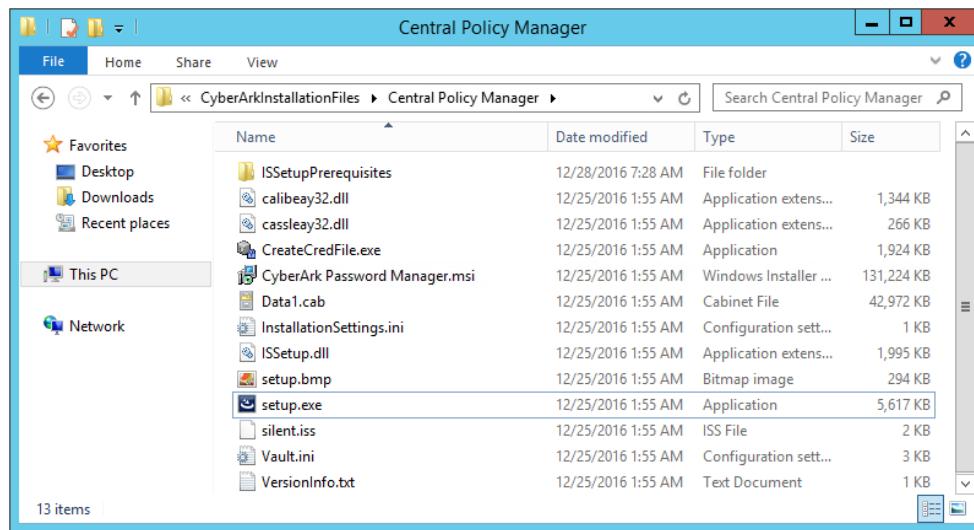
**Note:** The **CyberArk Enterprise Password Vault** is now installed. We are ready to begin installing the CyberArk components: the **Central Policy Manager – or CPM** – and the **Password Vault Web Access – or PVWA**.



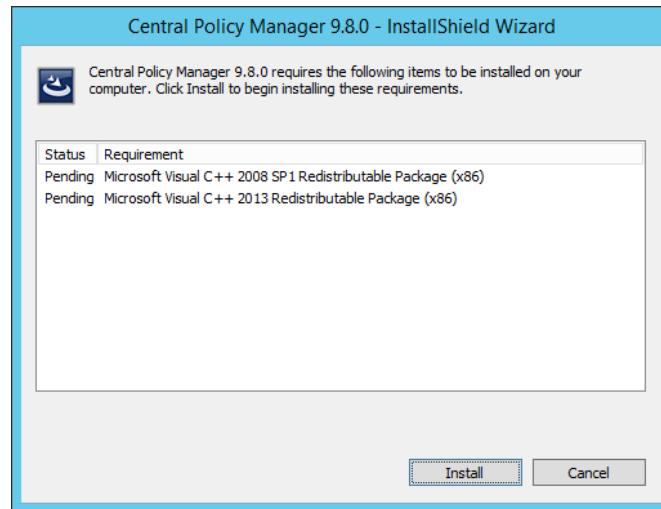
## Install CPM (distributed)

### Install 1<sup>st</sup> CPM

1. Login to your **Component A** (Comp01a) server as administrator.
2. Go to **C:\CyberArkInstallationFiles\Central Policy Manager\** and double-click the **setup.exe** application.



3. Press **Install** to install the required Windows components. This will take a few minutes.



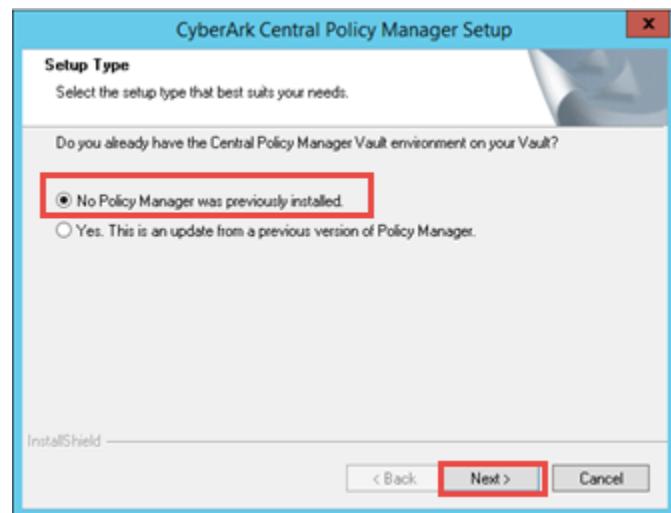


4. Accept the default options on the next four windows, including your company name (e.g. CyberArk) on the **Customer Information** page.

The image displays four windows from the CyberArk Central Policy Manager Setup wizard:

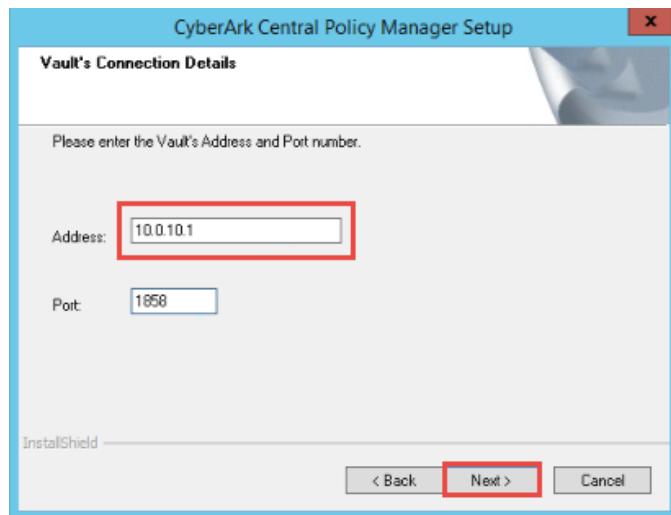
- Welcome to the InstallShield Wizard for CyberArk Central Policy Manager:** Shows a graphic of a vault door and the text: "Welcome to the CyberArk Central Policy Manager v10.1.0 Setup program. This program will install CyberArk Central Policy Manager on your computer". Buttons: < Back, Next >, Cancel.
- License Agreement:** Displays the "SOFTWARE LICENSE AGREEMENT" with a scroll icon. It includes a note: "Please read the following license agreement carefully. Press the PAGE DOWN key to see the rest of the agreement." A checkbox asks: "Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install CyberArk Central Policy Manager, you must accept this agreement." Buttons: < Back, Yes, No.
- Customer Information:** Requests "User Name" (CyberArk) and "Company Name" (CyberArk). Buttons: < Back, Next >, Cancel.
- Choose Destination Location:** Asks to "Select folder where setup will install files" (C:\Program Files (x86)\CyberArk\). A "Browse..." button is available. Buttons: < Back, Next >, Cancel.

5. Accept the default option, “**No Policy Manager was previously installed**” and press **Next**.



**Note:** This question relates to installing **CPM software** using an existing licensed CPM user, not installing an additional CPM that will consume a new license.

6. Enter the IP Address of your **Vault** (i.e., **10.0.10.1**) and press **Next**.

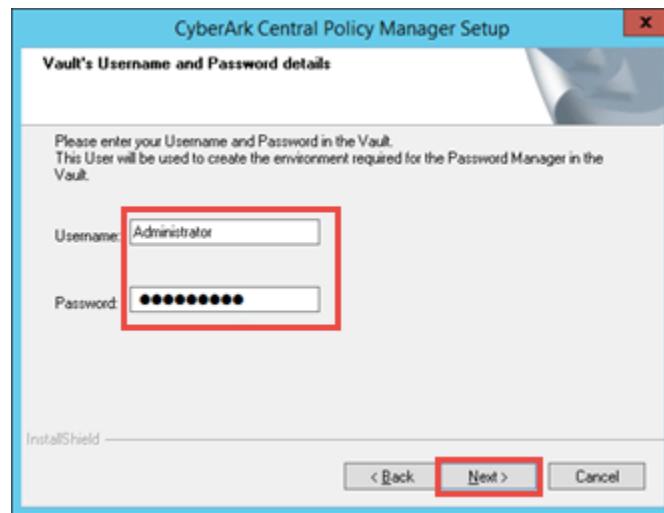


7. Enter **Administrator** as the *Username* and **Cyberark1** for the *Password* and press **Next**

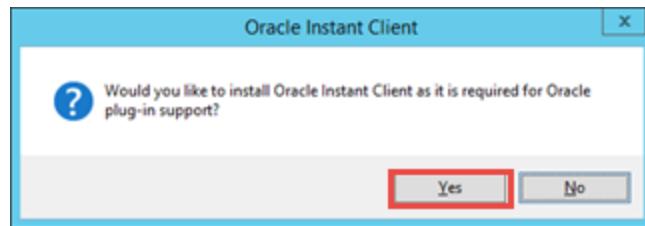


CYBERARK®

## Privileged Account Security Install & Configure, v10.x



8. Press **Yes** to install the *Oracle Instant Client*



9. Press the **Finish** button





10. Immediately following the CPM installation, review the *CPMInstall.log* file created in "C:\Users\Administrator\AppData\Local\Temp\1". To access this directory, in the File Explorer address window, type %appdata%, then change from Roaming to Local and navigate to the \Temp\1 directory. This file contains a list of all the activities performed when the CPM environment in the Vault is created during the installation procedure.

**Note:** The installer has created a CPM user in the vault called *PasswordManager*. We will rename the CPM user later, after we add second CPM.

11. Next, we need to add exceptions to Microsoft Windows Data Execution Prevention utility for the CyberArk utility PMTerminal.exe and Plink.exe. This is necessary to enable the CPM to manage target systems such as Unix/Linux.

12. Right click the Start Menu and select the Run command.

13. Type sysdm.cpl and select Ok.

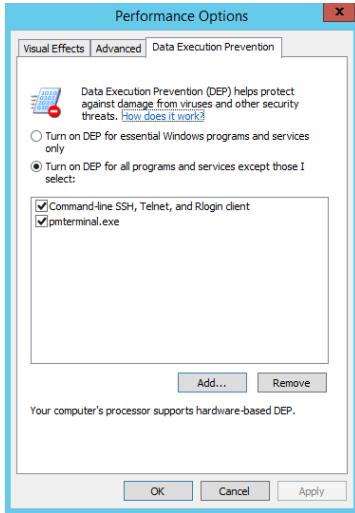
14. Select the Advanced tab, and click the Performance, Settings button.

15. Select the Data Execution Prevention tab and click the Add... button.

16. Navigate in the dialog to "C:\Program Files (x86)\CyberArk\Password Manager\bin"

17. Select Plink.exe and click the Open button

18. Click Add... again, select PMTerminal.exe and click the Open button.



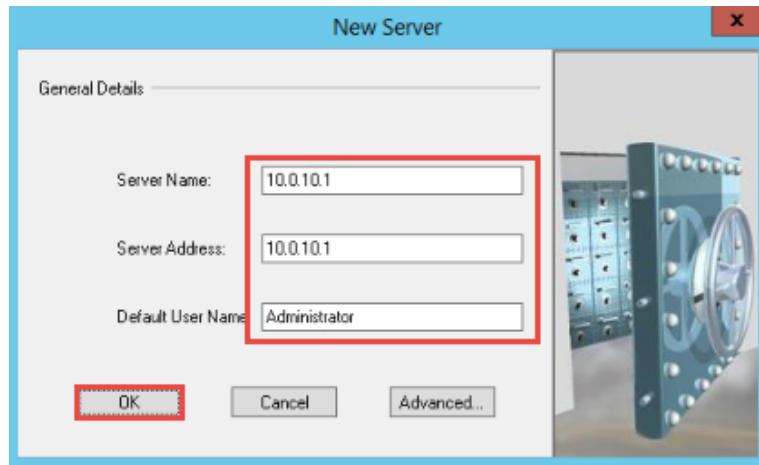
19. Click Ok.



**Note:** It is not recommended to completely disable Microsoft's Data Execution Prevention (DEP) security feature. Disabling DEP may require an exception to security policy at a customer site and also requires a restart of the Windows Server.

### Install the PrivateArk Client on the Component server

**Objective:** In this section, you will repeat the steps for installing the **PrivateArk Client**, this time on the Comp01a server, though with one small change. This time, when creating the first connection to the **Vault** server, put the Vault IP address (i.e., **10.0.10.1**) in the *Server Name* field. This will later allow you to connect to the **PrivateArk Client** via the **PSM**.



### Following the CPM Installation

After the server restarts, login to the Comp01a server and review the following.

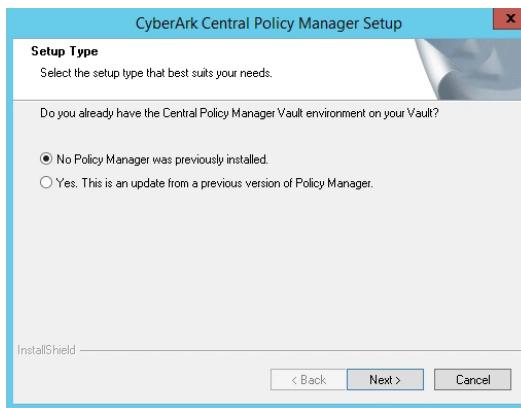
1. Navigate to "C:\Program Files (x86)\CyberArk\Password Manager\Logs". Check the *pm.log* and *pm\_error.log* file for errors.
2. Check the **CPM** services are installed and running.
  - a. CyberArk Password Manager Service.
  - b. CyberArk Central Policy Manager Scanner.

### Install 2<sup>nd</sup> CPM

**Objective:** You will now repeat the steps in [Install 1<sup>st</sup> CPM](#), but pay very careful attention to the instructions. There are slight differences in the installation on the second component server.

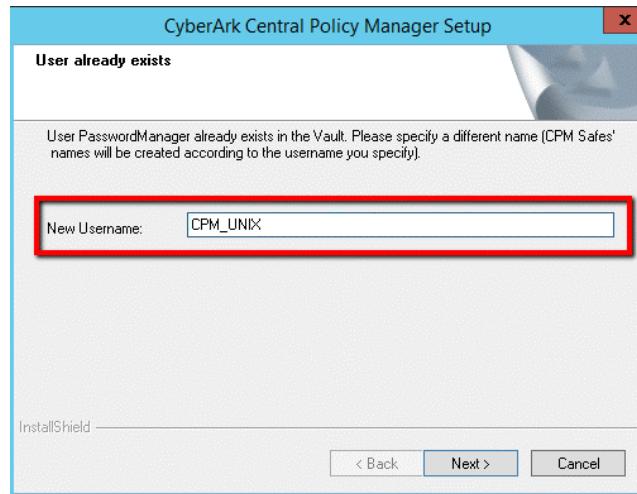


1. Log into your **Component B (Comp01b)** server as *Administrator* and launch *setup.exe* for the **CPM**. Select the default “**No Policy Manager was previously installed**” when asked if a CPM environment exists.



**Note:** This question relates to installing **CPM software** using an existing licensed CPM user, not installing an additional CPM that will consume a new license.

2. This time, the installer will ask you to specify a username for this CPM (Since another CPM has already been installed on this Vault). Enter **CPM\_UNIX** in the *New Username* field, then complete the installation.



**Reminder:** When the installer completes, don't forget to configure exceptions for PMTerminal.exe and Plink.exe in the Microsoft's Data Execution Prevention (DEP) security feature.

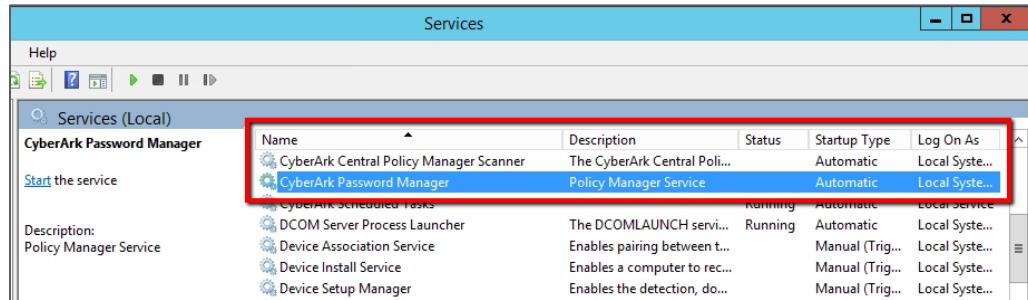


## Install the PrivateArk Client on the Comp01b server

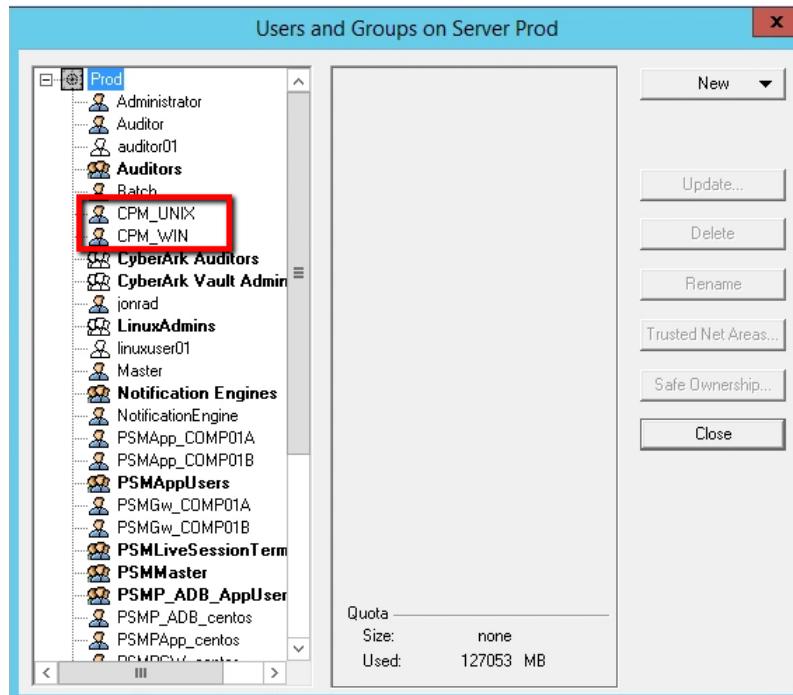
**Objective:** In this section, you will repeat the steps on page 39 to [Install the PrivateArk Client](#), this time on the Comp01b server.

### Rename 1<sup>st</sup> CPM

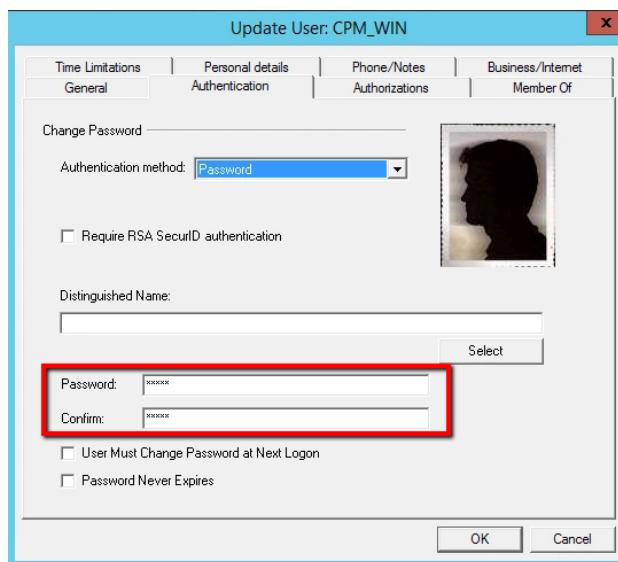
1. Log on to the **Comp01A** Server, and stop both CPM Services.



2. Launch the **PrivateArk Client** and log in as **Administrator**. In **Tools > Users and Groups**, find the **PasswordManager** user and press **F2** to rename. Rename the user as **CPM\_WIN**.



3. Click **Update** and reset the user's password to **Cyberark1** on the **Authentication** tab.



4. Rename the following safes in the **PrivateArk Client**:

<i>Old Name</i>	<i>New Name</i>
<i>PasswordManager</i>	<b>CPM_WIN</b>
<i>PasswordManager_ADIinternal</i>	<b>CPM_WIN_ADIinternal</b>
<i>PasswordManager_info</i>	<b>CPM_WIN_info</b>
<i>PasswordManager_workspace</i>	<b>CPM_WIN_workspace</b>

**Note:** Open (**SHIFT+ENTER**) each safe individually and then press **F2** on the *Safe Icon* to rename. This is easier if you switch from **Icon** view to **Details** view. **DO NOT** rename *PasswordManager\_Pending* or *PasswordManagerShared*.

5. Logoff the **PrivateArk Client**.
6. Open a command prompt and navigate to **C:\Program Files (x86)\CyberArk\Password Manager\Vault**. Run the following command:  
**CreateCredFile.exe user.ini**
7. Enter the *Vault Username* and *Password* for the new CPM user at the prompts. Press **Enter** to accept the default for the remaining prompts.

<i>Username:</i>	<b>CPM_WIN</b>
<i>Password:</i>	<b>Cyberark1</b>



```
C:\>Program Files (<x86>)\CyberArk\Password Manager\Vault>CreateCredFile.exe user.ini
Vault Username [PasswordManager] ==> CPM_WIN
Vault Password <will be encrypted in credential file> ==> *****
Disable wait for DR synchronization before allowing password change <yes/no> [No] ==>
External Authentication Facility <LDAP/Radius/No> [No] ==>
Restrict to Application Type [optional] ==>
Restrict to Executable Path [optional] ==>
Restrict to current machine IP <yes/no> [No] ==>
Restrict to current machine hostname <yes/no> [No] ==>
Restrict to OS User name [optional] ==>
Display Restrictions in output file <yes/no> [No] ==>
Use Operating System Protected Storage for credentials file secret <Machine/User/No> [No] ==>
Command ended successfully

C:\>Program Files (<x86>)\CyberArk\Password Manager\Vault>
```

8. Start the **CPM** Services. Check the *pm.log* and *pm\_error.log* files to verify they start successfully and without errors. The *pm.log* file should begin with log entry “CACPM117I Starting Password Manager 10.1.0 (10.1.0.12)”, followed by a listing of each active platform, e.g., “CACPM670I Effective policy updated. ID: 2, Policy ID: 2, Platform Name: Unix via SSH”



## Install PVWA (load balanced)

**Objective:** Install the PVWA on the **Component** servers in preparation for configuring them in a load-balanced environment. It is important to perform these tasks ***in the order they are presented here.***

In this chapter, you will perform the tasks in the following order:

- **PVWA Pre-requisites**
- **Use HTTP over SSL (PVWA)**
- **Install 1st PVWA**
- **Install 2nd PVWA**
- **Hardening the CyberArk CPM and PVWA Servers**
- **Configure the External Load Balancer for the PVWA servers**

### PVWA Pre-requisites

1. Complete the following pre-requisite tasks on both Comp01a and Comp01b servers. Prior to installing PVWA you must first install the Web Server Role (IIS) on both of your **Component** servers. In the **Server Manager**, select **Add Roles and features** and add the **Web Server (IIS)** role with the following **Role Services**:

Service	Features
Common HTTP:	All features
Health and Diagnostics:	HTTP Logging Request Monitor
Security:	Request Filtering Basic Authentication Windows Authentication
Application Development:	.NET Extensibility 4.5 ASP ASP.NET 4.5 ISAPI extensions ISAPI filter
Management Tools:	All features

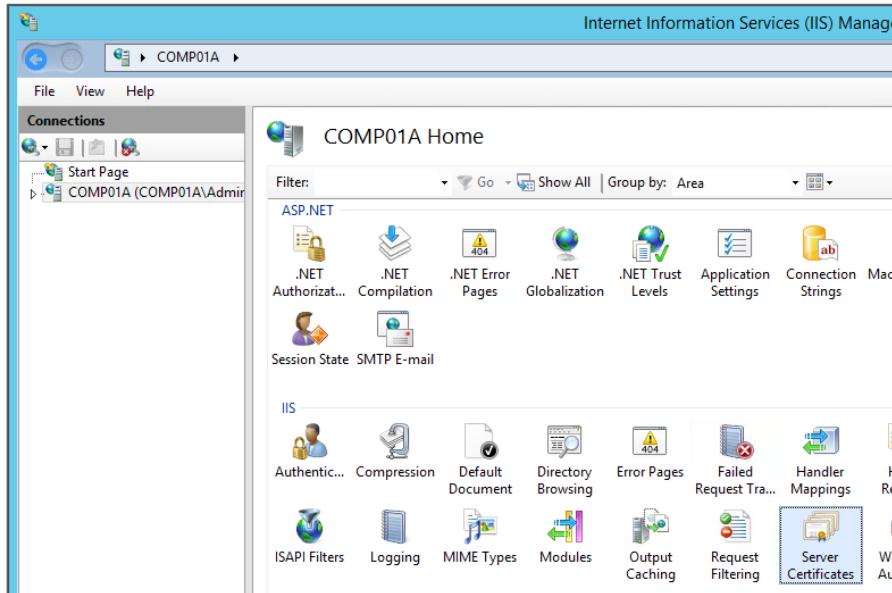


## Use HTTP over SSL (PVWA)

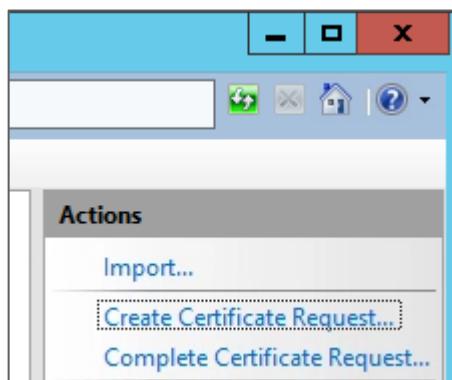
**Objective:** In this section we will configure IIS to require connections over SSL by issuing a certificate for the component servers. This part is also a prerequisite for later authentication sections.

**Must be completed on Comp01a and Comp01b servers.**

1. Begin by launching **IIS Manager (INETMGR)** on your **Component** server.
2. On the Connections column, click on the server name and double-click the **Server Certificates** icon.

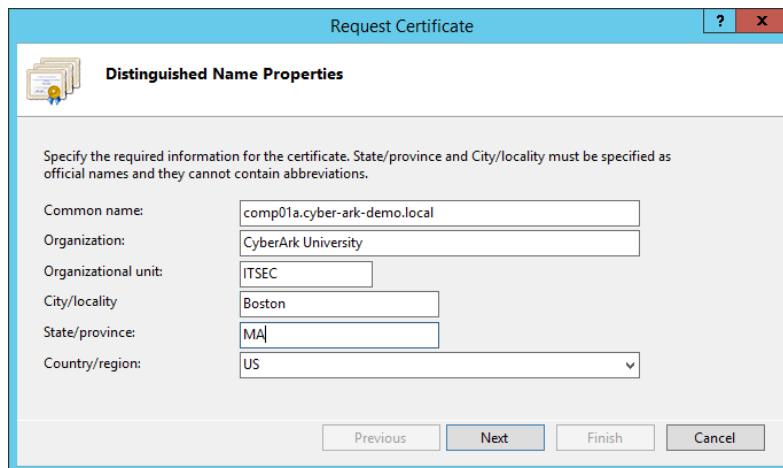


3. Click **Create Certificate Request...**

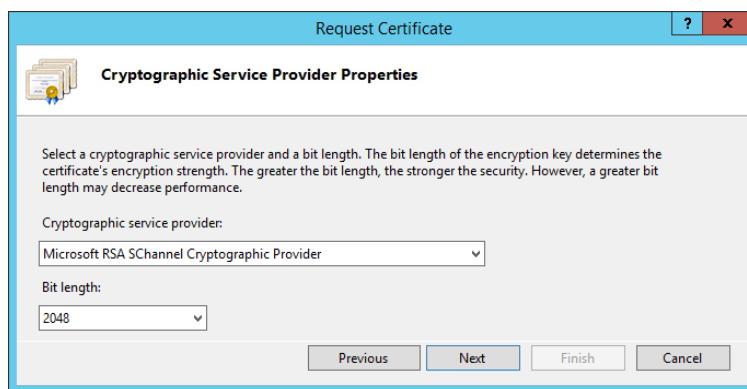


4. Enter the following values into the certificate request and click next. Ensure that you update the common name with the actual name of the component server, i.e., Comp01a or Comp01b.

<b>Common name:</b>	comp01a.cyber-ark-demo.local
<b>Organization:</b>	CyberArk University
<b>Organizational Unit:</b>	ITSEC
<b>City/Locality:</b>	Boston
<b>State/Province:</b>	MA
<b>Country/region:</b>	US



5. Choose **Microsoft RSA SChannel Cryptographic Provider** as the service provider and a bit length of **2048**, then click **Next**.

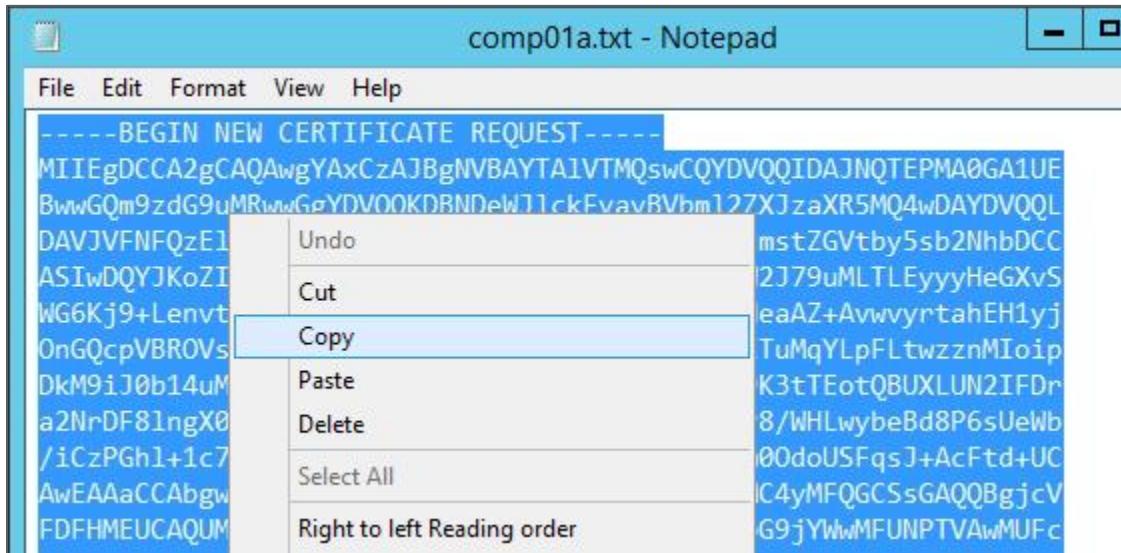




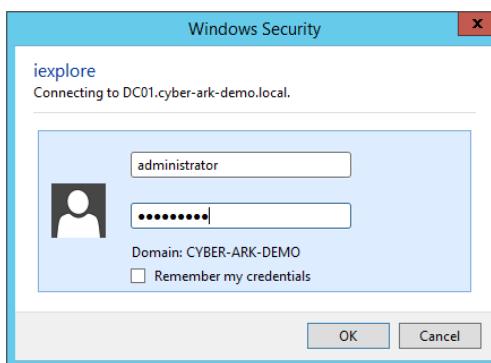
6. Save your certificate request to the desktop as **comp01a.txt** or **comp01b.txt**, as is appropriate and click **Finish**.



7. Open the .txt file created in the previous step in notepad. Copy the entire contents of the file to your clipboard.



8. Browse to <https://dc01.cyber-ark-demo.local/certsrv> in **Internet Explorer** and login as **Administrator / Cyberark1**. There is a shortcut in the browsers Favorites Bar, called CA.



## 9. Click Request a certificate.

The screenshot shows the Microsoft Active Directory Certificate Services home page for the domain "cyber-ark-demo-DC01-CA". The title bar says "Microsoft Active Directory Certificate Services – cyber-ark-demo-DC01-CA" and "Home". The main content area has a "Welcome" section with instructions for requesting certificates. Below it is a "Select a task:" section with three options: "Request a certificate" (which is highlighted with a red border), "View the status of a pending certificate request", and "Download a CA certificate, certificate chain, or CRL".

## 10. Click advanced certificate request.

The screenshot shows the "Request a Certificate" page. The title bar is the same as the previous page. The main content area has a "Request a Certificate" section with the instruction "Select the certificate type:" followed by a link "User Certificate". Below it is another link "Or, submit an [advanced certificate request](#)".

## 11. Choose the second option Submit a certificate request by using a base-64-encoded CMC...

The screenshot shows the "Advanced Certificate Request" page. The title bar is the same. The main content area has a section about policy: "The policy of the CA determines the types of certificates you can request. Click one of the following options to:". Below this are two links: "Create and submit a request to this CA" and "Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file". The second link is highlighted with a red border.



12. In the saved request field paste in the entire contents of the .txt file created earlier. Choose **Web Server** for the *Certificate Template* and Click **Submit**.

