
CyberArk University

Privileged Access Security Administration

Exercise Guide

Contents

CONTENTS.....	2
INTRODUCTION	7
USING SKYTAP	7
INTERNATIONAL USERS	10
USER MANAGEMENT.....	13
CREATING A CUSTOM USER MAPPING.....	13
NESTING THE POWER USERS GROUP UNDER THE BUILT-IN CYBERARK GROUPS	19
<i>Nesting the Power Users group under Vault Admins.....</i>	19
<i>Nesting the Power Users group under the PWAMonitor group.....</i>	22
<i>Viewing the differences between Vault Admins and Power Users groups.....</i>	24
PASSWORD MANAGEMENT – PART 1.....	27
EDITING THE MASTER POLICY	27
<i>Disable Require users to specify reason for access.....</i>	27
<i>Change passwords daily instead of weekly.....</i>	28
<i>Activate the PSM.....</i>	29
MANAGING LINUX ACCOUNTS WITH SSH.....	29
<i>Creating a Safe.....</i>	29
<i>Duplicating a Platform.....</i>	32
<i>Adding a Linux account.....</i>	35
<i>Changing the password.....</i>	39
<i>Auditing Account Activity.....</i>	41
MANAGING WINDOWS DOMAIN ACCOUNTS	42
<i>Duplicating a Platform.....</i>	42
<i>Creating a Safe.....</i>	45
<i>Adding a Windows Account.....</i>	46
<i>Create a Second Windows Domain Account.....</i>	48
CONFIGURING THE MASTER POLICY	50
PRIVILEGED ACCESS WORKFLOWS.....	50
<i>Require dual control access approval.....</i>	50
<i>Require users to specify reason.....</i>	52
PASSWORD MANAGEMENT	52
PASSWORD MANAGEMENT – PART 2.....	53
CONFIGURING A LOG-ON ACCOUNT	53
MANAGING A WINDOWS LOCAL SERVER ACCOUNT WITH RECONCILIATION.....	56
<i>Duplicating a Platform.....</i>	56

<i>Creating a Safe.....</i>	58
<i>Adding an Account.....</i>	59
CONFIGURE AND TEST DUAL CONTROL	62
<i>Adding a manager to an existing safe.....</i>	62
<i>Testing Dual Control.....</i>	64
EXCLUSIVE PASSWORDS WITH AUTOMATED RELEASE AND ONE-TIME USE.....	68
<i>Adding a Master Policy exception for Exclusive Passwords.....</i>	68
<i>Adding a Master Policy exception for One-Time Passwords.....</i>	70
<i>Reducing the Minimum Validity Period.....</i>	70
<i>Testing Exclusive Passwords.....</i>	71
MANAGING AN ORACLE ACCOUNT	73
<i>Creating a Safe.....</i>	73
<i>Duplicating a Platform.....</i>	74
<i>Adding an Account.....</i>	76
OPTIONAL: MANAGING A LINUX ACCOUNT WITH SSH KEY.....	77
<i>Generating a Key-Pair.....</i>	78
<i>Verify You Are Able to Log in with the Private Key.....</i>	83
<i>Duplicating a Platform.....</i>	84
<i>Add an Account with an SSH key.....</i>	85
ONBOARDING ACCOUNTS.....	87
ACCOUNTS FEED	87
<i>Configure Automatic Onboarding Rules.....</i>	87
<i>Configure and Run Windows Accounts Discovery.....</i>	89
<i>Verify Automatically Onboarded Accounts.....</i>	93
<i>Manually onboard discovered accounts.....</i>	94
PASSWORD UPLOAD UTILITY	96
<i>Add the Administrator as a member of template safe.....</i>	96
<i>Configure and run PUU.....</i>	97
PRIVILEGED SESSION MANAGEMENT	104
PRIVILEGED SESSION MANAGER.....	104
<i>Enabling PSM.....</i>	104
<i>Connect with a Linux Account.....</i>	106
<i>Connect with an Oracle Account.....</i>	109
<i>Connect via HTML5 Gateway.....</i>	111
<i>Connect using PSM Ad-Hoc Connection.....</i>	112
PRIVILEGED SESSION MANAGER FOR WINDOWS	115
PRIVILEGED SESSION MANAGER FOR SSH	118
AUDITING USER ACTIVITY IN THE PSM (MONITORING).....	119
<i>Monitor Active Sessions.....</i>	119
<i>Monitor Recordings.....</i>	120

PRIVILEGED THREAT ANALYTICS.....	123
UNMANAGED PRIVILEGED ACCESS.....	123
SUSPECTED CREDENTIAL THEFT AND AUTOMATIC PASSWORD ROTATION	125
SUSPICIOUS PASSWORD CHANGE AND AUTOMATIC RECONCILIATION.....	128
SUSPICIOUS ACTIVITIES IN A SESSION AND AUTOMATIC SUSPENSION	130
SECURITY RULES EXCEPTIONS.....	132
CONNECT TO THE PTA ADMINISTRATION INTERFACE.....	134
REPORTS.....	135
GENERATE "PRIVILEGED ACCOUNTS INVENTORY" REPORT	135
GENERATE "SAFES LIST" REPORT AND "USERS LIST" REPORT	137
COMMON ADMINISTRATIVE TASKS.....	140
BACKUP AND RESTORE.....	140
<i>Enabling the Backup and DR users.</i>	140
<i>Installing the PrivateArk Replicator.</i>	142
<i>Create a Safe and an Account to test Backup.</i>	147
<i>Running a Backup</i>	148
<i>Delete the Linux02 Safe</i>	148
<i>Running a Restore</i>	149
REMOTE CONTROL CLIENT	150
<i>Configuring the Remote Control Client on the Vault:</i>	150
<i>Connecting with the Remote Control Client from the Components server:</i>	151
<i>Create a password file for the Remote Agent.</i>	152
<i>Verify the changes made with the Remote Control Client</i>	153
ROTATING CPM LOGS.....	153
LOG IN WITH MASTER.....	154
OPTIONAL EXERCISES.....	156
AD HOC ACCESS	156
<i>Set up the Ad Hoc Access Platform</i>	157
<i>Add the Local Administrator Account</i>	159
<i>CPM Scanner Configuration</i>	159
<i>Test Ad Hoc Access</i>	160
USAGES	162
<i>Manage a Scheduled Task Usage</i>	162
<i>Managing a Configuration File Usage</i>	167
CUSTOM FILE CATEGORIES	171
<i>Creating the Custom File Category</i>	171
<i>Adding the Custom File Category to the Platform</i>	173
<i>Making the File Categorical Searchable</i>	174
<i>Testing the New File Category</i>	175

Important Notice

Conditions and Restrictions

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

This guide contains proprietary information belonging to CyberArk Software Ltd. Such information is supplied solely for the purpose of assisting explicitly and properly authorized users of the CyberArk 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 CyberArk 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 CyberArk Vault may be subject to terms and conditions listed on 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.

Copyright

© 2000-2015 CyberArk Software Ltd. All rights reserved.
US Patent No 6,356,941.

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

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

Information in this document is subject to change without notice.

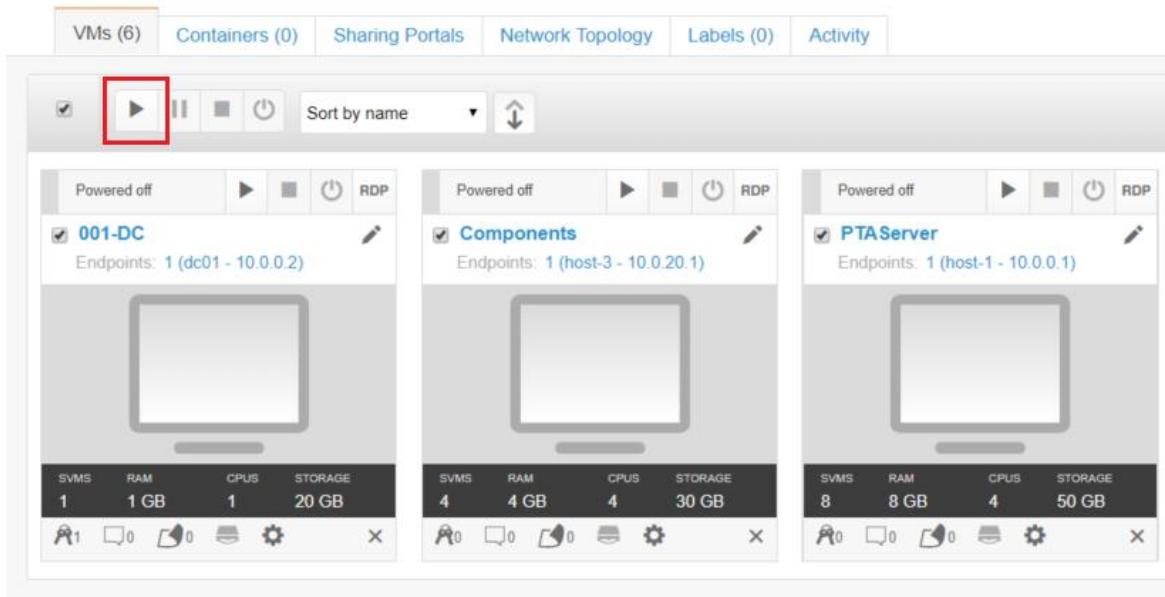


Introduction

Using Skytap

Before beginning exercises, here are a few tips to help you navigate the labs more effectively. You can refer to the section for **International Users** for instructions on changing the keyboard.

1. The virtual machines need to be running in order for you to be able to do the exercises. You can start all of the virtual machines with one click by pressing the start button (highlighted in red in the image below).



Note: The number and names of virtual machines vary by course. The image above is given as an example and might not match exactly what you see.

The environments have been set up to start up gradually: first the domain controller, then the Vault, and so on. It will take a few minutes for them to get up and running. Also note, that some machines are designed *not* to start automatically. This is the case of the **PTA Server** in the image below. It is not needed until later in the course, so you can start it when instructed in the manual or by the CyberArk trainer.