Microsoft Active Directory Certificate Services – cyber-ark-demo-DC01-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN NEW CERTIFICATE REQUEST-----  
HAAQtRty1dBc9O3z6N3uceXSMY5UsxurCieYhoagA  
x8spFJ09pileOV57t2ILnJwF6SRE30StRxq5tjWv  
EL5T0m2aX1fnPeFoUxFvH8NSh8D8j9Dy-eVPhacq  
LdvtqphH8w9tFw==  
-----END NEW CERTIFICATE REQUEST-----
```

Certificate Template:

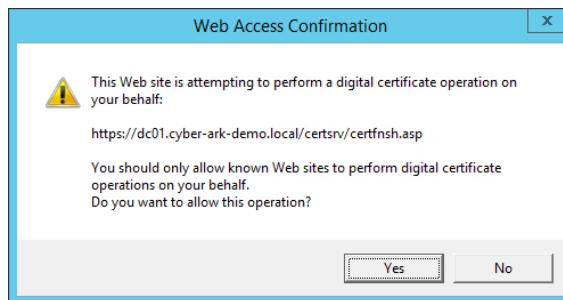
Web Server

Additional Attributes:

Attributes:

Submit >

13. Click **Yes** when prompted to allow the website to perform a certificate operation.

**Note:**

Our Certificate Authority (CA) will automatically issue a certificate immediately. Some production CAs may require a manual approval process before certificates are issued, which could delay obtaining a certificate.

14. Leave **DER encoded** selected and click **Download Certificate**.



**Certificate Issued**

The certificate you requested was issued to you.

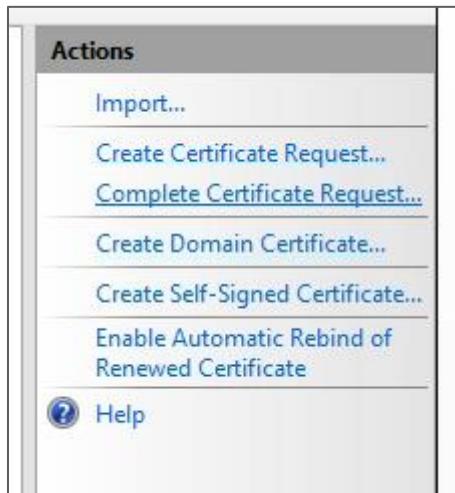
DER encoded or  Base 64 encoded

 [Download certificate](#) [Download certificate chain](#)

15. Click **Save** to store the certificate in your **Downloads** folder.



16. Return to the IIS Manager and click **Complete Certificate Request...**

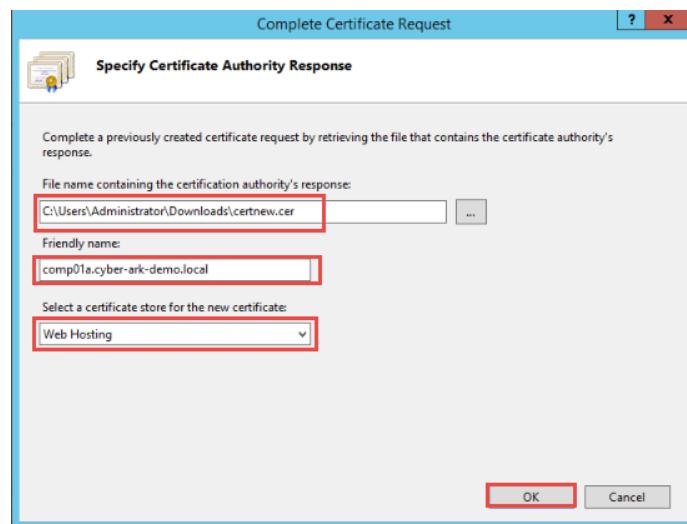


17. Select the .cer file downloaded in the previous step, in the *Friendly name* field enter the Common Name (e.g. **comp01a.cyber-ark-demo.local**) you used in the certificate request and select **Web Hosting** as the *certificate store*, then click **OK**.

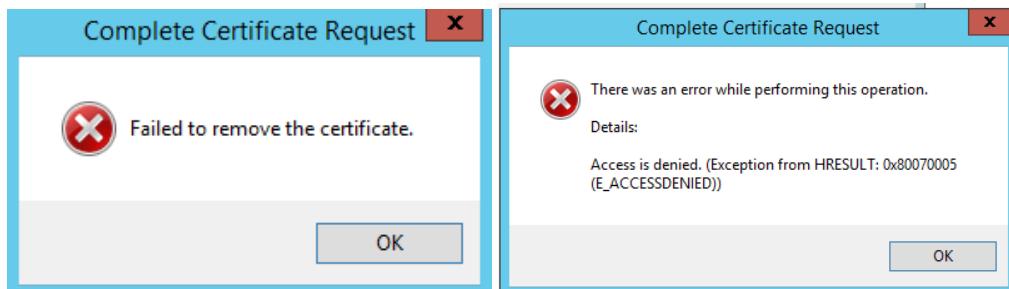


CYBERARK®

## Privileged Account Security Install &amp; Configure, v10.x



18. You will receive the following 2 errors (this is normal in our environment) click **OK** for each then **Cancel**. Close the errors and verify that you can see the new certificate in the list after pressing **F5**.



19. If successful, you will see the new certificate listed, as shown in the graphic here. Skip step 20 and go directly to step 21.

Server Certificates

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

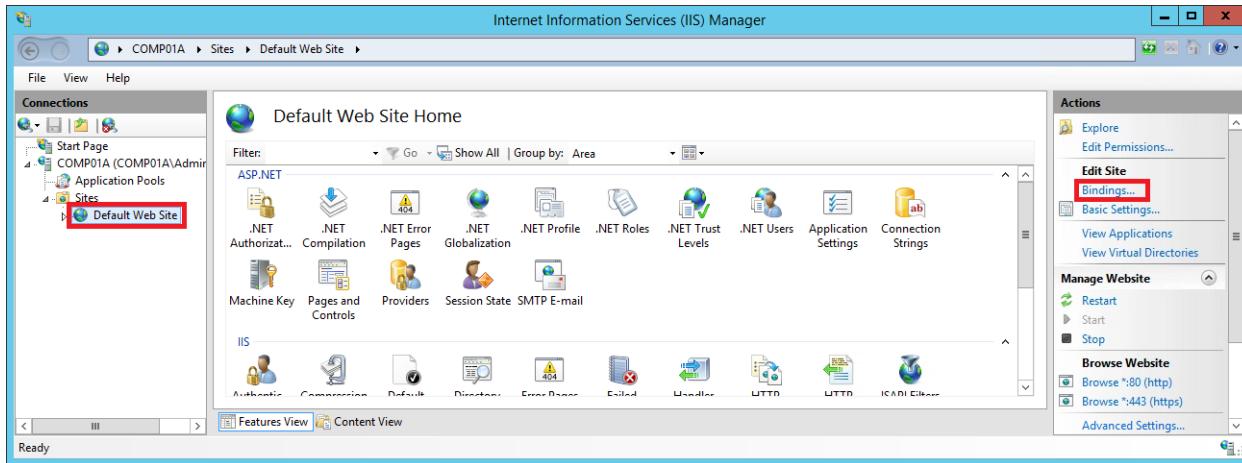
Name	Issued To	Issued By	Expiration Date	Certificate Hash	Certificate Store
comp01a.cyber-ark-demo.local	comp01a.cyber-ark-demo.local	cyber-ark-demo-DC01-CA	2/26/2020 2:54:06 ...	794D44F6AEC3757A4E21B789...	WebHosting
WMSVC	WMSvc-COMP01A	WMSvc-COMP01A	2/24/2028 2:32:50 ...	BED35D4EE295548278F2EE6A...	Personal



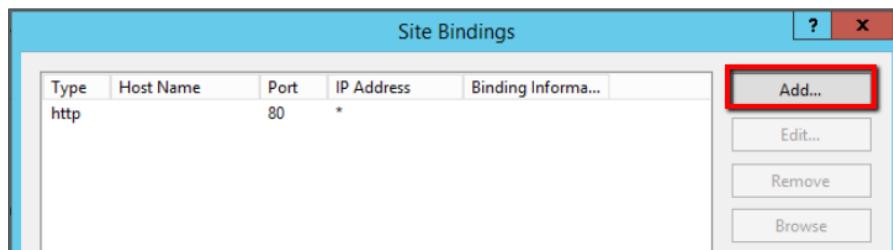
**Note:** You will need to make sure that the certificate is in fact placed in the **Web Hosting** certificate store and not in the **Personal** store. There appears to be an issue with the way Microsoft is importing the signed certificates. You can move the certificate by opening a Microsoft Management Console (mmc.exe), adding a **Certificates** snap-in for the Local Computer, and then just cutting and pasting the certificate into the appropriate store.

20. If the certificate does not immediately appear in the list of certificates, open an explorer window, right-click the **certnew.cer** file in the *Downloads* folder and select **Install Certificate**.
  - a. In the *Certificate Import Wizard* window, select **Local Machine** as the Store Location and click **Next**.
  - b. Select **Place all certificates in the following store**.
  - c. Click the **Browse** button and select the **Web Hosting** certificate store.
  - d. Click **Next** to proceed.
  - e. Select **Finish**

21. In the **IIS Manager** drill down to the **Default Web Site**, and click **Bindings...**

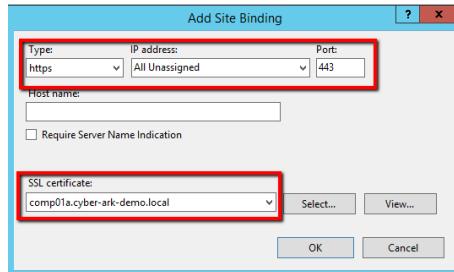


22. Click on **Add...**

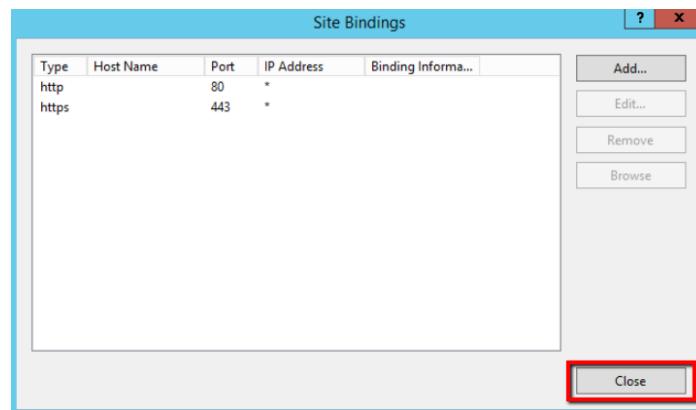


23. Enter the following properties and click **OK**.

Type:	https
IP address:	All Unassigned
Port	443
SSL Certificate:	Choose your certificate from the drop-down menu. (e.g. comp01a.cyber-ark-demo.local)



24. Click **Close**.



25. Go to **Default Web Site Home** and double click **SSL Settings** (golden padlock). Select *Require SSL* and click **Apply** in the **Actions** menu.

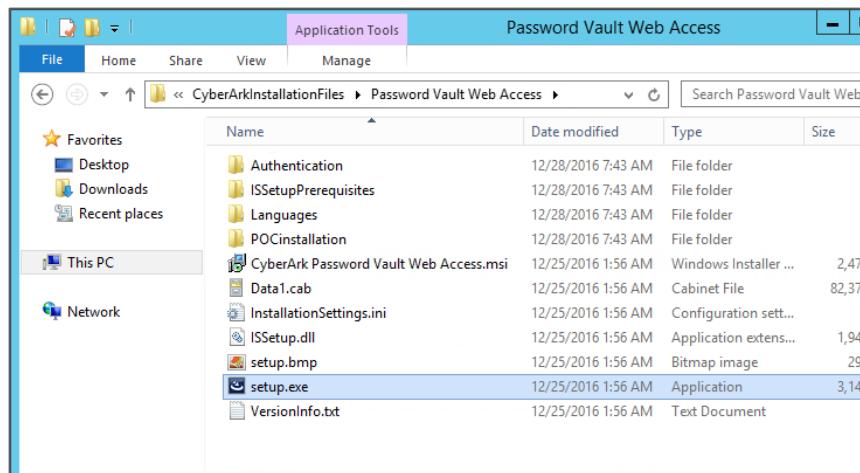
26. Validate the IIS installation. This is an important step to confirm that the IIS server is functioning correctly prior to the **PVWA** software installation. Open Internet Explorer and attempt to connect to the default web site on each component server with http and https URL's. What is the expected behavior of each?

- <http://comp01a.cyber-ark-demo.local/>
- <https://comp01a.cyber-ark-demo.local/>

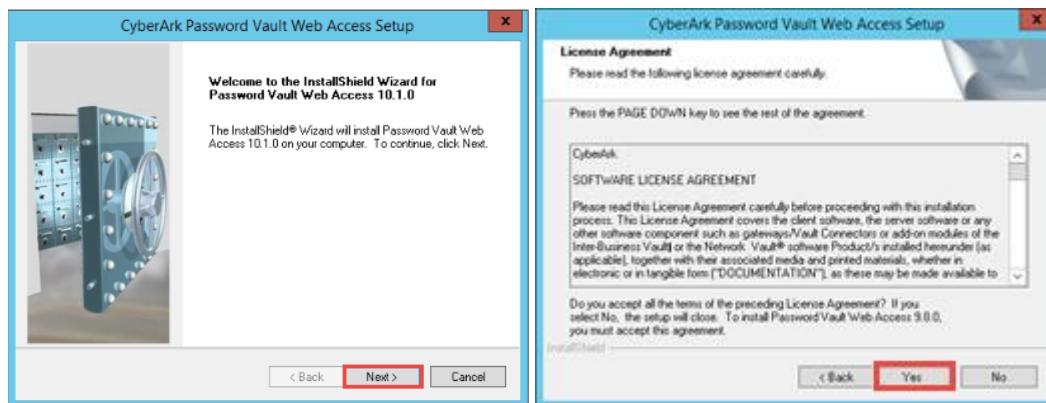
### Install 1st PVWA

**Objective:** Install the **PVWA** on Comp01a.

- On the **Comp01A** server, go to *C:\CyberArk\InstallationFiles\Password Vault Web Access* and double click *setup.exe*.

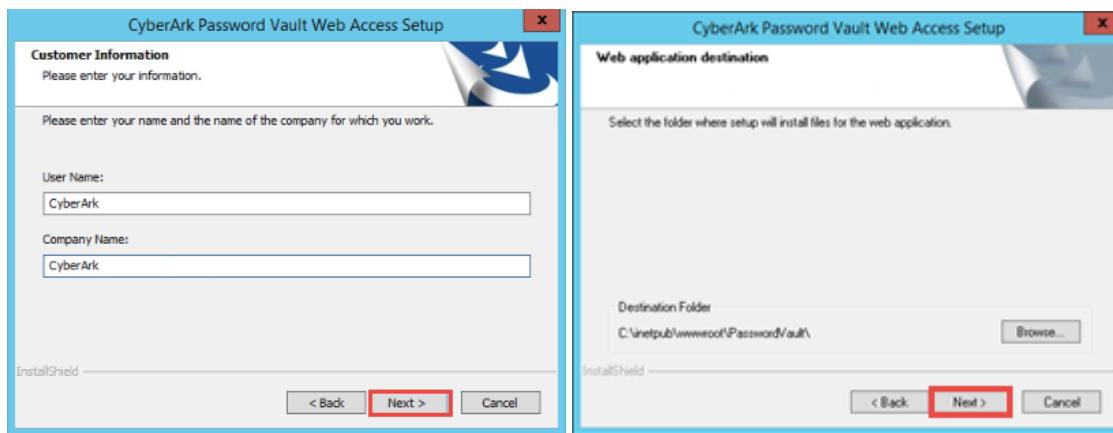


- Press the **Next** button, then click **Yes** to agree to the license agreement.

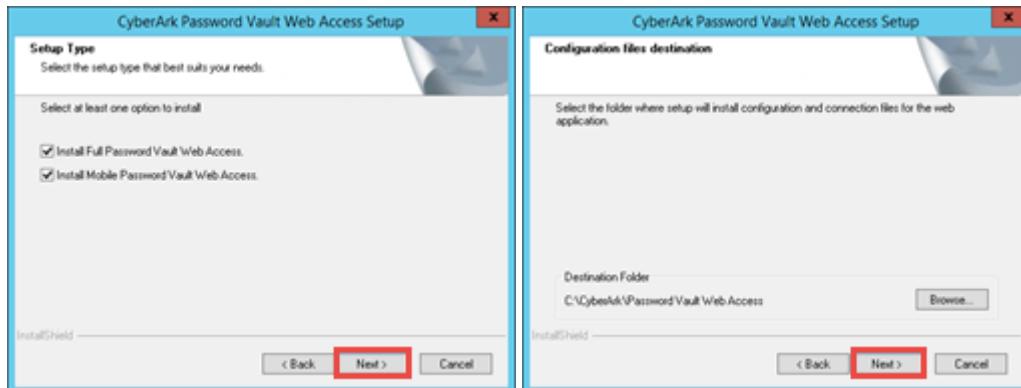




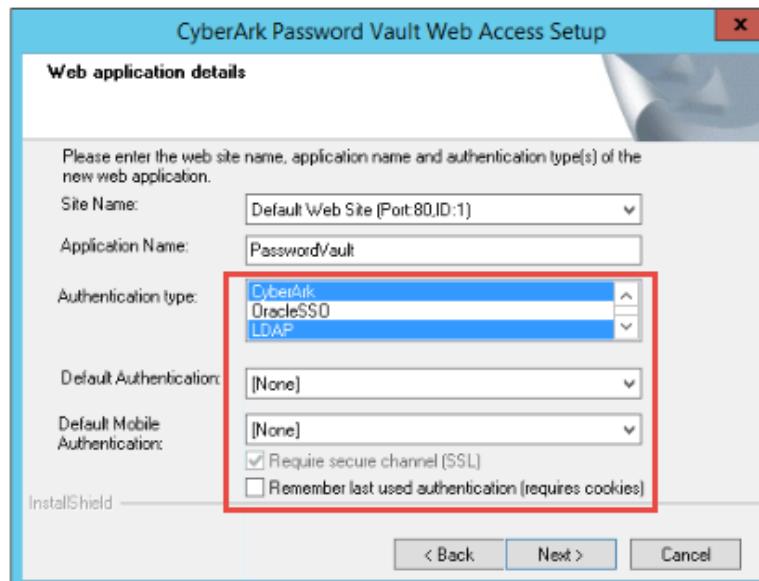
3. Enter a *User name* and *Company name*, press **Next**, then press **Next** to accept the default Web application destination.



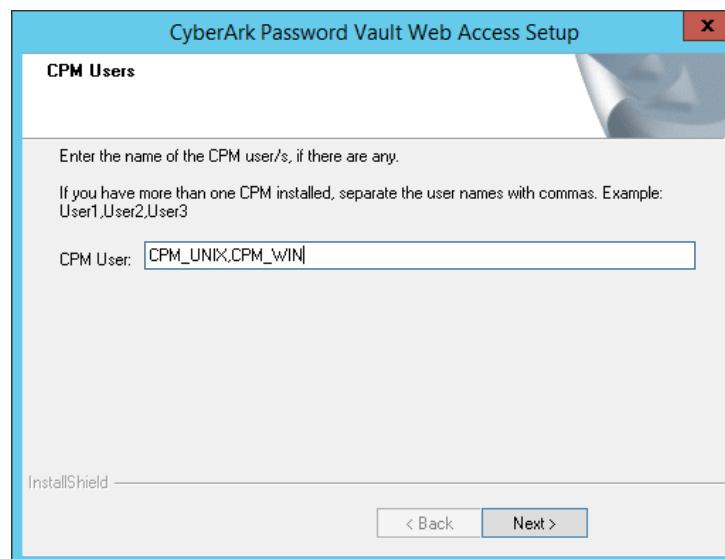
4. Press **Next** to accept the default **Configuration files destination** and press **Next** to accept both **Setup Type** options.



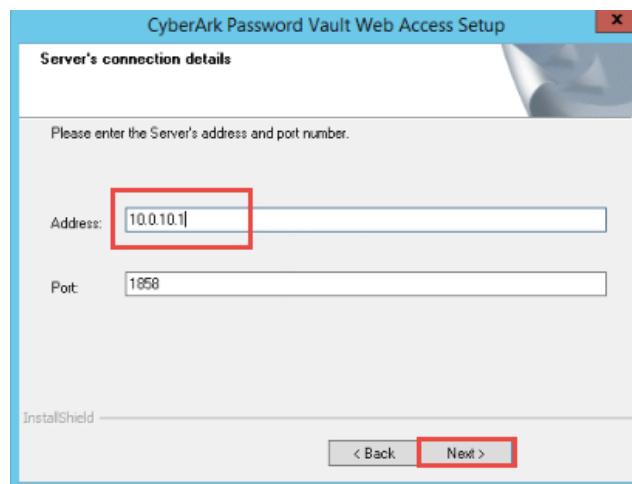
5. On the Web application details window, select **CyberArk** and **LDAP** as the *Authentication Type*. Choose **None** in *Default Authentication* and *Default Mobile Authentication* fields and confirm that “**Require secure channel (SSL)**” is selected and cannot be edited.



6. Enter **CPM\_UNIX,CPM\_WIN** in the *CPM User* field and press **Next**.



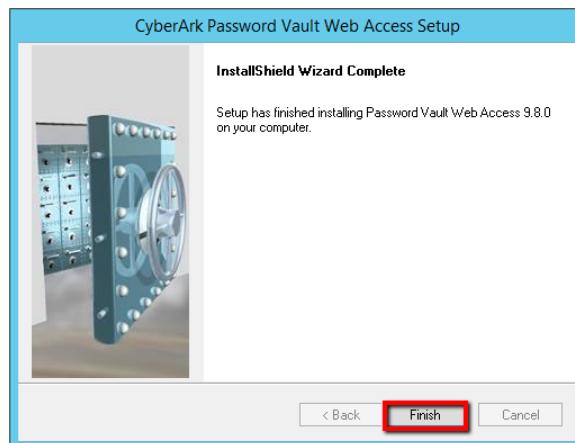
7. Enter your Vault IP (e.g. **10.0.10.1**) and press **Next**.



8. Leave **Administrator** as the username and enter **Cyberark1** as the password, then click **Next**



9. Press the **Finish** button



10. Validate the **PVWA** installation:

- a. Check the **PVWAInstall.log** in directory **C:\Users\Administrator\AppData\Local\Temp\1**.



- b. Open Internet Explorer and confirm that the **PVWA** login page is displayed. This step validates that the **PasswordVault** application is communicating with the PrivateArk Server. Use URL “<https://comp01a.cyber-ark-demo.local/PasswordVault>”

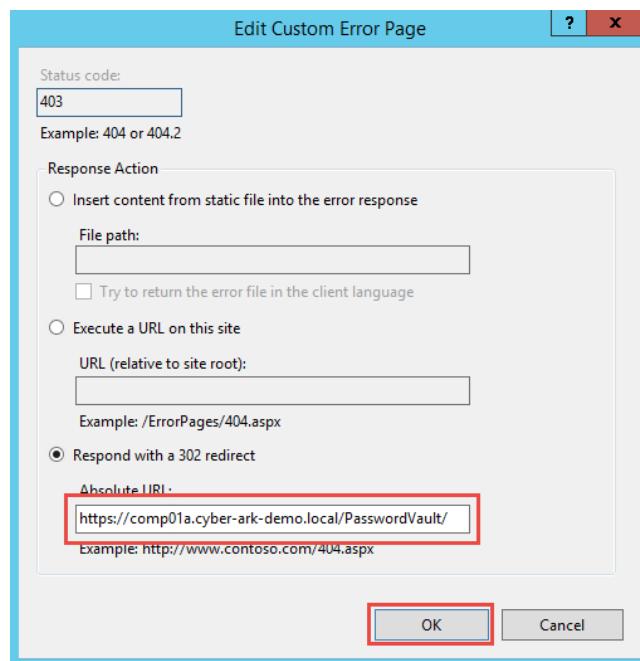
Next, we will configure an IIS response to a 403 error code, effectively redirecting HTTP traffic to HTTPS (443). We will also prevent browser access to the default web site.

1. Open **Internet Information Service (IIS) Manager**
2. Navigate to the **Default Web Site Home**, select **Error Pages** and then double-click the **403** status code.

The screenshot shows two windows side-by-side. The left window is the 'Default Web Site Home' under 'IIS Manager'. It displays various configuration icons for .NET, Application Settings, and IIS. The 'Error Pages' icon is highlighted with a red box. The right window is the 'Error Pages' configuration window. It lists error codes (401, 403, 404, 405, 406, 412, 500, 501, 502) and their corresponding paths and types. The '403' entry is selected.

Status Code	Path	Type
401	%SystemDrive%\inetpu...	File
403	%SystemDrive%\inetpu...	File
404	%SystemDrive%\inetpu...	File
405	%SystemDrive%\inetpu...	File
406	%SystemDrive%\inetpu...	File
412	%SystemDrive%\inetpu...	File
500	%SystemDrive%\inetpu...	File
501	%SystemDrive%\inetpu...	File
502	%SystemDrive%\inetpu...	File

3. Select **Respond with a 302 redirect** and type the full URL to the PVWA web site (e.g. <https://comp01a.cyber-ark-demo.local/PasswordVault/>) then click **OK**. Be sure to update the URL with the FQDN of the current server.

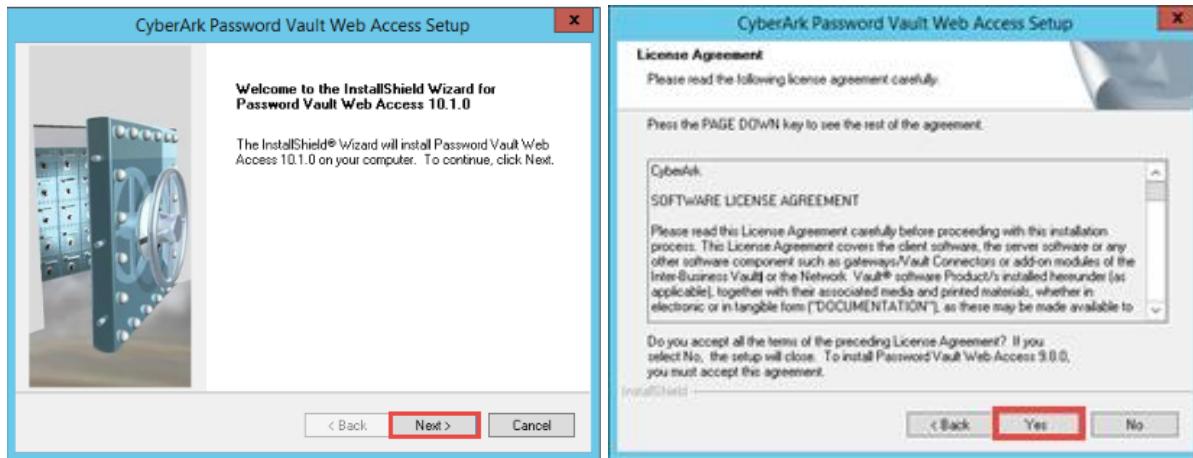


4. In INETMGR, navigate to **Default WebSite**, double click **Default Document**. Move *Default.asp* to the top.
5. Add an IIS redirect to prevent users from accessing the default web site. Using Notepad, create a new text file named *default.asp* in directory “c:\inetpub\wwwroot”. Ensure the file extension is .asp and not .asp.txt. Add the following content to the file.
  - a. `<% Response.Redirect "/PasswordVault/" %>`
6. Run IISRESET and test.
  - a. Open a browser and make sure you can login to the PVWA using https (<https://comp01a.cyber-ark-demo.local/passwordvault/>).
  - b. Test IIS redirection with an attempt to access the default web site, and connecting to the /PasswordVault application using HTTP. Also attempt to connect to the default web site on each component server.
  - c. Make sure to test from the other component server. IIS will not redirect local requests.

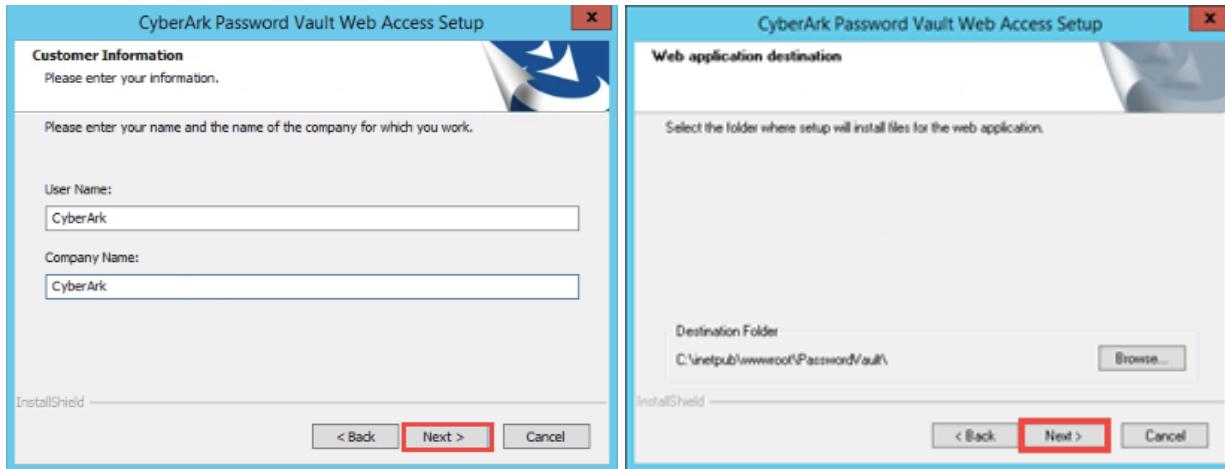


## Install 2<sup>nd</sup> PVWA

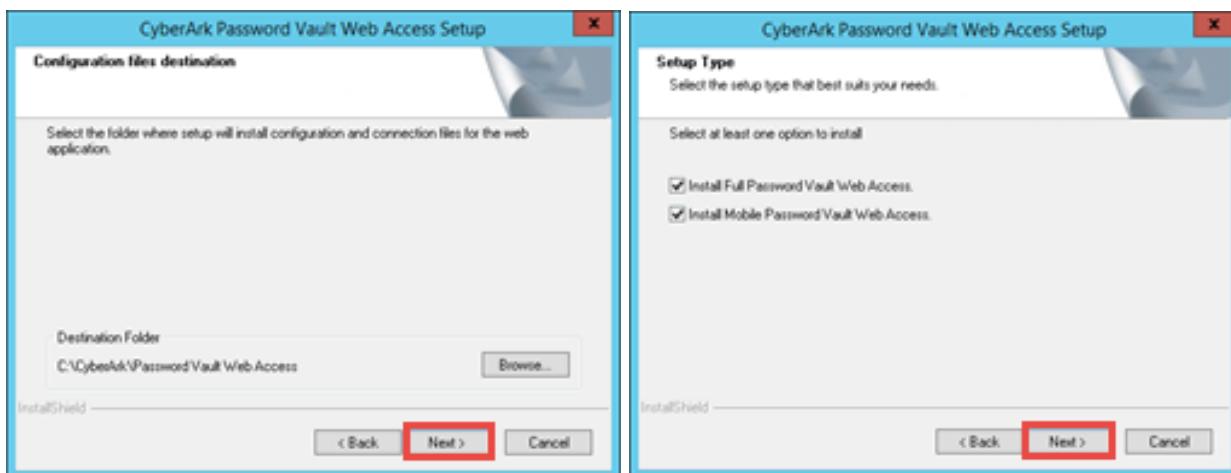
1. Login to **Comp01b** server. Navigate to *C:\CyberArk\InstallationFiles\Password Vault Web Access* and double click **setup.exe**.
2. Press the **Next** button, then click **Yes** to agree to the license agreement.



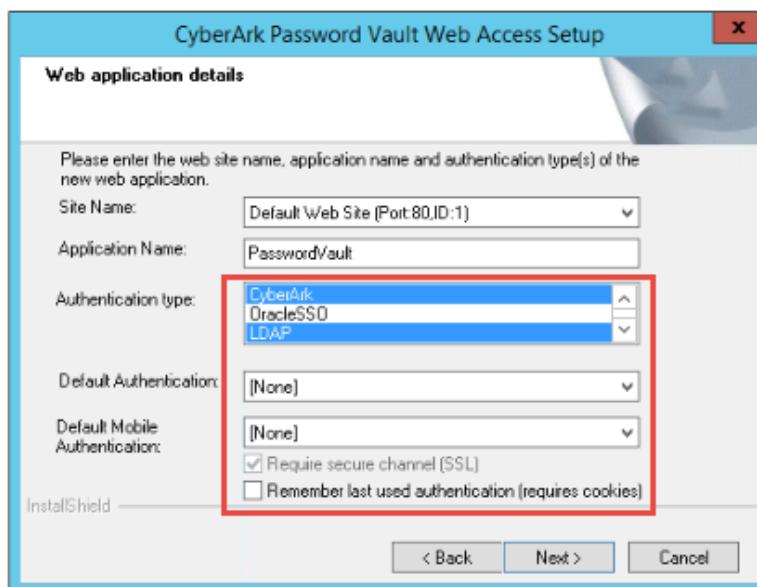
3. Enter a *User name* and *Company name*, press **Next**, then press **Next** to accept the default Web application destination.



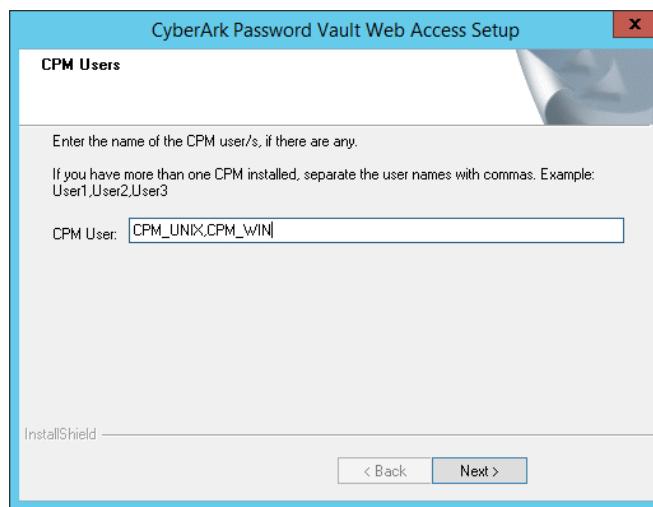
4. Press **Next** to accept the default Configuration files destination and press **Next** to accept both **Setup Type** options.



5. On the **Web application details** window, select **CyberArk** and **LDAP** as the *Authentication Type*. Choose **None** in *Default Authentication* and *Default Mobile Authentication* fields and confirm that **Require secure channel (SSL)** is checked.



6. Enter **CPM\_UNIX,CPM\_WIN** in the *CPM User* field and press **Next**.



7. Validate the PVWA installation.
  - a. Check the PVWAInstall.log in directory "C:\Users\Administrator\AppData\Local\Temp\1"
  - b. Open Internet Explorer and confirm that the PVWA login page is displayed. This step validates that the PasswordVault application is communicating with the PrivateArk Server. Use URL "<https://comp01b.cyber-ark-demo.local/PasswordVault/>"
8. Configure the IIS 403 error page redirecting HTTP traffic to HTTPS (443), and add an IIS redirect to prevent users from accessing the default web site, as you did on the first component server. However make sure to redirect using the specific FQDN of the current Comp01b server, in the URL (i.e., <https://comp01b.cyber-ark-demo.local/PasswordVault>).
9. Run IISRESET and test.
  - a. Open a browser and make sure you can login to the PVWA using https (<https://comp01a.cyber-ark-demo.local/passwordvault/>).
  - b. Test IIS redirection with an attempt to access the default web site, and connecting to the /PasswordVault application using HTTP.
  - c. Make sure to test from the other component server. IIS will not redirect local requests.



## Hardening the CyberArk CPM and PVWA Servers

Hardening the component servers is a combination of automatic and manual procedures. The instructor has provided the “Hardening the CPM and PVWA Servers” guide for this class. This document is used as a reference during these exercises.

We will not be implementing automatic hardening via GPO in this lab, but we will be reviewing the documentation and implementing a few manual hardening procedures.

### **General Configuration for all Deployments**

Review section “General Configuration for all Deployments” for guidance on recommended security practices for hardening the CyberArk components in your organization. Many of these recommendations may already be standard practice for many companies.

### **IIS Hardening (PVWA Only)**

1. Search on “IIS Hardening (PVWA Only)” and execute the following listed procedures to harden Comp01a and Comp01b servers. Restart the servers as needed.
  - a. Shares (**Skip this step**)
    - i. Because this lab will co-host PSM and PVWA, we cannot disable the Administrative Shares.
  - b. Application Pool
  - c. Web Distributed Authoring and Versioning (WebDAV)
  - d. MIME Types (Recommend making a backup copy of applicationHost.config prior to changes)
  - e. SSL/TLS Settings
    - i. Disable SSL V2.0, v3.0 and TLS 1.0 and TLS 1.1.
    - ii. Enable TLS 1.2
    - iii. Be certain to enable .NET Framework to use TLS1.2



## Configure the External Load Balancer for the PVWA servers

1. Open a browser on the **Comp01a** server to log on to the **Load Balancer** using the address: <https://10.0.0.5:444> (**User Name: admin/Password: admin**). You should also be able to find a bookmark on your browser. Prior to performing this step, make sure that your Load Balancer is powered on.



2. First, go to “**Settings > Interfaces**”, then click on the “**add virtual network interface**” button.

Table interfaces						
Name	Addr	HWaddr	Netmask	Gateway	Status	Actions
eth0	10.0.0.5	00:50:56:09:1f:de	255.255.0.0	-	green	
eth0:1	10.0.22.1	00:50:56:09:1f:de	255.255.0.0		adding	

3. Set the *Name* to **eth0:1** and *Addr* to **10.0.22.1**, then click on the “Save Virtual Interface” option, located in the Actions column as shown below.

Table interfaces						
Name	Addr	HWaddr	Netmask	Gateway	Status	Actions
eth0	10.0.0.5	00:50:56:09:1f:de	255.255.0.0	-	green	
eth0:1	10.0.22.1	00:50:56:09:1f:de	255.255.0.0		adding	

4. Next, Click on **Manage > Farms** to configure a new farm.
5. Enter **PVWA** in the **Farm Description Name** field and change the Profile type to **HTTP**.
6. Click on **Save and Continue**.



Manage::Farms::PVWA

Configure a new Farm

Farm Description Name: PVWA Profile: HTTP

Save & continue Cancel

7. Select the new interface **eth0:1->10.0.22.01** in *Virtual IP*, enter **80** as the *Virtual Port* for the farm and click **Save**.

Manage::Farms::PVWA

Configure a new Farm

Farm Description Name: PVWA Profile: HTTP

Virtual IP: eth0:1->10.0.22.1 or add new VIP interface. Virtual Port(s): 80

Save Cancel

8. Next, click on “**Edit the PVWA Farm**”.

**Note:** The Farm Management window may open in a separate browser window.

Manage::Farms::PVWA

SUCCESS! The PVWA farm has been added to VIP 10.0.22.1 over eth0:1, now you can manage it

Farms table

Name	Virtual IP	Virtual Port(s)	Status	Profile	Edit the PVWA Farm
PVWA	10.0.22.1	80	●	http	

9. Scroll down to *Add Service*. Enter **PasswordVault** as the name and click **Add**.



Rewrite Location headers.  
disabled

HTTP verbs accepted.  
standard HTTP request

Farm listener.  
HTTP

Farm Virtual IP and Virtual port.  
10.0.22.1  80

Add service. \*manage virtual host, url, redirect, persistence and backends  
**PasswordVault**

10. Scroll down to section “Service “PasswordVault”. Change *Persistence Session* to IP: **client address** and click **Modify**.

Service "PasswordVault"

Virtual Host. \*empty value disabled

Url pattern. \*empty value disabled

Redirect. \*empty value disabled

Persistence session.  
**IP: client address**

Persistence session time to limit.  
120

HTTPS Backends

11. Next, scroll down to add the real servers (IP addresses for Comp01A and Comp01b, e.g. **10.0.20.1** and **10.0.21.1**, Port: **80**, Timeout: **30**, Weight: **1** ).

Server	Address	Port	Timeout	Weight	Actions
0	10.0.20.1	80	30	1	
1	10.0.21.1	80	30	1	

12. Scroll back to the top of the screen and click the link labeled “Restart HERE!” to restart the farm to apply all the changes.



**SUCCESS!** The real server with ID and IP 10.0.21.1 of the PVWA farm has been modified.

**TIP!** There're changes that need to be applied, stop and start farm to apply them! Restart HERE

13. Make sure the status of the farm changes to “*up*” after you save the configurations and restart the farm:

**Manage::Farms**

Farms table					
Name	Virtual IP	Virtual Port(s)	Status	Profile	Actions
pvwa	10.0.22.1	80		http	

14. Next, use the browser to login to the PVWA using the virtual IP of the farm, e.g. **http://10.0.22.1/PasswordVault**. As there is no SSL certificate on the load balancer, do not use **https** for the VIP, but note that the IIS redirects configured earlier will redirect the http request to HTTPS.

Username	Address
PSMConnect	10.0.21.1
PSMConnect	10.0.20.1
root01	10.0.20
admin01	cyber-ark-demo.local
localadmin01	10.0.10.50

15. Try opening multiple sessions.

- You may discover that the ZEN LB'er does not alternate every connection. This is a ZEN issue that we will not attempt to resolve in this lab exercise.
- You can test the LB'er by stopping the World Wide Web Publishing service on either PVWA server, then attempt to access <http://10.0.22.1/passwordvault>. The LB'er should direct you to the only available PVWA.



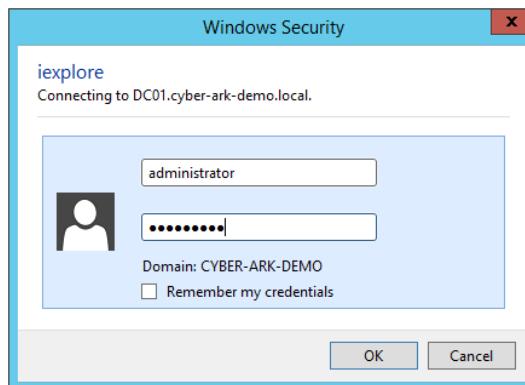
## Integrations

### LDAP Authentication (over SSL)

To configure the vault to use LDAP over SSL connections, we first need to acquire, then import the Certificate Authority root Certificate that signed the certificate used by the External Directory, into the Windows certificate store on the Vault Server to facilitate an SSL connection between the Vault and the External Directory.

Please note when integrating with LDAP that the Customer has already created 3 LDAP groups required for the initial directory mappings: **CyberArk Vault Admins**, **CyberArk Auditors** and **CyberArk Users**. Once you complete the LDAP integration, you will be able to log on with your administrative user *vaultadmin01* and your auditor user *Auditor01*.

1. On either component server, browse to <https://dc01.cyber-ark-demo.local/certsrv>. Prior to performing this step, make sure that your DC server is powered on.
  - a. Log into the web page as *Administrator/Cyberark1*.

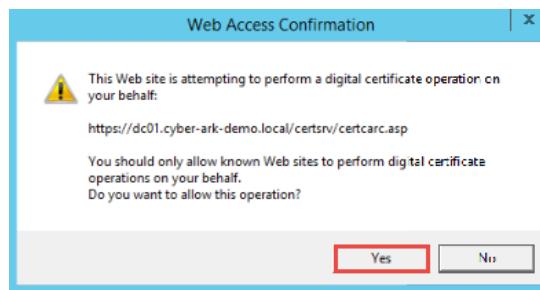


2. Click on Download a CA certificate, certificate chain, or CRL.



The screenshot shows a Microsoft Internet Explorer browser window with the URL <https://dc01.cyber-ark-demo.local/certsrv/>. The page title is "Microsoft Active Directory Certificate Services - cyber-ark-demo-DC01 CA". The main content area has a heading "Welcome" and instructions for requesting certificates. Below this, there is a section titled "Select a task:" with three options: "Request a certificate", "View the status of a pending certificate request", and "Download a CA certificate, certificate chain, or CRL". The third option is highlighted with a red rectangular box.

3. Click Yes to allow this operation.



4. Click Download CA certificate.



Microsoft Active Directory Certificate Services - Windows Internet Explorer  
https://dc01.cyber-ark... Microsoft Active Directory C...  
File Edit View Favorites Tools Help  
Tomcat Example Home  
Microsoft Active Directory Certificate Services – cyber-ark-demo-DC01-CA  
Download a CA Certificate, Certificate Chain, or CRL  
To trust certificates issued from this certification authority, install this CA certificate chain.  
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.  
CA certificate:  
Current [cyber-ark-demo-DC01-CA]  
Encoding method:  
• DER  
• Base 64  
Download CA certificate  
Download CA certificate chain  
Download latest base CRL  
Download latest delta CRL  
Waiting for response from cyber-ark-demo.local... 100%

5. Click **Save** to store the certificate in the Downloads folder.

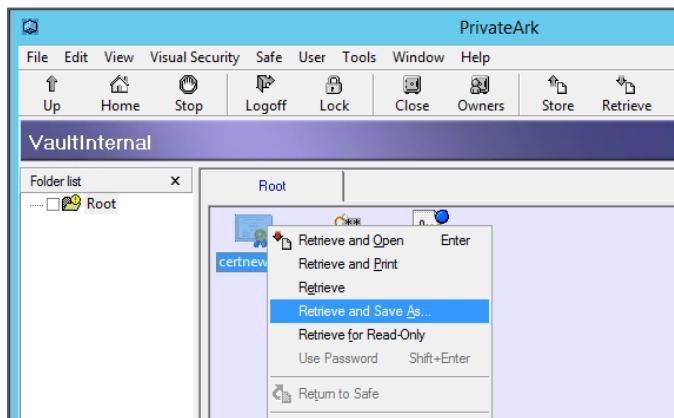


6. Log into PrivateArk Client as Administrator.
7. Open and Enter the VaultInternal safe.
8. Click the Store menu option, or right click in the body of the safe, and select Store, Move File to Safe. Navigate to the Downloads folder and select the file just downloaded, certnew.cer.

PrivateArk  
File Edit View Visual Security Safe User Tools Window Help  
Up Home Stop Logoff Lock Close Owners Store Retrieve Return Delete Inspect Reset  
VaultInternal  
Folder list Root  
Root CAUDeploy... cyber-ark-d... LDAPConf.xml  
New Store Versions... Paste Ctrl+V View Refresh F5  
Move File to Safe... Copy File to Safe... Upload Files...



9. Logoff from PrivateArk Client on the Components Server.
10. Log into PrivateArk Client on the Vault server as Administrator.
11. Open and Step into the VaultInternal safe. Right click certnew.cer and click Retrieve and Save As...



12. Save the file to the Desktop.
13. Right click the Start Menu and select Command Prompt (Admin). Change the current directory to "c:\Users\Administrator\Desktop" and enter the following command.

**Note:** Confirm the file name to be accurate.

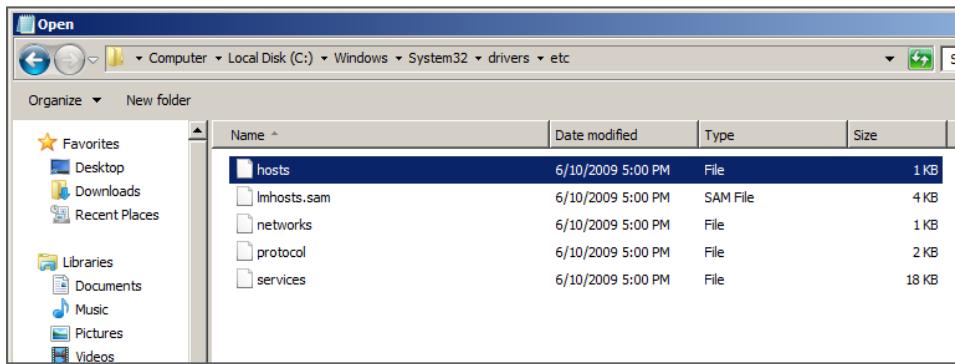
```
certutil -addstore "Root" certnew.cer
```

```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd c:\Users\Administrator\Desktop
c:\Users\Administrator\Desktop>certutil -addstore "Root" certnew.cer
Root "Trusted Root Certification Authorities"
Signature matches Public Key
Certificate "cyber-ark-demo-DC01-CA" added to store.
CertUtil: -addstore command completed successfully.

c:\Users\Administrator\Desktop>
```

14. Remain at the Administrator Command Prompt, and launch Notepad.
15. In Notepad, open C:\Windows\System32\drivers\etc\hosts. Hint: it may be hidden.



16. Add the following line to the end of the file.

10.0.0.2 dc01.cyber-ark-demo.local

17. Log off the Vault, and log back onto either Component Server.

18. Login to the PVWA as Administrator using CyberArk authentication.

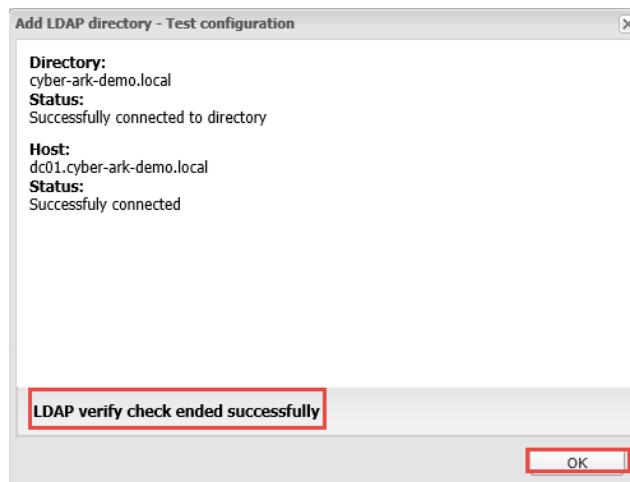
19. Navigate to the Administration tab and run the Setup Wizard.

20. Select LDAP integration and configure with the following parameters.

<b>Name:</b>	cyber-ark-demo.local
<b>Directory Type:</b>	MicrosoftADProfile.ini
<b>Address:</b>	dc01.cyber-ark-demo.local
<b>Port:</b>	636
<b>LDAP Bind User:</b>	BindAccount
<b>LDAP Bind Password:</b>	Cyberark1
<b>LDAP Base Context:</b>	dc=cyber-ark-demo,dc=local

21. Test the connection and if successful, click Save and continue. Troubleshoot as needed.

- a. Tip: Change the Address to the IP Address of DC01, 10.0.0.2 without changing any other parameter and retest. If successful, what might be solution?
- b. Tip: Change the port to 389 without changing any other parameter and retest. If successful, what might be solution?



22. At the 'LDAP Configuration Setup' screen, type the word Cyber in each field, and wait for the vault to query the external directory and display a list of groups that match.
- Select the appropriate group for each field.
  - When complete, click Finish.

<b>Define Vault Admin Group:</b>	CyberArk Vault Admins
<b>Define Auditors Group:</b>	CyberArk Auditors
<b>Define Users Group:</b>	CyberArk Users

23. Login to the PVWA as vaultadmin01/Cyberark1 and navigate to ADMINISTRATION > LDAP Integration.  
24. Expand Directories, and select cyber-ark-demo.local.  
25. Ensure that parameter SSLConnect is set to Yes.  
26. Ensure that each host defined below the directory entry, is configured to ServerPort 636 and SSLConnect=Yes.

Name	Value
ServerName	dc01.cyber-ark-demo.local
ServerPort	636
SSLConnect	Yes

27. Test your LDAP/S integration by logging into PVWA as vaultadmin01/Cyberark1 using LDAP authentication.



## SMTP Integration

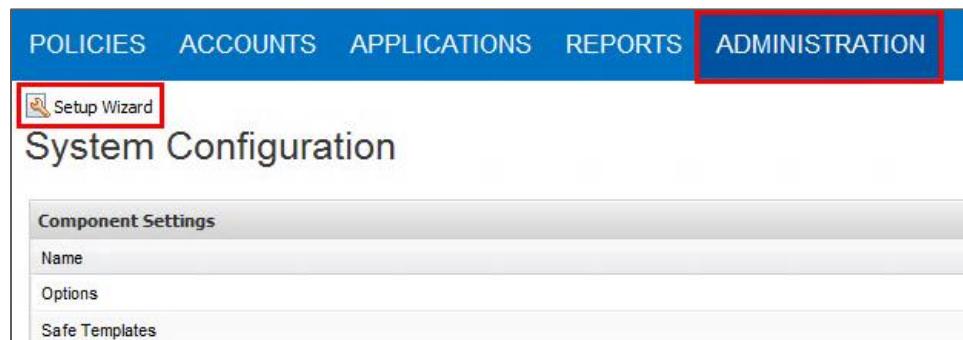
For this section, we are going to login as the vaultadmin01 (an LDAP user) and configure the SMTP integration. By logging in as vaultadmin01 you will create the user profile in the **Vault** and allow a test email to be sent to vaultadmin01.

**Note:** Prior to setting up the SMTP integration, verify that the *CyberArk Event Notification Engine (ENE)* service is running on the **Vault**, otherwise you will not receive the test email.

Services (Local)					
Cyber-Ark Event Notification Engine		Name	Description	Status	Startup Type
<a href="#">Stop the service</a>		Computer Browser	Maintains a...	Manual (Trig...	Local Syste...
<a href="#">Restart the service</a>		Credential Manager	Provides se...	Manual	Local Syste...
		Cryptographic Services	Provides the...	Running	Automatic
		Cyber-Ark Event Notification Engine	Running	Automatic (D...	Local Syste...
		CyberArk Logic Container	Running	Automatic	Local Syste...
		DCOM Server Process Launcher	The DCOM...	Running	Automatic
		Device Association Service	Enables pair...	Manual (Trig...	Local Syste...
		Device Install Service	Enables a c...	Manual (Trig...	Local Syste...

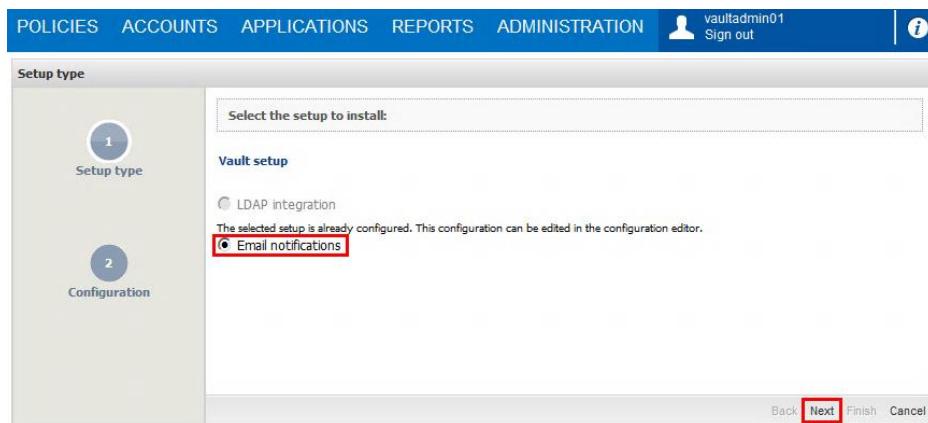
16. On the **Components** Server, launch the **PWVA** and select **LDAP** as the Authentication method.  
Login as vaultadmin01.

17. Go to the **ADMINISTRATION** tab and Press the **Setup Wizard** button.





18. Select *Email Notifications* and click **Next**.

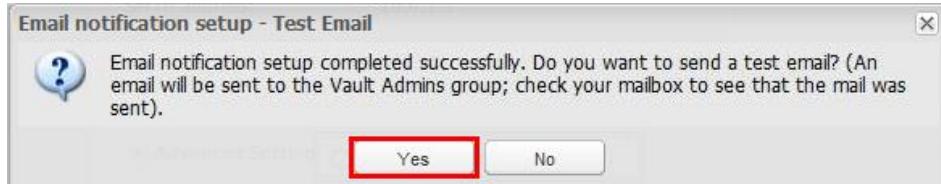


19. Enter the following:

SMTP address:	10.0.0.2
Sender Email:	<a href="mailto:vaultadmin01@cyber-ark-demo.local">vaultadmin01@cyber-ark-demo.local</a>
Sender Display Name:	VaultAdmin01
SMTP Port:	25
PVWA URL:	<a href="#">Accept the default</a>

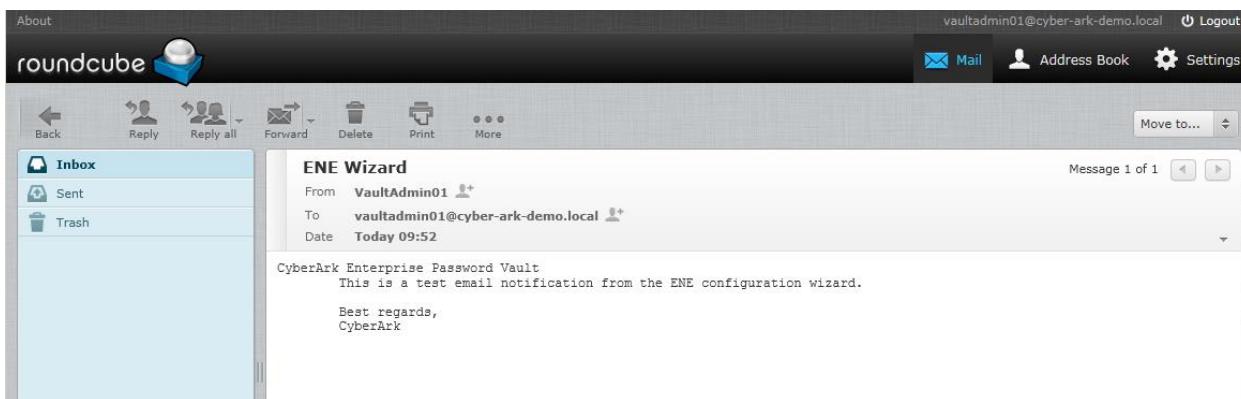
20. Press **Finish**.

21. Press **Yes** to send a test e-mail.



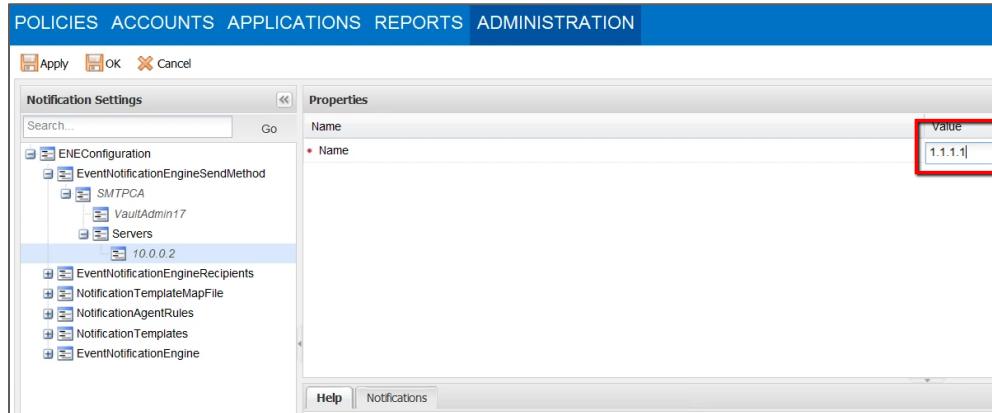
22. On the **Component Server**, browse to the email client at <http://cyber-ark-demo.local:8073/webmail/>. There should be a link called "Webmail" in the bookmarks bar.

- a. Login as *vaultadmin01 / Cyberark1*.
- b. Ensure that you receive the email from the ENE Wizard.



23. Close the Webmail application.

**Troubleshooting:** If you need to run the wizard again, you can change the IP address of the SMTP server to 1.1.1.1 and save, as shown below.



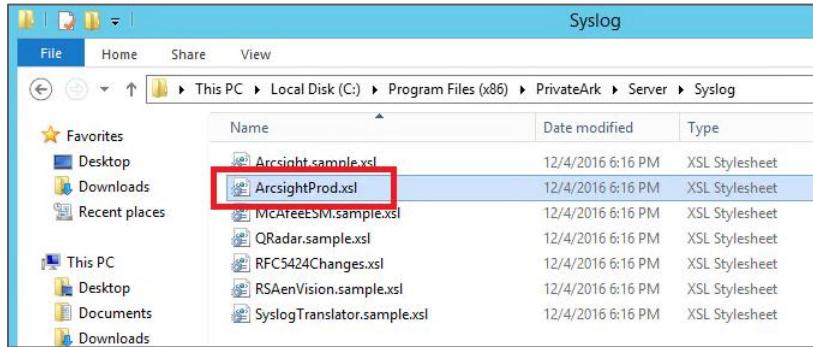
## SIEM Integration

For the first part of this exercise we will login to the **Vault** server to prepare the vault to communicate with the SIEM. This section will demonstrate how to forward audit records to a SIEM server, such as *Arcsight* or *enVision*.

### Setting up SIEM Integration



1. Login to the **Vault** server as *Administrator / Cyberark1*.
2. Open Windows File Explorer and navigate to:  
C:\Program Files(x86)\PrivateArk\Server\Syslog.
3. Make a copy of the file *Arcsight.sample.xsl* and rename to *ArcsightProd.xsl*.



4. Go to C:\Program Files(x86)\PrivateArk\Server.
  - a. Edit the DBPARM.sample.ini file. Copy the entire [SYSLOG] section.
  - b. Edit the dbparm.ini file. Paste the entire [SYSLOG] section to the bottom of the file, overwriting the existing [SYSLOG] section.
  - c. Edit the [SYSLOG] section as shown below. Be sure to remove the \* from the beginning of each line.

```
SyslogTranslatorFile="Syslog\ArcsightProd.xsl"
SyslogServerIP=10.0.0.20
SyslogServerPort=514
SyslogServerProtocol=UDP
SyslogMessageCodeFilter=0-999
SyslogSendBOMPrefix=NO
UseLegacySyslogFormat=yes
```

**Note:** The settings above will forward all *syslog* messages to the SIEM server. See the PIM Suite implementation guide for instructions on filtering these messages.

5. Save and exit the file.
6. Restart the PrivateArk Server service to read the changes made to dbparm.ini into memory. It is best to do this from the Server Central Administration applet, on your desktop.
7. If the server fails to start, check for typos in the *dbparm.ini* file.

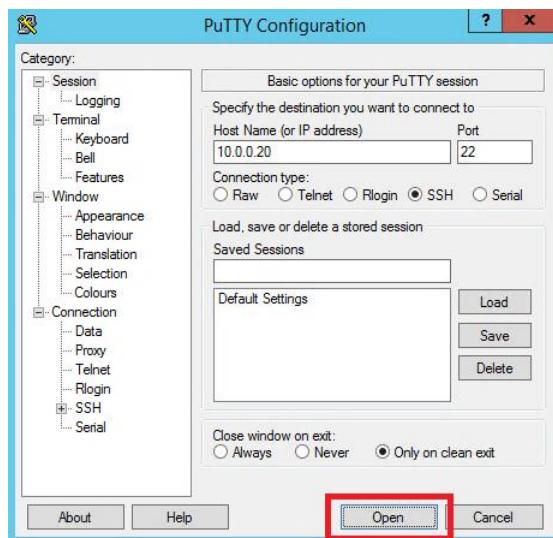
**Note:** For this next section of the exercise we will be using the **Component Server**.



1. Login to either component server.
2. Launch **putty** from the *Windows Taskbar*.



3. Enter **10.0.0.20** as the **Host Name or IP address**) and click **Open** to launch an SSH connection.



4. Click **Yes** to accept the server's key.





5. Login as *root01* with the password *Cyberark1*. Accept any security warning you may receive.

```
root@centos-target01:~  
login as: root  
root@10.0.0.20's password:  
Last login: Mon Jun  8 17:28:34 2015 from 66.37.42.2  
[root@centos-target01 ~]#
```

6. Launch the following command. Be sure to replace XX with your user number.

```
cat /var/log/messages | grep VAULT01
```

```
root@centos-target01:~  
t Id" cn1= "Ticket Id" cn2= "msg=  
Mar 30 12:10:09 VAULT01A CEF: 0|Cyber-Ark|Vault|9.10.0000|98|Open File (Write Only)|5|act=Open File (Write Only) suser=PVWAAppUser fname=Root\YWRtaW5pc3RyYXRvcg \|= dvc= shost=10.0.20.1 dhost= duser= externalId= app= reason= cs1Label="Affected User Name" cs1= cs2Label="Safe Name" cs2=PVWAPrivateUserPrefs cs3Label="Device Type" cs3= cs4Label="Database" cs4= cs5Label="Other info" cs5= cn1Label="Request Id" cn1= cn2Label="Ticket Id" cn2= "msg=  
Mar 30 12:10:09 VAULT01A CEF: 0|Cyber-Ark|Vault|9.10.0000|50|Store File|5|act=Store File suser=PVWAAppUser fname=Root\YWRtaW5pc3RyYXRvcg \|= dvc= shost=10.0.20.1 dhost= duser= externalId= app= reason= cs1Label="Affected User Name" cs1= cs2Label="Safe Name" cs2=PVWAPrivateUserPrefs cs3Label="Device Type" cs3= cs4Label="Database" cs4= cs5Label="Other info" cs5= cn1Label="Request Id" cn1= cn2Label="Ticket Id" cn2= "msg=  
Mar 30 12:10:18 VAULT01A CEF: 0|Cyber-Ark|Vault|9.10.0000|19|Full Gateway Connection|5|act=Full Gateway Connection suser=Administrator fname= dvc=10.0.20.1 shost=127.0.0.1 dhost= duser= externalId= app= reason= cs1Label="Affected User Name" cs1= PVWAGWUser cs2Label="Safe Name" cs2= cs3Label="Device Type" cs3= cs4Label="Database" cs4= cs5Label="Other info" cs5=10.0.20.1 cn1Label="Request Id" cn1= cn2Label="Ticket Id" cn2= "msg=  
Mar 30 12:10:18 VAULT01A CEF: 0|Cyber-Ark|Vault|9.10.0000|7|Logon|5|act=Logon suser=Administrator fname= dvc=10.0.20.1 shost=127.0.0.1 dhost= duser= externalId= app= reason= cs1Label="Affected User Name" cs1= cs2Label="Safe Name" cs2= cs3Label="Device Type" cs3= cs4Label="Database" cs4= cs5Label="Other info" cs5=10.0.20.1 cn1Label="Request Id" cn1= cn2Label="Ticket Id" cn2= "msg=
```

**Note:**

If you want to view the running activity log of your **Vault** in this window, you can modify the command and leave this window open with this command running while you work on other exercises and view what activities are logged as you go. To do this, replace “cat” with “tail -f”.



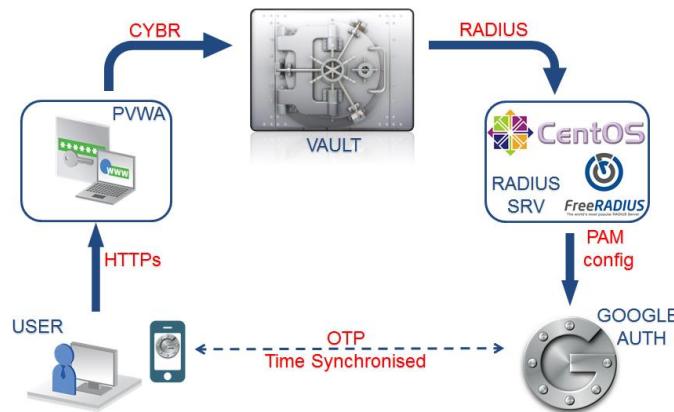
## Authentication Types

In this section you will configure multiple authentication methods. Detailed information on authentication can be found in the Privileged Account Security Installation Guide in section “Authenticating to the Privileged Account Security Solution”.

### RADIUS Authentication

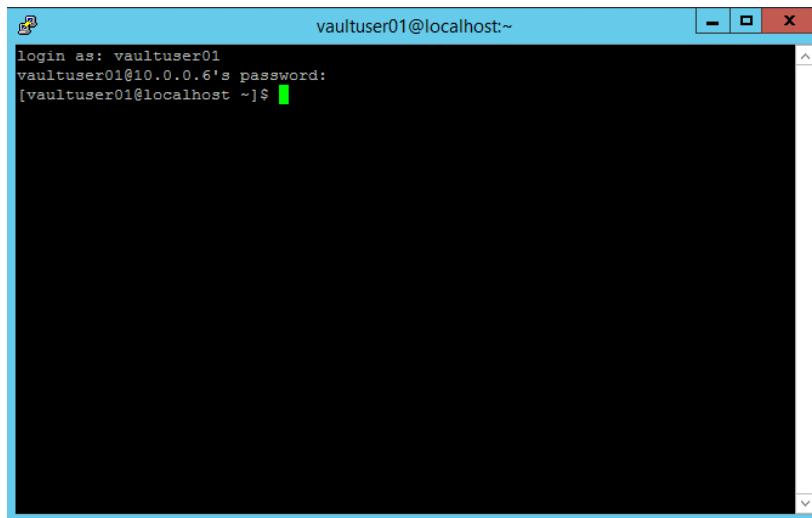
In this section you will enable RADIUS authentication for the customer, and test 2 Factor Authentication.

NOTE: For this assignment you have the option to download the application “Google Authenticator” to your smartphone. If you do not wish to install the app on your phone you may use the emergency scratch codes that will be provided to you when you register your **vaultuser01** user to Google Authenticator.





1. First, launch PuTTY from the Components server and use SSH to connect to the RADIUS server (10.0.0.6) with **vaultuser01/Cyberark1**.



2. Next, run the command “google-authenticator” to register your vaultuser01 account:

```
[vaultuser01@localhost ~]$ google-authenticator

Do you want authentication tokens to be time-based (y/n) y
https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/vaultadmin01@localhost.localdomain%3Fsecret%3D3CLLATZIIKJUZ737

Your new secret key is: 3CLLATZIIKJUZ737
Your verification code is 604700
Your emergency scratch codes are:
  57556538
  55330792
  36858217
  20147572
  18965930

Do you want me to update your "/home/vaultuser01/.google_authenticator" file (y/n) y

Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n) n

By default, tokens are good for 30 seconds and in order to compensate for
possible time-skew between the client and the server, we allow an extra
token before and after the current time. If you experience problems with poor
time synchronization, you can increase the window from its default
```

size of 1:30min to about 4min. Do you want to do so (y/n) **n**

If the computer that you are logging into isn't hardened against brute-force login attempts, you can enable rate-limiting for the authentication module.

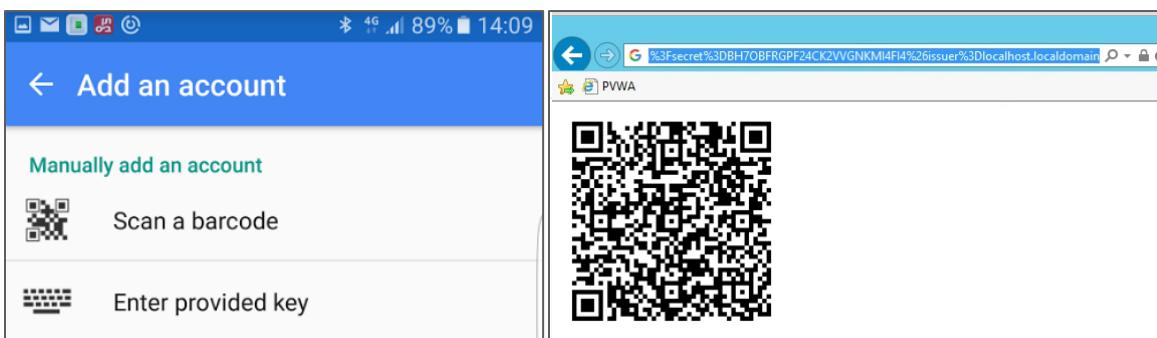
By default, this limits attackers to no more than 3 login attempts every 30s.

Do you want to enable rate-limiting (y/n) **y**

3. Copy the URL displayed by Google Authenticator and paste it into your browser to register this new user on your Google Authenticator App. (Tip: click the top left context menu and select "Copy All to Clipboard", then paste into Notepad) This app will present you with a new OTP every x seconds to be used to authenticate as this user.<sup>62</sup>

As mentioned before, if you do not wish to install the app on your phone you may use the emergency scratch codes that were provided to you when you register your *vaultuser01* user to Google Authenticator.<sup>63</sup>

Simply copy the link from the PuTTY session to the browser. The link will present you a QR code that you can easily scan to setup the new account. Alternatively, you could use the secret key to manually create the account.



4. To verify the radius integration works locally, use the following command and verify you receive Access-Accept in the reply:

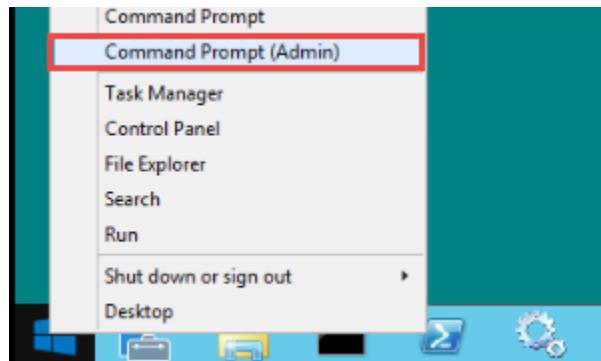
```
radtest vaultuser01 <token> localhost 18120 testing123
```



```
vaultuser01@localhost:~$ [vaultuser01@localhost ~]$ [vaultuser01@localhost ~]$ [vaultuser01@localhost ~]$ [vaultuser01@localhost ~]$ [vaultuser01@localhost ~]$ radtest vaultuser01 483070 localhost 18120 testing123 Sending Access-Request of id 151 to 127.0.0.1 port 1812 User-Name = "vaultuser01" User-Password = "483070" NAS-IP-Address = 127.0.0.1 NAS-Port = 18120 Message-Authenticator = 0x00000000000000000000000000000000 rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=151, length=20 [vaultuser01@localhost ~]$
```

In this lab, the vault server has already been defined as a RADIUS Client at the RADIUS Server. The following steps will enable the vault to authenticate with the RADIUS Server using a RADIUS Secret (Cyberark1) created by the RADIUS Administrator.

5. Save the RADIUS Secret to the encrypted file name, radiussecret.dat. Login to the Vault server and open a command line prompt as administrator.



6. Enter the following commands

```
cd \"Program Files (x86)\PrivateArk\Server\"  
CAVaultManager.exe SecureSecretFiles /SecretType RADIUS /Secret Cyberark1  
/SecuredFileName radiussecret.dat
```



```
C:\ Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright © 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd "Program Files (x86)\PrivateArk\Server"

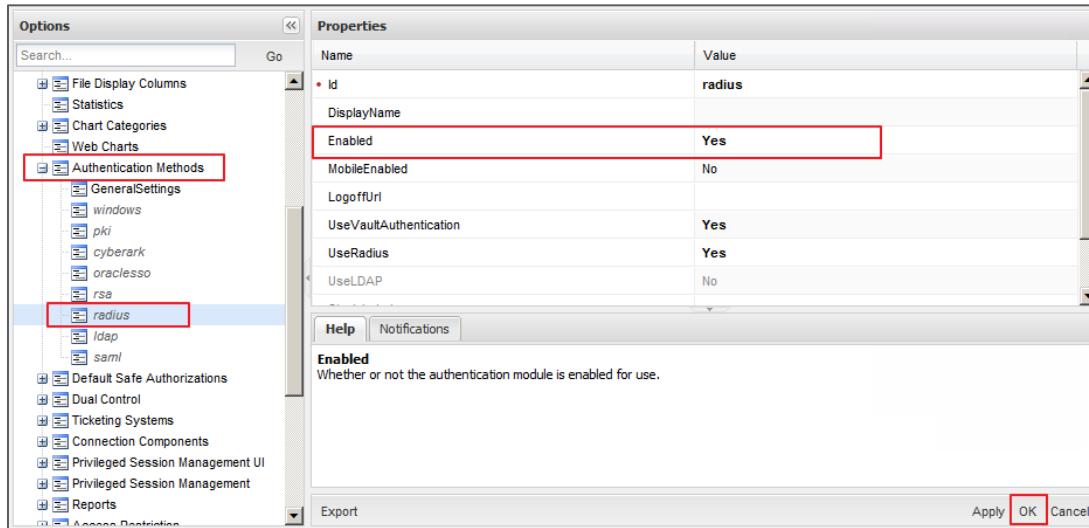
C:\Program Files (x86)\PrivateArk\Server>C:\VaultManager.exe SecureSecretFiles /secretType RADIUS /secret Cyberark1 /SecuredFileName radiussecret.dat
ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit, RSA (2048 bit), SHA1.
CAULIB44I RADIUS secret was secured successfully.

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

7. Next, open dbparm.ini in notepad and add the following two lines to the end of the file. Save the changes to the dbparm.ini and restart the PrivateArk Server.

```
[RADIUS]
RadiusServersInfo=10.0.0.6;1812;vault01a;radiussecret.dat
```

8. Restart the PrivateArk Server service to read the changes made to dbparm.ini into memory. It is best to do this from the Server Central Administration applet, on your desktop.
9. Login to the PVWA from a component server, as VaultAdmin01.
10. Navigate to Administration > Web Options > Authentication Methods > radius and Enable Radius authentication. You can also add a custom entry for “PasswordFieldLabel” to notify the user they need to authenticate using the token.





11. Logout of the PVWA.
12. Using the PrivateArk Client, login to the Vault as Administrator.
13. Update the Vault Users Directory Mapping. Edit the User Template, Authentication method to RADIUS Authentication. This will cause all new vault users from that group to use RADIUS.

The screenshot shows the PVWA interface with the 'Tools' menu open. Under 'Administrative Tools', the 'Directory Mapping...' option is highlighted with a red box.

The 'Directory Mapping for Server Vault' dialog box is open. The 'Vault Users Mapping' entry in the list is highlighted with a red box. The 'Update...' button is also highlighted with a red box.

The 'New/Update Directory Map' dialog box is open. The 'User Template...' button is highlighted with a red box.

The 'Update Directory Map: Vault Users Mapping' dialog box is open. The 'Authentication method' dropdown is set to 'RADIUS Authentication' and is highlighted with a red box.



14. Logout of the PrivateArk Client.
15. At the PVWA login, attempt to login as vaultuser01 using RADIUS authentication. Verify you can login using the OTP provided to you by google-authenticator:

**SIGN IN**

Please choose an authentication method

Windows    CyberArk    RADIUS    LDAP

The "RADIUS" button is highlighted with a red box.

**SIGN IN**

Specify your authentication details

X

**Sign in**



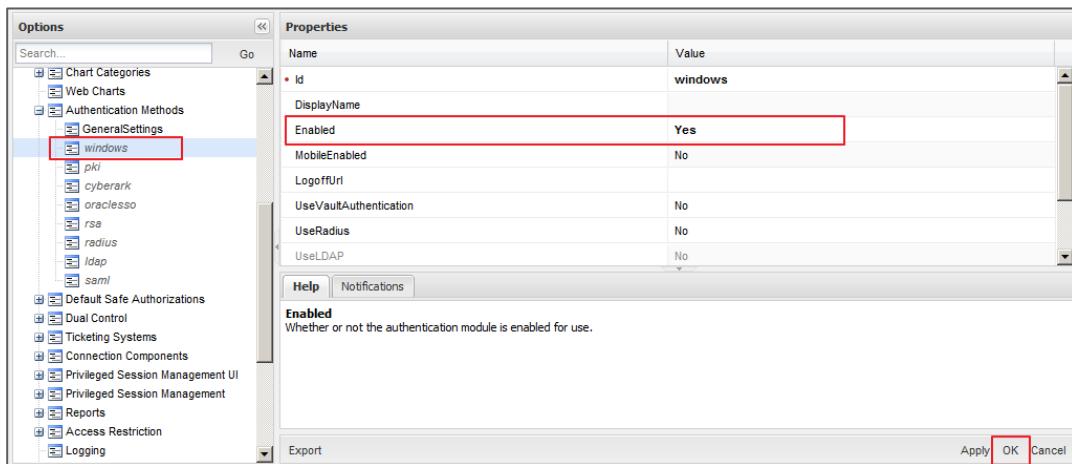
## Windows Authentication

**Note:** Windows Authentication for the PVWA is subject to IE security policies and the user experience will be highly dependent on the Intranet and / or Trusted Site settings.

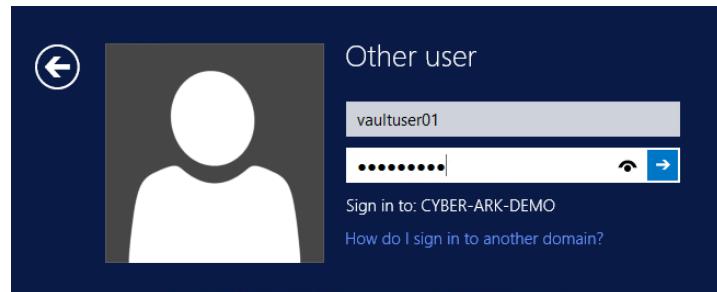
The next exercises will be using the vaultuser01 account using LDAP authentication. You should reset the CyberArk Users directory map to require LDAP authentication, and delete the vaultuser01 account from the PrivateArk Client.



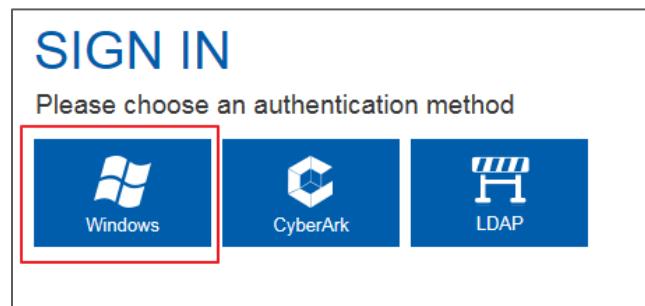
1. Login to the PVWA as Vaultadmin01.
2. Navigate to Administration > Options > Authentication Methods > windows and set *Enabled* to Yes.



3. Logoff from the components server and login as vaultuser01/Cyberark1. If the Windows Authentication option is not available, run an IISRESET.