Occasionally, for reasons outside our control, one or more machine may fail to start up when requested. If you notice that a particular machine is not responding to a ping or if you cannot log in using Active Directory, you should check your virtual machines to make sure they are all running properly.



The screenshot shows the CyberArk Privileged Access Security interface with the 'VMs (6)' tab selected. There are three virtual machines listed:

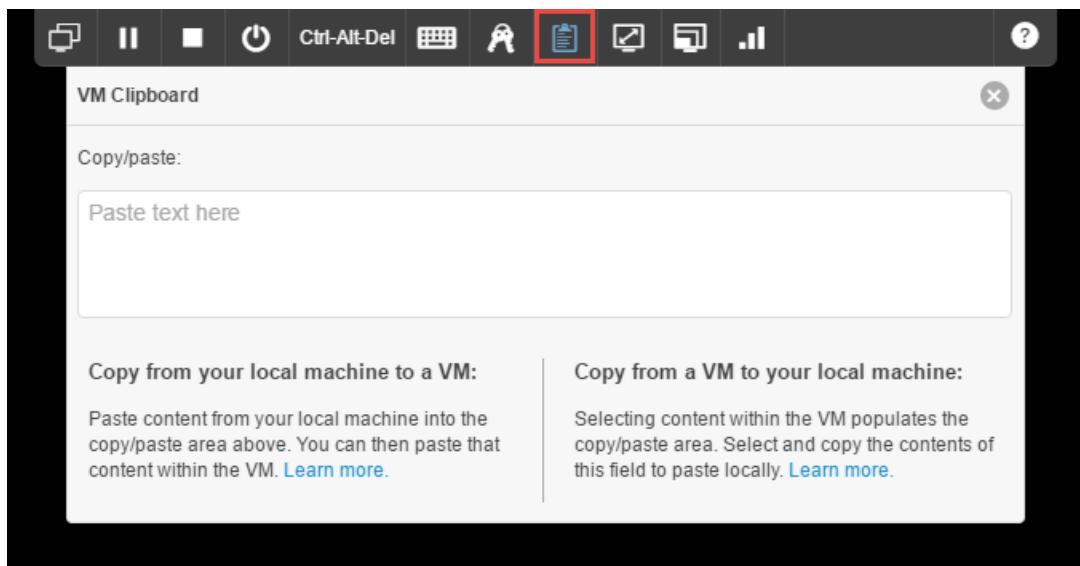
- 001-DC**: Running, 1 endpoint (dc01 - 10.0.0.2). Configuration: 2 SVMS, 2 RAM (2 GB), 2 CPUs, 20 GB storage. Tools: RDP, clipboard, settings, close.
- Components**: Running, 1 endpoint (host-3 - 10.0.20.1). Configuration: 4 SVMS, 4 RAM (4 GB), 4 CPUs, 30 GB storage. Tools: RDP, clipboard, settings, close.
- PTA Server**: Powered off. Configuration: 8 SVMS, 8 RAM (8 GB), 4 CPUs, 50 GB storage. Tools: RDP, clipboard, settings, close.

At the top, there is a toolbar with icons for VM control (play, pause, stop, power) and sorting.

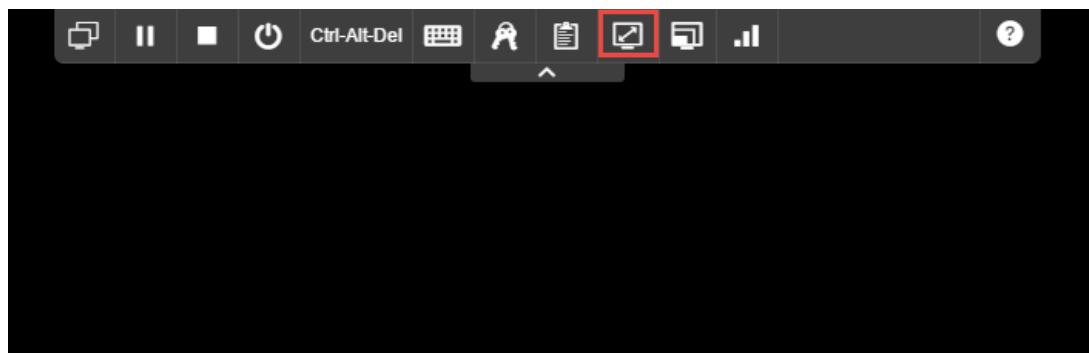
2. Click on the large monitor icon to connect to a virtual machine with the HTML 5 client.
3. Use the **Ctrl-Alt-Del** button on the tool bar to send a Ctrl-Alt-Del to the machine.



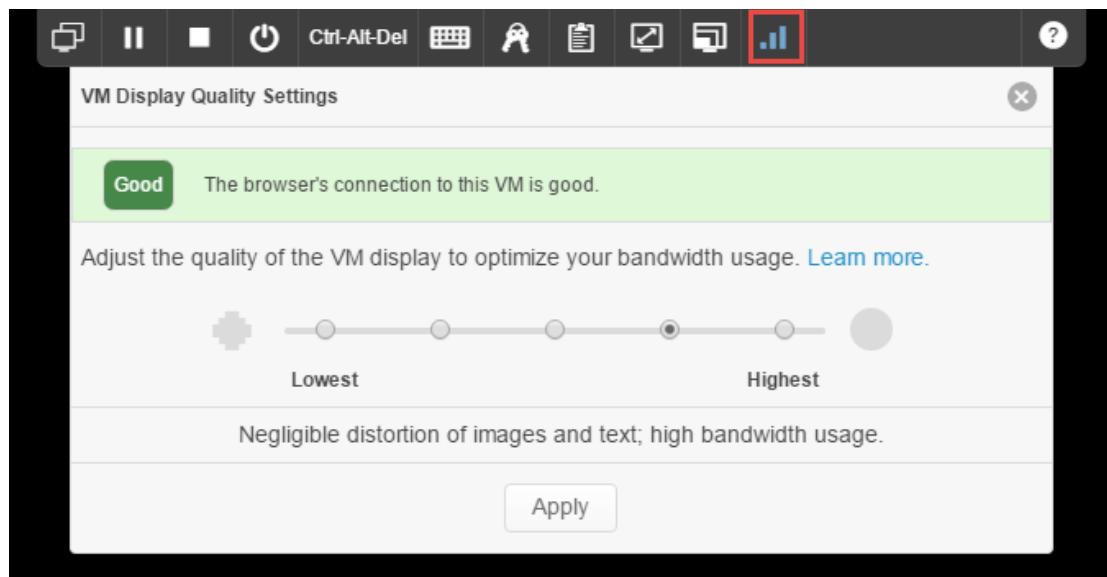
4. The clipboard icon will allow you to copy and paste text between your computer and your lab machine.



5. The full screen icon will resize your virtual screen to adapt to your computer's screen settings to avoid scrolling.



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

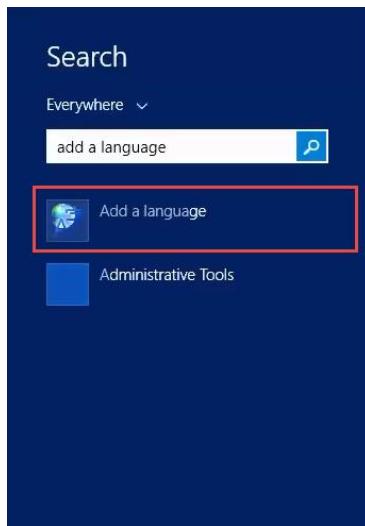




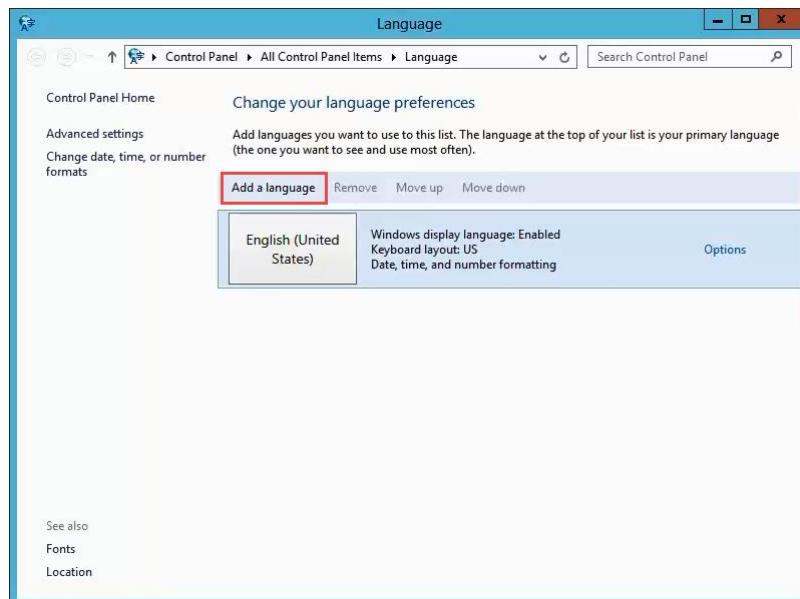
International Users

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.

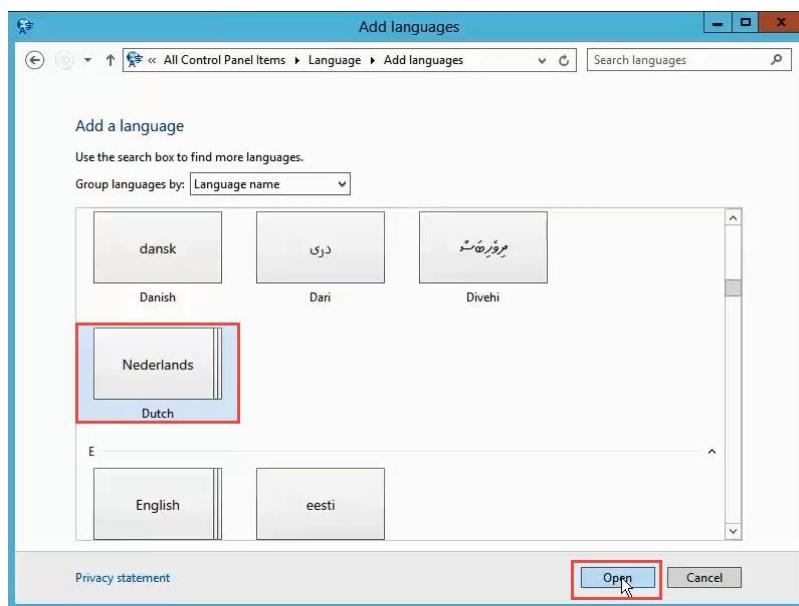
1. From the **Start Menu** launch “Add a language.”



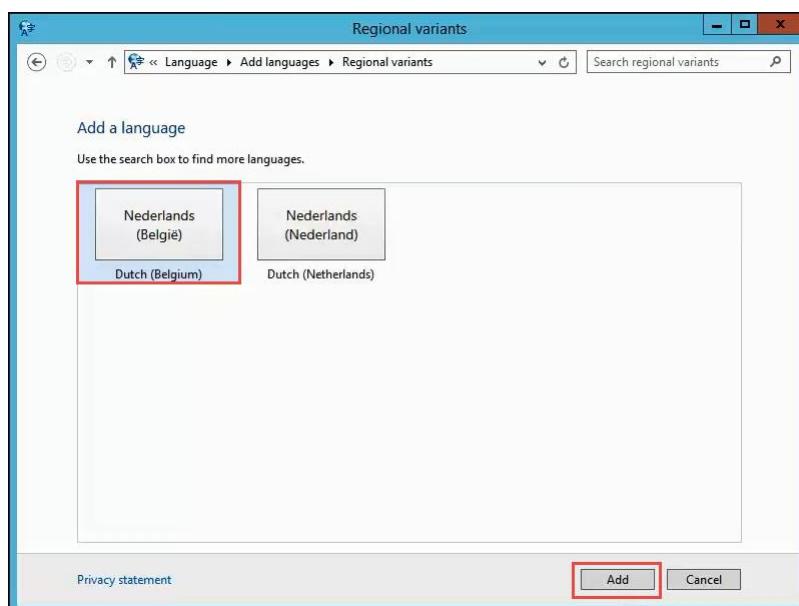
2. Click “Add a language.”



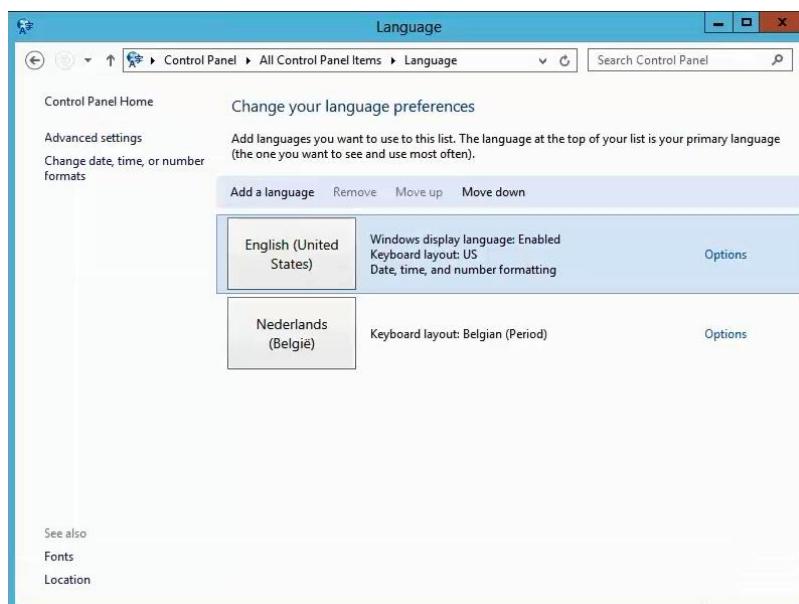
3. Select your language. Click **Open**.



4. Select your specific locality or dialect. Click **Add**.



5. 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.

6. 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.



User Management

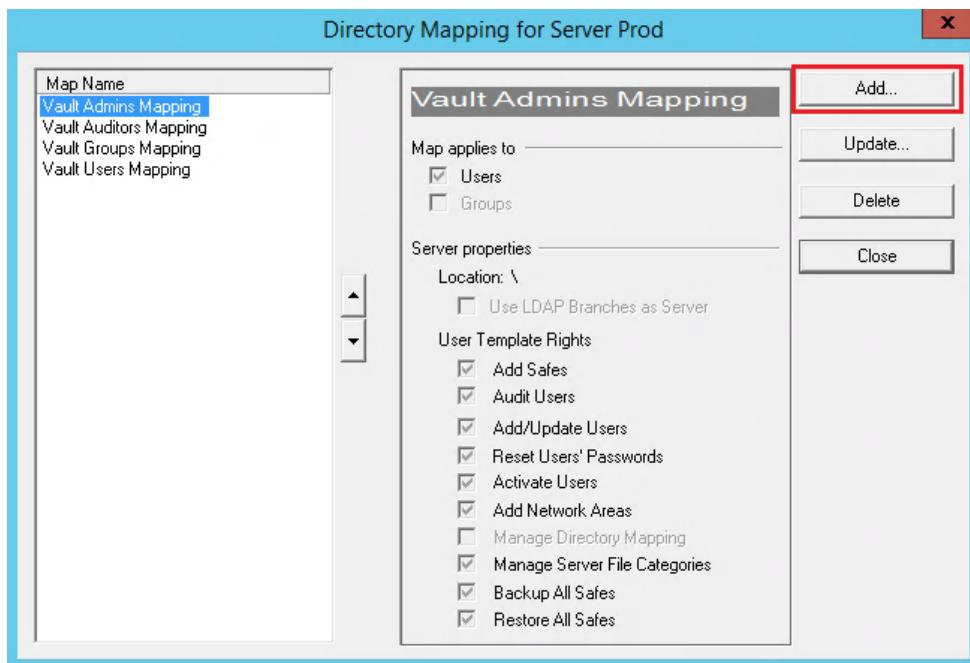
Creating a Custom User Mapping

In this first exercise, you will create a custom user mapping that will map a group of ‘Power Users’. This group will have the ability to modify the Master Policy and platforms, view reports, and reset users’ passwords, but will not be able perform other **Vault** functions, such as adding safes.

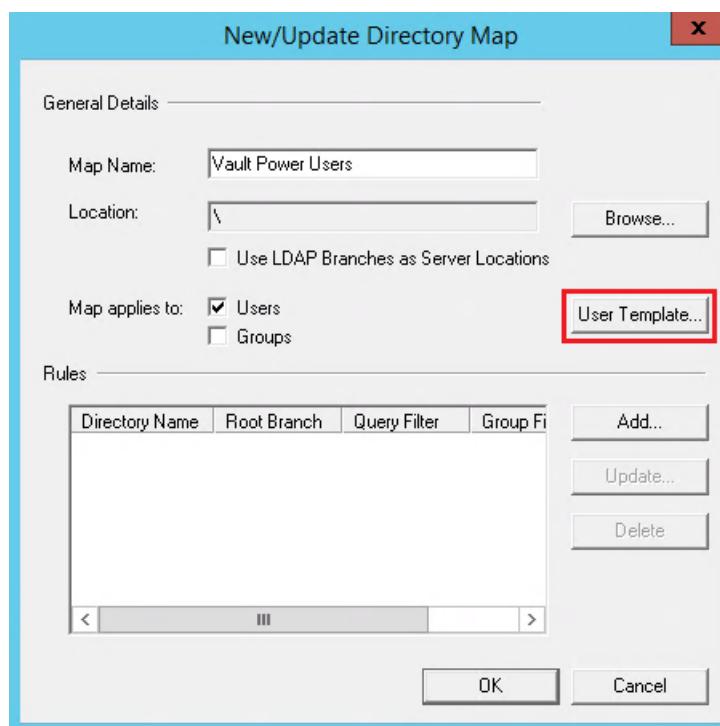
1. On the **Components Server**, open the **PrivateArk Client** and log in to the *Prod* Vault as the *Administrator* user with the password *Cyberark1*.
2. You will probably see a message like the one below. This appears because the user *Administrator* has not connected to the system recently. Just click **Yes** to clear expired history.



3. Go the **Tools** menu, select **Administrative tools**, then **Directory Mapping**.
4. On the *Directory Mapping for Server Prod* screen, press the **Add** button.



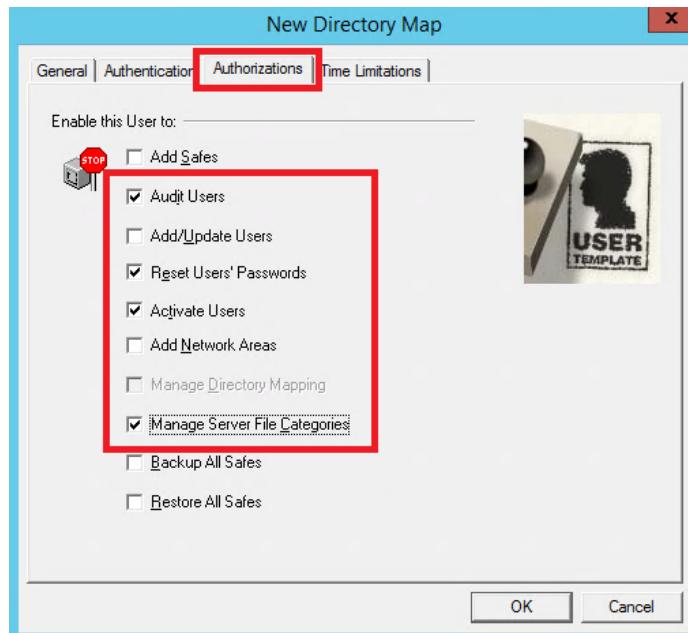
5. On the *New/Update Directory Map* in the **Map Name** field, enter **Vault Power Users** and check the **Users** check box.
6. Click the **User Template...** button.