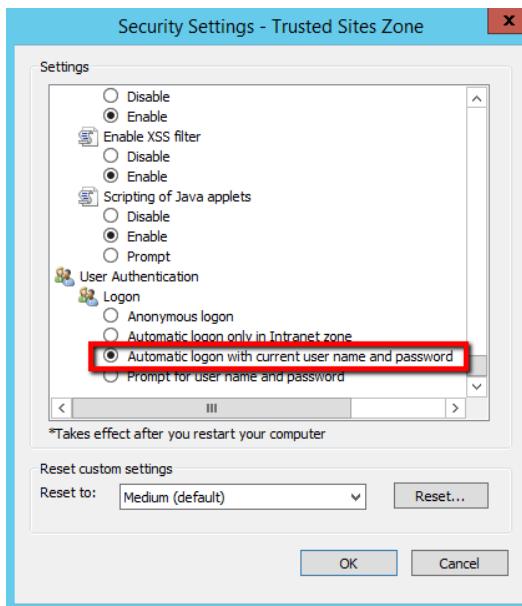


4. Browse to the PVWA via the load balanced VIP (10.0.22.1) or (<http://comp01X.cyber-ark-demo.local/passwordvault/>) and choose the Windows Authentication Method.





Note: You may still be prompted for credentials depending on the Security Settings for the Intranet or Trusted Sites zone. To use Windows authentication as single sign-on, add the URL of the PVWA to the list of trusted sites and change the browser's security settings for Trusted Sites as follows:



## PKI Authentication

PKI authentication allows the user to authenticate via Digital Certificate that can be stored on a SmartCard or USB token. In this lab, we will provision a Digital Certificate that will be stored in the users Personal Certificate Store in Windows.



1. Login to the PVWA as Vaultadmin01. Open the Web Options Configuration.

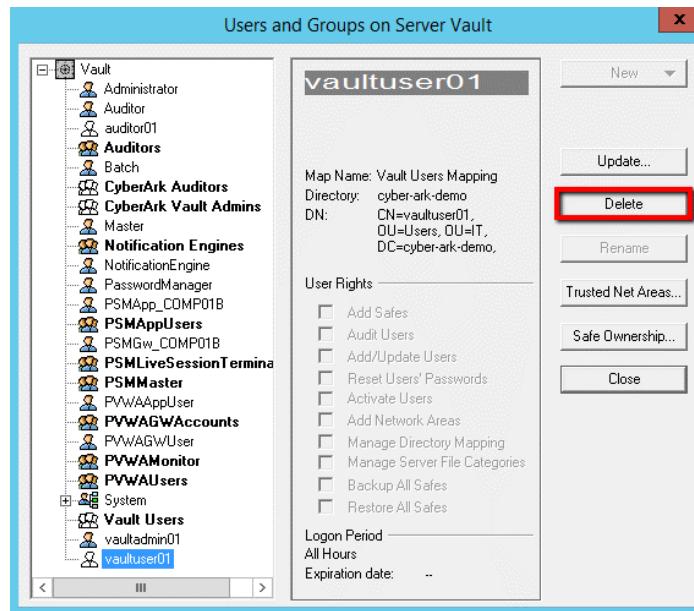
The screenshot shows the CyberArk Privileged Account Security (PVWA) interface. The top navigation bar has tabs: POLICIES, ACCOUNTS, APPLICATIONS, REPORTS, ADMINISTRATION (which is highlighted with a red box), and Administrator. Below the navigation is a 'Setup Wizard' icon and a 'Customize' button. The main content area is titled 'System Configuration'. It contains two sections: 'Component Settings' and 'Central Policy Manager'. In 'Component Settings', there is a table with columns 'Name' and 'Component'. The 'Name' column lists 'Options', 'Safe Templates', 'LDAP Integration', 'Notification Settings', and 'Platform Management'. The 'Component' column lists 'Web Access', 'Vault', and 'Platform Management' each with edit icons. A red box highlights the 'Options' entry in the 'Name' column. An 'Export All ...' button is at the bottom right of the table. In the 'Central Policy Manager' section, there is a dropdown menu set to 'PasswordManager', and buttons for 'CPM Settings' and 'Auto-detection'.

2. Navigate to Authentication Methods > pki and Enable PKI authentication.

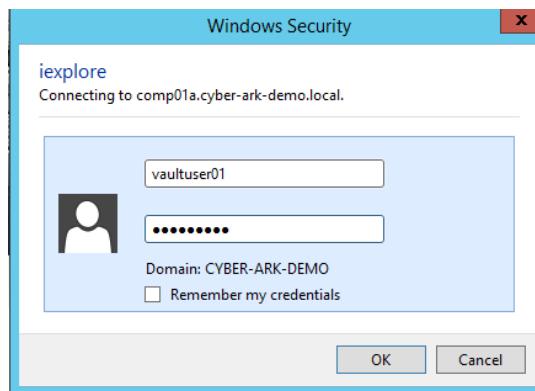
The screenshot shows the 'Options' dialog box. On the left is a tree view of configuration categories. The 'Authentication Methods' category is expanded, and its 'pki' sub-node is selected and highlighted with a red box. On the right is a 'Properties' grid. The 'Name' column lists properties: 'Id', 'DisplayName', 'Enabled', 'MobileEnabled', 'LogoffUrl', 'UseVaultAuthentication', 'UserRadius', 'UsLDAP', 'SignInLabel', and 'UsernameFieldLabel'. The 'Value' column shows their current values: 'pki', 'pki', 'Yes' (which is highlighted with a red box), 'No', 'No', 'No', 'No', 'No', and '''. At the bottom of the grid, there is a note: 'Enabled Whether or not the authentication module is enabled for use.' At the very bottom of the dialog are buttons for 'Help', 'Notifications', 'Export', 'Apply', 'OK' (which is highlighted with a red box), and 'Cancel'.



3. Login to the PrivateArk client as administrator and delete your vaultuser01 user:



4. Log off of the components server and log back in as vaultuser01.
5. Using Internet Explorer (not FF or Chrome) browse to <https://dc01.cyber-ark-demo.local/CertSrv>. If prompted login as vaultuser01/Cyberark1.





6. Click Request a certificate.

**Welcome**

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

**Select a task:**

[Request a certificate](#) Request a certificate

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

7. Click User Certificate.

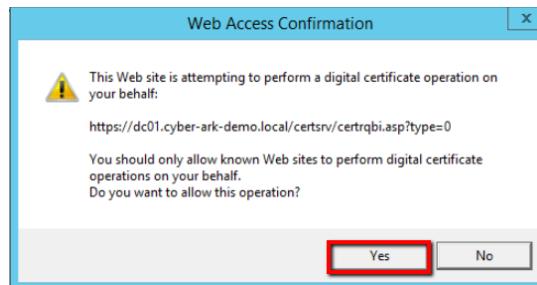
**Request a Certificate**

Select the certificate type:

[User Certificate](#) User Certificate

Or, submit an [advanced certificate request](#).

8. Click yes to the warning.





9. Click Submit.

Microsoft Active Directory Certificate Services -- cyber-ark-demo-DC01-CA [Home](#)

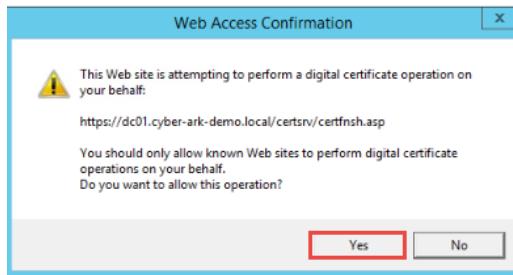
**User Certificate - Identifying Information**

No further identifying information is required. To complete your certificate, press submit.

[More Options >>](#)

**Submit >**

10. Click yes to the warning.



11. Click Install this certificate.

Microsoft Active Directory Certificate Services -- cyber-ark-demo-DC01-CA [Home](#)

**Certificate Issued**

The certificate you requested was issued to you.

[Install this certificate](#)

Save response

12. You should receive the following successful message.

Microsoft Active Directory Certificate Services -- cyber-ark-demo-DC01-CA

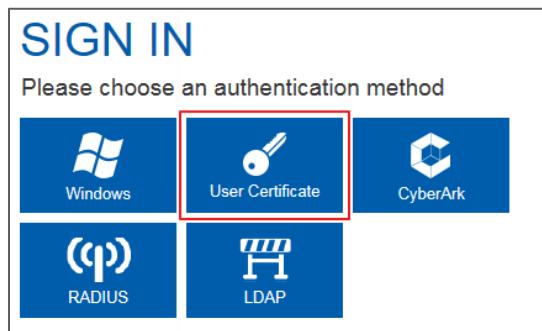
**Certificate Installed**

Your new certificate has been successfully installed.

13. Browse to the PVWA using the LB'er VIP or at URL <http://comp01X.cyber-ark-demo.local/passwordvault/> and choose User Certificate authentication.

14. A note on the behavior of PKI Authentication using IE on Windows.

- If the URL is in the Intranet Zone and the certificate is valid, the user will be authenticated successfully and passed directly to the accounts page.
- If the URL is in the Trusted Sites Zone and the certificate is valid, the user will be prompted to confirm the certificate.

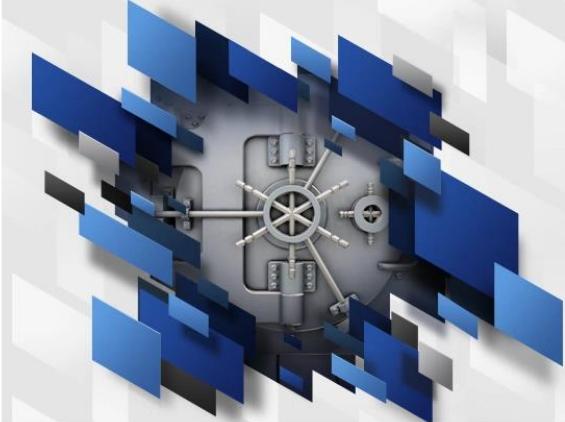


## Two Factor Authentication (2FA)

Now that you have tested the different types of authentication, try to use a combination of two methods (ONE IIS + ONE Vault) to enforce a Two Factor Authentication policy for vaultadmin01. To accomplish this you must combine a primary and a secondary authentication method.

In CyberArk There are 2 groups of authentications.

PVWA (IIS) level or Primary authentication	<ul style="list-style-type: none"> <li>Windows, Oracle SSO, PKI (Client Certificate) RSA, SAML.</li> </ul>
Vault level or Secondary authentication	<ul style="list-style-type: none"> <li>CyberArk</li> <li>LDAP, RADIUS</li> </ul>



## SIGN IN

Enter Token

**Sign in**

Copyright © 1999-2016 CyberArk Software Ltd. All Rights Reserved.  
Version 9.7.0 (9.70.0.403) [About](#) | [Mobile version](#)

## EPV Implementations

In this section you will create several accounts and **CPM** usages according to the customer's requirements. Please read the requirements set out by the customer carefully.

### Windows Requirements

- The Customer has one Domain Controller (10.0.0.2) and one windows server in the domain (10.0.10.50).
- The domain administrator account is **admin01**.
- The local administrator account on the domain member (10.0.10.50) is **localadmin01** (the password for the local admin account is unknown).
- On the domain member there is a scheduled task (**SchedTask01**) that runs under the **localadmin01** user and is programmed to send the vault administrator (**vaultadmin01**) an email every time it runs.
- Note that although the scheduled task runs under the credentials of localadmin01, only admin01 has permissions to change the password for SchedTask01.
- In order to run the scheduled task run the following command:
  - `schtasks /run /s 10.0.10.50 /tn schedtask01`.
- winadmin01 is a member of the WindowsAdmins group in LDAP. Members of the WindowsAdmins group should be given permissions on all Windows accounts.

### UNIX Requirements

- The Customer has one Linux server (10.0.0.20).
- The root account on the server is called **root01**.
- The account *linuxadmin01* is a member of the *LinuxAdmins* group in LDAP.
- Members of the *LinuxAdmins* group must be granted permissions on all the Linux accounts.

### Database Requirements

- The Linux server mentioned above (10.0.0.20) also hosts an oracle database.
  - database name is **xe**.
  - The port is **1521**.
  - The root account on the database is called **dba01**.

In addition, there is an application on the Linux server that connects to the Oracle database *using* the **dba01** credentials. The credentials are stored in the text file **/var/opt/app/app01.ini**. When the **CPM** changes the password for *dba01*, it must also change the password stored in the **app01.ini** file. Note that only *root01* has permissions to change the password in the file.

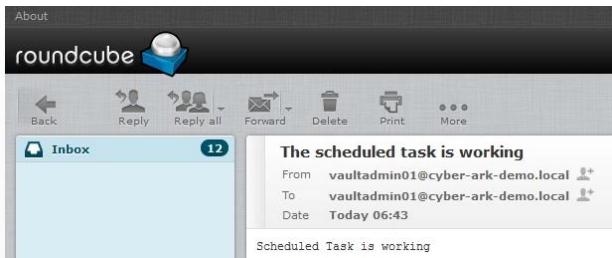
- *OracleAdmin01* is a member of the **OracleAdmins** group in LDAP. Members of the **OracleAdmins** group should be granted permissions on all oracle accounts.

### Based on the requirements mentioned above:

1. Add the required privileged accounts to the system, including their dependencies. You will need to create the proper Safes and duplicate the relevant platforms in order to do so. You may add accounts manually or by using the accounts discovery mechanism (Hint: Accounts Discovery can detect Windows dependencies automatically).



2. Windows accounts should be managed by CPM\_WIN and all Linux and DB accounts should be managed by CPM\_UNIX. Use the CPMs to change the passwords (reconcile if needed).
3. Make sure all dependencies are changed:
  - a. **localadmin01** - run the scheduled task and verify **vaultadmin01** receives the email;
  - b. **dba01** - verify that the password in **app01.ini** is updated<sup>12</sup>.



```
[root@server2 app]# cat app22.ini |grep Password
ShowPasswordDialog=N
Password=@Ne8P1K*
[root@server2 app]#
[root@server2 app]#
```

4. Assign the LDAP users and/or groups the required permissions on the relevant safes ensuring the users (winadmin01, linuxadmin01 and oracleadmin01) can access the relevant accounts.

<sup>1</sup> Hint: add the INICofigFile usage in the Oracle platform and make sure the "SearchForUsages" parameter in the platform is set to YES  
<sup>2</sup> use root/Cyberark1 to login to the UNIX server to verify the password in app01.ini changed.

## Install PSM/PSMP

The Customer has purchased CyberArk's **Privileged Session Management** (PSM) in order to monitor and record and activity related to privileged accounts in the network:

PSM	2 servers (PSM Farm IP: <b>10.0.22.1</b> )
PSMP (SSH Proxy)	1 server ( <b>10.0.1.16</b> )

**Note:** The customer requires that connections to all Windows and Oracle accounts be done via Load Balanced PSM Servers. Connections to the UNIX devices can be done via the Load Balanced PSM servers, or PSMP.

### In the following sections you will be asked to:

1. Install a standalone PSM
2. Secure and harden the PSM server
3. Enable the PSM and make sure you can connect to all target devices (Windows, UNIX and Oracle).
4. Make sure you can see the relevant recordings for each session.
5. Install the 2nd PSM server and test connections via a load balancer.
6. Install PSMP and make sure you can connect to the UNIX device via the PSMP.

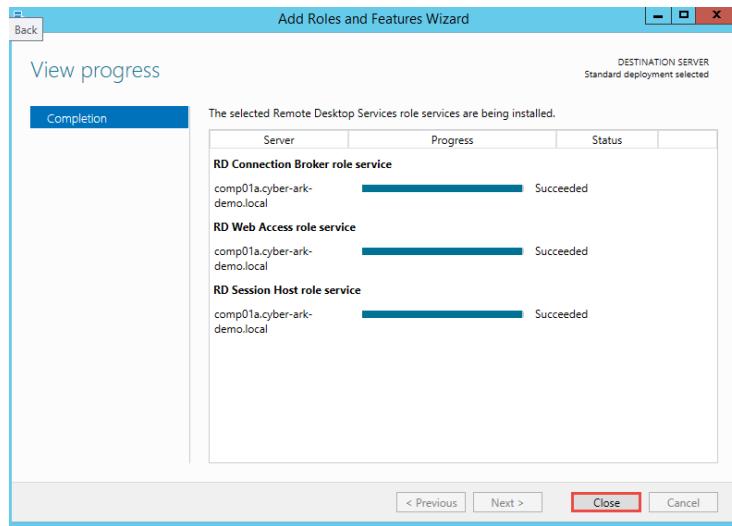


## Standalone PSM Installation

### PSM Installation

Installation of Microsoft's Remote Desktop Services is a pre-requisite for PSM and must be completed while logged in as a Domain User that is a member of the local administrators group on the PSM Server.

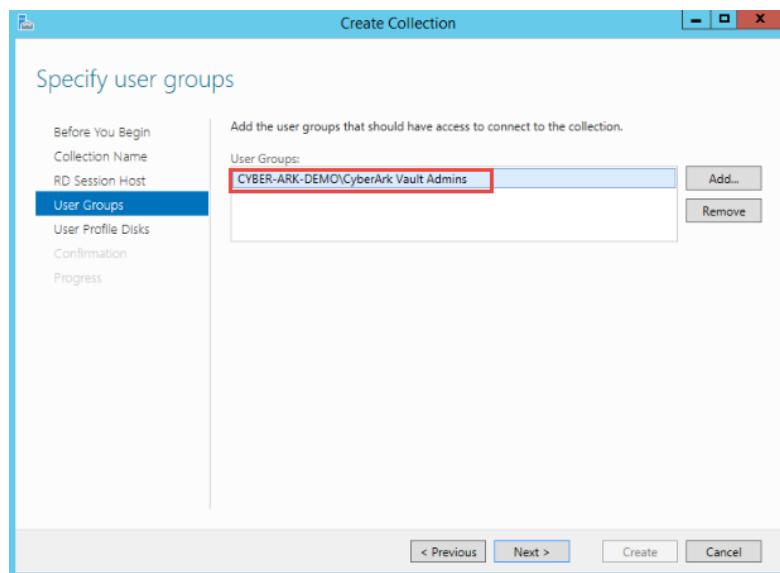
1. Open the PAS Installation Guide v10.1 and proceed to page 154, section RDS on a PSM Server:
2. Sign out of the Comp01A server and sign as domain user Admin01@cyber-ark-demo.local.
3. Follow the instructions to install Remote Desktop Services.
  - a. Complete steps 1 through 7.
  - b. After the server reboots, ensure that you sign in with the same domain user, Admin01@cyber-ark-demo.local.
  - c. Be patient, the installation wizard will restart automatically. Start Server Manager if you have prevented it from starting automatically.
  - d. When complete and you see the following Window, proceed to the next step.



4. Complete steps 8 and 9, to create a session collection.
  - a. Name the session collection "PSM\_servername". So the session collection for server comp01a will be "PSM\_comp01a"
  - b. Remove CYBER-ARK-DEMO\Domain Users and replace with CYBER-ARK-DEMO\CyberArk Vault



Admins.

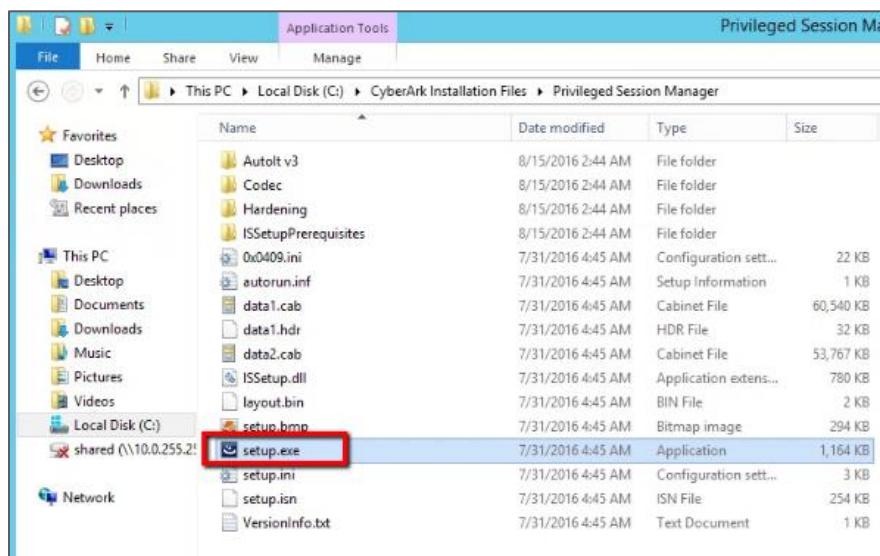


5. Select the collection PSM\_comp01A
  - a. In PROPERTIES, Choose tasks, Edit Properties.
  - b. Navigate to Security and clear the box "Allow connections only from computers running Remote Desktop with Network Level Authentication"
  - c. Select OK to save and exit.
6. Close Server Manager

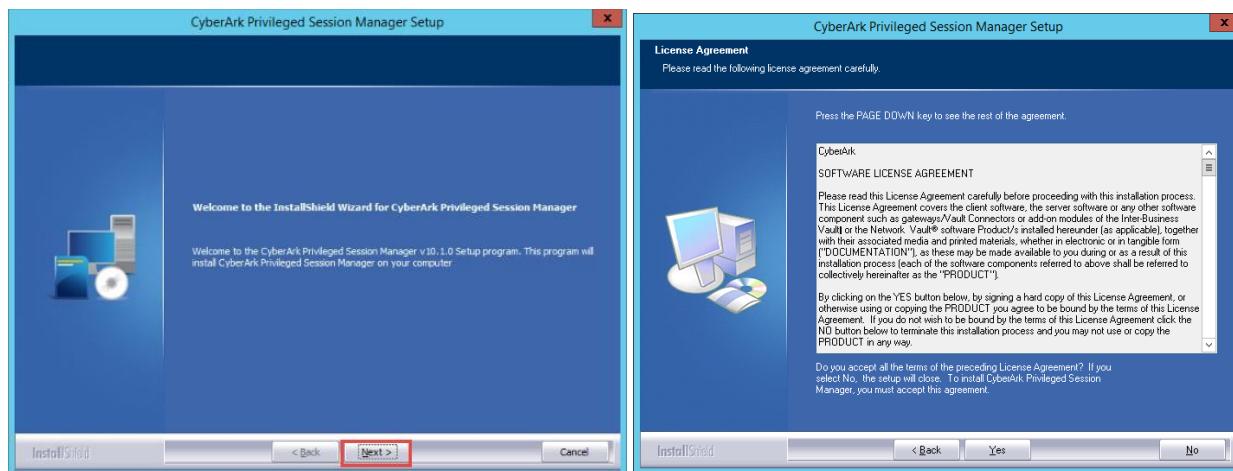
### **Install the PSM**

**Note:** To enable RemoteApp program features, PSM installation must be completed while logged in as a domain user, with local Administrator rights. Install the PSM logged in as cyber-ark-demo.local\Admin01.

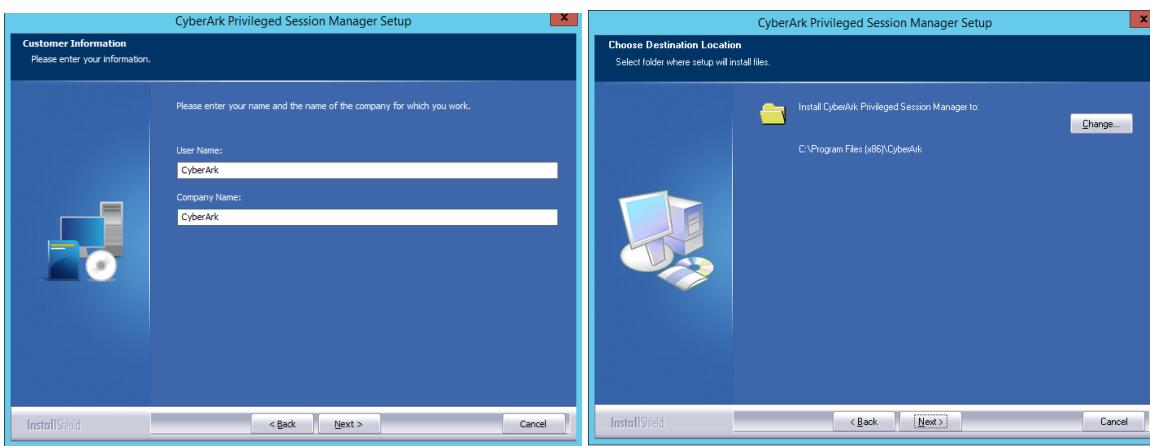
1. Go to **C:\CyberArkInstallationFiles\Privileged Session Manager** and double click **setup.exe**



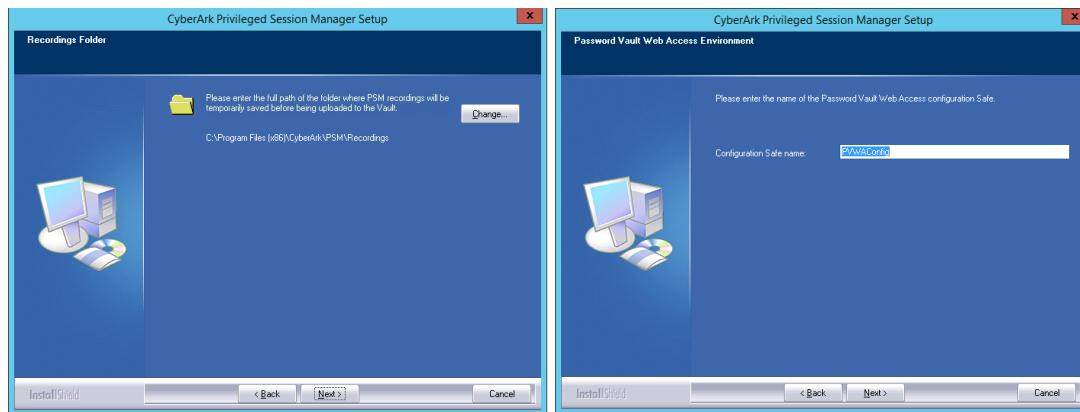
2. Click **Next** on the welcome screen, then **Yes** to agree to the license agreement



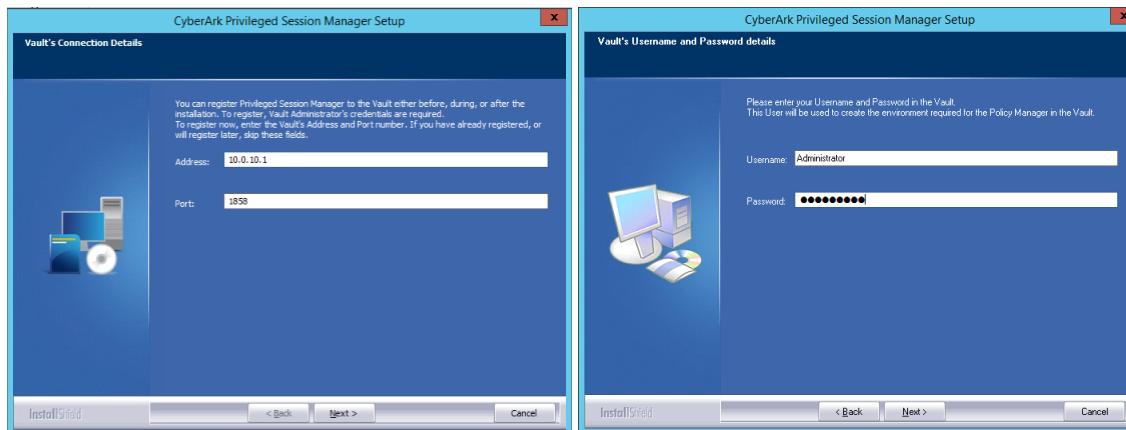
3. Enter a company name, click **Next**, then leave the default destination folder and click **Next**.



4. Leave the default recordings temporary folder and click **Next**, then leave the default *Configuration safes* name and click **Next**. The first part of the installation now takes place, there will be a short delay until the next screen appears.

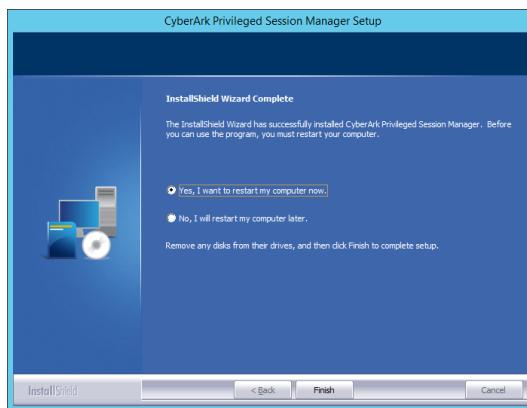


5. Enter the **IP Address** of your vault (i.e., **10.0.10.1**) and click **Next**, then enter the username **Administrator**, password **Cyberark1** and click **Next**.





6. Select “Yes, I want to restart my computer now” selected and click **Finish**.



## PSM Post Installation and Hardening Tasks

**Note:** The following tasks must be performed by an administrator of the Component server, for example, Admin01 or the local Administrator user.

### Hardening the PSM

Open the PAS Installation Guide v10.1, and go to page 169 “Post installation tasks” and complete the following sections.

1. Check the installation log files.
2. “Disable the screen saver for the PSM Local Users”
3. “Configure users for PSM sessions”.
  - a. Ensure “User cannot change password” and “Password never expires” is selected for both users.
4. “Harden the PSM server machine”.
  - a. Continue to page 179 “PSM server hardening workflow”.

### Run the Hardening Script

1. Enable PowerShell Scripts on the PSM machine, page 180
  - Note: Run PowerShell as Administrator
2. Modify the PSM Hardening Script, page 181
  - Enable PSM to Connect to Web applications
  - Do not make any other changes to the script.
  - Take note and review the settings defined in this section.
3. Run the PSM Hardening Script, page 181

- Type “Yes” when prompted to remove all member of the RemoteDesktopUsers group
  - Open Computer Management and add the “CyberArk Vault Admins” group to the RemoteDesktopUsers group.
4. Review the PSM Hardening Script Output Log File, page 181.
- Actions taken by the script are detailed in the log.
  - Return the security level for running PowerShell scripts to “restricted”.

**After running the Hardening Script, page 182**

1. Hide PSM Local Drives in PSM Sessions
  - a. Restrict all drives
2. Block Internet Explorer Developer Tools
3. Block Internet Explorer context menu
  - a. Restrictions key must be added.
  - b. NoContextMenu DWord parameter must be added

**Configure AppLocker Rules**

1. Verification before running the AppLocker Script.
  - Note: Run PowerShell as Administrator
2. Run the AppLocker Script.
  - Review the sections of the PSMConfigureAppLocker.xml.
  - Locate the Microsoft IExplore processes section.
    1. Add the following line to support PSM-SSH connections.

```
<Application Name="Java" Type="Exe" Path="C:\Program Files (x86)\Java\jre1.8.0_101\bin\ssvagent.exe" Method="Hash" />
```

**Note:** The above line can be found on your component servers in file, “C:\3<sup>rd</sup> Party Installation Files\AppLocker-Rules-Examples.xml”

2. Remove the comments from this section to enable Microsoft Internet Explorer.
3. After the changes, the Microsoft IExplore processes section should look like the following image.

```
<!-- Microsoft IExplore processes -->
<Application Name="IExplore32" Type="Exe" Path="c:\Program Files (x86)\Internet Explorer\iexplore.exe" Method="Publisher" />
<Application Name="IExplore64" Type="Exe" Path="c:\Program Files\Internet Explorer\iexplore.exe" Method="Publisher" />
<Application Name="Java" Type="Exe" Path="C:\Program Files (x86)\Java\jre1.8.0_101\bin\ssvagent.exe" Method="Hash" />
```

- Manually confirm the executable paths in each line that begins with “Application Name=” in this section.

#### Run the Automatic PSM AppLocker Configuration Script

```
PS C:\Windows\system32> cd 'C:\Program Files (x86)\CyberArk\PSM\Hardening'
PS C:\Program Files (x86)\CyberArk\PSM\Hardening> .\PSMConfigureAppLocker.ps1
CyberArk AppLocker's configuration script ended successfully.
PS C:\Program Files (x86)\CyberArk\PSM\Hardening>
```

3. Return the Security Level for Running PowerShell after Running the AppLocker Script.

**Note:** Review “Automatic hardening in ‘In Domain’ deployments”. We will not be executing these procedures in the lab but you should review and become familiar with them.

#### Go to “(Optional) Configure the PSM Server Machine for Web Applications”

We have already run the hardening script with parameter \$SUPPORT\_WEB\_APPLICATIONS=true, but there are still settings that need to be configured. In this section beginning on page 221, configure the following:

“To Configure the PSM Server Machine for Web Applications”, skip procedures 1 and 2 and complete only the following procedures.

3. Disable IE Enhanced Security Configuration.
4. Configure the Internet Explorer First Run settings.

#### Deactivate UAC on the PSM Server

This step is required to support PSM Web Applications



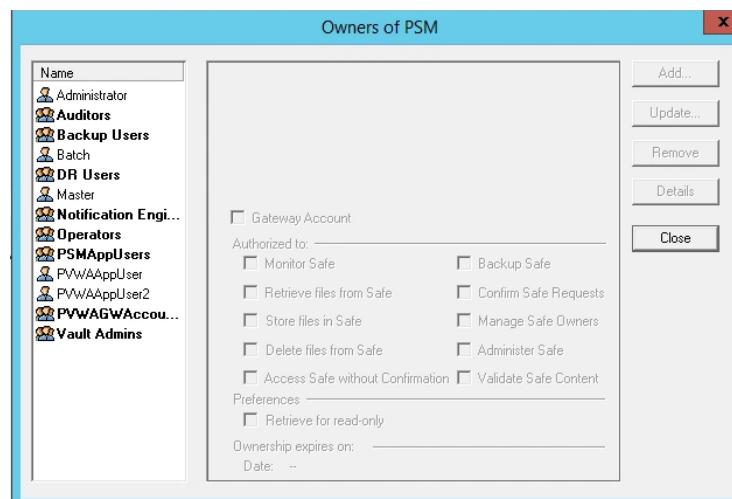
1. From the Start Menu, run "Regedit.exe".
2. Navigate to "HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system".
3. Update "EnableLUA" from 1 to 0.
4. Restart the PSM Server.

## PSM Testing and Validation

**Note:** Before testing the connections via the PSM we also need to grant **PVWAAppUser1** permissions on the relevant PSM Safes, otherwise connections from the 2<sup>nd</sup> PVWA will not work.

1. Before you can grant PVWAAppUser1 permissions on the PSM safes, you must first add the built-in CyberArk Administrator user to the **PSMMaster** group. After adding Administrator to the **PSMMaster** group, add PVWAAppUser1 to the following safes with permissions as described below.

Safe	Permissions
<b>PSM</b>	<b>List Files, Retrieve Files and Update Files</b>
<b>PSMLiveSessions</b>	<b>List Files</b>
<b>PSMSessions</b>	<b>Create Files</b>
<b>PSMUnmanagedSessionAccounts</b>	<b>List Files, Create Files, Update Files, Update File Properties, View Owners, Use Password, Create/Rename Folder and Manage Safe Owners</b>





2. After successful PSM installation and configuration of the 2<sup>nd</sup> PSM server, remove the built-in administrator user from the **PSMMaster** CyberArk group.
3. Login to the PVWA as **vaultadmin01** and enable the **PSM** in the **Master Policy**.

The screenshot shows the CyberArk Privileged Vulnerability Assessment (PVWA) interface. The top navigation bar includes links for POLICIES, ACCOUNTS, APPLICATIONS, REPORTS, and ADMINISTRATION. The main content area is titled "Policies > Master Policy" and "Master Policy". The left sidebar under "POLICIES" lists "Master Policy", "Policy by Platform", and "Access Control (Safes)". The right pane displays policy rules categorized under "Privileged Access Workflows", "Password Management", "Session Management", and "Audit". A red box highlights the "Value" column for the "Audit" section, which contains three entries: "Active", "Active", and "Active".

4. Go to **ADMINISTRATION > Options > Privileged Session Management UI** and set *ConnectPSMWithRDPActivex* to **Never** so that RDPFile will be used to establish connections regardless of the browser. If ByBrowser is selected, IE will use ActiveX to establish connections but alternate browsers will use RDPFile. This is necessary to use the RemoteApp feature with alternate browsers like Firefox and Chrome.
5. Click OK to save.

The screenshot shows the "Options" dialog in CyberArk PVWA. The left pane lists categories such as Chart Categories, Web Charts, Authentication Methods, Default Safe Authorizations, Dual Control, Ticketing Systems, Connection Components, and Privileged Session Management UI. The "Privileged Session Management UI" category is expanded, showing sub-options like Search Sessions, General, Recordings Displayed Column, Live Sessions Displayed Color, and Account Details Session Recording. The right pane displays the "Properties" table with the following rows:

Name	Value
RedirectToRecordingDetailsOnPlay	No
ConnectPSMWithRDPActivex	Never
NonIERemoteDesktopAccess	RDPFile
UseRemoteApp	Yes
PSMandPTAIntegration	No

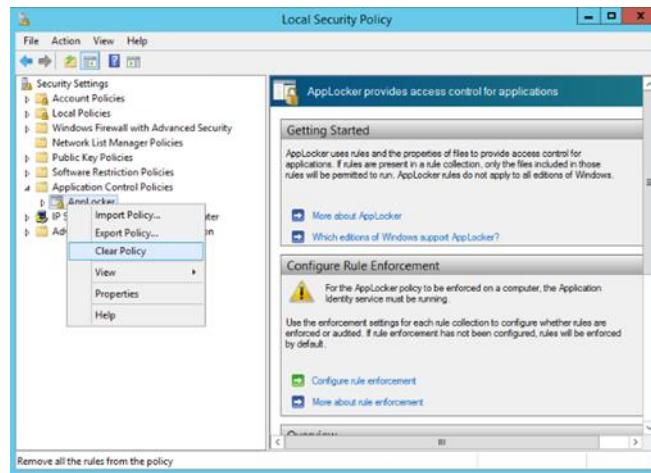
A red box highlights the "Value" column for the "ConnectPSMWithRDPActivex" property, which is set to "Never".

6. Attempt connecting to the customer's target devices using the relevant PSM Connection Components for all accounts (PSM-SSH, PSM-RDP, PSM-WinSCP and PSM-SQL\*).



## 7. Troubleshoot issues as needed.

- Known Issue: PSMSR126E and / or PSMSC036E error is displayed during PSM-SSH connection testing, it may be necessary to clear Applocker policies, and then reapply them. Launch secpol.msc from the Run window to clear the Applocker policies and retry the connection component. Reapply the Applocker policies, then test again. If a first attempt times out, retry a second time.



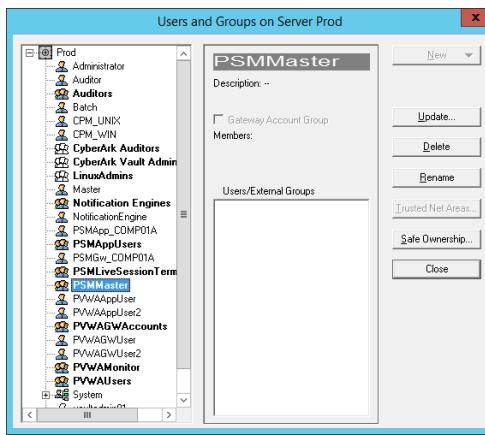


## Load Balanced PSM Installation

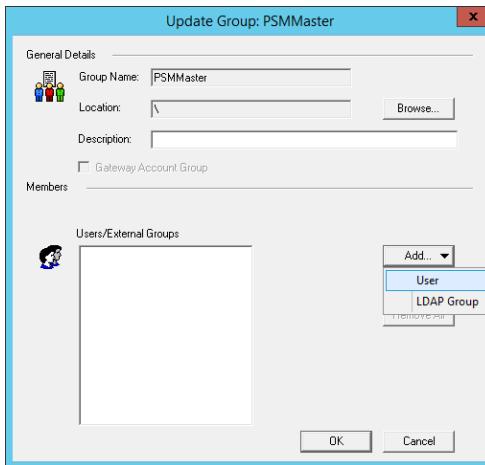
Note: in this section we will install the 2<sup>nd</sup> PSM server and test connecting to the PSM servers via a load balancer.

### Install 2nd PSM

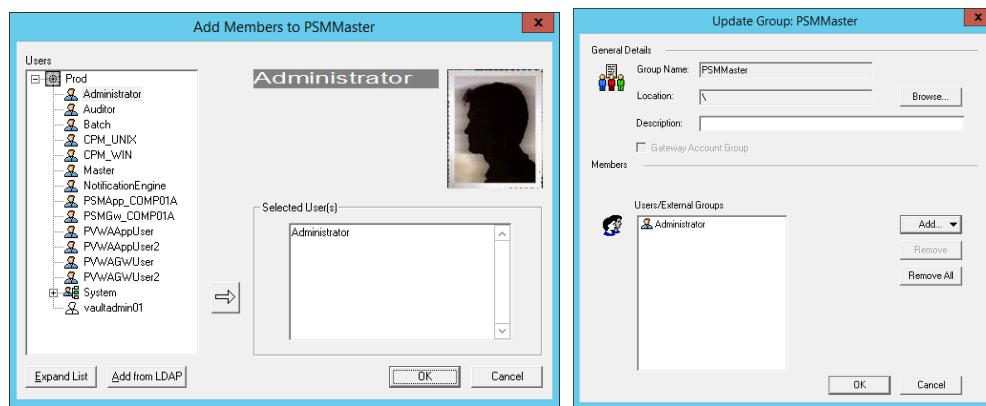
1. **Prior** to installing the 2<sup>nd</sup> PSM you must first add the **Administrator** user to the **PSMMaster** Group. Log in to **PrivateArk** as **Administrator** and go to **Tools > Administrative Tools > Users & Groups**. Select **PSMMaster** and Click **Update**.



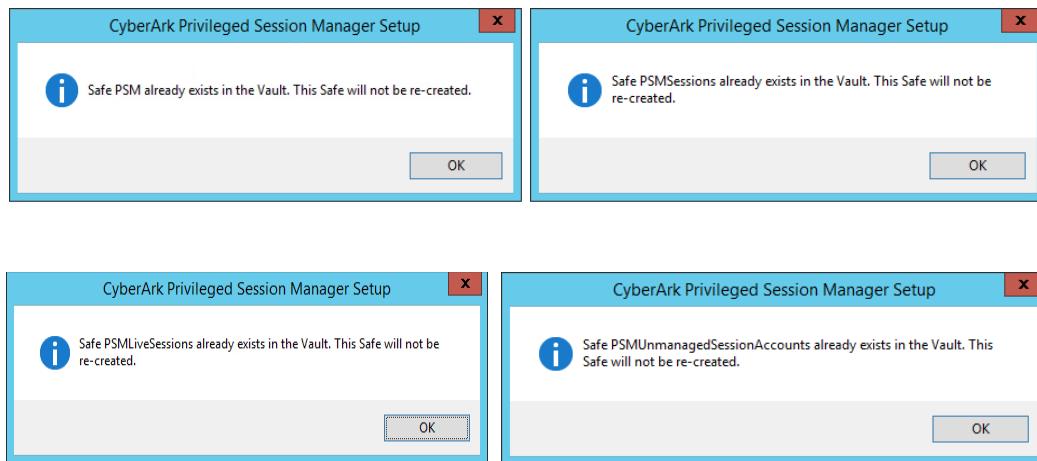
2. Click **Add** then **User**.



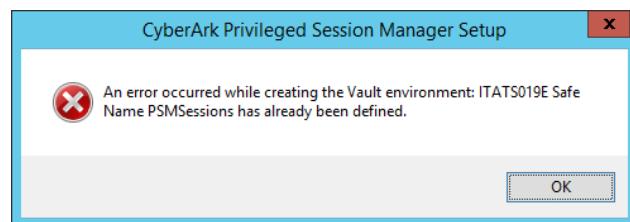
3. Double-click **Administrator**, then click **OK**, then click **OK** to update the group membership.



4. Log on to **Comp01b** as **cyber-ark-demo\admin01** and repeat the steps for [installing the 1<sup>st</sup> PSM](#) (including the installation and configuration of Remote Desktop Services, as well as the post installation and hardening steps). You will receive the following warnings during the installation of PSM software. This is normal.



5. If you see the error message ITATS019E as shown in the graphic below, this indicates that the CyberArk built-in Administrator user is not a member of the PSMMaster group. Uninstall PSM and add the CyberArk built-in Administrator user to the PSMMaster group, then proceed with the PSM installation.



6. Before configuring the Load Balancer, test the connections via the 2<sup>nd</sup> PSM server by changing the PSM-ID from **PSMServer** to **PSM-COMP01B** in the platform settings for all relevant platforms.

Name	Value
ID	PSM-COMP01B
SubnetPolicy	No
SessionRecorderSafe	PSMRecordings
MaxSessionDuration	-1
ShowRecordedSessionNotification	Yes
RecordedSessionNotificationDisplayTime	5
ShowLiveMonitoringNotification	Yes
LiveMonitoringNotificationDisplayTime	5
DisableDualControlForPSMConnections	No
EnablePrivilegedSSO	Yes
UsePersonalPassword	No

## Configure PSM Load Balancing

1. From **Comp01a** log on to the load balancer using a browser: <https://10.0.0.5:444> (*username: admin/password: admin*).
2. Navigate to **Manage > Farms** and click on the **Add New Farm** icon in the Actions column, to configure a new farm.
3. Set the *Farm Description Name* to **PSM** and select **L4xNAT** in *profile*, and choose **Save & Continue**.
4. Select Virtual IP: eth0:1>**10.0.22.1**, and Virtual Port: **3389** for RDP.
5. Click on **Save** then the **Edit the PSM Farm** icon.



## Manage::Farms

Farms table					
Name	Virtual IP	Virtual Port(s)	Status	Profile	Actions
pvwa	10.0.22.1	80	Green	http	
psm	10.0.22.1	3389	Green	l4xnat	 

6. Next, change the *Persistence mode* to **IP Persistence** and select **Modify**.

Farm's name \*service will be restarted.  
psm

Protocol type \*the service will be restarted.  
TCP

NAT type \*the service will be restarted.  
NAT

Load Balance Algorithm \*the service will be restarted.  
Weight: connection linear dispatching by weight

Persistence mode \*the service will be restarted.  
**IP persistence**  IP persistence

Source IP Address Persistence time to limit \*in secs, only for IP persistence.  
120

Use FarmGuardian to check Backend Servers.  
Check every  secs.  
Command to check   
 Enable farmguardian logs

Farm Virtual IP and Virtual port(s) \*the service will be restarted.  
10.0.22.1  3389

7. Scroll down to section 'Edit real IP servers configuration' and select the 'Add Real Server' link in the Actions column.
8. Add both PSM server IP addresses to the configuration and select the 'Save Real Server' link after each entry.

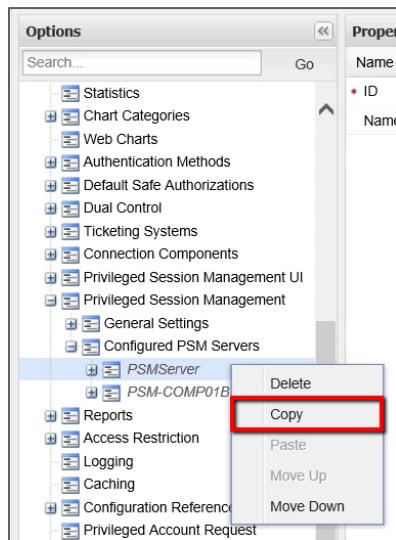
Edit real IP servers configuration						
Server	Address	Port	Weight	Priority	Actions	
0	10.0.20.1	3389	1	1		
1	10.0.21.1	3389	1	1		

9. Review the Farms Table and ensure that the PSM Farm is started.

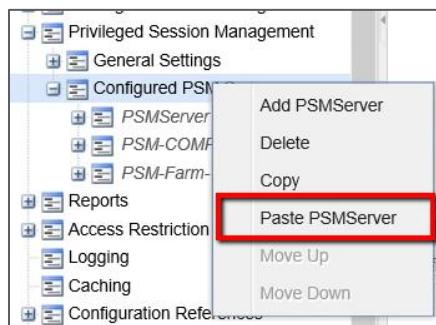
Farms table					
Name	Virtual IP	Virtual Port(s)	Status	Profile	Actions
PVWA	10.0.22.1	80	Green	http	
PSM	10.0.22.1	3389	Red	l4xnat	 



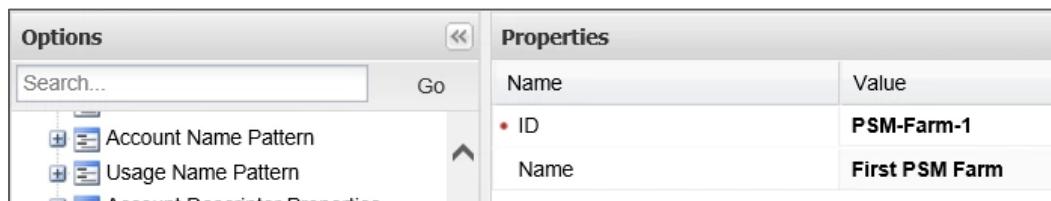
10. Exit the Zen Load Balancer GUI.
11. Login to the PVWA as **vaultadmin01** and go to **ADMINISTRATION > Options > Privileged Session Management > Configured PSM Servers** and copy PSMServer.



12. Right click on **Configured PSM Servers** and click on **Paste PSMServer**.

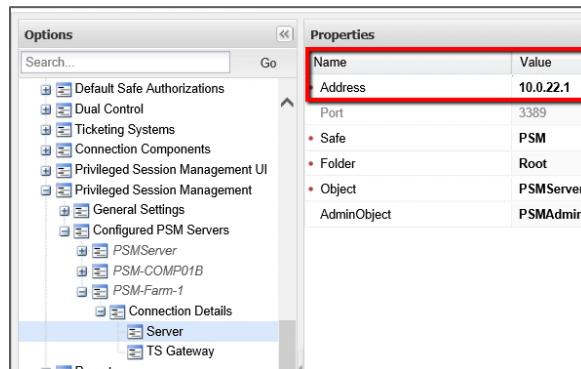


13. Go to the newly added **PSMServer** and change the ID to **PSM-Farm-1** and the name to **First PSM Farm**.





14. Expand PSM-Farm-1. Select **Connection Details > Server** and change the IP address to that of your PSM Farm virtual IP, 10.0.22.1. Click on **Apply** and **OK** to save the changes.



15. Next, change the *PSM ID* for the Unix platform you previously created to **PSM-Farm-1**.

16. At an Administrative Command Prompt, run IISRESET on both comp01x servers.

17. Try to connect to different target devices using the PSM farm (you can run multiple sessions at the same time), and look at the LB to see where the session lands using the monitoring option of the LB. try to do live monitoring as well using *Auditor01*.

Real servers status 2 servers, 2 active						
Server	Address	Port(s)	Status	Pending Conns	Established Conns	
0	10.0.20.1	3389	●	0	2	
1	10.0.21.1	3389	●	0	1	



## PSMP Installation

### Install PSMP

In this exercise you will configure a Linux server to run CyberArk's **PSM SSH Proxy** (PSMP) server. See the *Installing the Privileged Session Manager SSH Proxy* section of the *Privileged Account Security Installation Guide* for a full explanation of all the required steps.

### Install Linux prerequisites

1. Confirm that all the prerequisites installed properly by running `./psmpcheck.sh`. The script contains the following command: `yum list installed |grep 'redhat-lsb.x86\|elfutils.i686\|glibc.i\|ncurses-libs.i\|libuuid.i\|libgcc.i\'` and should return the following:

```
[root@centos ~]# ./psmpcheck.sh
elfutils.i686          0.152-1.el6      @elfutils-0.152-1.el6.i686
glibc.i686              2.12-1.132.el6_5.2
libgcc.i686             4.4.6-4.el6      installed
libuuid.i686            2.17.2-12.7.el6  installed
ncurses-libs.i686        5.7-3.20090208.el6
redhat-lsb.x86_64        4.0-7.el6.centos @base
[root@centos ~]# _
```

### Install the PSMP package

Before running the installer, we need to make a few advance preparations.

First, we will create an administrative user on the PSM SSH Proxy server and edit the vault.ini file, then create a credential file for the built-in administrator user so the installer can create the vault environment for the PSMP. Finally, we will edit the PSMP parameters file to specify the installation directory and accept the End User License Agreement.

1. Administrative users can connect to the PSMP machine to perform management tasks on the machine itself without being forwarded to a target machine. In addition to the built-in root users, the PSMP identifies proxymng as an administrative user when they connect to the PSMP server. Run **useradd proxymng** and **passwd proxymng as shown**. Set the password as Cyberark1

```
[root@psmp01 ~]# useradd proxymng
[root@psmp01 ~]# passwd proxymng
Changing password for user proxymng.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```



2. Next we need to inform the PSMP installer where to find the vault server on the network.  
Change directories to **/root/PSM-SSHProxy-Installation/** directory and update the **vault.ini** file using the **VI** editor.

```
cd /root/PSM-SSHProxy-Installation/  
vi vault.ini
```

3. Update the address vault to the VIP address of your vault server (e.g. **10.0.10.1**). Use the arrow keys to move the cursor to the text you want to amend, type **\*R** (case-sensitive) to make the changes and hit **Esc** to stop editing.
4. When finished, enter **:wq!** to save the file and quit vi.

```
Vault = "Demo Vault"  
ADDRESS=10.0.10.1  
PORT=1858
```

5. Now we need to create a credential file for the administrator user, who will authenticate to the Vault and create the **Vault** environment during installation.
  - a. Change directories to **/root/PSM-SSHProxy-Installation**.
  - b. Enter the following command to assign read, write and execute permissions to CreateCredFile, “**chmod 755 CreateCredFile**” as show in the graphic below.

```
[root@psmp01 PSM-SSHProxy-Installation]# chmod 755 CreateCredFile  
[root@psmp01 PSM-SSHProxy-Installation]# ls -l  
total 81432  
-rw-r--r--. 1 root root 12332224 Jun 19 11:44 accountuploader  
-rw-r--r--. 1 root root 33886828 Jun 19 11:44 CARKpsmp-7.2.11-0.i386.rpm  
-rwxr-xr-x. 1 root root 11959220 Jun 19 11:44 CreateCredFile  
-rw-r--r--. 1 root root 318 Jun 19 11:44 createPSMPenv  
-rw-r--r--. 1 root root 16008080 Jun 19 11:45 icudt421.dat  
drwxr-xr-x. 4 root root 4096 Jun 19 07:35 Pre-Requisites  
-rw-r--r--. 1 root root 467 Jun 19 11:45 psmpparms.sample  
-rw-r--r--. 1 root root 9174704 Jun 19 11:45 sshd  
-rw-r--r--. 1 root root 1969 Aug 13 12:49 Vault.ini
```

- c. Run **./CreateCredFile user.cred**, enter **Administrator** as the **Vault Username** and **Cyberark1** as the **Vault Password**. Accept the default values for the remaining prompts.



```
[root@psmp01 PSM-SSHProxy-Installation]# ./CreateCredFile user.cred
Vault Username [mandatory] ==> administrator
Vault Password (will be encrypted in credential file) ==> [REDACTED]
Disable wait for DR synchronization before allowing password change (yes/no) [No] ==>
External Authentication Facility (LDAP/Radius/No) [No] ==>
Restrict to Application Type [optional] ==>
Restrict to Executable Path [optional] ==>
Restrict to current machine IP (yes/no) [No] ==>
Restrict to current machine hostname (yes/no) [No] ==>
Restrict to OS User name [optional] ==>
Display Restrictions in output file (yes/no) [No] ==>
Command ended successfully
```

6. Next, we need to create and edit the psmpparms file to define the installation folder, and accept the End User License Agreement.

- Move *psmpparms.sample* to the **/var/tmp** directory and rename it to psmpparms using the command in the following example.

```
[root@psmp01 PSM-SSHProxy-Installation]#
[root@psmp01 PSM-SSHProxy-Installation]# mv psmpparms.sample /var/tmp/psmpparms
[root@psmp01 PSM-SSHProxy-Installation]#
```

- Edit the **psmpparms** file.

```
vi /var/tmp/psmpparms
```

- Edit the following lines and save the changes.

```
InstallationFolder=/root/PSM-SSHProxy-Installation
AcceptCyberArkEULA=Yes
```

```
[Main]
# -----
# The folder to which the installation CD was copied.
# -----
InstallationFolder=/root/PSM-SSHProxy-Installation

# -----
# Whether or not the CyberArk SSHD service should be installed.
# The CyberArk SSHD service is required for tunneling and for connecting with the SSH
# command in the following syntax:
# <ssh client> vaultuser@targetuser#domainaddress@targetmachine#targetport@targetpassword@proxyaddress
# -----
InstallCyberArkSSHD=Yes

# -----
# Whether or not you accept all the terms of the PSMP end user license agreement.
# This agreement is on the installation CD in the PSMProxy installation package.
# Open this agreement and read it carefully, then set this parameter to Yes.
# -----
AcceptCyberArkEULA=Yes

#PSMPAppUser=PSMPApp_<host_name>
#PSMPGWUser=PSMPGW_<hostname>
#PSMPConfigurationSafe=PWAConfig
```



- Run the PSMP installation by running **rpm -i CARKpsmp-10.1.0-44.x86\_64.rpm** from the PSMP installation directory (the version number in the screenshot may not be identical, you can type the first characters of the filename and then press tab to auto-complete).

```
[root@centos PSM-SSHProxy-Installation]# rpm -i CARKpsmp-10.1.0-44.x86_64.rpm
warning: CARKpsmp-10.1.0-44.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID 0
8beaa44: NOKEY
Installation process is starting...
```

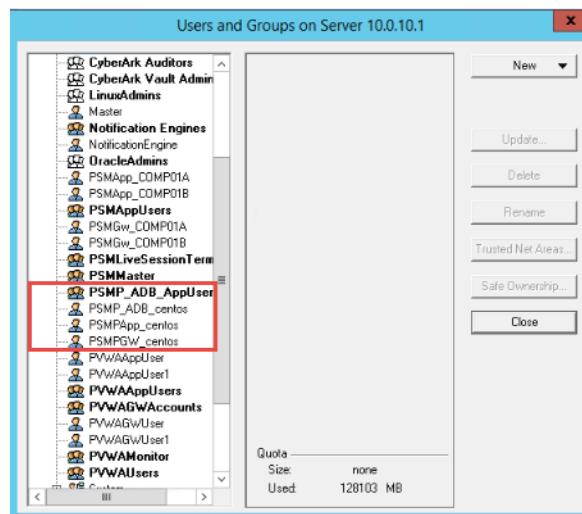
- Run **service psmpsrv status** or **/etc/init.d/psmpsrv status** to ensure that the server is running as the installation has completed

```
[root@psmp01 PSM-SSHProxy-Installation]# /etc/init.d/psmpsrv status
PSM SSH Proxy is running.
PSMP ADBridge is running.
```

- Review log using **cat /var/tmp/psmp\_install.log**

```
Wed Mar 2 11:33:47 EST 2016 | Updating [sshd]...
Wed Mar 2 11:33:47 EST 2016 | Configuring the [sshd_config] file...
Wed Mar 2 11:33:47 EST 2016 | Configuring [sshd_config] file has finished.
Wed Mar 2 11:33:47 EST 2016 | Configuring the [sshd] service initialization script...
Wed Mar 2 11:33:47 EST 2016 | Configuring the [sshd] service initialization script has finished.
Wed Mar 2 11:33:47 EST 2016 | Replacing the [sshd] executable...
Wed Mar 2 11:33:47 EST 2016 | Starting the [sshd] executable...
Wed Mar 2 11:33:48 EST 2016 | The [sshd] executable was started successfully.
Wed Mar 2 11:33:48 EST 2016 | Replacing the [sshd] executable has finished.
Wed Mar 2 11:33:48 EST 2016 | Updating [sshd] has finished.
Wed Mar 2 11:33:48 EST 2016 | Script execution has finished.
Wed Mar 2 11:33:48 EST 2016 | Installation process was completed successfully.
```

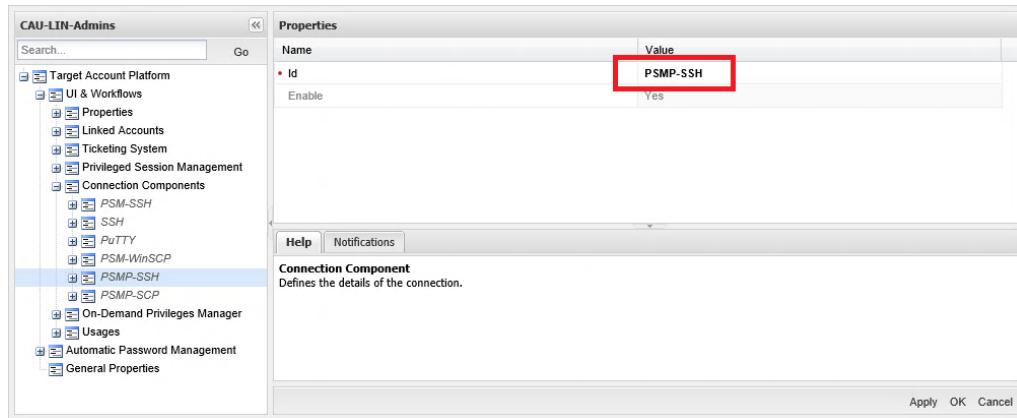
- Check that the **PSMPApp\_<hostname>** users and groups were added to the **Vault**.



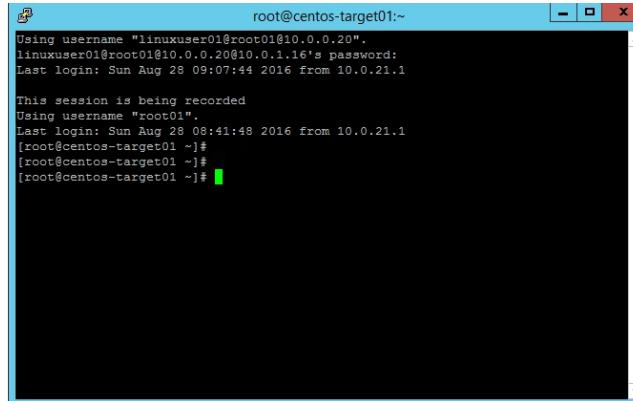


11. Add the PSMP-SSH Connection Component to the platform managing account

Root01@10.0.0.20. If the Platform managing the *root01* account was duplicated, you will need to manually create the reference to the *Connection Component*, as shown in the image below.



12. From the **Components** server, open **PuTTY**  and enter the following connection string in *Host Name* to verify that you can log in with *linuxadmin01* to the Linux Server (10.0.0.20) using *root01* via the PSMP: **linuxadmin01@root01@10.0.0.20@10.0.1.16**.



13. Make sure you can see the recording of your session in the PVWA

## Troubleshooting

1. If the installation fails you can view errors in the following logs:

- /var/tmp/psmp\_install.log** – This log file describes the activities that occurred during the installation process.

- b. **/var/opt/CARKpsmp/temp/CreateEnv.log** – This log file describes the activities that occurred when the Vault environment for PSMP was created.
2. View the logs with the **less** command to view the logs and browse the pages using the **space** button.