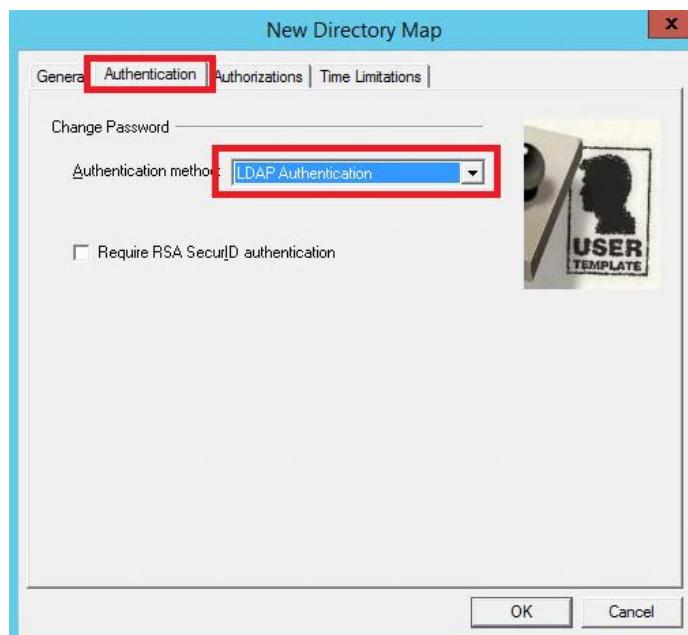
7. In the *New Directory Map Window*, select the **Authorizations** tab



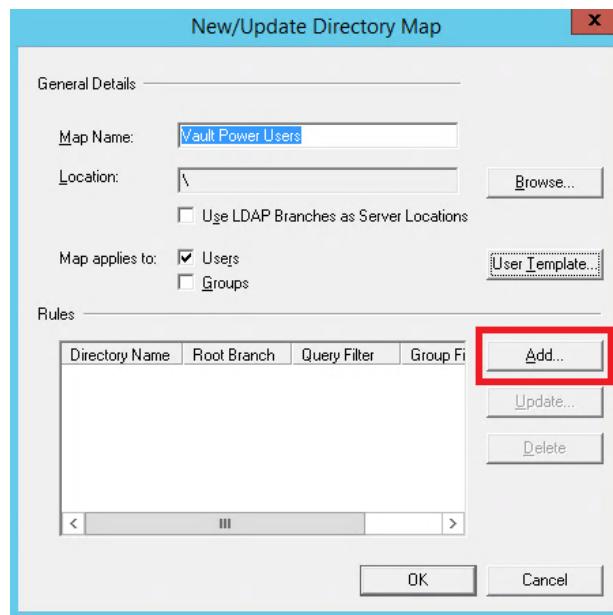
8. Check the following boxes: *Audit Users, Reset Users' Passwords, Activate Users, and Manage Server File Categories.*



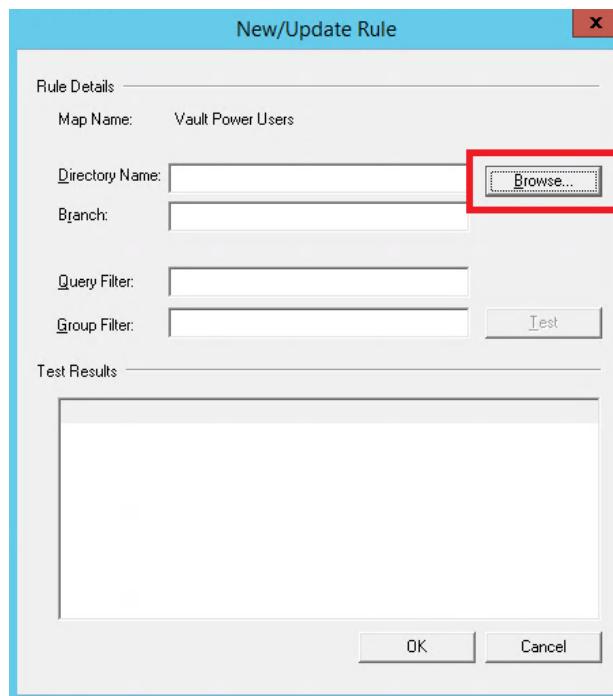
9. Select the **Authentication** tab.
10. Click on the pull-down and examine the *Authentication methods* options available.
11. Select *LDAP Authentication* and press **OK**.



12. Back on the *New/Update Directory Map*, press the **Add...** button to create a new rule.

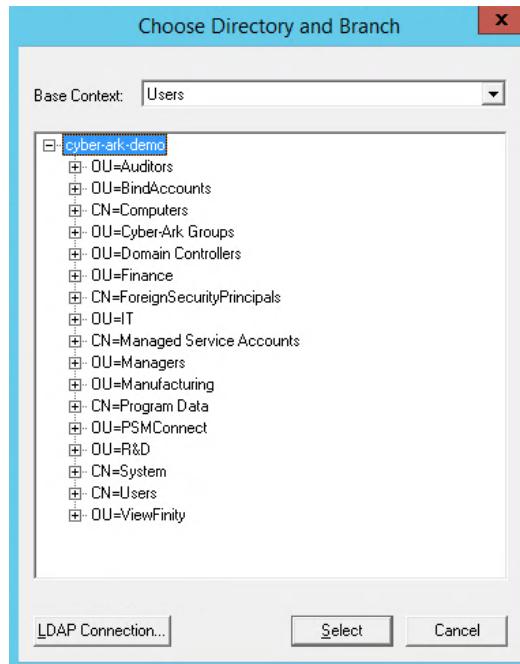


13. Press the **Browse...** button to locate the *Directory Name*.



Hint: If you cannot see the Active Directory tree structure, you might be performing the exercise on the wrong server.

14. On the *Choose Directory and Branch* window, highlight **cyber-ark-demo**.
 15. Expand the directory so that you can see the contents. Then press **Select**.

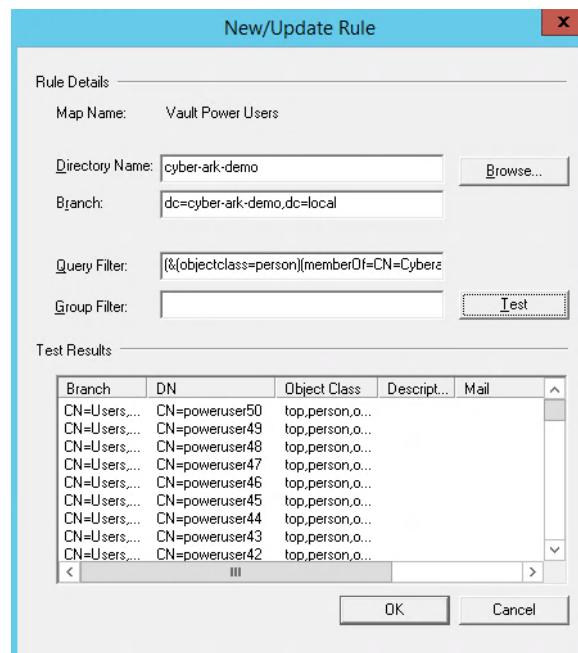


16. In the **Query Filter** field, enter:

```
(&(objectclass=person)(memberOf=CN=CyberArk Power Users,ou=Cyber-Ark Groups,DC=Cyber-Ark-demo,dc=local))
```

Note: This “Power Users” query is available in the *LDAPQueries.txt* file located on the Desktop of the **Components** server along with other sample queries.

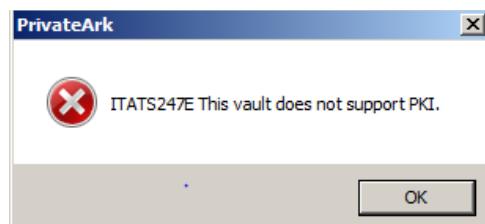
17. Press the **Test** button to confirm that the query returns include “CN=poweruser01”.





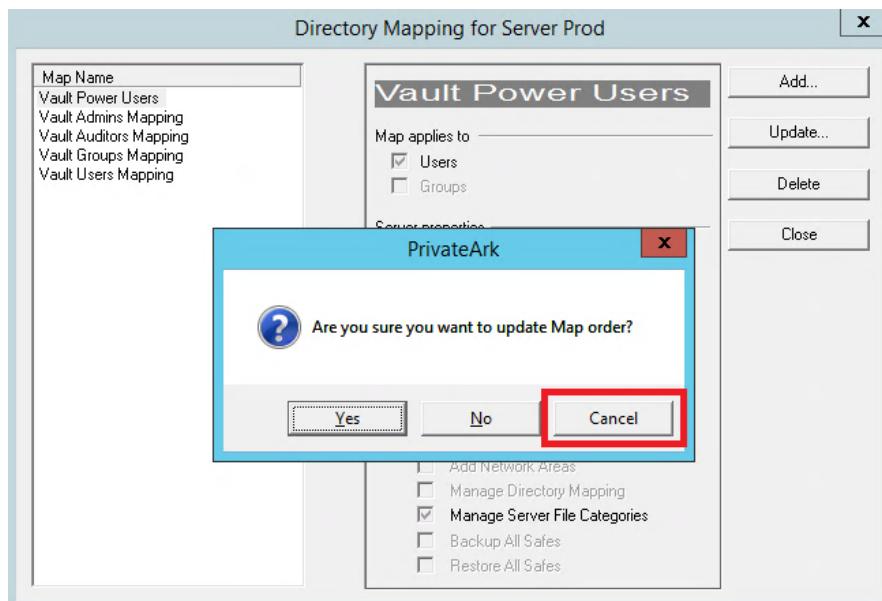
18. If the query results include “power user” entries, continue on to the next step.
19. Press **OK** and then **OK** again to exit the *New/Update Directory Map* window.

**** You may receive an error message that the Vault does not support PKI ****



If you get the error message above, go back to your user template, select the *Authentication* tab, click on the pull-down and specifically choose **LDAP authentication** for your *Authentication method*, even though it may already be selected.

20. After adding the new mapping, press the **Close** button.
21. You will receive a message asking ‘Are you sure you want to update Map order?’ Press **Cancel**.

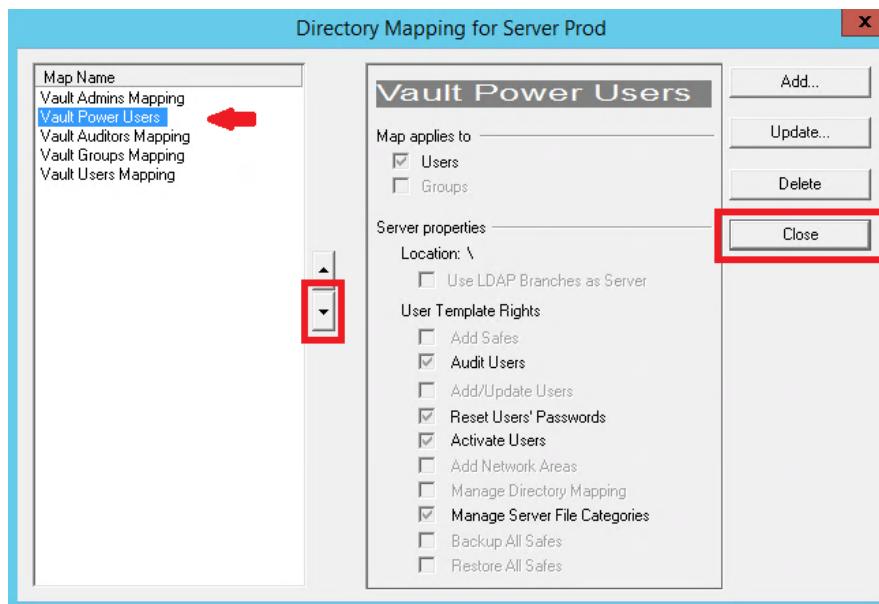




About ‘Mapping Order’

The mapping order is important for users who belong to multiple groups/mappings. For example, if a user belongs to both *Power Users* and *Vault Admins* mappings, the user will receive the privileges for the first mapping listed. If *Power Users* was listed first, a user who is also a *Vault Admin* user would only receive the subset of vault authorizations for *Vault Power Users*, instead of the full set provided by the *Vault Admins* mapping.

22. Highlight the *Vault Power Users* mapping and press the **down** button to move it below the *Vault Admins Mapping*.
23. After reordering the map order, press **Close**.



24. This time, you can press **Yes** when asked ‘Are you sure you want to update the Map order?’

Nesting the Power Users group under the built-in CyberArk groups

In this section, we will place the mapped LDAP group *CyberArk Power Users* under the CyberArk internal groups *Vault Admins* and *PVWAMonitor*. This will give members of the group access to the **POLICIES**, **REPORTS**, and **ADMINISTRATION** tabs in the **PWAA**.

Nesting the Power Users group under Vault Admins

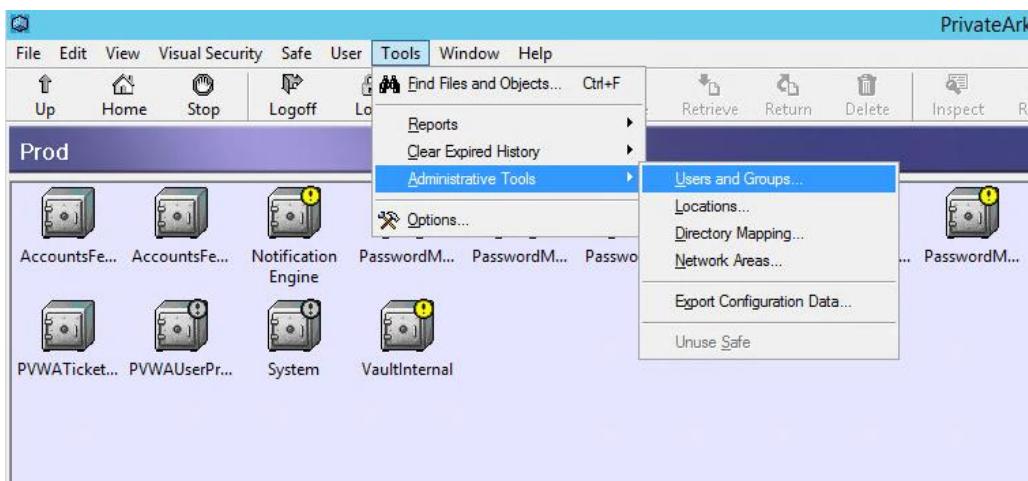
In this step you will nest the LDAP group *CyberArk Power Users* under the internal *Vault Admins* group. This will allow members of the Power Users group to view the **POLICIES** and **ADMINISTRATION** tabs in the **PVWA**.



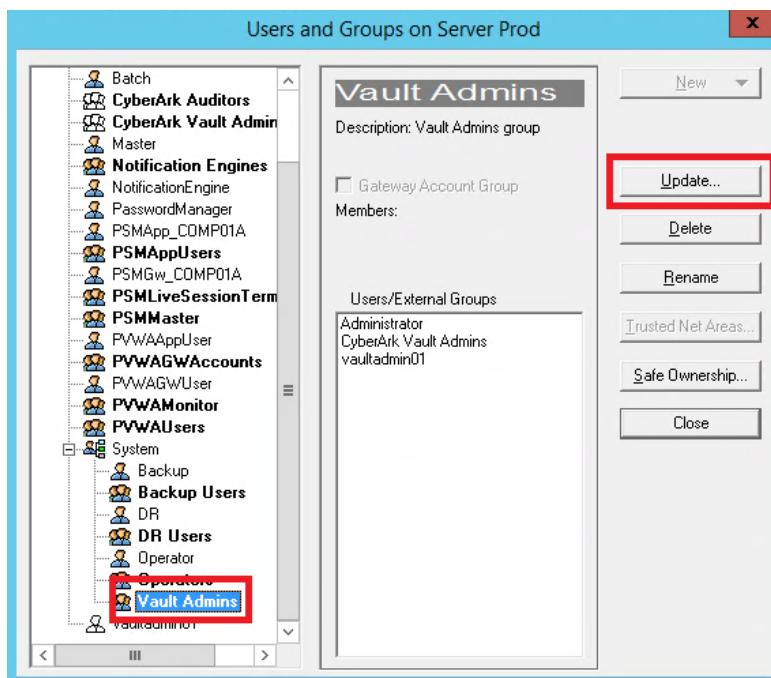
CYBERARK®

CyberArk Privileged Access Security – Administration

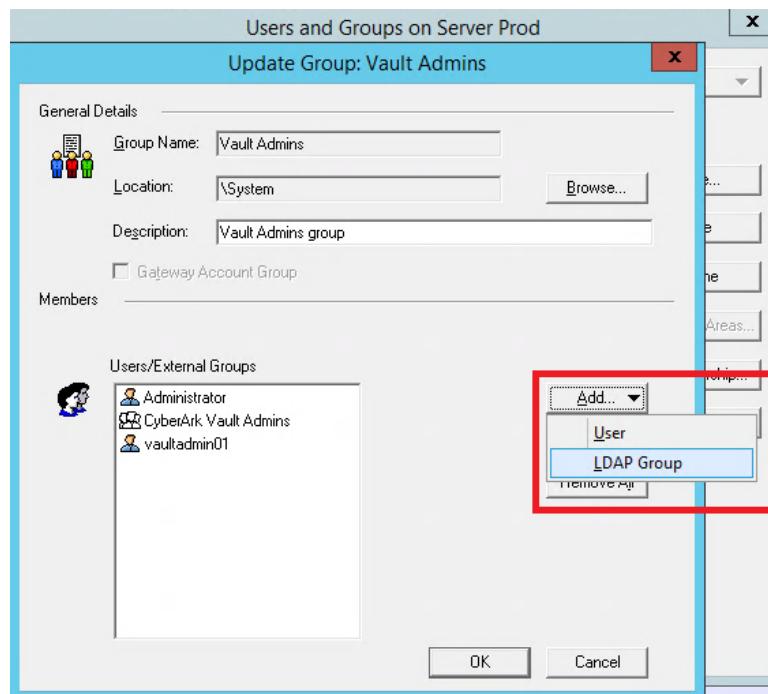
1. Go to Tools > Administrative Tools > Users and Groups...



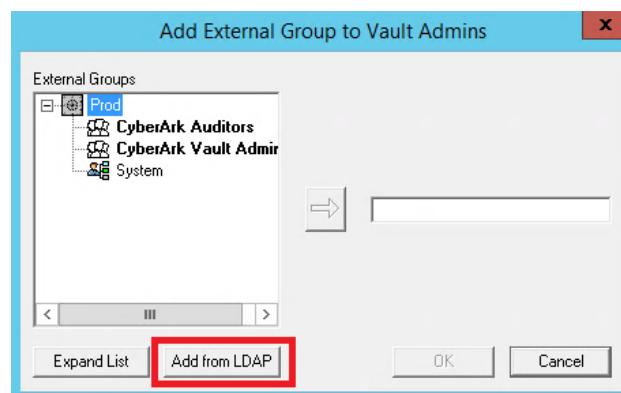
2. Navigate to System > Vault Admins and press Update...



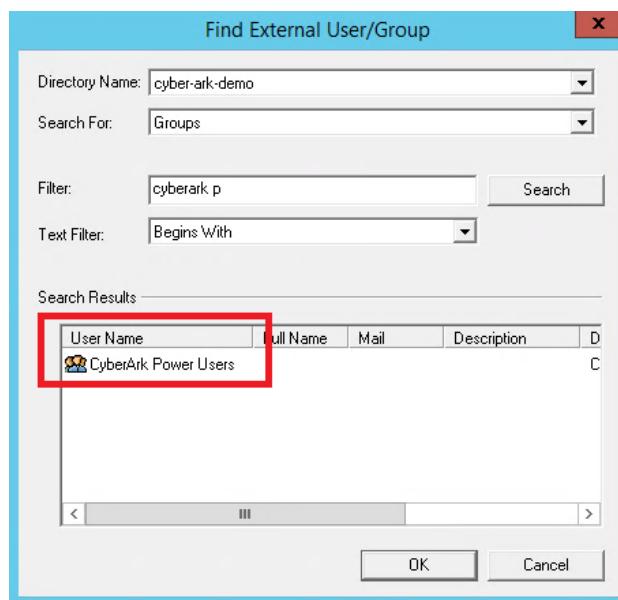
3. Press Add... > LDAP Group.