```
[root@centos PSM-SSHProxy-Installation]#  
[root@centos PSM-SSHProxy-Installation]# less /var/tmp/psmp_install.log _
```

3. Run **rpm -e CARKpsmp** in order to remove the existing PSMP package and try to install again.
4. If the installation completes successfully, but you cannot connect successfully via the PSMP, check the following logfile:
  - a. **/var/opt/CARKpsmp/logs/PSMPConsole.log**

### (Optional) Advanced PSMP Implementations

Requirements:

1. The Customer wants to implement ADB functionality with SSH Access Control.
2. The user `linuxuser01` is a member of the `LinuxUsers` group in LDAP.
3. Members of `LinuxUsers` are only allowed to login to the UNIX device with their own named accounts using their AD credentials.
4. The Customer wants to use the PSMP to prevent end users from switching to the `root01` account.

Objectives:

1. Implement ADB functionality and make sure you can log in to the UNIX device using `linuxuser01` (the user should be created 'on the fly').
2. Implement SSH Access Control in order to prevent `linuxuser01` from performing '`su – root01`'

### Advanced PSMP Implementations (Proposed Solution)

#### AD Bridge

Implementing AD Bridge to allow members of `LinuxUsers` to login with their AD credentials requires us to do the following:

1. Duplicate *Unix via SSH* to "**Unix via SSH with Provisioning**".
2. Edit the new platform. Under UI & Workflows, Privileged Session Management, SSH Proxy, add **User Provisioning**.
3. Set parameter **EnableUserProvisioning** to Yes.



The screenshot shows the 'Properties' tab for the 'Unix via SSH with Provisioning' configuration. The left pane displays a tree view of properties under 'Target Account Platform' and 'UI & Workflows'. The right pane lists properties with their values. A red box highlights the 'EnableUserProvisioning' property, which is set to 'Yes'.

Name	Value
EnableUserProvisioning	Yes

- Set Privileged Session Management, EnablePrivilegedSSO = No and 'UsePersonalPassword' = Yes.

The screenshot shows the 'Properties' tab for the 'Unix via SSH with Provisioning' configuration. The left pane displays a tree view of properties under 'Target Account Platform' and 'UI & Workflows'. The right pane lists properties with their values. A red box highlights the 'EnablePrivilegedSSO' property, which is set to 'No', and the 'UsePersonalPassword' property, which is set to 'Yes'.

Name	Value
ID	PSMServer
SubnetPolicy	No
SessionRecorderSafe	PSMRecordings
MaxSessionDuration	-1
ShowRecordedSessionNotification	Yes
RecordedSessionNotificationDisplayTime	5
ShowLiveMonitoringNotification	Yes
LiveMonitoringNotificationDisplayTime	5
DisableDualControlForPSMConnections	No
EnablePrivilegedSSO	No
UsePersonalPassword	Yes

- Delete the required property **Username**, leaving only **Address**.
- Delete both Linked Accounts i.e., **LogonAccount** and **ReconcileAccount**.

The screenshot shows the 'Properties' tab for the 'Unix via SSH with Provisioning' configuration. The left pane displays a tree view of properties under 'Target Account Platform' and 'UI & Workflows'. The right pane lists properties with their values. A red box highlights the 'Required' node under the 'Properties' section. A message in the right pane states: 'The selected item exposes no properties. Please choose another item.'



7. Create safe “AD-Prov-Target-Accounts” to store the *Target Machine Account*. Grant **LinuxUsers** *Use* and *List* permissions on the safe.

**Safe Details: AD-Prov-Target-Accounts**

Name: **AD-Prov-Target-Accounts**  

Description: Object level access is not enabled

Assigned CPM: CPM\_UNIX

Saved accounts: Account versions from the last 7 days

**Members**

User Name	Use	Retri...	List	Add	Upda...	Upda...	CPM	Rena...	Delete	Unlock	Mana...
CPM_UNIX	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
<b>LinuxUsers</b>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
vaultadmin01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

8. We will use the *root01@10.0.0.20* account as the “Provisioning Account”, thus we must also assign permissions on the **Linux Accounts** safe where *root01* resides, providing access for the **PSMP\_ADB\_AppUsers** group.

Note: If the environment has Dual Control enabled so that access to *root01* requires authorization from *mgr01*, grant the ADB app user group the **Access safe with confirmation** permission.

**Safe Details: Linux Accounts**

Name: **Linux Accounts**  

Description: Object level access is not enabled

Assigned CPM: CPM\_UNIX

Saved accounts: Account versions from the last 7 days

**Members**

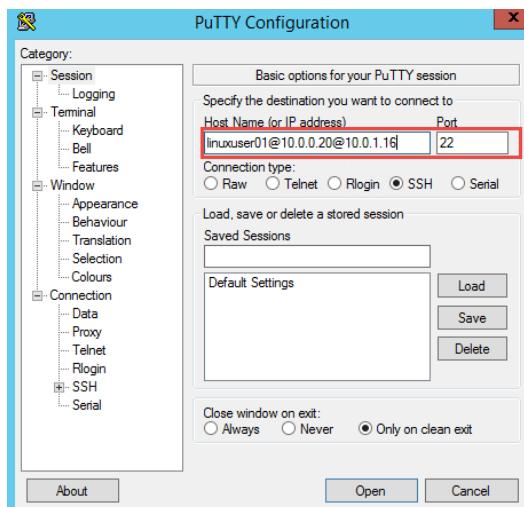
User Name	Use	Retri...	List	Add	Upda...	Upda...	CPM	Re...
CPM_UNIX	✓	✓	✓	✓	✓	✓	✓	✓
LinuxAdmins	✓	✓	✓	✓	✓	✓	✓	✓
<b>mgr01</b>	✓	✓	✓	✓	✓	✓	✓	✓
OracleAdmins	✓	✓	✓	✓	✓	✓	✓	✓
<b>PSMP_ADB_AppUsers</b>	✓	✓	✓	✓	✓	✓	✓	✓
vaultadmin01	✓	✓	✓	✓	✓	✓	✓	✓

9. Next, create the target machine account for **10.0.0.20** and associate the new account with *root01* as the provisioning account. Notice this account has no username, no password and no linked accounts (this is normal).



The screenshot shows two windows side-by-side. The left window is a detailed view of a provisioning account. It includes fields for Password (\*\*\*\*\*), SSH, Platform Name (Unix via SSH with Provisioning), Device Type (Operating System), Safe (AD-Prov-Target-Accounts), Name (Operating System- UnixviaSSHwithProvisioning-10.0.0.20), Last verified (N/A), Last modified (vaultadmin01 (1/31/2017 8:58:09 AM)), Last used (linuxuser01 (2/19/2017 6:20:52 AM)), and Address (10.0.0.20). The right window is the User Provisioning tab of the CyberArk interface, showing the same provisioning account information.

10. Open Putty and enter linuxuser01@10.0.0.20@10.0.1.16 and press open. Please note that linuxuser01 exists in Active Directory but not on the Linux target server.



## SSH Command Access Control

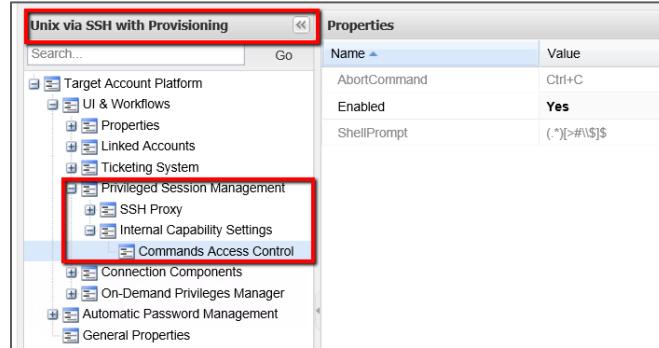
Implementing SSH Command Access control to block members of **LinuxUsers** from using the switch user (SU) command requires us to do the following:

### Configure commands access control

1. Logged in as VaultAdmin01, Click ADMINISTRATION to display the System Configuration page, then click Options and navigate to:
2. Privileged Session Management > General Settings > Connection Client Settings.
3. Right-click and add Capabilities, then right click Capabilities and from the menu select Add Commands Access Control. A Commands Access Control capability with default settings appears.



4. Commands Access Control is disabled by default. Enabling of Commands Access Control is performed at the Platform level. This will be done later in the procedure.
  5. Navigate to Options, Connection Components, and expand PSM-SSH or PSMP-SSH, or any other connection component that is used for SSH connections and requires the use of Commands Access Control.
  6. Expand Target Settings, and right-click Supported Capabilities.
  7. From the menu, select Add Capability. The Properties area of the new capability appears.
  8. In the Id value field, specify CommandsAccessControl.
  9. Click OK to save the new configuration.
10. Edit **Unix via SSH with Provisioning** platform.
11. Add **Internal Capability Settings** and enable **Commands Access Control** to the *Privileged Session Management* section.



12. All commands are denied by default once Command Access Control is enabled so we must first allow all commands and then begin blacklisting specific commands. Configure the allowed/blocked list of commands to allow all commands for all users, and deny the switch user (**SU**) command for members of the **LinuxUsers** group.



Command	UserGroup	Type	Restrictions
(/bin/)?:su.*	LinuxUsers	Deny	
.*	<b>(All users)</b>	Allow	

13. Restart the PSMP service on the PSMP server using the command:

**service psmpsrv restart**

14. Using putty, attempt to login as linuxuser01 and su to root.



## Securing CyberArk

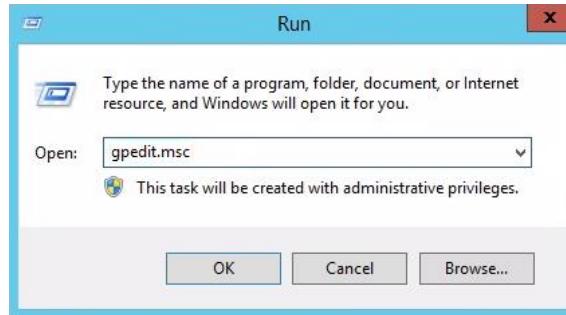
In this section you will be asked to perform several tasks to make your existing CyberArk platform more secure.

### Use RDP over SSL

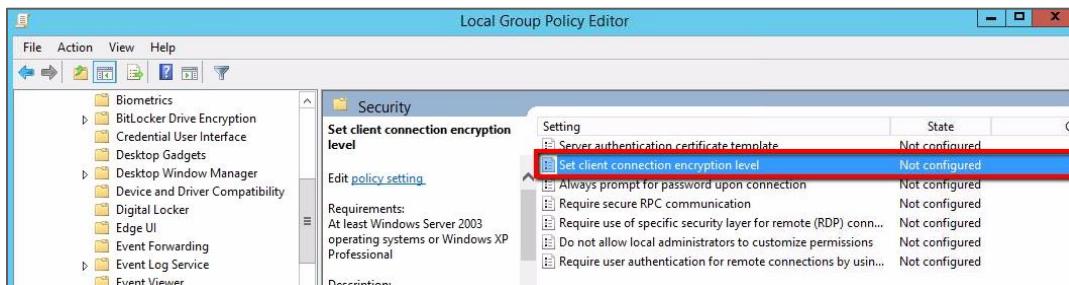
In this section you will configure the PSM server to accept RDP connections over SSL.

**NOTE:** Connections to the **PSM** require a certificate on the **PSM** machine. By default, Windows generates a self-signed certificate, but you can and should use a certificate that is distributed by your Enterprise Certificate Authority.

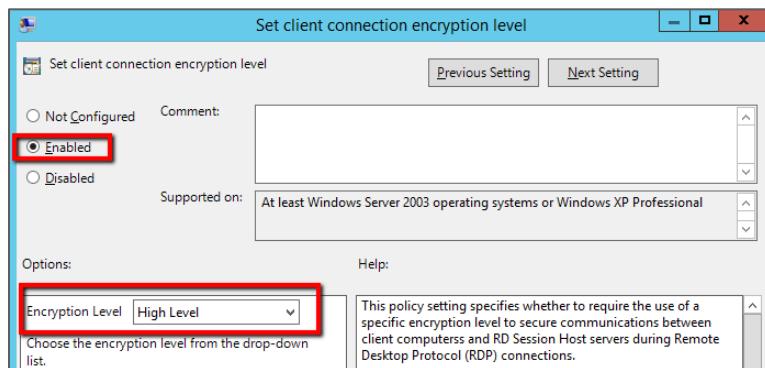
1. Login to **comp01a** and run **gpedit.msc**.



2. Navigate to **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security**.

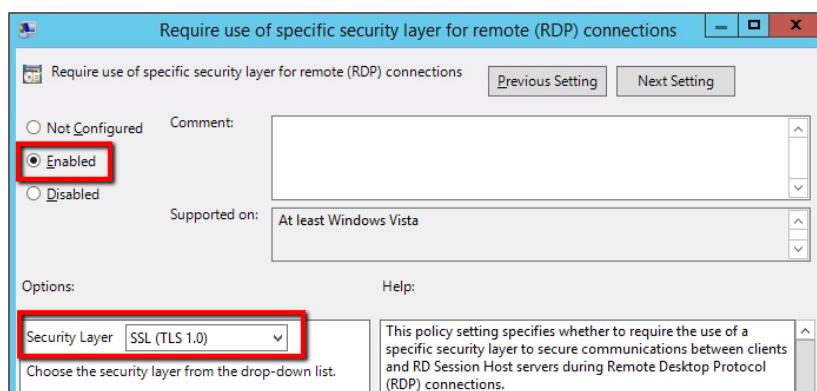


3. Open the Security settings for: **Set client connection encryption level**. Click on **Enabled** and set the encryption level to **High Level** then click **OK**.



4. Open the setting for: **Require use of specific security layer for remote (RDP) connections.**

Click on **Enabled** and set the *Security Layer* to **SSL (TLS 1.0)** and click **OK**.



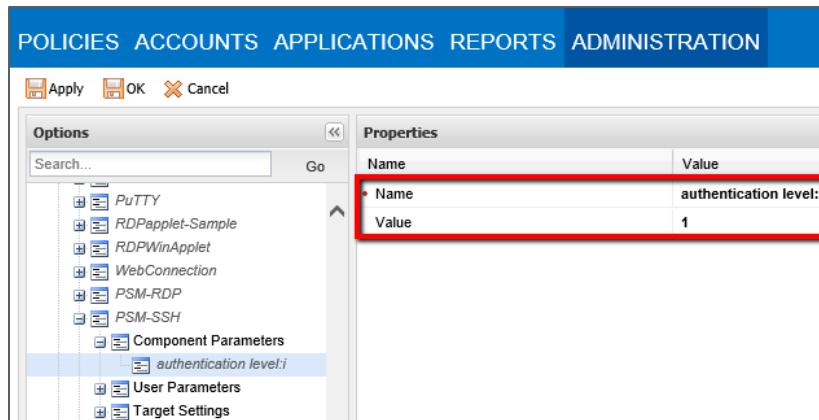
5. Login to the **PVWA** as **vaultadmin01** and go to **ADMINISTRATION > Options > Privileged Session Management > Configured PSM Servers > PSMServer > Connection Details > Server** and change the *Address* attribute to the FQDN of the **PSM** server (so that it matches the name of the **PSM** server certificate). Click **OK** to save the changes.



**Note:** If you were using the **PSM** farm in your platforms, you must also change the PSM server ID back to **PSMServer** on those platforms. This is required due to limitations of the ZEN LB appliance.

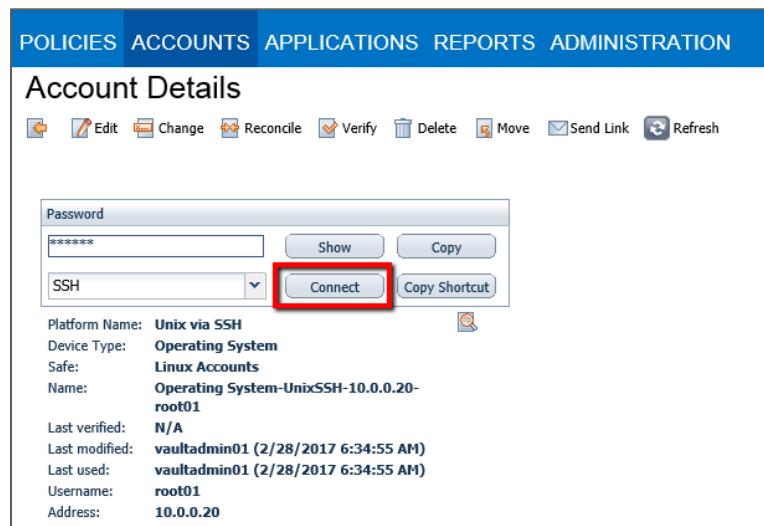
- In the **PVWA**, open **Administration > Component Settings > Options > Connection Components > PSM-SSH > Component Parameters**. Add a new parameter named **authentication level:i** and set the **Value** to **1**.

**Note:** For connections with ActiveX or an external tool, the Name should be **AdvancedSettings4.AuthenticationLevel** with a Value of 1).



**Note:** You will need to do the same for each active connection component in order to enable RDP over SSL connections to the **PSM** machine.

- Restart the PSM service (as the PSM needs to refresh the configuration changes done to the connection component in the PVWA)
- Next, try to connect to one of the accounts you previously configured via the **PSM** (this time using RDP over SSL).

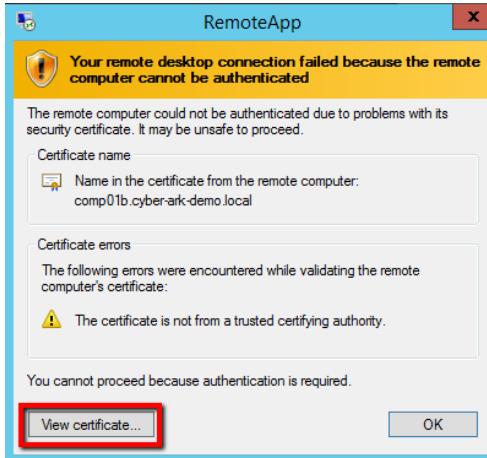


**Account Details**

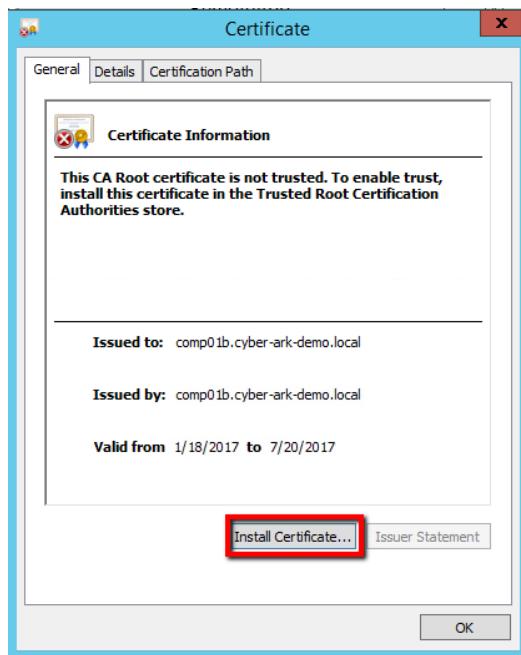
Platform Name: Unix via SSH  
 Device Type: Operating System  
 Safe: Linux Accounts  
 Name: Operating System-UnixSSH-10.0.0.20-root01  
 Last verified: N/A  
 Last modified: vaultadmin01 (2/28/2017 6:34:55 AM)  
 Last used: vaultadmin01 (2/28/2017 6:34:55 AM)  
 Username: root01  
 Address: 10.0.0.20

**Note:** If this is the first time you try to use RDP over SSL you will also need to import the PSM server certificate to your Components server.

9. After clicking on the RDP file, click on **View certificate**.



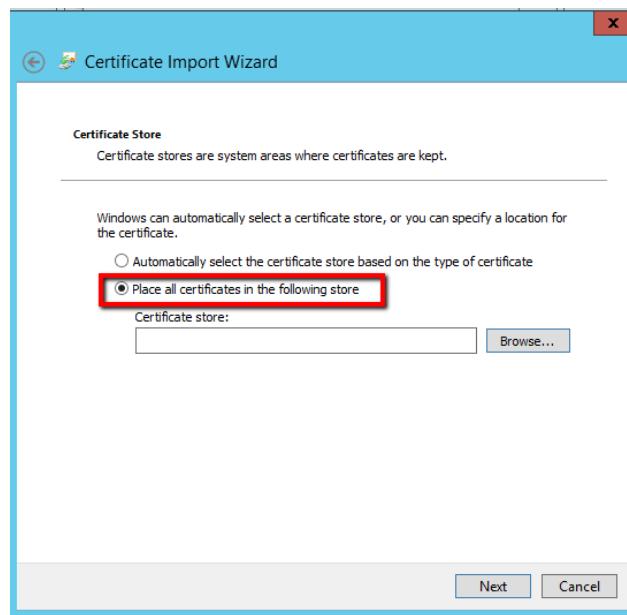
10. Click on **Install Certificate**.



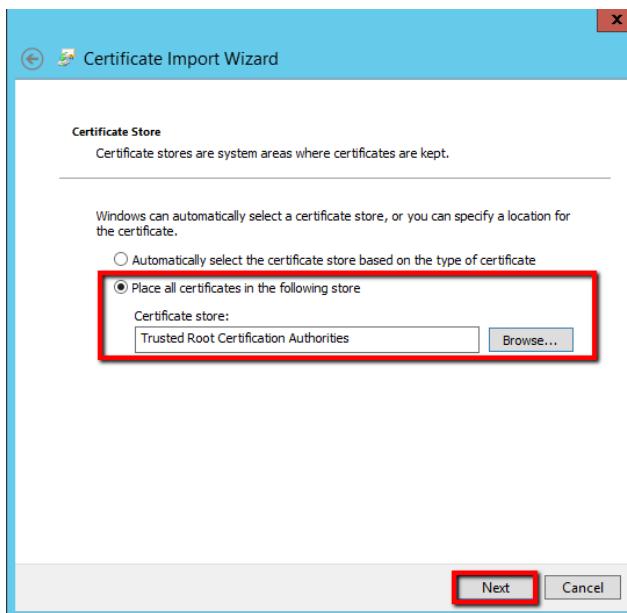
11. Click on **Local Machine** and click **Next**.



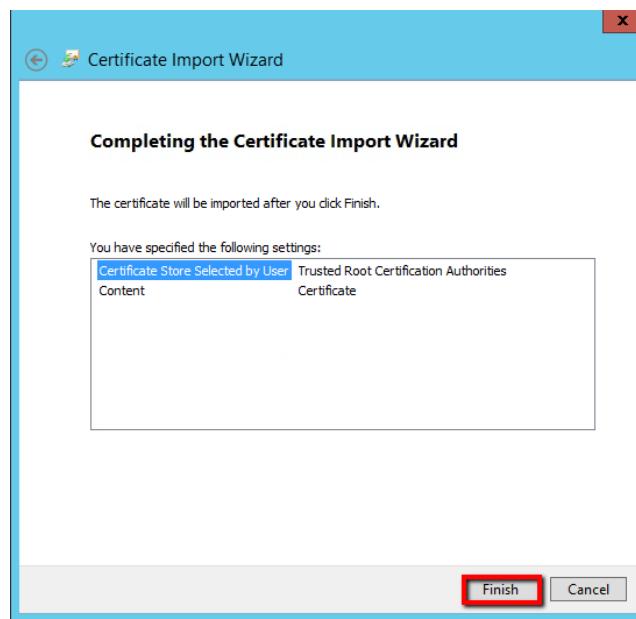
12. Click on **Place all certificates in the following store**.



13. Click on **Browse** and then choose **Trusted Root Certification Authorities**. Then click on **Next**.



14. Click on **Finish** then re-establish the connection, which will now succeed.



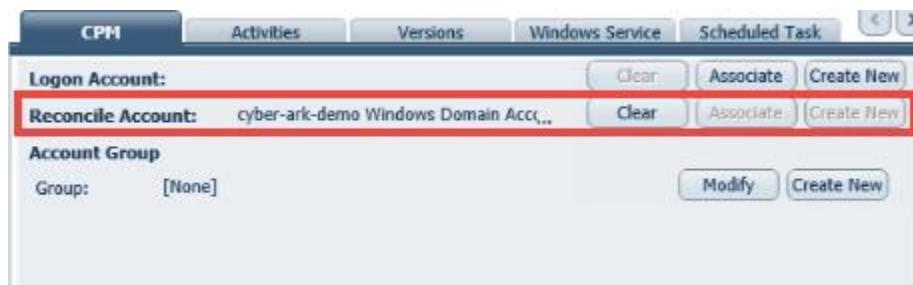
## Manage LDAP BindAccount

**NOTE:** Ensure that a reconcile account is associated with the BIND account.

1. Logon to the PVWA as Vaultadmin01.
2. Edit the VaultInternal safe and assign CPM: CPM\_WIN and Save.
3. Go to the Accounts tab and search for BindAccount.
4. Edit BindAccount. Select Resume to enable Automatic Management as seen in the following graphic.



5. In Account Details, associate a Reconcile Account by selecting Associate and choosing the Admin01 domain account.



6. Select the Change button to change the password of BindAccount.

**NOTE:** It is recommended to configure these password changes to take place “off hours” when user access to accounts in the vault is less likely. This can be accomplished by duplicating the Windows Domain Account platform, and configuring the platform settings accordingly.

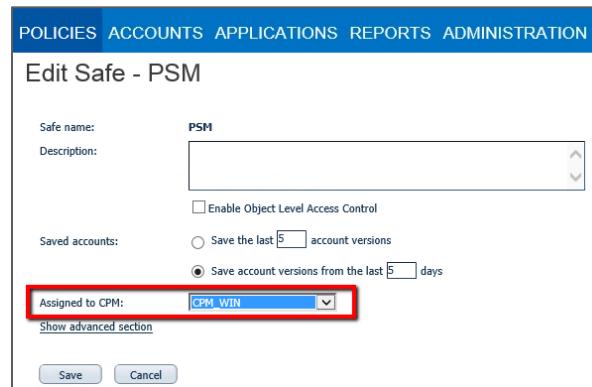
### Manage PSMConnect/PSMAdminConnect using the CPM

**NOTE:** Customers who manage *PSMConnect* and *PSMAdminConnect* user credentials with the **CPM** must make sure that a reconcile account is associated with these accounts, and that changes to the password are done via Reconcile.

1. Login to the PVWA as CyberArk user **Administrator** and go to **POLICIES > Access Control (Safes)** and choose the **PSM** safe. Click on **Edit**.



2. Assign to CPM: **CPM\_WIN**.



POLICIES ACCOUNTS APPLICATIONS REPORTS ADMINISTRATION

### Edit Safe - PSM

Safe name: **PSM**

Description:

Enable Object Level Access Control

Saved accounts:

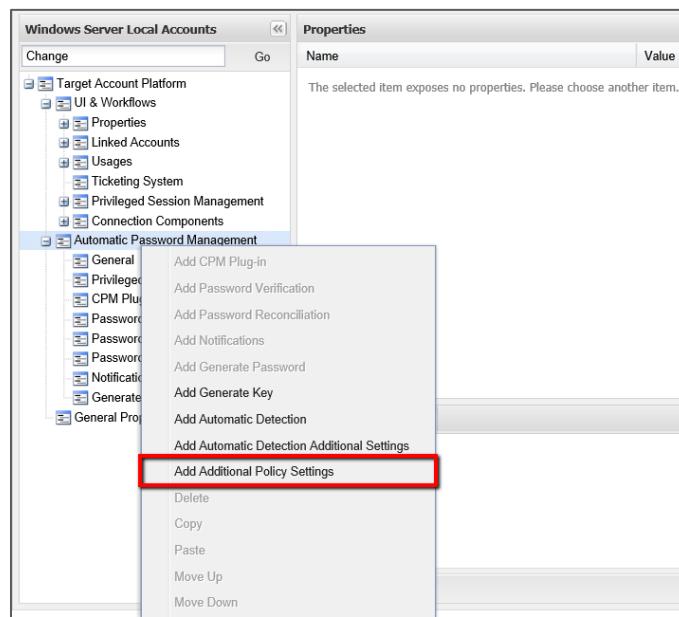
- Save the last **5** account versions
- Save account versions from the last **5** days

Assigned to CPM: **CPM\_WIN**

[Show advanced section](#)

**Save** **Cancel**

- Next, we need to assign the PSM users to the **Windows Local Server Accounts** or preferably a duplicated platform based on Windows Local Server Accounts, and configure the platform to perform changes using the Reconcile mechanism. Go to platform management and edit right click on Automatic Password Management > Add Additional Policy Settings:



- Set **ChangePasswordInResetMode** to Yes and click on OK to save.



The screenshot shows the 'Windows Server Local Accounts' properties dialog. The left pane lists various policy settings under 'Target Account Platform' and 'Automatic Password Management'. The right pane displays a table of properties. One row, 'ChangePasswordInResetMode', has its value 'Yes' highlighted with a red box. Below the table, a note explains: 'Defines whether or not password changes will be performed via reset mode using the reconciliation account. This is useful in cases where the reconciliation account does not have a password.'

5. Go to **ACCOUNTS**, and select both **PSMConnect** and both **PSMAdminConnect** users. Select the Modify button and click on **Edit**.

The screenshot shows the CyberArk Account views V10 interface. The top navigation bar includes 'POLICIES', 'ACCOUNTS', 'MONITORING', 'APPLICATIONS', 'REPORTS', 'ADMINISTRATION', and 'administrator'. The 'ACCOUNTS' tab is active. A search bar at the top right shows results for "PSM". The main table lists accounts under 'Incoming Requests (0)'. Two accounts, 'PSMAdminConnect' and 'PSMConnect', are selected (indicated by red boxes around their checkboxes). To the right of the table is a toolbar with buttons for 'Request Access', 'Manage', 'Modify' (which is highlighted with a red box), 'Add to', and 'Detect Now'. Below the table is a grid of icons for managing accounts.

6. Change **Device Type** to **Operating System** and **Platform Name** to “**Windows Server Local Accounts**” (or the platform you created) and select **Save**.



POLICIES ACCOUNTS APPLICATIONS REPORTS ADMINISTRATION

### Edit Account: PSMConnect-10.0.21.1

Store in Safe: **PSM** Change to:

Device Type: **PSM** Change to:

Platform Name: **10.0.21.1** Change to:

**Required Properties:**

Address: **10.0.21.1** Change to:   
Username: **PSMConnect** Change to:

**Optional Properties:**

Logon To: **COMP01B** Change to:    
 Location:   
 Owner Name:  Change to:  Change to:

Disable automatic management for this account  
Reason:

[Show advanced section](#)

7. In Account Details, associate a Reconcile Account for each **PSMConnect** and **PSMAdminConnect** user, by selecting Associate and choosing the Admin01 domain account. Alternatively, you can choose to define the Admin01 account as the Reconcile account at the platform level.

CPH Activities Versions Windows Service Scheduled Task

**Logon Account:**

**Reconcile Account:** **cyber-ark-demo Windows Domain Acc...**

**Account Group**  
Group: **[None]**

8. Select the Change button to change the password of all PSMConnect and PSMAAdminConnect users. You should be able to see that the CPM successfully reconciled the passwords.



The screenshot shows the 'Account Details' page for a Windows Server Local Account. The account information includes:

- Platform Name: Windows Server Local Accounts
- Device Type: Operating System
- Safe: PSM
- Name: PSMServer
- Last verified: N/A
- Last modified: CPM\_WIN (3/28/2017 9:32:13 AM) **(highlighted)**
- Last used: Administrator (3/28/2017 9:31:42 AM)
- Username: PSMConnect
- Logon To: COMP01A
- Address: 10.0.20.1

**NOTE:** It is recommended to configure these password changes to take place during the night or at another time when user access to accounts in the vault is less likely.

### Manage CyberArk Admin Accounts using the CPM

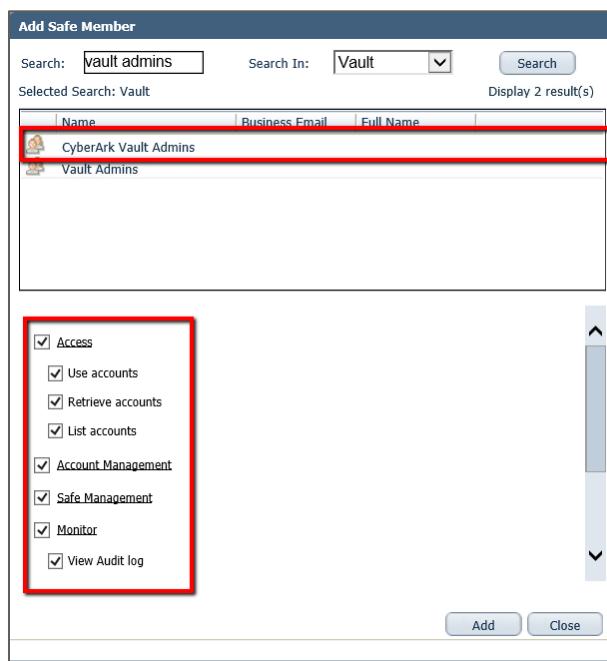
In this section you will configure the CPM to manage the password for the built-in CyberArk Administrator user.

**NOTE:** After this step the CPM will change the password for the built-in administrator and you will need to retrieve the password of *Administrator* from the Vault.

1. Login to the PVWA as **vaultadmin01** and activate the **CyberArk Vault** platform.

The screenshot shows the 'Platform Preview' section for the CyberArk Vault platform. The status is set to 'Active'. The 'Edit' button is highlighted with a red box.

2. Next, create a new safe called **CyberArk Administrators** to store CyberArk administrative accounts. Assign the safe to **CPM\_WIN** and grant the external CyberArk Vault Admins group full permissions to this safe.



3. Next, create a new account in the PVWA for **Administrator** with the following properties.

<b>Store in Safe</b>	<b>CyberArk Administrators</b>
<b>Device Type</b>	<b>Application</b>
<b>Platform</b>	<b>CyberArk Vault</b>
<b>Username</b>	<b>Administrator</b>
<b>Address</b>	<b>10.0.10.1</b>
<b>Password</b>	<b>Cyberark1</b>

4. Execute verify and password change operations for **Administrator**.



The screenshot shows the 'Account Details' page. At the top, there's a toolbar with buttons for Edit, Change (highlighted with a red box), Verify, Delete, Move, Send Link, and Refresh. Below the toolbar, there's a 'Password' field containing 'a1AGgI>R' (also highlighted with a red box), followed by Show and Copy buttons. A dropdown menu shows 'PSM-PVWA'. Below this, detailed account information is listed:

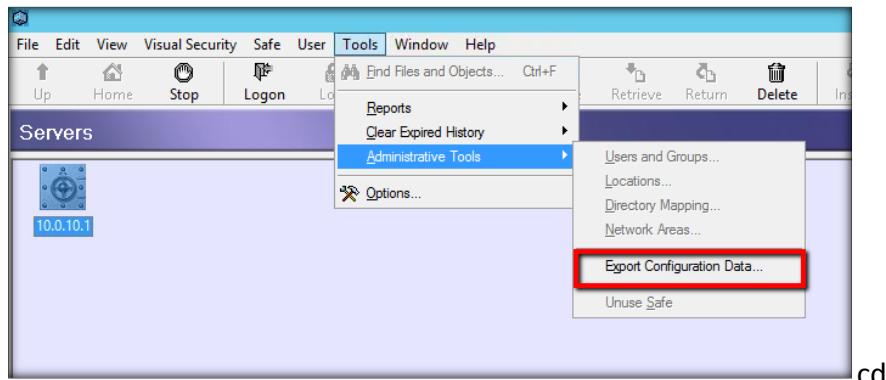
Platform Name:	CyberArk Vault
Device Type:	Application
Safe:	CyberArk Administrators
Name:	Application-CyberArk-10.0.12.1-administrator
Last verified:	N/A
Last modified:	CPM_WIN (3/29/2017 2:02:39 AM)
Last used:	vaultadmin01 (3/29/2017 2:02:09 AM)
Username:	administrator
Address:	10.0.12.1

## Connect with PSM-PrivateArk Client

In this section you will configure the PSM to support PrivateArk Client connections.

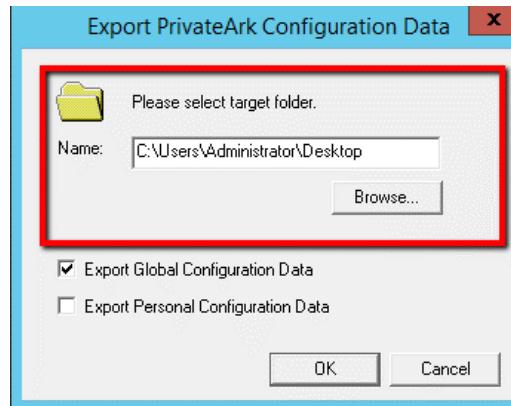
**Note:** In order to use the PSM to connect to the Vault using the PSM-PrivateArk connection component, the PrivateArk Client must be installed on the PSM server and be configured in *Global Configuration* mode. Global Client Configuration enables you to define Vault parameters once and then make these parameters available to all users. This feature reduces system administration time and streamlines Vault management.

1. First, login to the PSM server and run the PrivateArk Client from the desktop (no need to login). Go to **Tools > Administrative Tools > Export Configuration Data**.

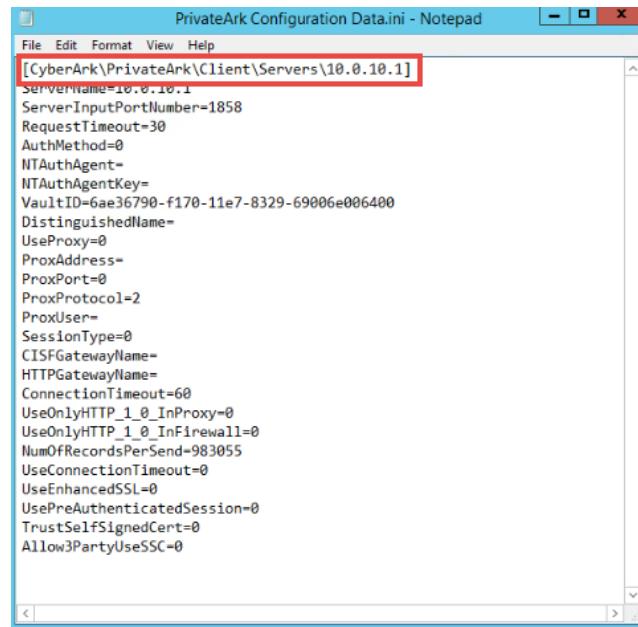




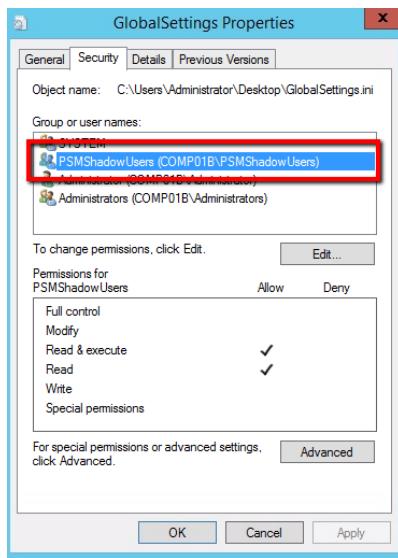
2. Export the Global Configuration Data to the **Desktop**.



3. Make sure that the **PrivateArk Configuration Data.ini** file was created successfully. Open the file and make sure that the IP address of the Vault server is in the path at the top of the file. Rename the file **GlobalSettings.ini**.

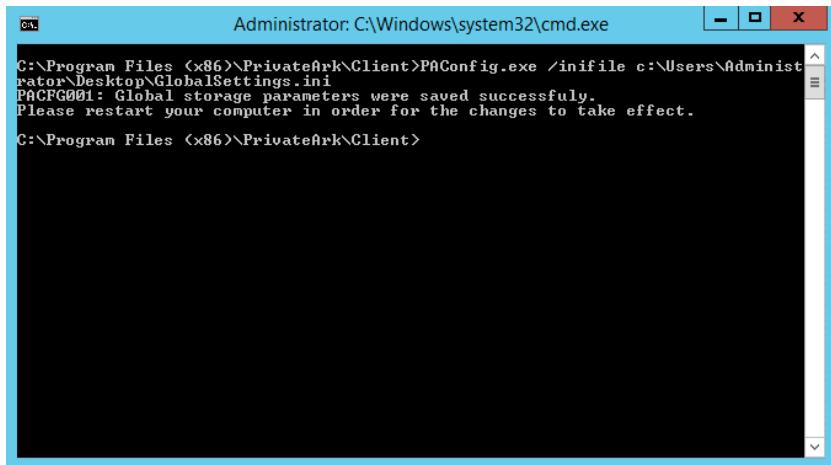


4. Next, open the **Properties** of the *GlobalSettings.ini* file. Go to the **Security** tab and give **Read & Execute** permissions on the file to the local **PSMShadowUsers** group on the PSM server.



5. Next, since the client is already installed in normal mode, you will use the *PAConfig* utility to change the configuration to Global Configuration. Simply open CMD in “C:\Program Files (x86)\PrivateArk\Client” and run the following command:

```
PAConfig.exe /ini file c:\Users\Administrator\Desktop\GlobalSettings.ini
```



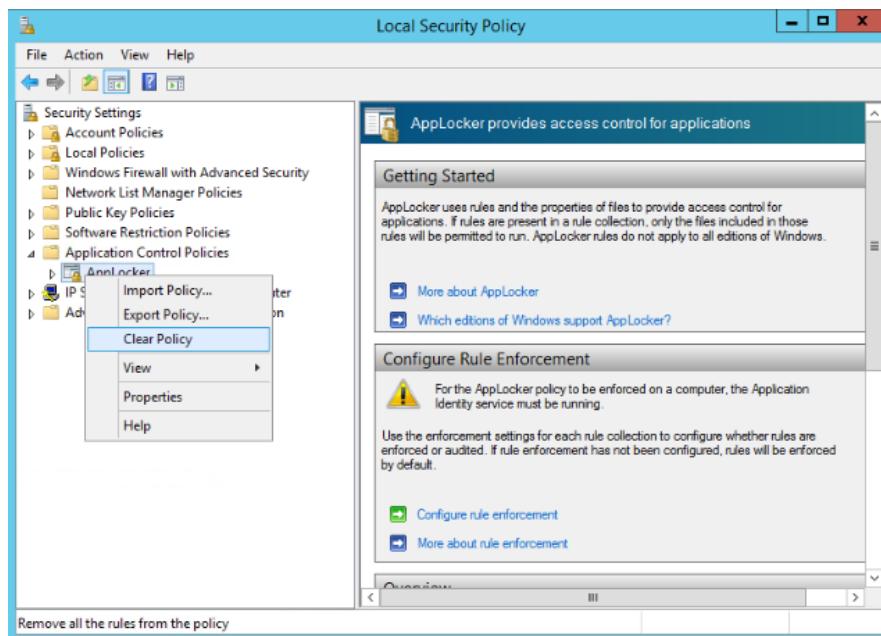
6. Restart the server.
7. Login to the PVWA as **Vaultadmin01** and add the Private Ark client executable as an authorized application in the Applocker configuration.



- a. In the PSMConfigureApplocker.xml file, go to the “Generic Client support” section at the bottom. Copy the “Generic client sample” line. Paste this line with the “Microsoft IExplore processes” (because it is not commented) and edit the Name and Path as follows:  
Name="PrivateArk Client", Path="C:\Program Files (x86)\PrivateArk\Client\Arkui.exe"

```
<!-- Microsoft IExplore processes -->
<Application Name="IExplore32" Type="Exe" Path="c:\Program Files (x86)\Internet Explorer\iexplore.exe" Method="Publisher" />
<Application Name="IExplore64" Type="Exe" Path="c:\Program Files\Internet Explorer\iexplore.exe" Method="Publisher" />
<Application Name="SQLPlus" Type="Exe" Path="c:\oracle\instantclient\sgplus.exe" Method="Hash" />
<Application Name="PrivateArk Client" Type="Exe" Path="C:\Program Files (x86)\PrivateArk\CLIENT\Arkui.exe" Method="Hash" />
```

8. Save the file.
9. Delete all Applocker rules before running the Applocker script.
  - a. Run SecPol.msc from the Start / Run menu.
  - b. Expand Application Control Policies and right click on Applocker.
  - c. Select Clear Policy.



10. Now reapply the Applocker rules by executing the PSMConfigureApplocker.ps1 script.

Note: Refer to section “Configure AppLocker Rules”



11. Verify that you can connect to the Vault with **Administrator** using the **PSM-PrivateArkClient** connection component (don't forget to enable RDP over SSL for the connection component by adding a new connection parameter called **authentication level:i** with a value of **1** and restarting the PSM service).

The screenshot shows the 'Account Details' page. At the top, there are tabs for POLICIES, ACCOUNTS, APPLICATIONS, REPORTS, and ADMINISTRATION. Below the tabs, there's a toolbar with icons for Edit, Change, Verify, Delete, Move, Send Link, and Refresh. The main area is titled 'Account Details' and contains a password field with a red box around its dropdown menu. The dropdown menu is open, showing 'PSM-PrivateArkClient' selected. Below the password field, there's a table with various account details:

Platform Name:	CyberArk Vault
Device Type:	Application
Safe:	CyberArk Administrators
Name:	Application-CyberArk-10.0.12.1-administrator
Last verified:	N/A
Last modified:	CPM_WIN (3/29/2017 2:02:39 AM)
Last used:	vaultadmin01 (3/29/2017 2:14:20 AM)
Username:	administrator
Address:	10.0.12.1

### Connect with PSM-PVWA

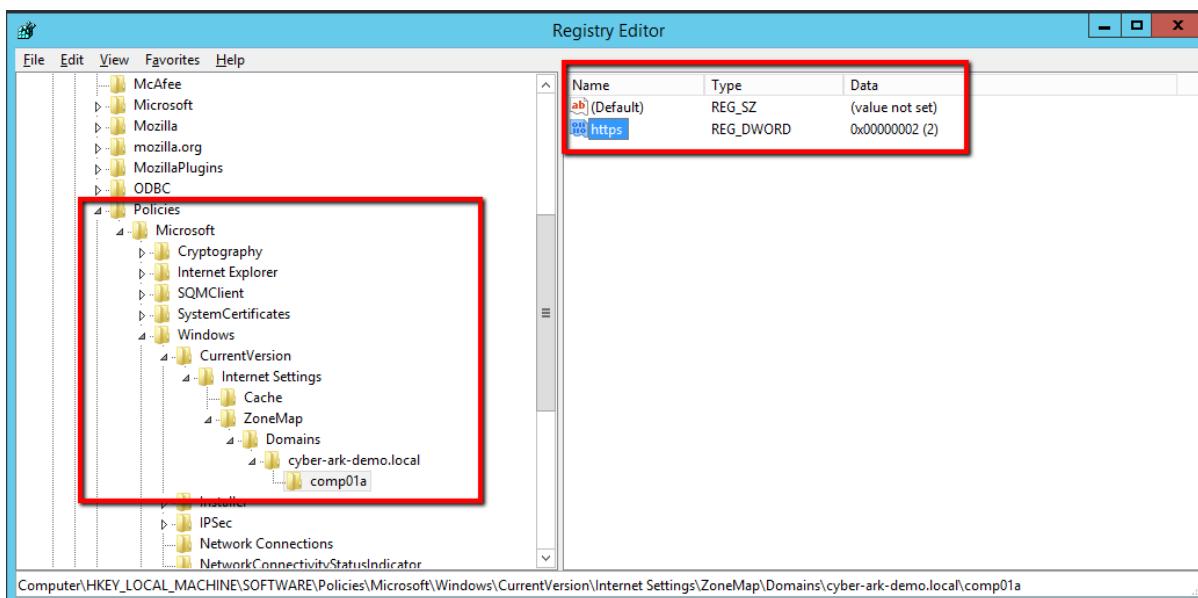
In this section you will configure the PSM to support connections with CyberArk administrative accounts to the Vault using the PVWA.

**Note:** In order for the PSM to support connections to the Vault using the PSM-PVWA connection component, the PSM must be configured to run Web Applications. This should have been accomplished by updating the PSMHardening.ps1 script to support Web Applications and then running the hardening script. If you skipped the section "Post Installation and Hardening Tasks", go back and perform these steps.

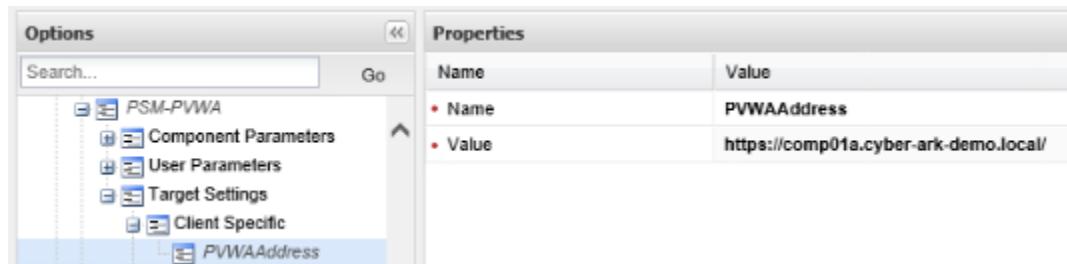
12. To support the *PSM-PVWA* connection component the URL of the PVWA must be added to the PSM server's IE *Trusted Sites* list. Since this needs to be done for all *PSMShadowUsers*, you will need to do this by creating the following key in the PSM machine Registry:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\cyber-ark-demo.local\comp01a**

13. Add a new DWORD value called **https** with a decimal value of **2**.



14. Login to the PVWA and navigate to **Options > Connection Components > PSM-PVWA > Target Settings > Client Specific > PVWAAddress** and change the *Value* parameter to the URL of the PVWA (e.g. <https://comp01a.cyber-ark-demo.local/>):



15. Enable RDP over SSL for the *PSM-PVWA* connection component by adding a new Component Parameter called **authentication level:i** with a value of **1**.



Name	Value
Name	authentication level:i
Value	1

16. We will disable RemoteApp for this connection component as well by adding a Component Parameter call **DisableRemoteApp** with a value of **Yes** and restart the PSM service.

Name	Value
Name	DisableRemoteApp
Value	Yes

17. You must also configure Applocker to run the following executable: "**C:\Program Files (x86)\Java\jre1.8.0\_101\bin\ssvagent.exe**". Add the following rule to Applocker and run the **PSMConfigureApplocker.ps1** script (if the executable is still blocked by Applocker when you run the connection component, clear the policies using **secpol.msc** and then try running the script again)