4. Press **Add from LDAP** (You may not see all of the groups shown below).



5. In the **Filter** field of the *Find External User/Group* screen, enter “cyberark p”. This will find the Power Users. Press **Search**.
6. Select the Cyberark Power Users in the **Search Results**.

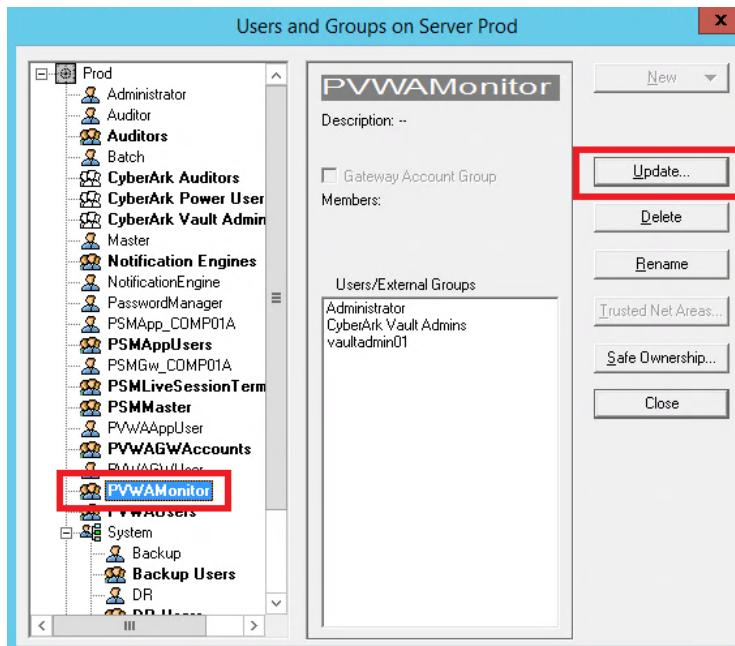


7. Press **OK** until you return to the *Users and Groups on Server Prod* window.

Nesting the Power Users group under the *PVWAMonitor* group

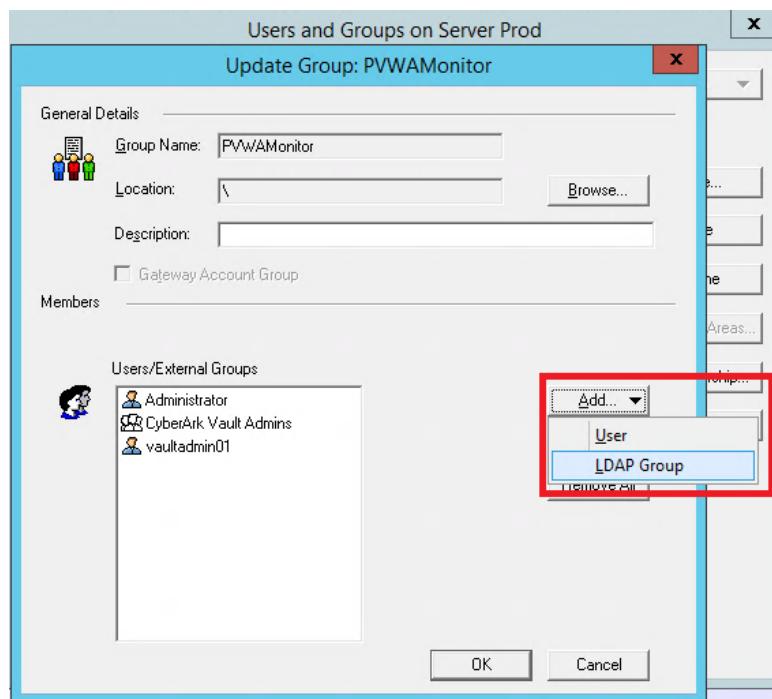
Next you will nest the LDAP group *CyberArk Power Users* under the internal *PVWAMonitor* group. This will allow members of the Power Users group to view the **REPORTS** tab in the [PVWA](#).

1. Within the **Users and Groups on Server Prod** window, highlight *PVWAMonitor* and press **Update...**

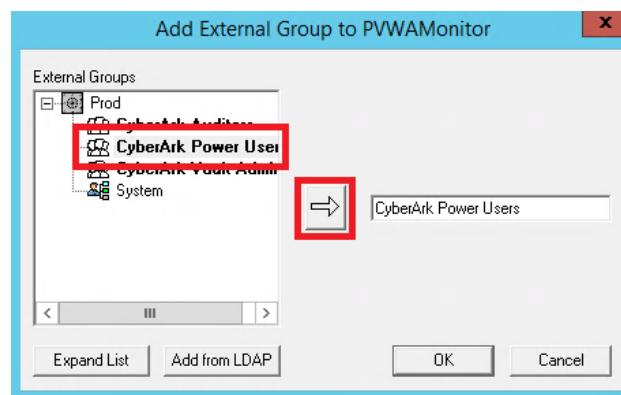




2. Press **Add** and select **LDAP Group**.



3. Select *CyberArk Power Users*.
4. Press the **Arrow** button to move it to the field on the right.
5. Press **OK**, to confirm the addition of *CyberArk Power Users* to the *PVWAMonitor* group.
6. Press **OK** again to close the *Update Groups: PVWAMonitor* window.



7. Press **Close** to close the 'Users and Groups on Server Prod' window and complete the nesting process.
8. Log off from the **PrivateArk Client**.



Viewing the differences between Vault Admins and Power Users groups

Next, you will login to the **PVWA** to view the differences between *Vault Admins* and *CyberArk Power Users* directory mappings within the **PVWA**.

Up to this point we have been logging in with users who were created on the **CyberArk** system and authenticated by **CyberArk**.

Since the LDAP integration has already been configured, we will log in to the **PVWA** with Active Directory credentials and be authenticated with LDAP. From this point forward, you will use LDAP Authentication for all users except *Administrator*. The *Administrator* user will use CyberArk Authentication.

Note: For the duration of this class, all passwords for all users and accounts will be *Cyberark1*, unless otherwise noted.

1. Open Chrome, go to the **PVWA** and choose **LDAP** as the authentication method.
2. Enter the username *vaultadmin01* and *Cyberark1* as the password. Press **Sign in**.



3. Confirm that your LDAP authentication was successful and you are able to view the **Policies**, **Reports**, and **Administration** tabs. This verifies that the LDAP user (*vaultadmin01*) has the correct *Vault Admins* and *PVWAMonitor* privileges.



Policy Rule	Value	Exceptions
Require dual control password access approval	Inactive	-
Enforce check-in/check-out exclusive access	Inactive	-
Enforce one-time password access	Inactive	-
Allow EPV transparent connections ('Click to connect')	Active	-
Require users to specify reason for access	Active	-

4. Go to **POLICIES > Access Control (Safes)** and verify that you can see the **Add Safe** button in the upper right hand corner of the window. This confirms that the *vaultadmin01* user has been provided the *Add Safes* vault authorization.

Safe Name
AccountsFeedADAccounts
AccountsFeedDiscoveryLogs
Notification Engine
PasswordManager
PasswordManager_Pending
PVWA/PublicData
PVWA/Reports
PVWA/TicketingSystem
VaultInternal

5. Log out of the **PVWA** and log back in as *poweruser01* using LDAP as the authentication method.

Note: This user should have access to the **Policies, Accounts, Applications, Reports, and Administration** tabs because the *CyberArk Power Users* group was nested under the *Vault Admins* and *PVWAMonitor* groups. However, it does not have access to the *Add Safe* button because 'Power Users' do not have the authorization to add safes.



6. Go to **POLICIES > Access Control (Safes)** and verify you do not see the **Add Safes** button.

The screenshot shows the CyberArk PVWA interface. The left sidebar has a 'POLICIES' section with three items: 'Master Policy', 'Policy by Platform', and 'Access Control (Safes)', which is highlighted with a red box. Below the sidebar are four icons: a blue folder (highlighted with a red box), a shield, a document, and a wrench. The main content area is titled 'Policies > Access Control (Safes)' and 'Access Control (Safes)'. It displays a list of 'Showing 9 safes' with the following names: AccountsFeedADAccounts, AccountsFeedDiscoveryLogs, Notification Engine, PasswordManager, PasswordManager_Pending, PVWA/PublicData, PVWAReports, PVWATicketingSystem, and VaultInternal. A yellow box highlights the empty space above the search bar.

7. Sign out of the **PVWA**.



Password Management – Part 1

In this chapter, we will be performing a number of tasks linked to account password management. Use the Chrome browser on your Components server in order to connect to the [PVWA](#).

Note: Some features may require the use of the UI's classic interface (pre-version 10). In order to access this, you may need to select "Additional details & actions in classic interface".

The screenshot shows a logon entry for 'logon01 On 10.0.0.20'. Below the entry, there is a status bar with 'Platform: Linux SSH 30' and 'Safe: Linux Finance'. To the right of the status bar are four buttons: 'Show', 'Copy', '...', and 'Connect'. A red box highlights the 'Additional details & actions in classic interface' link located above the status bar.

Editing the Master Policy

In this step, you will use the [PVWA](#) to modify the *Master Policy* to:

- Disable *Require users to specify reason for access*
- Verify passwords daily instead of weekly
- Activate the PSM

[Disable *Require users to specify reason for access*](#)

1. Launch the [PVWA](#) and using LDAP authentication and log in as *vaultadmin01*.
2. Go to the **POLICIES > Master Policy**.
3. Choose *Require users to specify reason for access* and then click **Edit Settings**.



The screenshot shows the CyberArk Privileged Access Security Administration interface. On the left, there's a sidebar with icons for Policies, Master Policy (highlighted with a red box), Policy by Platform, and Access Control (Safes). The main content area is titled 'Policies > Master Policy' and shows 'Master Policy'. It has sections for 'Privileged Access Workflows' and 'Advanced Settings'. In the 'Privileged Access Workflows' section, there's a table with rows for 'Require dual control password access approval', 'Enforce check-in/check-out exclusive access', 'Enforce one-time password access', 'Allow EPV transparent connections ('Click to connect')', and 'Require users to specify reason for access'. The last row is highlighted with a blue box. In the 'Advanced Settings' section, there's a table with rows for 'Allow users to specify free text reason for access' (set to Active) and 'Require users to specify reason for access' (set to Inactive). A red box highlights the 'Inactive' button. On the right, there's a 'Rule Preview' section, an 'EXCEPTIONS' section with a '+' button, and a bottom bar with 'Edit Settings' and 'Add Exception' buttons.

4. Change the **Basic Policy Rule** *Require users to specify reason for access* from **Active** to **Inactive**.
5. Press **Save & Close**.

The screenshot shows the 'Edit Rule Settings' dialog box for the 'Master Policy' basic policy rule. It has tabs for 'Privileged Access Workflows | Require users to specify reason for access' and 'Advanced Settings'. Under 'Basic Policy Rule', the 'Require users to specify reason for access' setting is set to 'Inactive' (highlighted with a red box). Under 'Advanced Settings', the 'Allow users to specify free text reason for access' setting is set to 'Active'. At the bottom, there are 'Save', 'Save & Close' (highlighted with a red box), and 'Cancel' buttons.

Change passwords daily instead of weekly

We will change the password change baseline policy from 90 days to 1 day in order to be able to see our **CPM** change passwords automatically during the training. This is not a recommended setting.

1. Expand the **Password Management** section. Highlight *Require password change every X days*.



2. In the right-hand pane, click the pencil icon to edit the *Value*.

The screenshot shows the CyberArk Privileged Access Security Administration interface. On the left, there's a sidebar with icons for Policies, Master Policy, Policy by Platform, Access Control (Safes), Session Management, Audit, and Help. The main area shows 'Policies > Master Policy' with 'Master Policy' selected. Under 'Master Policy', there are sections for 'Privileged Access Workflows' and 'Password Management'. In the 'Password Management' section, there's a table with a row for 'Require password change every X days' where the value '90' is highlighted with a red box. To the right, there's a 'Rule Preview' panel showing 'Require password change every X days' with a value of '90 Days'.

3. Change the value from **90** days to **1** and click the diskette icon to save the change.

Activate the PSM

The **PSM** is deactivated by default. In order to use it, we will need to activate it.

1. In the **Session Management** section, activate the option *Require privileged session monitoring and isolation*.
2. In the upper right-hand corner of the screen, click on the pencil next to the **Inactive** button. Select **Active**, click the diskette icon to save.
3. The **PSM** is now active. Open up the Windows Services (there is a short cut in the task bar) and make sure that the *Cyber-Ark Privileged Session Manager* service is running.

Managing Linux Accounts with SSH

In this section, we will perform the basic tasks required to manage a privileged account on a Linux server that we connect to using SSH. We will create a **Safe** to securely store the account and a **Platform** to manage the account. We will then add the new account, verify that we can connect with it, and see how an auditor can monitor the account activity.

Creating a Safe

1. If you are not already logged in, log in to the **PVWA** as **vaultadmin01**.
2. Go to **POLICIES > Access Control (Safes)**.
3. Click **Add Safe**.



Policies > Access Control (Safes)
Access Control (Safes) ?

Last sign in: 6/13

Showing 9 safes

Safe Name ▲

- AccountsFeedADAccounts
- AccountsFeedDiscoveryLogs
- Notification Engine
- PasswordManager
- PasswordManager_Pending
- PVWA/PublicData
- PVWA/Reports
- PVWA/TicketingSystem
- VaultInternal

Search 🔍

4. Enter **Linux Finance** as the **Safe Name**.
5. Optionally, provide a meaningful description like: “*Linux accounts, access restricted to Linux admins approved by Finance department – LinuxAdminsFin*”
6. Press **Save**.

Add Safe

Safe name:

Description:

Enable Object Level Access Control

Saved accounts:

Save the last account versions

Save account versions from the last days

Assigned to CPM:

Save Cancel

7. Press **Add Member** to grant other users access to the new safe.



Safe Details: Linux Finance

Back Edit Delete Safe Refresh

Name: Linux Finance
Description: Object level access is not enabled
Assigned CPM: PasswordManager
Saved accounts: Account versions from the last 7 days

Members

User Name	Use	Retri...	List	Add	Upd...	Upd...	CPM	Ren...	Delete	Unlock	Man...
PasswordMa...	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
vaultadmin01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Hide predefined users and groups

8. Enter *linuxad* in the **Search** field, select *cyber-ark-demo.local* in the **Search In** field and press **Search**. Select *LinuxAdminsFin*, uncheck the option *Retrieve accounts*, and press **Add**.

Add Safe Member

Search: Search In: Search

Selected Search: cyber-ark-demo.local Display 2 result(s)

Name	Business Email	Full Name
LinuxAdmins		
LinuxAdminsFin		

Access
 Use accounts
 Retrieve accounts
 List accounts

Account Management

Safe Management

Monitor
 View Audit log
 View Safe Members

Workflow

LinuxAdminsFin has been added.

Add Close

9. Close the **Add Safe Member** window.



Note: You should now see that the *LinAdminsFin* group has been added to the newly created *Linux Finance* safe. We removed the ‘Retrieve’ option so that users will never have access to the password. They can use it to connect, but never actually see it. Also note that the user logged in is the creator of the safe and is granted full permissions to the safe by default.

User Name	Use	Retri...	List	Add	Upd...	Upd...	CPM	Ren...	Delete	Unlock	Man...
LinuxAdmins...	✓	✓	✓								
PasswordMa...	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
vaultadmin01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Hide predefined users and groups

Duplicating a Platform

Next, you will create a platform to manage Linux accounts that connect with SSH.

1. Go to **ADMINISTRATION** and choose **Platform Management**.

System Configuration

Component Settings

Name	Component
Web Access	Web Access
Web Access	Web Access
Vault	Vault
Vault	Vault
Integration	Integration
Platform Management	Platform Management

Central Policy Manager

Export All



Note: Notice in the image below that some of the Platforms are *Active* while others are *Inactive*. It is recommended to deactivate any Platforms that are not being actively used. The Platforms we will be using in this course are:

- Oracle Database
- Unix via SSH
- Unix via SSH Keys
- Windows Domain Account
- Windows Server Local Accounts

You can deactivate all the other Platforms. Doing so is best practice and will help avoid errors.

2. Choose *Unix via SSH* and press **Duplicate**.

The screenshot shows the CyberArk Platform Management interface. On the left is a sidebar with various icons. The main area has a header "Administration > Platform Management" and "Platform Management". Below the header is a table titled "Target Account Platforms" with a link to "Service Account Platforms". The table columns are "Name", "Device Type", and "Status". A red box highlights the row for "Unix via SSH". The right side of the screen contains an "Overview" panel with text about platform management, a note about selecting a platform to edit its settings, and a note about duplicating a process.

Name	Device Type	Status
Amazon Web Services - AWS	Cloud Service	Active
Amazon Web Services - AWS - Access Keys	Cloud Service	Active
Cisco router via SSH	Network Device	Active
Microsoft Azure Management	Cloud Service	Active
Microsoft Azure Password Management	Cloud Service	Active
Microsoft SQL Server	Database	Active
Oracle Database	Database	Active
RSA Authentication Manager	Application	Active
Unix via SSH	Operating System	Active
Unix via SSH Keys	Operating System	Active
VMWare ESX Account	Operating System	Active
VMWare vCenter Personal	Application	Active
VMWare vCenter Shared Accounts	Application	Active
Windows Desktop Local Accounts	Operating System	Active
Windows Domain Account	Operating System	Active
Windows Server Local Accounts	Operating System	Active
[Sample Password Group Platform]	Misc	Inactive
[Sample SSH Key Group Platform]	Misc	Inactive
AS400	Operating System	Inactive
RMC Remedy	Application	Inactive

3. Enter *Linux via SSH 30* in the **Name** field and optionally something like *Linux servers via SSH, rotate passwords every 30 days* for a description and then press **Save & Close**.



Duplicate Target Account Platform

Source Platform
Unix via SSH

Duplicate to

Name
Linux via SSH 30

Description
Linux servers via SSH, rotate passwords every 30 days

Save & Close Cancel

Important! The name you give your Platform does not matter. You can call it whatever you want. However, for the purposes of this training, the name you give it DOES matter because we will be referring to it later in the course. If you choose not to follow the instructions as they are given, do not be surprised if you struggle to get later exercises working.

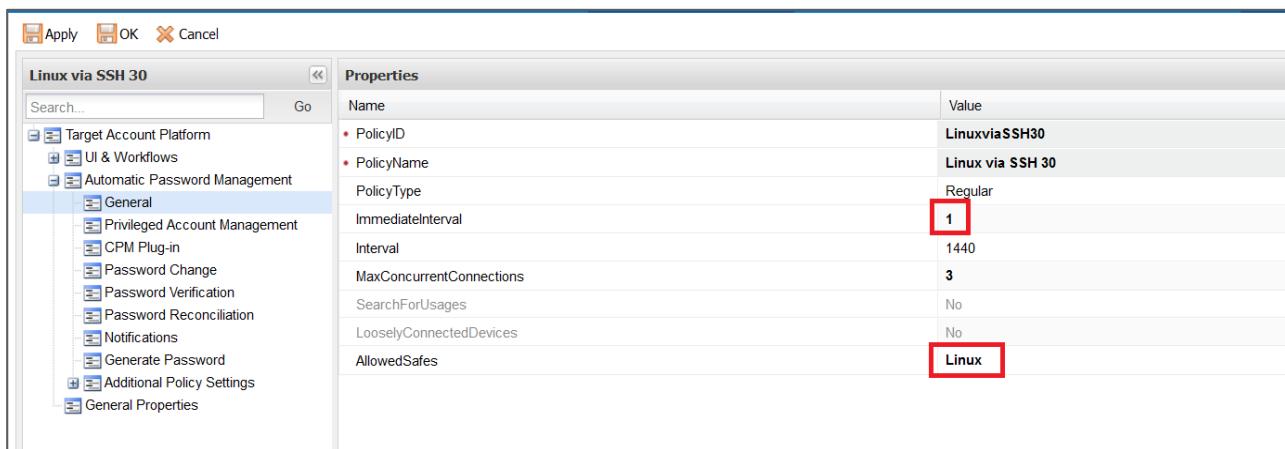
4. Highlight the newly created platform and press **Edit**.