```
<!-- Microsoft IExplore processes -->
<Application Name="IExplore32" Type="Exe" Path="c:\Program Files (x86)\Internet Explorer\iexplore.exe" Method="Publisher" />
<Application Name="IExplore64" Type="Exe" Path="c:\Program Files (x86)\Internet Explorer\iexplore.exe" Method="Publisher" />
<Application Name="PrivateArk Client" Type="Java" Path="C:\Program Files (x86)\PrivateArk\Client\lrvui.exe" Method="Hash" />
<Application Name="PVWA" Type="Exe" Path="C:\Program Files (x86)\Java\jre1.8.0_101\bin\ssvagent.exe" Method="Hash" />
```

18. Next, login to the PVWA as **Vaultadmin01** (don't forget to choose LDAP authentication) and try to connect with **Administrator** to the Vault using the **PSM-PVWA** connection component.

The screenshot shows the CyberArk Privileged Account Security interface. The top navigation bar includes tabs for POLICIES, ACCOUNTS, APPLICATIONS, REPORTS, and ADMINISTRATION. The APPLICATIONS tab is currently selected. Below the tabs, the title "Account Details" is displayed. On the left, there are several icons: a left arrow, a house, a pencil, an edit icon, a change icon, a checkmark icon, a delete icon, a move icon, a send link icon, and a refresh icon. The main area contains a password field with the value "a1AGgI>R" and buttons for "Show" and "Copy". Below this is a dropdown menu set to "PSM-PVWA" with a "Connect" button next to it, which is highlighted with a red box. Further down, detailed account information is listed:

Platform Name:	CyberArk Vault
Device Type:	Application
Safe:	CyberArk Administrators
Name:	Application-CyberArk-10.0.12.1-administrator
Last verified:	N/A
Last modified:	CPM_WIN (3/29/2017 2:02:39 AM)
Last used:	vaultadmin01 (3/29/2017 2:28:16 AM)
Username:	administrator
Address:	10.0.12.1

19. Verify that you can view the recordings of your PrivateArk Client and PVWA sessions (you can login with **Auditor01** who is an LDAP user to view the recordings).



	Username	Address	Safe	Platform ID				
	PSMConnect	10.0.20.1	PSM	WinServerLocal				
	BindAccount	10.0.0.2	VaultInternal	WinDomain				
			VaultInternal					

## Remove Unnecessary CyberArk Administrative Privileges

**Note:** Now that you have successfully connected to CyberArk administrative interfaces via the PSM, it is time to remove the admin authorizations of the CyberArk Vault Admins group. From this point on, all administrative activity on CyberArk will be done via the built-in administrator, fully monitored and audited by the PSM.

1. First, assign the external CyberArk Vault Admins group permissions on your privileged accounts safes (Linux, windows and Database). Assign the group all permissions except for “Use accounts” and “Retrieve accounts”. This is done to allow Vault Admins to manage the safes where accounts are stored but not have access to the passwords themselves. Note that CyberArk Vault Admins should still have all permissions (including “Use Accounts and “Retrieve Accounts”) on the CyberArk Administrators safe.



CYBERARK®

## Privileged Account Security Install & Configure, v10.x

Add Safe Member

Search: Cyberark vault ad    Search In: Vault    Search    Selected Search: Vault    Display 1 result(s)

Name	Business Email	Full Name
CyberArk Vault Admins		

Access  
 Use accounts  
 Retrieve accounts  
 List accounts  
 Account Management  
 Safe Management  
 Monitor  
 View Audit log

Add    Close

2. Next, login to the PrivateArk Client as administrator and go to **Tools > Administrative Tools > Directory Mapping**. Select the Vault Admins Directory mapping and click on update.

Directory Mapping for Server 10.0.10.1

Map Name: **Vault Admins Mapping**

Vault Admins Mapping

Map applies to:  Users    Groups

Server properties: Location: \

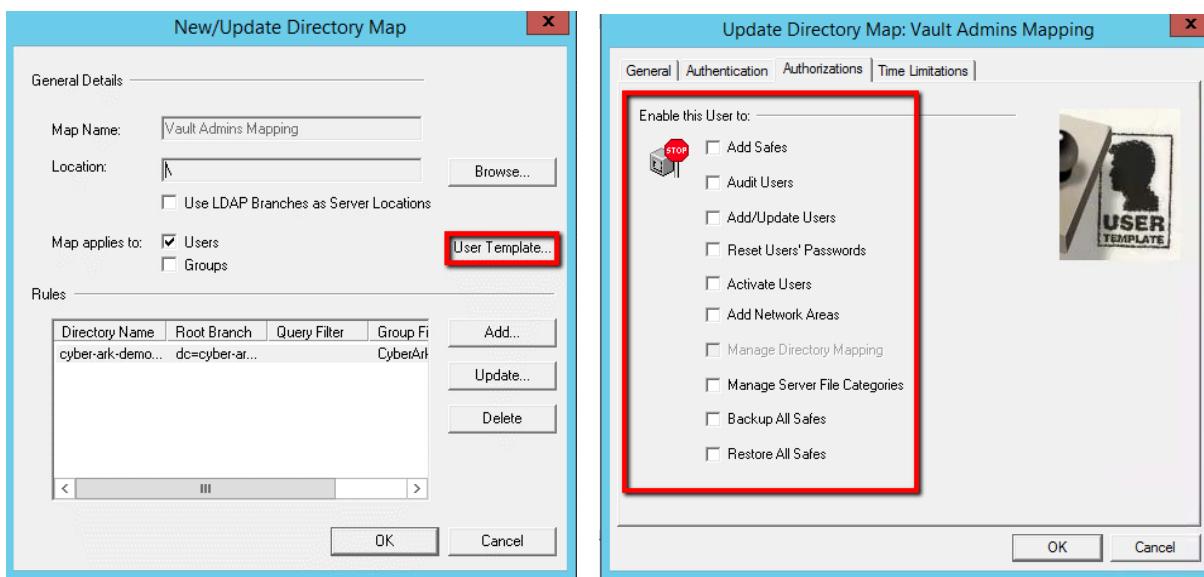
Use LDAP Branches as Server

User Template Rights:

- Add Safes
- Audit Users
- Add/Update Users
- Reset Users' Passwords
- Activate Users
- Add Network Areas
- Manage Directory Mapping
- Manage Server File Categories
- Backup All Safes
- Restore All Safes

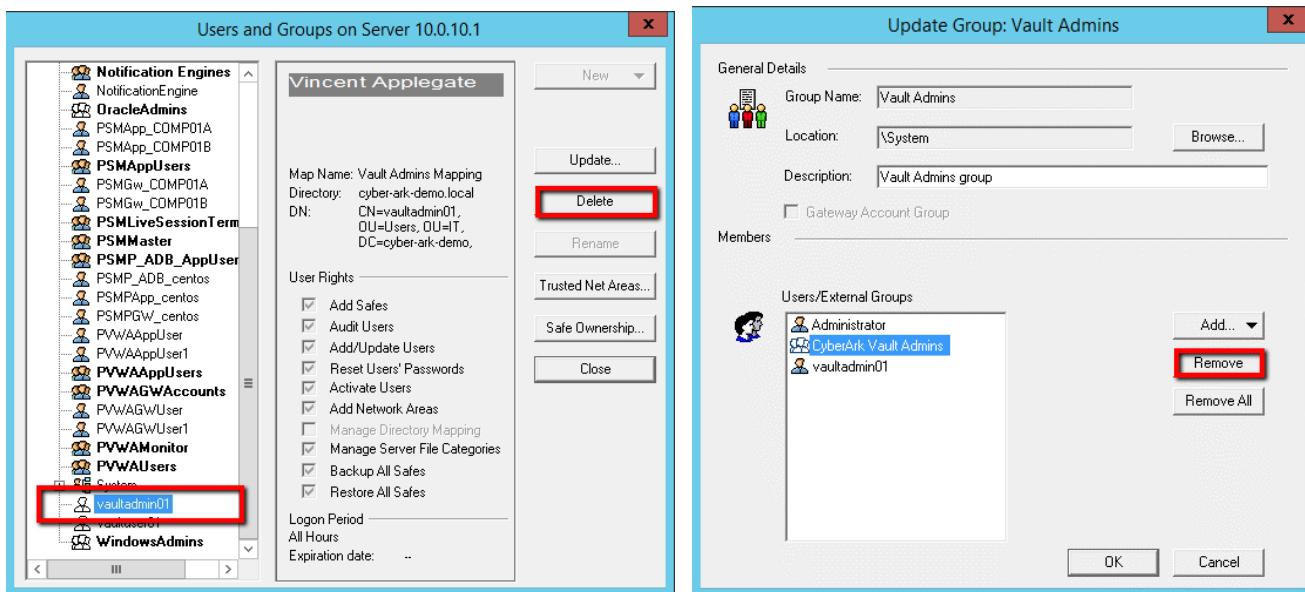
Add...    Update...    Delete    Close

**3. Select User Template and then remove all the Vault Authorizations.**



**4.**

**5. Remove the external CyberArk Vault Admins group from the built-in Vault admins group and delete Vaultadmin01 from the Vault. Logoff from the PrivateArk Client.**





6. At this stage Vaultadmin01 should be logged off from the PVWA automatically. Login to the PVWA again as **Vaultadmin01**. You should be able to see the accounts you previously created, but you should not see the Administrative tabs anymore. From now on, any administrative work should be done with the built-in administrator via the PSM.

The screenshot shows the CyberArk Privileged Account Security interface. The top navigation bar includes 'POLICIES', 'ACCOUNTS' (which is selected), and 'REPORTS'. The title bar says 'Account views V10 interface > vaultadmin01'. On the left, there's a sidebar with 'Requests Views' (My Requests (0), Incoming Requests (0)) and 'Operational Views' (Failed accounts, Failed service accounts, Disabled by users, Disabled by CPM). The main content area displays a table of accounts with columns: Username, Address, Safe, and Platform. The table data is as follows:

	Username	Address	Safe	Platform
<input type="checkbox"/>	root01	10.0.0.20	LinuxRestore	UnixSSH
<input type="checkbox"/>	Admin01	cyber-ark-demo.local	Windows Accounts	WinDomain
<input type="checkbox"/>	administrator	10.0.10.1	CyberArk Administrators	CyberArk
<input type="checkbox"/>	dba01	10.0.0.20	Database Accounts	Oracle
<input type="checkbox"/>	localadmin01	DomainMember.cyber-ark-demo.local	Windows Accounts	WinServer

Below the table are buttons for 'Request Access', 'Manage', 'Modify', and 'Add to'.

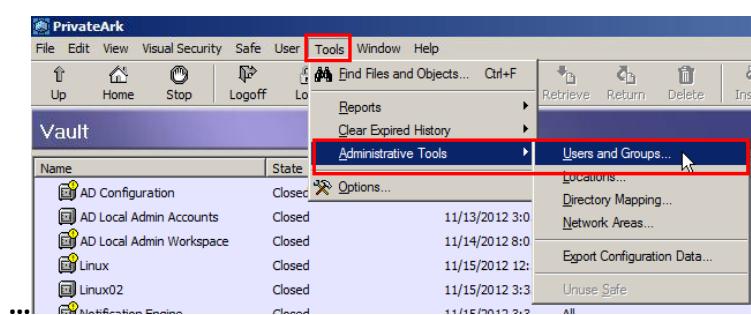


## Backup

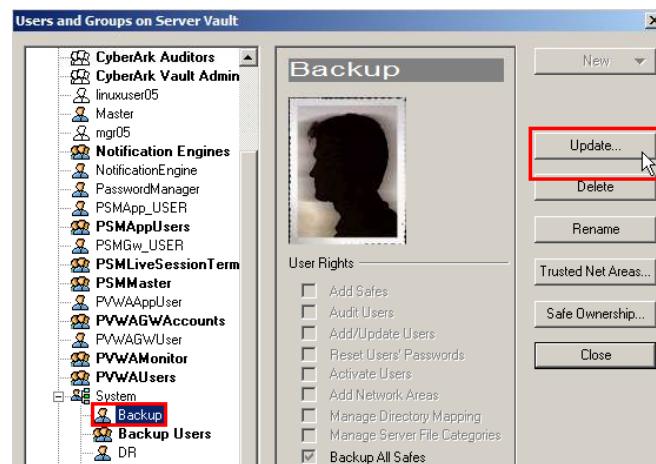
### Enable the Backup and Users

For this section of the exercise, you will first login to the **PrivateArk Client** on **Comp01A Server** in order to enable the users required to run a backup.

1. Use the **PrivateArk** client to log into the **Vault** as **administrator** (use the PSM-PrivateArk Client connection component).
2. Go to **Tools > Administrative Tools > Users and Groups**.



3. Highlight the **Backup** user (located under System) and press **Update**.

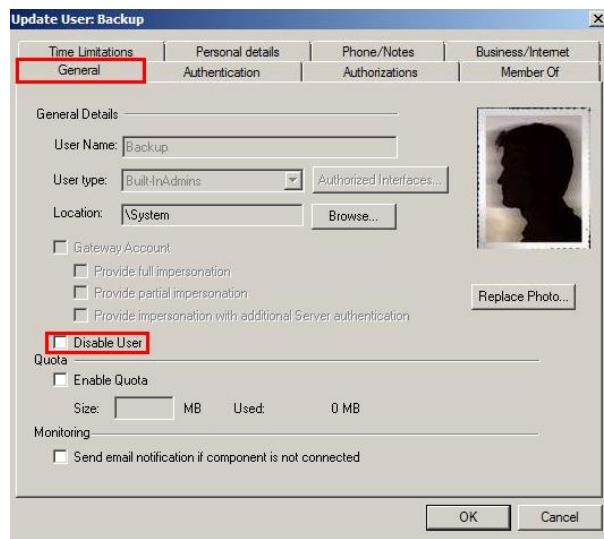




CYBERARK®

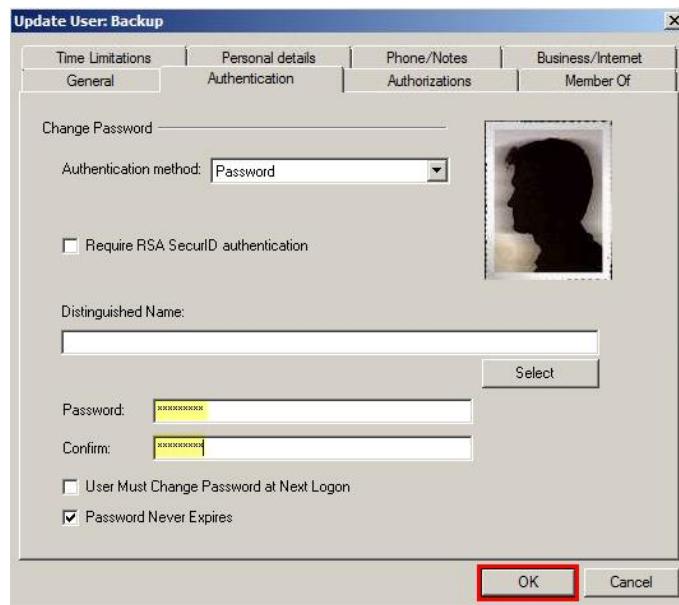
## Privileged Account Security Install & Configure, v10.x

4. On the **General** tab uncheck the *Disable User* checkbox.



5. On the **Authentication** tab enter *Cyberark1* in the **Password** and **Confirm** fields.

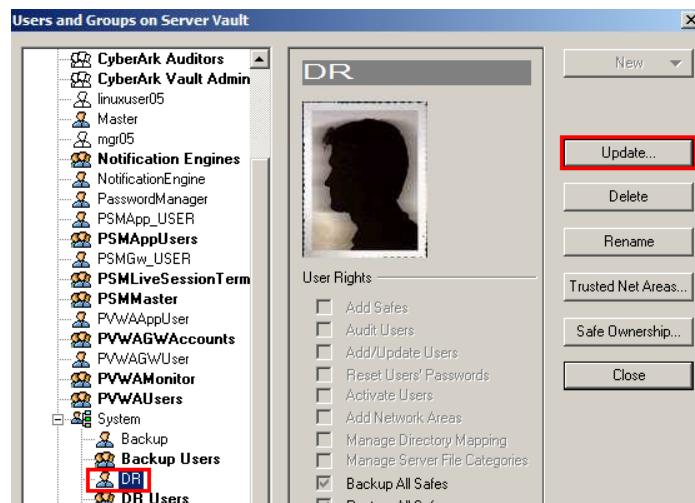
6. Press **OK**.



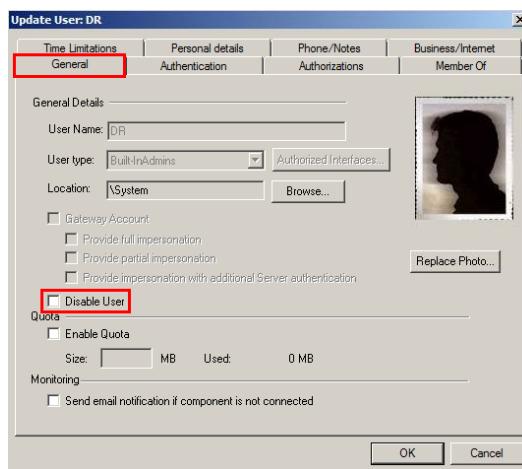
The DR user will be used in the Disaster Recovery exercise. We will enable it now.



7. Highlight the DR user (located under System) and press **Update**.



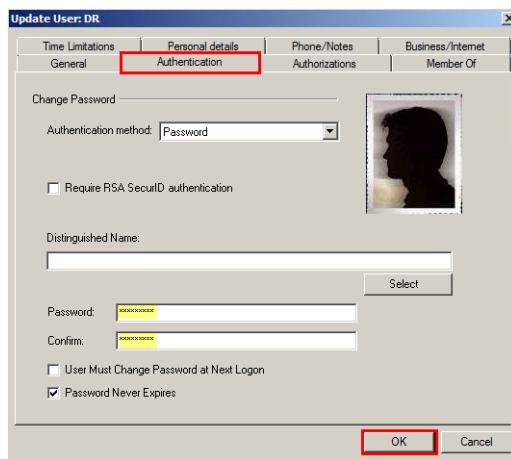
8. On the **General** tab uncheck the *Disable User* checkbox.





9. On the **Authentication** tab enter **Cyberark1** in the **Password** and **Confirm** fields

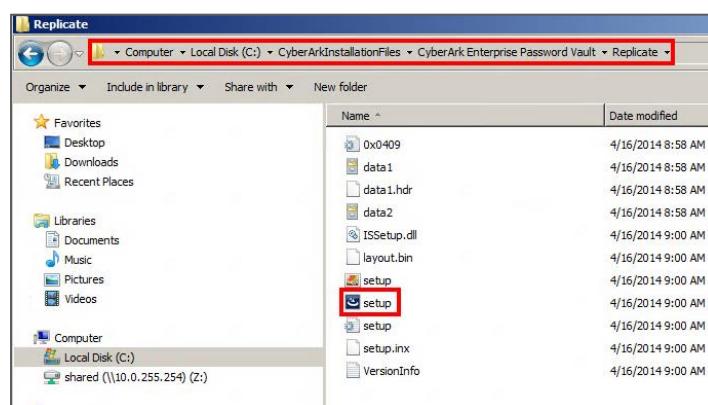
10. Press **OK**.



11. Log out of **PrivateArk Client**.

### Install the PrivateArk Replicator

1. On the **Components Server**, open *Windows File Explorer* and go to *C:\CyberArk\InstallationFiles\CyberArk Enterprise Password Vault\Replicate*.
2. Double-click the **setup** icon.

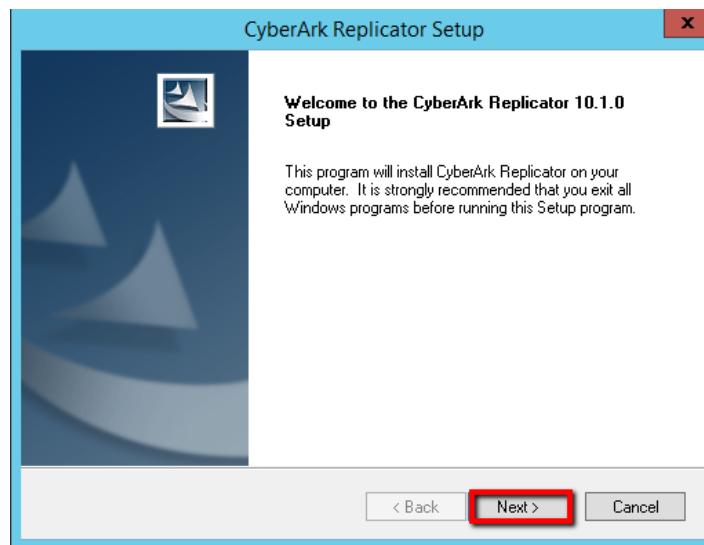




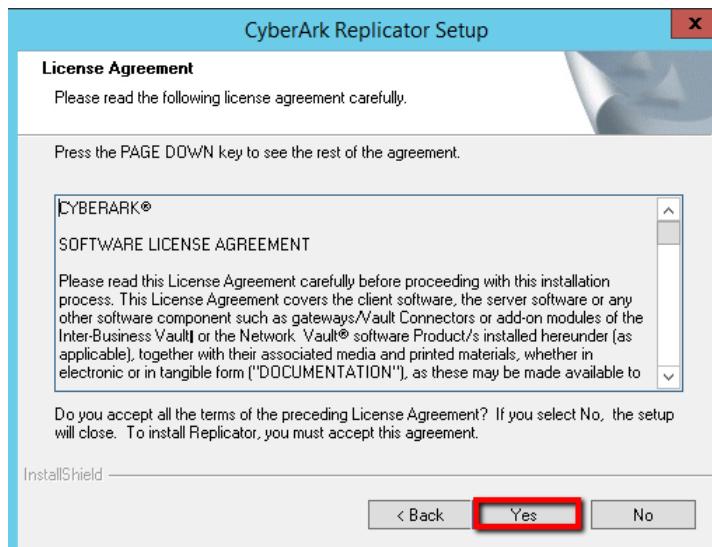
CYBERARK®

## Privileged Account Security Install & Configure, v10.x

3. Accept all of the default parameters to complete the installation. On the first screen enter **Next**.



4. Click **Yes** to accept the license agreement.

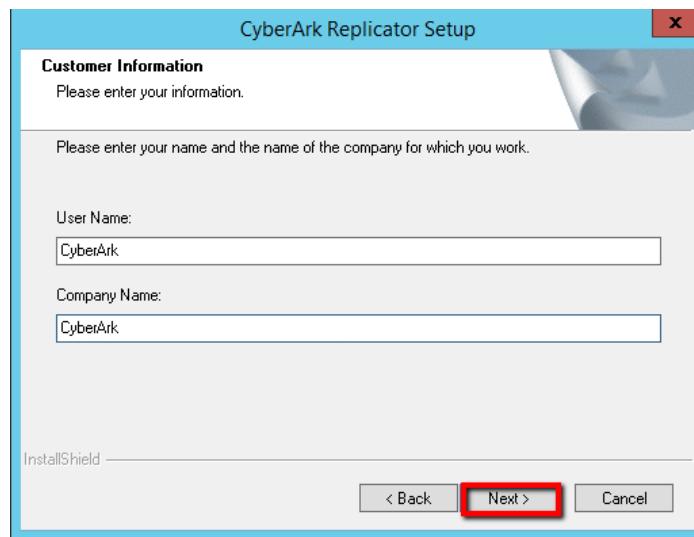




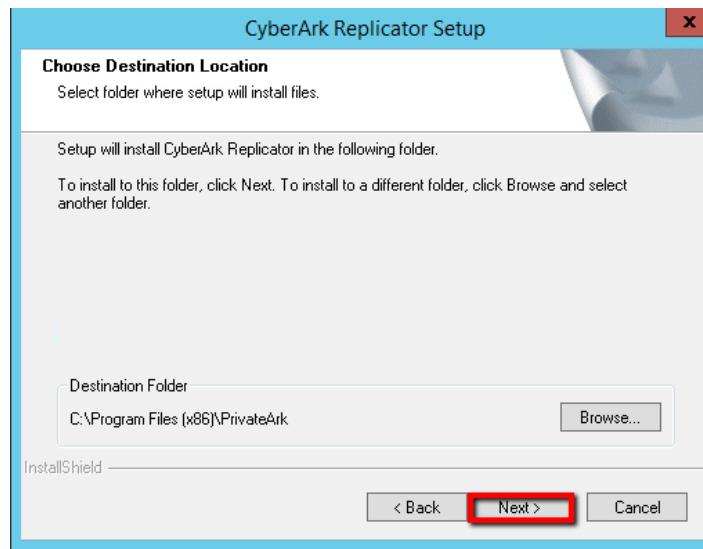
CYBERARK®

## Privileged Account Security Install & Configure, v10.x

5. Enter *CyberArk* for the user and company names and press **Next**.

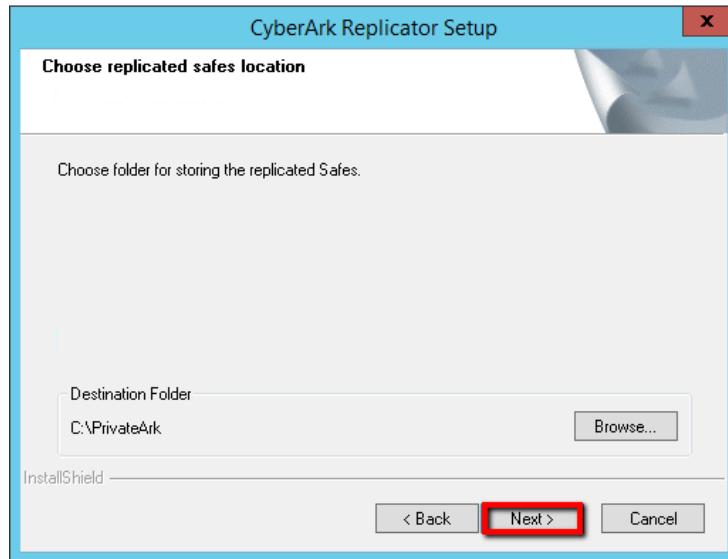


6. Press **Next** to accept the default destination location.

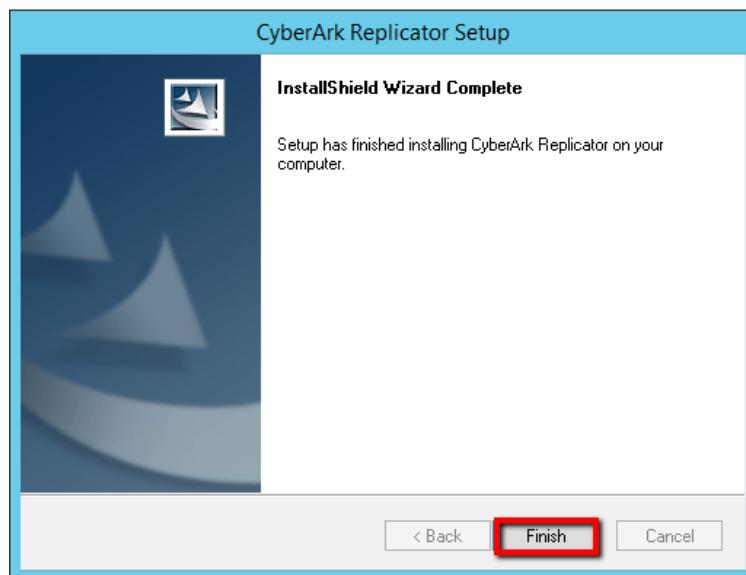




7. Press **Next** to accept the default **Safes** location.

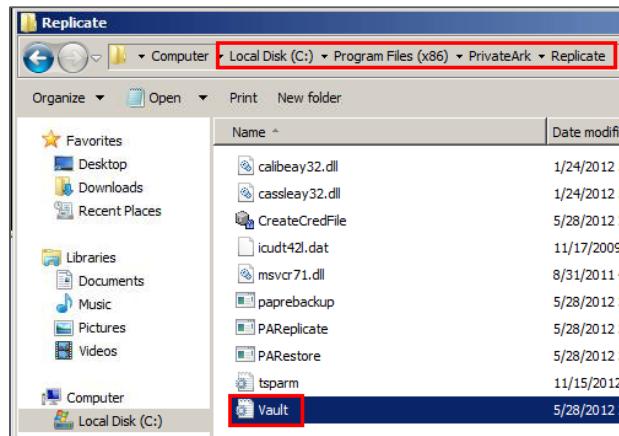


8. Click the **Finish** button.



9. In *Windows File Explorer*, go to *C:\Program Files (x86)\PrivateArk\Replicate*.

10. Double-click the **Vault.ini** file.

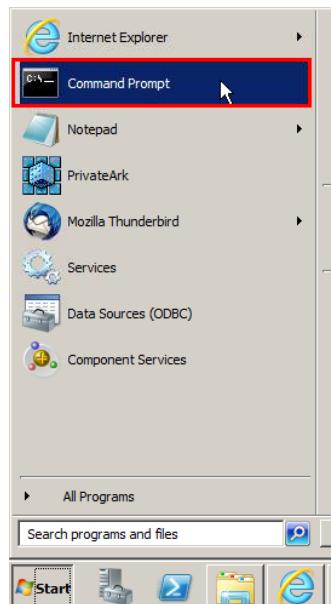


11. In the *vault.ini* file, enter “Vault” for the **VAULT** parameter.
12. Enter the IP address of your **Vault** server in the **address** parameter.
13. Save and close the file.

```
VAULT = "Vault"  
ADDRESS=10.0.0.10.X  
PORT=1858
```



14. Open a Command Prompt.



15. Enter the following: `cd "C:\Program Files (x86)\PrivateArk\Replicate"`

A screenshot of a Command Prompt window titled 'Administrator: Command Prompt'. The window shows the following text:  
Microsoft Windows [Version 6.1.7601]  
Copyright © 2009 Microsoft Corporation. All rights reserved.  
C:\Users\Administrator>cd "c:\Program Files (x86)\PrivateArk\Replicate"  
c:\Program Files (x86)\PrivateArk\Replicate>

16. Run the following:

```
CreateCredFile.exe user.ini  
Vault Username [mandatory] ==> Backup  
Vault Password...==> Cyberark1
```



17. Press **Enter** to accept the defaults for the remaining questions.

```
c:\Program Files (<x86>)\PrivateArk\Replicate>CreateCredFile.exe user.ini
Vault Username [mandatory] ==> backup
Vault Password {will be encrypted in credential file} ==> *****
Disable wait for DR synchronization before allowing password change {yes/no} [No]
[ ] ==>
External Authentication Facility {LDAP/Radius/No} [No] ==>
Restrict to Application Type [optional] ==>
Restrict to Executable Path [optional] ==>
Restrict to current machine IP {yes/no} [No] ==>
Restrict to current machine hostname {yes/no} [No] ==>
Restrict to OS User name [optional] ==>
Display Restrictions in output file {yes/no} [No] ==>
Command ended successfully

c:\Program Files (<x86>)\PrivateArk\Replicate>
```

18. To run the backup, enter:

```
PAREplicate.exe vault.ini /logonfromfile user.ini /FullBackup
```

```
c:\Program Files (<x86>)\PrivateArk\Replicate>PAREplicate.exe vault.ini /logonfrom
file user.ini /FullBackup
```

If the backup is successful, you should see a number of messages indicating that files are being replicated with a final message stating that the replication process has ended.

```
PAREP013I Replicating Safe PSMRecordings.
PAREP016I Replicating file root\4f36dd5f-1942-4122-8c94-af825245e942.vid.#000000
000000009#.avi.
PAREP016I Replicating file root\538799cd-235d-4da4-8d3a-dc94af533ffb.sql.#000000
000000006#.txt.
PAREP016I Replicating file root\538799cd-235d-4da4-8d3a-dc94af533ffb.vid.#000000
000000007#.avi.
PAREP016I Replicating file root\3f9fc7f-cdce-4a58-99fa-abee8ed750d4.ssh.#000000
000000003#.txt.
PAREP016I Replicating file root\3f9fc7f-cdce-4a58-99fa-abee8ed750d4.vid.#000000
000000004#.avi.
PAREP013I Replicating Safe Linux02.
PAREP016I Replicating file root\root.backup.#0000000000000001#.test.
PAREP022I Replication process of Vault Replicate {First IP 10.0.0.12} ended.

c:\Program Files (<x86>)\PrivateArk\Replicate>
```

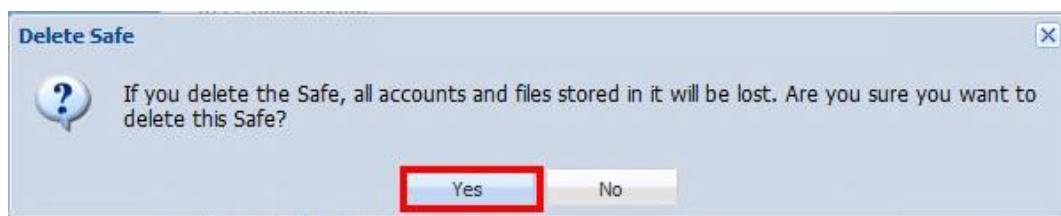


## Testing the Backup/Restore Process

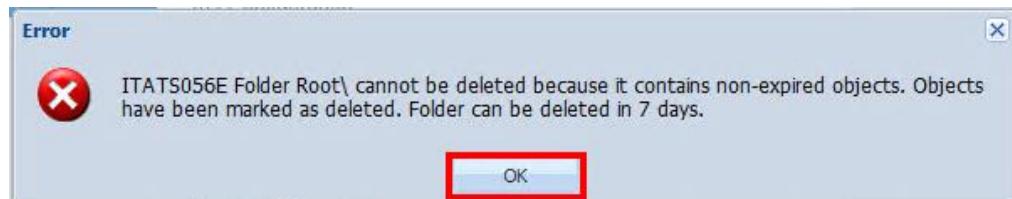
1. Login to the **PVWA** as **Vaultadmin01**.
2. Go to **POLICIES > Access Control (Safes)**.
3. Highlight your Linux accounts safe (for example, Linux02) and press the **Delete** button.

The screenshot shows the PVWA interface under the 'POLICIES' tab. The 'Access Control (Safes)' section is active. A specific safe named 'Linux02' is selected and highlighted with a red box. The 'Delete' button at the bottom right of the list area is also highlighted with a red box.

4. Press **Yes** to confirm that you would like to delete the **Safe** and its contents.



5. You will receive a message that the Root folder cannot be deleted for 7 days. However, the contents of the **Safe** should have been removed.





6. To confirm that the contents of the **Safe** have been deleted, go to the **Accounts** page.
7. Enter *root* in the search box and press the **Search** button.
8. The root account that you created earlier in this exercise using address *10.0.0.21*, should not appear.

9. Go back to the command prompt and run the following:

```
PARestore.exe vault.ini dr /RestoreSafe <Your Linux Safe Name> /TargetSafe  
LinuxRestore
```

Note: If the command doesn't run, check the syntax and make sure you have entered all of the spaces correctly. Use quotations for the safe name in case there is a space in the safe name (for example, if the name of the safe is Linux Account then use – "Linux Accounts").

10. Enter the DR user's password (*Cyberark1*).

```
c:\Program Files (x86)\PrivateArk\Replicate>PARestore.exe vault.ini dr /RestoreSafe  
Linux02 /TargetSafe LinuxRestore  
Password: *****
```



11. You should receive a message stating that the restore process has ended.

```
PARST011I Restore process of Vault Restore <10.0.0.12> started at Thu Nov 15 16:37:45 2012
PARST021I Restoring Metadata file backup-dump.sql.gz.
PARST009I Restoring file backup-dump.sql.gz.
PARST021I Restoring Metadata file cfg.backup-encrcfile.ini.gz.
PARST009I Restoring file cfg.backup-encrcfile.ini.gz.
PARST019I 1 out of 1 dump files restored successfully.
PARST020I 0 out of 0 Binary Logs restored successfully.
PARST027I 1 out of 1 Configuration files restored successfully.
PARST009I Restoring file root\root.backup.#00000000000001#.test.
PARST008I 1 out of 1 files restored successfully.
ITATS414I Synchronizing owners of Safe LinuxRestore.

ITATS659I Setting user Administrator as owner of Safe LinuxRestore.
ITATS659I Setting user Master as owner of Safe LinuxRestore.
ITATS659I Setting user Batch as owner of Safe LinuxRestore.
ITATS659I Setting user Backup Users as owner of Safe LinuxRestore.
ITATS659I Setting user Auditors as owner of Safe LinuxRestore.
ITATS659I Setting user Operators as owner of Safe LinuxRestore.
ITATS659I Setting user DR Users as owner of Safe LinuxRestore.
ITATS659I Setting user Notification Engines as owner of Safe LinuxRestore.
ITATS659I Setting user PUWAGMAccounts as owner of Safe LinuxRestore.
ITATS659I Setting user PasswordManager as owner of Safe LinuxRestore.
ITATS408I Synchronizing objects of Safe LinuxRestore...
ITATS412I Moving restored object root\root.backup.#00000000000001#.test to Root\root.backup.#00000000000001#.test.

PARST012I Restore process of Vault Restore <10.0.0.12> ended at Thu Nov 15 16:37:49 2012
:49 2012
c:\Program Files (x86)\PrivateArk\Replicate>
```

12. Go back to the **PVWA** as **Vaultadmin01** and search for *root* again.

13. You should now see the *root01* account residing in the **Safe LinuxRestore**.

The screenshot shows the PVWA interface with the following details:

- Header: APPLICATIONS REPORTS ADMINISTRATION, Account views V10 interface >, vaultadmin01
- Search bar: Search accounts results: "root" (with a dropdown menu), Secure Connect, Add SSH Key, Add Account, Customize, search input: root, clear button.
- Toolbar: Request Access, Manage, Modify, Add to, Detect Now.
- Table: A list of accounts with columns: Username, Address, Safe, Platform ID, and actions (Edit, Delete, etc.). The account "root01" is highlighted with a red border.

	Username	Address	Safe	Platform ID	
<input type="checkbox"/>	root01	10.0.0.20	LinuxRestore	UnixSSH	



## Disaster Recovery

In this section we will install and test the Disaster Recovery module. Prior to installing the DR software, the DR server must have the **Private Ark Server** installed. The **PrivateArk Server** and **Client** software has already been installed on your DR machine.

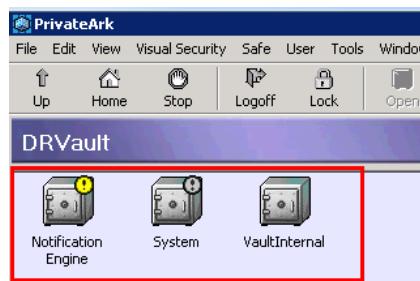
**Note:** The first step in Disaster Recovery is to create or enable a user to run the DR process .If you have completed the backup exercise, the DR user has already been enabled. If you haven't enabled the user yet please refer to the “**Enable the Backup and DR users**” section.

### Install the Disaster Recovery Module

1. Login to the Disaster Recovery server as *Administrator*.
2. Open the **PrivateArk** client and login to the **DRVault** as administrator.

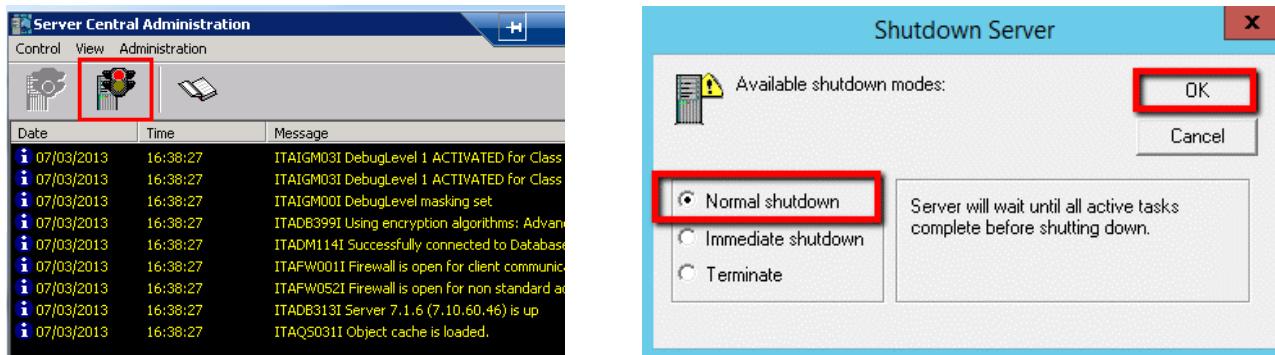


Note that the only **Safes** in the **Vault** are the three built-in Safes.

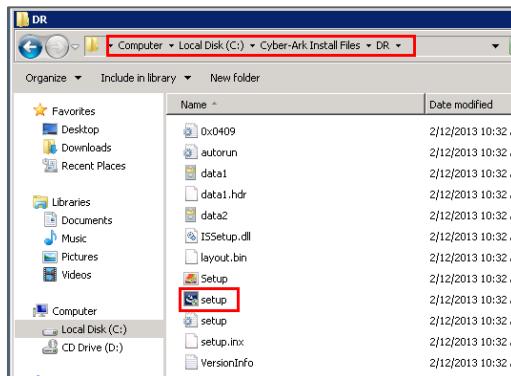




3. Logoff and close the **PrivateArk Client** application.
4. Double-click the **PrivateArk Server** icon on the desktop and press the **Stop** button. Disaster Recovery cannot be installed if the **PrivateArk** server service is running. Choose a *Normal shutdown*.



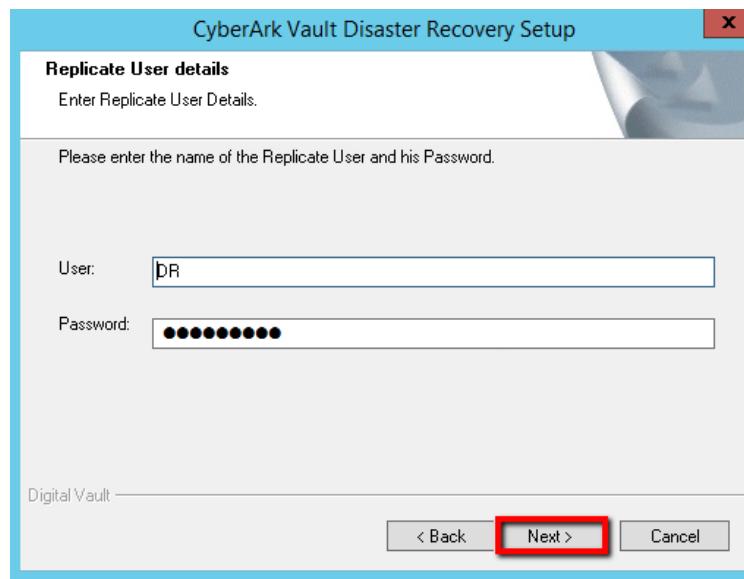
5. Close the **PrivateArk Server** GUI
6. Go to *C:\CyberArk Installation Files\Disaster Recovery* and double click **setup.exe**.



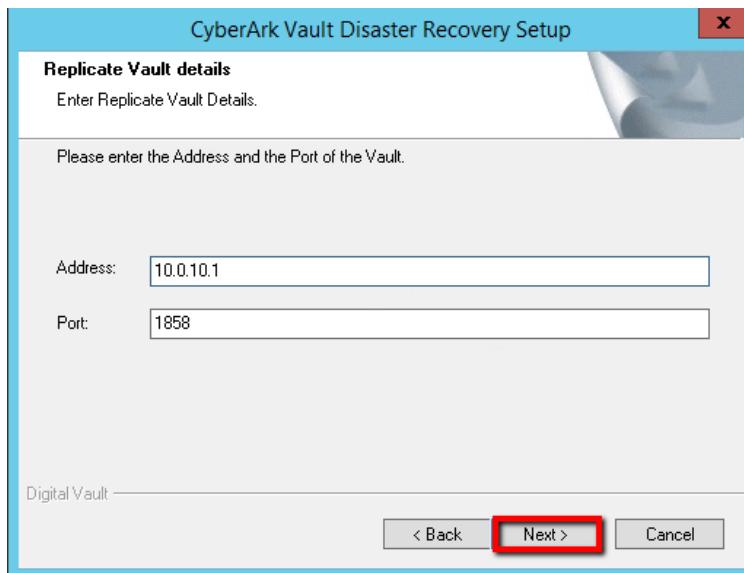
7. Press **Next** on the welcome screen and **Yes** to accept the license agreement. The enter *CyberArk* for **Name** and **Company** on the user information screen and click **Next** to accept the default destination folder.



8. Enter *dr* as the user and *Cyberark1* as the password and click **Next**.



9. Enter your **Primary Vault** IP and click **Next**,

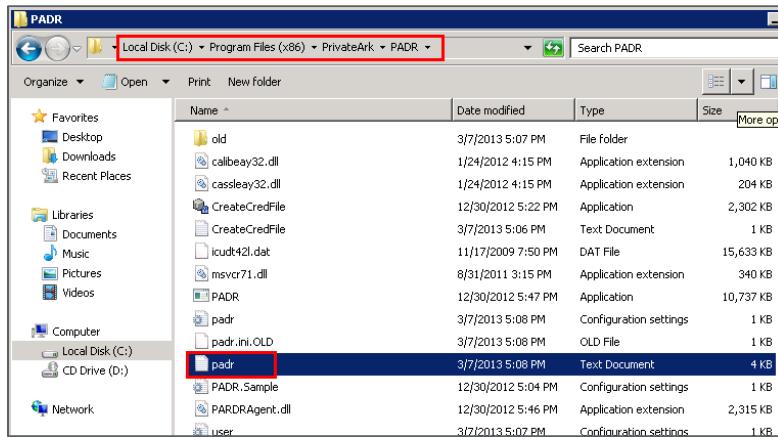


10. Finally allow the server to restart by pressing **Finish**.



## Validate the Replication was successful

1. After the server restarts, Log back in to the **DR server** as **administrator**.
2. Go to '*C:\Program Files (x86)\PrivateArk\PADR*'. Accept all notifications from User Account Control to edit security.
3. Using Notepad, open the *padr.log* file.



4. Confirm that the production **Vault** replicated correctly. You should see entries with informational codes PAREP013I Replicating Safe and at the end, PADR0010I Replicate ended.

The screenshot shows a Notepad window titled 'padr.log - Notepad'. The log file contains several lines of text representing log entries. A red box highlights the last two lines, which indicate the replication process has completed successfully:

```
[15/01/2018 12:36:56.537741] :: PAREP013I Replicating Safe PWATaskDefinitions.  
[15/01/2018 12:36:56.559827] :: PAREP013I Replicating Safe PWAPrivateUserPrefs.  
[15/01/2018 12:36:57.509159] :: PAREP013I Replicating Safe PWAPublicData.  
[15/01/2018 12:36:57.524058] :: PAREP013I Replicating Safe Windows Accounts.  
[15/01/2018 12:36:57.617202] :: PAREP013I Replicating Safe Linux Accounts.  
[15/01/2018 12:36:57.664312] :: PAREP013I Replicating Safe Database Accounts.  
[15/01/2018 12:36:57.727091] :: PAREP013I Replicating Safe PSM.  
[15/01/2018 12:36:57.984543] :: PAREP013I Replicating Safe PSMSessions.  
[15/01/2018 12:36:58.461047] :: PAREP013I Replicating Safe PSMLiveSessions.  
[15/01/2018 12:36:58.478298] :: PAREP013I Replicating Safe PSMNotifications.  
[15/01/2018 12:36:58.492816] :: PAREP013I Replicating Safe PSMUmanagedSessionAccounts.  
[15/01/2018 12:36:58.509094] :: PAREP013I Replicating Safe PSMRecordings.  
[15/01/2018 12:36:59.797519] :: PAREP013I Replicating Safe PSMPADBridgeConf.  
[15/01/2018 12:36:59.963160] :: PAREP013I Replicating Safe PSMPADBUserProfile.  
[15/01/2018 12:36:59.977633] :: PAREP013I Replicating Safe PSMPADBridgeCustom.  
[15/01/2018 12:37:00.053343] :: PAREP013I Replicating Safe CyberArk Administrators.  
[15/01/2018 12:37:00.085661] :: PAREP013I Replicating Safe LinuxRestore.  
[15/01/2018 12:37:00.159349] :: GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR]  
[15/01/2018 12:37:00.159410] :: C:\PADR\WorkingDir\Replicate ended [C:\Program Files (x86)\PrivateArk\PADR]  
[15/01/2018 12:37:00.161249] :: PADR0010I Replicate ended.  
[15/01/2018 12:37:01.196599] :: PADR00991 Metadata Replication is running successfully.
```

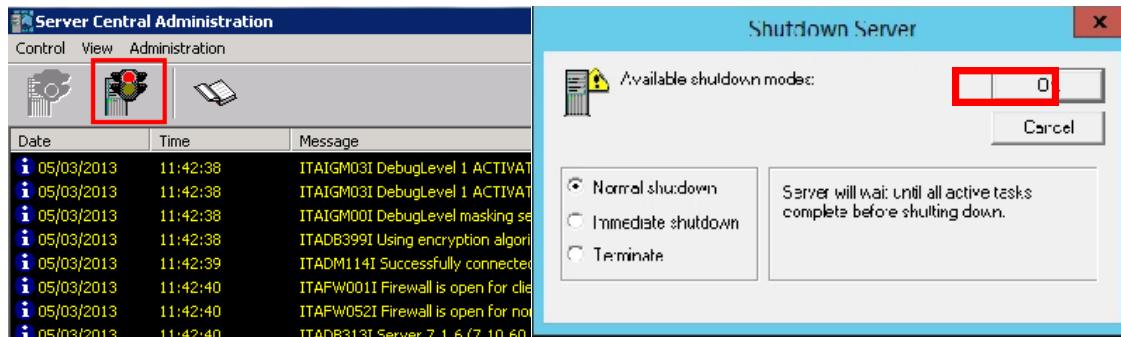


5. Open *PADR.ini* file and note that **FailoverMode** is equal to No.

```
[MAIN]
ReplicateLogonFromFile="C:\Program Files (x86)\PrivateArk\PADR\user.i
EnableCheck=Yes
EnableReplicate=Yes
EnableFailover=Yes
EnableDbSync=Yes
CheckInterval=60
CheckRetriesCount=5
CheckRetriesInterval=30
ReplicateInterval=3600
ReplicateRetriesInterval=300
AccessVaultForInactivity=Yes
FailoverMode=No
NextBinaryLogNumberToStartAt=0
LastDataReplicationTimestamp=1515960510416571
```

### Execute Automatic Failover Test

1. Logon to the console of your **Primary Vault** server,.
2. Stop the **PrivateArk Server** service, by clicking the **stoplight** as shown in the graphic. Select *Normal shutdown* and click **OK** and **Yes** at the confirmation popup.





3. On the console of the **DR Server**, open the PADR log file. You should see messages stating that the **DR Vault** cannot reach the production **Vault**.

Date	Time	Message
[07/03/2013]	17:07:50.417060	PADR0066I Replicating Metadata.
[07/03/2013]	17:07:50.417338	GetPADRworkingdirectory returned [C:\Program Files (x86)\PrivateArk\PADR]
[07/03/2013]	17:07:50.512172	PAREP061I Generating Full backup.
[07/03/2013]	17:08:13.626277	GetPADRworkingdirectory returned [C:\Program Files (x86)\PrivateArk\PADR]
[07/03/2013]	17:08:13.707122	PAREP013I Replicating Safe System.
[07/03/2013]	17:08:13.934927	PAREP013I Replicating Safe Pictures.
[07/03/2013]	17:08:14.006364	PAREP013I Replicating Safe vaultInternal.
[07/03/2013]	17:08:14.309716	PAREP013I Replicating Safe Notification Engine.
[07/03/2013]	17:08:14.576058	PAREP013I Replicating Safe Training01.
[07/03/2013]	17:08:14.751287	PAREP013I Replicating Safe PasswordManager.
[07/03/2013]	17:08:21.023305	PAREP013I Replicating safe PasswordManager_workspace.
[07/03/2013]	17:08:21.122726	PAREP013I Replicating safe PasswordManager_AdInternal1.
[07/03/2013]	17:08:21.165399	PAREP013I Replicating safe PasswordManager_Info.
[07/03/2013]	17:08:22.123110	PAREP013I Replicating safe PWUserPrefs.
[07/03/2013]	17:08:22.365409	PAREP013I Replicating safe PWAConfig.
[07/03/2013]	17:08:23.776456	PAREP013I Replicating safe PWReports.
[07/03/2013]	17:08:23.883792	PAREP013I Replicating safe PWATicketingSystem.
[07/03/2013]	17:08:23.923725	PAREP013I Replicating Safe PWATaskDefinitions.
[07/03/2013]	17:08:23.970337	PAREP013I Replicating Safe PWAPrivateuserPrefs.
[07/03/2013]	17:08:28.809559	PAREP013I Replicating Safe PWAPublicData.
[07/03/2013]	17:08:28.858002	PAREP013I Replicating Safe Linux.
[07/03/2013]	17:08:30.648150	PAREP013I Replicating Safe WinDomain.
[07/03/2013]	17:08:31.168036	PAREP013I Replicating Safe Oracle.
[07/03/2013]	17:08:31.392886	PAREP013I Replicating Safe Oracle02.
[07/03/2013]	17:08:31.457065	PAREP013I Replicating Safe PSM.
[07/03/2013]	17:08:31.643046	PAREP013I Replicating Safe PSMliveSessions.
[07/03/2013]	17:08:31.690795	PAREP013I Replicating Safe PSMUnmanagedSessionAccounts.
[07/03/2013]	17:08:32.534467	PAREP013I Replicating Safe PSMRecordings.
[07/03/2013]	17:08:34.681776	GetPADRworkingdirectory returned [C:\Program Files (x86)\PrivateArk\PADR]
[07/03/2013]	17:08:34.792523	PADR0010T Replicate ended
[07/03/2013]	17:16:35.254049	PADR0014E Attempt to test vault availability failed (code=1).
[07/03/2013]	17:17:35.688701	PADR0015E Attempt to test vault availability failed 2 times (code=-1066062).

4. Alternatively, follow the tail of the *padr.log* using Windows Powershell.



- Open Windows Powershell from the taskbar.
- Change directories to *C:\Program Files (x86)\PrivateArk\PADR*.
- Type the following command without the double quotes; **“Get-Content .\padr.log –wait”**



5. After a few minutes (5 failures by default), the DR **Vault** will go into failover mode.

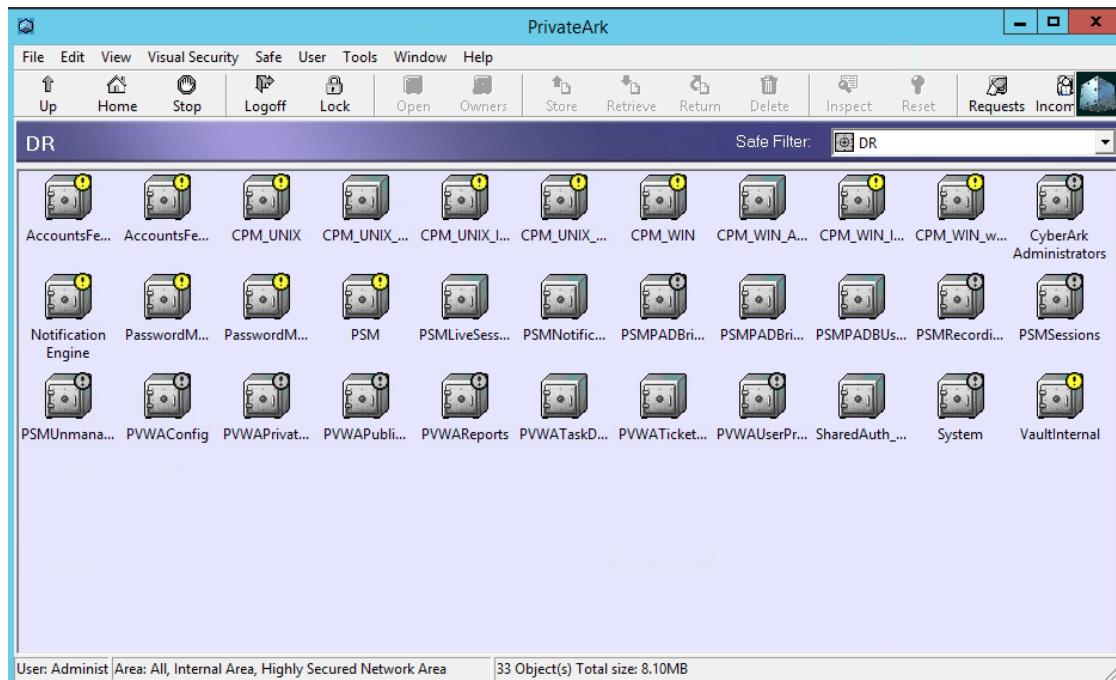
The screenshot shows a Windows Notepad window titled "padr.log - Notepad". The log file contains several entries related to the failover process:

```
[29/11/2017 12:37:46.940242] :: PADR0014E Attempt to test vault availability failed (code=1).
[29/11/2017 12:38:46.362197] :: PADR0015E Attempt to test vault availability failed 2 times (code=-1066062)
[29/11/2017 12:39:46.768290] :: PADR0015E Attempt to test vault availability failed 3 times (code=-1066062)
[29/11/2017 12:40:10.127875] :: PADR0099I Metadata Replication is running successfully.
[29/11/2017 12:40:46.221334] :: PADR0015E Attempt to test vault availability failed 4 times (code=-1066062)
[29/11/2017 12:41:46.628254] :: PADR0015E Attempt to test vault availability failed 5 times (code=-1066062)
[29/11/2017 12:41:46.628886] :: PADR0016E Vault availability test failed, failover started.

[29/11/2017 12:41:46.629185] :: PADR0101I Failover process started.
[29/11/2017 12:41:46.633409] :: GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR]
[29/11/2017 12:41:46.633433] :: GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR]
[29/11/2017 12:41:46.636165] :: PADR0024I Synchronizing vault data and metadata.
[29/11/2017 12:41:46.644734] :: ITATS408I Synchronizing objects of Safe Notification Engine...
[29/11/2017 12:41:46.645818] :: ITATS408I Synchronizing objects of Safe PVWAConfig...
[29/11/2017 12:41:46.646990] :: ITATS158I Deleting total of 0 objects.
[29/11/2017 12:41:46.647011] :: TTATS159T Updating total of 0 top version objects.

[29/11/2017 12:41:57.691180] :: PADR0025I Failover process ended successfully.
[29/11/2017 12:41:57.691215] :: PADR0067I Starting Vault service.
[29/11/2017 12:42:01.782015] :: PADR0017I Failover completed, PADR service is shutting down.
[29/11/2017 12:42:03.315484] :: PADR0022I Disaster Recovery service terminated.
```

6. On the **DR Vault** server, open the PrivateArk client from the desktop. Login as *Administrator* (don't forget the password for administrator has changed and must be retrieved from the Vault). Note that the Safes and data match those in the **Primary Vault**.

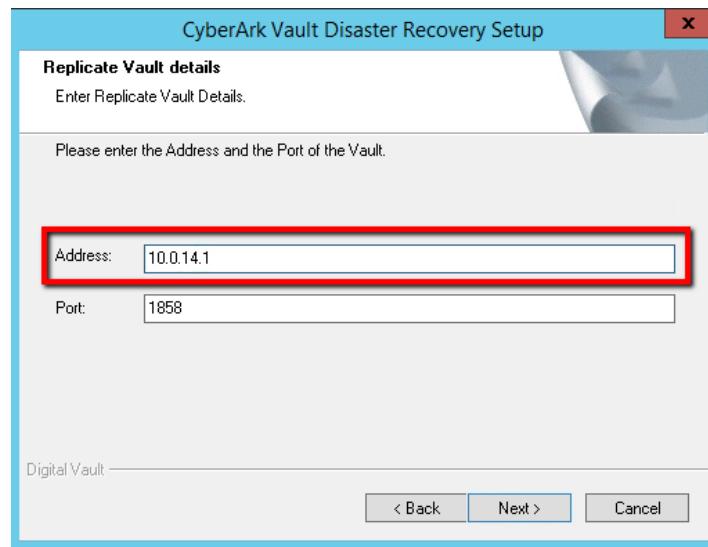


### Execute Fallback Procedure Using Manual Failover

In the next steps, you will replicate data back from the **DR Vault** to the **Primary Vault**, perform a **Manual Failover** to the **Primary Vault** up and set the DR server back to DR mode.



1. Login to the **Primary Vault Server** and Repeat the steps for Installing the DR module on the Primary Vault, this time configuring the DR module to replicate data from the DR Vault.



2. After restart, verify that the Primary Vault has replicated all the changes from the DR Vault.

```
padr.log - Notepad
File Edit Format View Help
[15/01/2018 12:36:56.537741] :: PAREP013I Replicating Safe PWATaskDefinitions.
[15/01/2018 12:36:56.559827] :: PAREP013I Replicating Safe PWAPrivateUserPrefs.
[15/01/2018 12:36:57.509159] :: PAREP013I Replicating Safe PWAPublicData.
[15/01/2018 12:36:57.524058] :: PAREP013I Replicating Safe Windows Accounts.
[15/01/2018 12:36:57.617202] :: PAREP013I Replicating Safe Linux Accounts.
[15/01/2018 12:36:57.664312] :: PAREP013I Replicating Safe Database Accounts.
[15/01/2018 12:36:57.727091] :: PAREP013I Replicating Safe PSM.
[15/01/2018 12:36:57.984543] :: PAREP013I Replicating Safe PSMSessions.
[15/01/2018 12:36:58.461047] :: PAREP013I Replicating Safe PSMLiveSessions.
[15/01/2018 12:36:58.478298] :: PAREP013I Replicating Safe PSMNotifications.
[15/01/2018 12:36:58.492816] :: PAREP013I Replicating Safe PSUmanagedSessionAccounts.
[15/01/2018 12:36:58.509094] :: PAREP013I Replicating Safe PSMRecordings.
[15/01/2018 12:36:59.797519] :: PAREP013I Replicating Safe PSMPADBridgeConf.
[15/01/2018 12:36:59.963160] :: PAREP013I Replicating Safe PSMPADBUserProfile.
[15/01/2018 12:36:59.977633] :: PAREP013I Replicating Safe PSMPADBridgeCustom.
[15/01/2018 12:37:00.053343] :: PAREP013I Replicating Safe CyberArk Administrators.
[15/01/2018 12:37:00.085661] :: PAREP013I Replicating Safe LinuxRestore.
[15/01/2018 12:37:00.159349] :: GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR]
[15/01/2018 12:37:00.159481] :: GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR]
[15/01/2018 12:37:00.161249] :: PADR0010I Replicate ended.
[15/01/2018 12:37:01.196599] :: PADR0099I Metadata Replication is running successfully.
```

3. On the **Primary server** edit the PADR.ini file.

- a. Set EnableFailover=No
- b. Add the following line: ActivateManualFailover=Yes
- c. Save the file and exit.



```
[MAIN]
ReplicateLogonFromFile="C:\Program Files (x86)\PrivateArk\PADR\user
EnableCheck=Yes
EnableReplicate=Yes
EnableFailover=No
EnableSync=Yes
CheckInterval=60
CheckRetriesCount=5
CheckRetriesInterval=30
ReplicateInterval=3600
ReplicateRetriesInterval=300
AccessVaultForInactivity=Yes
FailoverMode=No
ActivateManualFailover=Yes
NextBinaryLogNumberToStartAt=0
LastDataReplicationTimestamp=1516022791966811
```

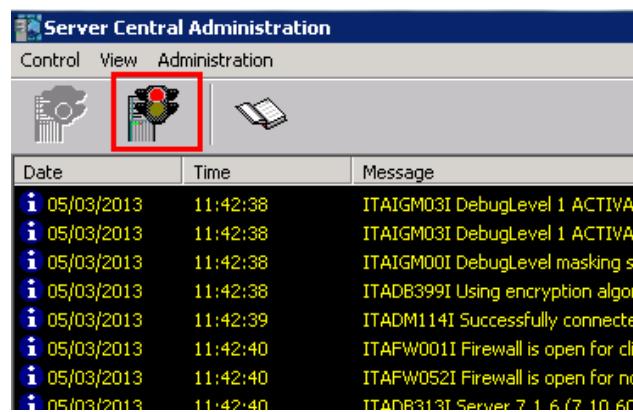
4. Restart the Disaster Recovery Service on the Primary Server. The service will start and stop immediately (because of the “ActivateManualFailover” parameter), followed by the Vault being started. Verify that the Vault has started successfully on the Primary server.



5. On the **DR server** edit the PADR.ini file.
  - a. Change *Failover mode* from **Yes** to **No**.
  - b. Delete the last two lines (log number and timestamp of the last successful replication) in the file.
  - c. Save and exit the file.

```
[MAIN]
ReplicateLogonFromFile="C:\Program Files (x86)\PrivateArk\PADR\user.ini"
EnableCheck=yes
EnableReplicate=yes
EnableFailover=yes
EnabledDbSync=yes
CheckInterval=60
CheckRetriesCount=5
CheckRetriesInterval=30
ReplicateInterval=3600
MetadataReplicateInterval=3600
MetadataReplicateFromHour=0
MetadataReplicateToHour=24
ReplicateRetriesInterval=300
AccessVaultForInactivity=Yes
FailoverMode=No
NextBinaryLogNumberToStartAt=3_
LastDataReplicationTimestamp=1362694009986808
```

6. Open the **PrivateArk Server GUI** and stop the **PrivateArk Server** service, by clicking the **stoplight** as shown in the graphic. Exit the PrivateArk Server GUI.





7. Open Windows Services and **Start** the *CyberArk Vault Disaster Recovery* service.



8. Check the PADR log file and confirm that the replication process started and that the replication (from the Primary Server to the DR Server) has ended successfully.

```
[[07/03/2013 17:28:49.300589] :: PAREP013I Replicating safe NOTIFICATION_Engine.  
[07/03/2013 17:28:49.382508] :: PAREP013I Replicating Safe_Training01.  
[07/03/2013 17:28:49.453385] :: PAREP013I Replicating safe PasswordManager.  
[07/03/2013 17:28:49.522656] :: PAREP013I Replicating safe PasswordManager_workspace.  
[07/03/2013 17:28:49.583829] :: PAREP013I Replicating safe PasswordManager_AdInternal.  
[07/03/2013 17:28:49.628205] :: PAREP013I Replicating safe PasswordManager_info.  
[07/03/2013 17:28:49.670601] :: PAREP013I Replicating safe PVWAUserPrefs.  
[07/03/2013 17:28:49.719965] :: PAREP013I Replicating safe PVWAConfig.  
[07/03/2013 17:28:49.893507] :: PAREP013I Replicating safe PVWAREports.  
[07/03/2013 17:28:49.945417] :: PAREP013I Replicating safe PVWATicketingSystem.  
[07/03/2013 17:28:50.045052] :: PAREP013I Replicating safe PVWATaskDefinitions.  
[07/03/2013 17:28:50.117108] :: PAREP013I Replicating safe PVWAPrivateUserPrefs.  
[07/03/2013 17:28:50.163862] :: PAREP013I Replicating safe PVWAPublicData.  
[07/03/2013 17:28:50.258949] :: PAREP013I Replicating safe Linux.  
[07/03/2013 17:28:50.334745] :: PAREP013I Replicating safe winDomain.  
[07/03/2013 17:28:50.420406] :: PAREP013I Replicating safe oracle.  
[07/03/2013 17:28:50.470065] :: PAREP013I Replicating safe oracle02.  
[07/03/2013 17:28:50.511606] :: PAREP013I Replicating safe PSM.  
[07/03/2013 17:28:50.586695] :: PAREP013I Replicating safe PSMLiveSessions.  
[07/03/2013 17:28:50.636587] :: PAREP013I Replicating safe PSMUnmanagedSessionAccounts.  
[07/03/2013 17:28:51.507068] :: PAREP013I Replicating safe PSMRecordings.  
[07/03/2013 17:28:51.579867] :: GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR]  
[07/03/2013 17:28:51.648598] :: PARD0010I Replicate ended.
```



## EPV Implementations (Proposed Solution)

Note: The following instructions are meant to assist you in case you get stuck during the advanced EPV implementations. These instructions are only meant to be used as a reference for this lab.

### Windows

***The Customer has one Domain Controller (10.0.0.2) and one windows server in the domain (10.0.10.50). The domain administrator account is admin01...winadmin01 is a member of the WindowsAdmins group in LDAP. Members of the WindowsAdmins group should be given permissions on all Windows accounts***

These two sections require us to create a safe to store Windows Accounts and create one windows domain account. You should duplicate the “Windows Domain Accounts” platform. Since all members of *WindowsAdmins* should have access to all windows accounts, it’s ok to use just one safe to store the domain accounts and the local accounts.

What requirement would force you to create separate safes for domain and local accounts?

1. Create safe ‘Windows Accounts’ and assign CPM: CPM\_WIN
2. Add the ldap group WindowsAdmins with default permissions.
  - a. Duplicate the Windows Domain Accounts platform and name it “cyberark lab Windows Domain Accounts” (may require an IISRESET or a 20 minute wait for the PVWA to refresh the active policy list)
3. Create Admin01 ldap account
  - a. Add the domains FQDN to the address field.
  - b. Select “Logon To:” parameter and select Resolve to populate the field.

**Members**

User Name	Use	Retri...	List	Add	Upda...	Upda...	CPM	Rena...	Delete	Un
CPM_WIN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
vaultadmin01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
<b>WindowsAdmins</b>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

**Password**

*****	Show	Copy
PSM-RDP	Connect	Copy Shortcut
Platform Name: cyber-ark-demo Windows Domain Accounts	<input type="button" value=""/>	
Device Type: Operating System		
Safe: Windows Accounts		
Name: Operating System-WinDomain-cyber-ark-demo.local-admin01		
Last verified: 1/7/2018 1:22:29 PM		
Last modified: vaultadmin01 (1/9/2018 3:27:05 PM)		
Last used: vaultadmin01 (1/9/2018 3:27:05 PM)		
Username: admin01		
Logon To: CYBER-ARK-DEMO		
Address: cyber-ark-demo.local		



***"The local administrator account on the domain member (10.0.10.50) is localadmin01 (the password for the local admin account is unknown)".***

This section requires us to create a Windows Local Server Account and reconcile the local account using admin01. You have 2 options; use Accounts Discovery or add the account manually. Regardless of your choice ensure the following steps.

1. Duplicate the ‘Windows Server Local Accounts’ platform and name it, “cyberark lab Windows Server Local Accounts” (may require an IISRESET or a 20 minute wait for the PVWA to refresh the active policy list)
2. Create account 10.0.10.50\localadmin01 in safe ‘Windows Accounts’ and assign it to the platform created in step 1. Leave the password field blank.
3. Associate Reconcile Account cyber-ark-demo\admin01 and execute a Reconcile operation.

The screenshot shows two windows side-by-side. The left window is titled 'CPM' and contains fields for 'Logon Account' (set to 'Administrator') and 'Reconcile Account' (set to 'Windows Domain Account-admin01-cy...'). It also shows an 'Account Group' section with 'Group: [None]'. The right window is titled 'Password' and displays a password field containing '\*\*\*\*\*', a 'Show' button, a 'Copy' button, and a dropdown menu set to 'RDP' with 'Connect' and 'Copy Shortcut' buttons. Below these are detailed account properties:

Platform Name:	Windows Server Local Accounts
Device Type:	Operating System
Safe:	Windows Accounts
Name:	DomainMember.cyber-ark-demo.local-localadmin01-5c421cc6-c4cb-4b1d-a48c-9e3c7effab21
Last verified:	N/A
Last modified:	CPM_WIN (1/31/2017 2:13:53 AM)
Last used:	winadmin01 (2/2/2017 4:06:34 AM)
Username:	localadmin01
Address:	DomainMember.cyber-ark-demo.local

***"On the domain member there is a scheduled task (SchedTask01) that runs under the context of the localadmin01 user and is programmed to send the vault administrator (vaultadmin01) an email every time it runs. Note that although the scheduled task runs under the credentials of localadmin01, only admin01 has permissions to change the password for SchedTask01".***

This section requires us to add a **Windows Scheduled** task to the **localadmin01** account, and use **admin01** as the logon account for the usage. This usage can be added manually or discovered automatically using Accounts Discovery but the logon account must be assigned to the Scheduled Task usage manually.



1. Add a Windows Scheduled task usage to the localadmin01 account.
  - o Task Name = SchedTask01
  - o Address = 10.0.10.50 (or domainmember.cyber-ark-demo.local)
2. Assign logon account Admin01, to usage.
3. Ensure “SearchForUsages” parameter is set to Yes in the account platform.
4. Change the localadmin01 account password. Wait for the next CPM cycle to update the SchedTask01 usage.
5. Test by running command “schtasks /run /s 10.0.10.50 /tn schedtask01” and login to the WebMail client for confirmation.

The left window shows the 'Logon Account' search results. The right window shows the 'Scheduled Task' list with one entry: 'SchedTask01' (Address: 'DomainMember.cyber-ark-demo.local').

## UNIX

***The Customer has one Linux server (10.0.0.20). The root account on the server is called root01. linuxadmin01 is a member of the LinuxAdmins group in LDAP... Members of the LinuxAdmins group should be granted permissions on all the Linux accounts.***

This section only requires us to create a safe to store Unix accounts (in my example it's called **Linux Accounts**), assign permissions to **LinuxAdmins** and create a single Unix account. Duplicate the **Unix via SSH** platform.



1. Create a safe to store Unix accounts named “Linux Accounts”
2. Assign CPM: CPM\_UNIX
3. Assign default permissions to ldap group LinuxAdmins
4. Duplicate the ‘Unix via SSH’ platform. Name it “cyberark lab Unix via SSH”
5. Create the Unix account root01 in safe Linux Accounts.
  - o Assign to “cyber-ark-demo Unix via SSH” platform created in the previous step.
  - o Address = 10.0.0.20
  - o Password = Cyberark1

The left screenshot shows the 'Platform' configuration for 'cyberark lab Unix via SSH'. The right screenshot shows the 'Members' list where the 'LinuxAdmins' group is selected and highlighted with a red border.

## Database

***The Linux server mentioned above (10.0.0.20) also hosts an Oracle database .The name of the database is xe. The port is 1521. The database administrator account is named dba01...OracleAdmin01 is a member of the OracleAdmins group in LDAP. Members of the OracleAdmins group should be granted permissions on all Oracle Accounts”***

These two sections require us to create a safe to store Database/Oracle accounts and create an oracle account called **dba01**. Duplicate the **Oracle Database** platform.



1. Create a safe named 'Database Accounts'. Assign CPM\_Unix.
2. Assign default permissions to ldap group, OracleAdmins.
3. Duplicate the 'Oracle Database' platform. Name it 'cyberark lab Oracle Database'
4. Edit the 'cyberark lab Oracle Database' platform.
  - o Navigate to Automatic Password Management > Generate Password. Update the MinSpecial parameter to a value of -1.
5. Create Oracle account dba01 in 'Database Accounts' safe, assigned to the 'cyberark lab Oracle Database' platform created in the previous step.
  - o Address = 10.0.0.20
  - o Database = xe
  - o Port = 1521
  - o Password = Cyberark1

The screenshot shows two windows from the CyberArk PAM interface. On the left is the 'Members' list window, which displays users and their permissions across various platforms. The 'Platform Name' column is sorted, and the first three rows are highlighted with a red border: 'CPM UNIX', 'OracleAdmins', and 'vaultadmin01'. The 'Safe' column indicates they are members of the 'Database Accounts' safe. On the right is a detailed view of the 'Platform Name: cyberark lab Oracle Database'. This view includes fields for Device Type (Database), Safe (Database Accounts), and specific connection details: Name, Last verified, Last modified, Last used, Username, Port, Address, and Database. The 'Platform Name' field is also highlighted with a red border.

*"In addition, there is an application on the Linux server that connects to the Oracle database using the dba01 credentials. The credentials are stored in a text file (/var/opt/app/app01.ini). When the CPM changes the password for dba01, it must also change the password stored in the app01.ini file. Note that only root01 has permissions to change the password in the file".*

This section requires us to create an **INI configuration file** usage for dba01 and set **root01** as the logon account for the usage. Before we can do so, we must add a usage called **INIConfigFile** to the "cyberark lab Oracle Database" platform, and set **SearchForUsages** to **Yes**. Then we can add the INI configuration file to the dba01 account and associate the account **root01** as the logon account for that usage.



1. INI Section = Server
2. INI Parameter Name = Password
3. Connection Type: SSH

The screenshot shows the Oracle Database Properties window. On the left is a tree view of database components: Target Account Platform, UI & Workflows, Properties, Linked Accounts, Ticketing System, Privileged Session Management, Connection Components, Usages, INIConfigFile, Automatic Password Management, General, and Privileged Account Management. The 'Properties' tab is selected on the right, displaying a table of properties:

Name	Value
PolicyID	Oracle
PolicyName	Oracle Database
PolicyType	Regular
ImmediateInterval	5
Interval	1440
MaxConcurrentConnections	3
<b>SearchForUsages</b>	<b>Yes</b>
LooselyConnectedDevices	No
AllowedSafes	*

The screenshot shows the Oracle Database Properties window. The 'INIConfigFile' node is selected in the tree view on the left. The 'Properties' tab is selected on the right, displaying a table of properties:

Name	Value
<b>Name</b>	<b>INIConfigFile</b>

The screenshot shows the INI Config File interface. The 'INI Config File' tab is selected. On the left, there is a table with columns: CPM, Activities, Versions, INI Config File, and Advanced. The 'INI Config File' column has buttons for 'Add' and 'Edit'. The main area shows a table with one row:

File Path	INI Parameter Name	Address
/var/opt/app/app01.ini	Password	10.0.0.20

On the right, there is a panel with tabs: CPM, Activities, Advanced. The 'Logon Account:' field contains 'Unix via SSH-root01-10.0.0.20'. There are 'Clear', 'Associate', and 'Create New' buttons.



**Note:** If you've done everything correctly, by the end of this entire part you should end up with four main accounts in total (as well as two usages).

	Username	Address	Safe ▾	Platform ID
<input type="checkbox"/>	localadmin01	DomainMember.cyber-ark-demo.local	Windows Accounts	WinServerLocal
<input type="checkbox"/>	admin01	cyber-ark-demo.local	Windows Accounts	WinDomain
<input type="checkbox"/>	root01	10.0.0.20	Linux Accounts	UnixSSH
<input type="checkbox"/>	dba01	10.0.0.20	Database Accounts	Oracle