ADMINISTRATION		Administration > Platform Management		Platform Preview
		Platform Management		Import Platform
Platform Management		Target Account Platforms Service Account Platforms		
		Name	Device Type	Status
		Amazon Web Services - AWS	Cloud Service	Active
		Amazon Web Services - AWS - Access Keys	Cloud Service	Active
		Cisco router via SSH	Network Device	Active
		Linux via SSH 30	Operating System	Active
		Microsoft Azure Management	Cloud Service	Active
		Microsoft Azure Password Management	Cloud Service	Active
		Microsoft SQL Server	Database	Active
		Oracle Database	Database	Active
		RSA Authentication Manager	Application	Active
		Unix via SSH	Operating System	Active
		Unix via SSH Keys	Operating System	Active
		VMWare ESX Account	Operating System	Active
		VMWare vCenter Personal	Application	Active
		VMWare vCenter Shared Accounts	Application	Active
		Windows Desktop Local Accounts	Operating System	Active
		Windows Domain Account	Operating System	Active
		Windows Server Local Accounts	Operating System	Active
		[Sample Password Group Platform]	Misc	Inactive
		[Sample SSH Key Group Platform]	Misc	Inactive
		AS400	Operating System	Inactive
		BMC Remedy	Application	Inactive
		Check Point Firewall-1	Security Appliance	Inactive
		Check Point GAIA via SSH	Security Appliance	Inactive
		Cisco Pix via SSH	Security Appliance	Inactive
		Cisco Pix via Telnet	Security Appliance	Inactive

5. Go **Automatic Password Management > General**.
6. Change *ImmediateInterval* to **1**.

Note: Changing the *ImmediateInterval* field to 1 is only suitable for testing but should set to 5 or higher in a real environment.

7. Change **AllowedSafes** to **Linux** (case sensitive). This determines which safes can use this platform.
8. Click **Apply** to save your changes, but do not exit the platform just yet.



9. Now go to **Password Change** and change the value of the parameter *PerformPeriodicChange* from **No** to **Yes**. This will enable the application of the Master Policy rule *Require password change every X days* to accounts managed by this platform.
10. Within the same window, go to **Password Verification** and change *VFPerformPeriodicVerification* from **No** to **Yes**. This will allow the password to be verified by the **CPM** automatically and without user intervention.
11. Finally, in **Generate Password**, note that the default password length for Unix machines is 8 characters. We might want to set this to a higher value.
12. Click **Apply** and **OK**.

Adding a Linux account

Now you will add your first Linux account and store it in the *Linux Finance* safe and manage it with the *Linux via SSH 30* platform.

1. Go to **ACCOUNTS** and click **Add Account**.



The screenshot shows the CyberArk Accounts View interface. At the top right, there is a sign-in message "Last sign in: 10/9/2018 | vaultadmin01" and several navigation icons. Below the header, there's a search bar and tabs for "Views", "Recent", and "Saved". On the left, a sidebar lists "My accounts" with categories like "All accounts (default)", "Recently used", "Favorites", and "Checked-out". To the right, sections show "Status" (Disabled by CPM, Failed, Newly added, Deleted) and "Operational state" (Scheduled for Change, Scheduled for Verification, Scheduled for Reconciliation, Successfully Reconciled). A red box highlights the "Add account" button in the top right corner.

2. On the *Add Account* page, first select the system type *NIX and click **Next**:

The screenshot shows the "Add Account" wizard. The title is "Add Account" and the step is "1. Select system type". On the left, a vertical list shows steps 1 through 4: "Select system type" (highlighted with a blue circle), "Assign to platform", "Store in Safe", and "Define properties". The main area shows two options: "Windows" and "*NIX". The "*NIX" option is highlighted with a red box. At the bottom right are "Cancel" and "Next >" buttons.

3. Select the *Linux via SSH 30* platform and click **Next**:

The screenshot shows the "Add Account" wizard. The title is "Add Account" and the step is "2. Select platform". On the left, a vertical list shows steps 1 and 2 completed (indicated by green checkmarks): "Select system type (*NIX)" and "Assign to platform". The main area shows a list of platforms with one item: "Linux via SSH 30", which is highlighted with a red box. To the right is a "Filter list by platform name" input field. At the bottom right are "Cancel", "< Back", and "Next >" buttons.



Note: In the image above, only one platform appears. Why is that?

4. Select the safe we created earlier: *Linux Finance* and click **Next**.

Add Account

1. Select system type *NIX
2. Assign to platform Linux via SSH 30
3. Store in Safe
4. Define properties

3. Select Safe [object Object] Filter list by Safe name

Linux Finance

Cancel < Back Next >

5. Enter the account details shown below and click on **Add**:

Address:	10.0.0.20
User Name:	logon01
Password:	Cyberark1
Confirm Password:	Cyberark1



Add Account

1. Select system type *NIX

2. Assign to platform Linux via SSH 30

3. Store in Safe Linux Finance

4. Define properties

4. Define account properties

Primary properties

Address: 10.0.0.20

Username: logon01

Password (optional):

Confirm Password:

Customize account name:

Additional properties

UseSudoOnReconcile (optional):

Account management

Allow automatic password management:

Cancel < Back Add

6. On the **Accounts** page, select the newly created account.

My accounts	Status	Operational state
All accounts (default)	Disabled by CPM	Scheduled for Change
Recently used	Failed	Scheduled for Verification
Favorites	Newly added	Scheduled for Reconciliation
Checked-out	Deleted	Successfully Reconciled

3 results for: All accounts

Star	Status	Username	Address	Platform ID	Safe ↑	Access Request	
★	⚡	logon01	10.0.0.20	LinuxviaSSH30	Linux Finance	-	<button>Connect</button> <button>...</button>
★	⌚ ⚡	BindAccount	dc01.cyber-ark-demo.local	WinDomain	VaultInternal	-	<button>Connect</button> <button>...</button>
★	⌚ ⚡	bindAccount	dc01.cyber-ark-demo.local	WinDomain	VaultInternal	-	<button>Connect</button> <button>...</button>

7. On the **Account Details** page, press the **Verify** button to confirm that you have created the account correctly.



The screenshot shows the CyberArk Privileged Access Security interface. At the top, it displays 'logon01 On 10.0.0.20'. Below this, there are tabs for 'Overview' (which is selected), 'Details', 'Activities', and 'Versions'. The 'Overview' section includes a 'Compliance Status' card showing 'Compliant' with a green circle icon and '0 Days ago'. It also shows a 'Last Verified' card with 'Never Verified' and 'Created 2 minutes ago', and a 'Verify' button which is highlighted with a red box. The 'Activities' section lists five entries from 'Sep 3 2:15:18 PM': 'vaultadmin01 Add File Category'. The 'Last Access' section shows a recent access by 'vaultadmin01 Today'.

8. Press the **Refresh** button.



Account is marked for verification



Note: You will see a message saying that '*The account is scheduled for immediate verification*'.

9. After a few minutes, the message should disappear and the *Last verified* field will be updated.

The screenshot shows the 'Last Verified' section of the interface. It now displays '0 Days ago' with a green circle icon, 'Verified by PasswordManager Sep 3, 2018 2:20 PM', and a 'Verify' button.

Changing the password

1. On the *Account Details* page, press the **Change** button.



logon01 On 10.0.0.20

Platform: Linux via SSH 30 Safe: Linux Finance

Overview Details Activities Versions

Compliance Status Compliant

0 Days ago

Changed by vaultadmin01 Sep 3, 2018 2:15 PM

Reconcile Change

Activities (Last 5)

Sep 3 2:20:31 PM P
Sep 3 2:19:36 PM v
Sep 3 v

10. Press the **Change** button.

logon01 On 10.0.0.20

Change password for account logon01 on 10.0.0.20

The CPM will change the password to a new random password

Cancel Change

Note: You will see a message saying ‘Account is marked for change.

Account is marked for change

11. After a minute or two, press **Refresh**. The message should disappear and you will see the message “Changed by PasswordManager” followed by a recent timestamp.

Compliance Status Compliant

0 Days ago

Changed by PasswordManager... Sep 3, 2018 2:24 PM

Reconcile Change



12. Sign out of the PVWA.

Auditing Account Activity

In this step you will review all of the activity related to the *logon01* account.

1. Sign out of the **PVWA** and using **LDAP Authentication**, sign back in as *auditor01*.
2. On the **Accounts** page, click on the magnifying glass icon in the top right corner to view all accounts the auditor has permissions to view.
3. Click on the *logon01* account.

The screenshot shows the CyberArk PVWA interface. The left sidebar has icons for Accounts, Groups, and Devices. The main header says "Accounts". A search bar at the top right contains "Search for accounts". Below it are tabs for "Views", "Recent", and "Saved". A button labeled "AD_HOC_CONNECT_ACTION" is on the far right. The left sidebar under "My accounts" shows "All accounts (default)", "Recently used", "Favorites", and "Checked-out". The main area displays a table of accounts with columns: Status, Username, Address, Platform ID, Safe, and Access Request. The first row, "logon01", is highlighted with a red border. The table also includes rows for "PSMAdminConnect", "PSMConnect", "root10", "BindAccount", and "bindAccount". Each row has "Connect" and "..." buttons on the right.

Status	Username	Address	Platform ID	Safe ↑	Access Request
⚡	logon01	10.0.0.20	LinuxviaSSH30	Linux Finance	[Connect] [...]
-	PSMAdminConnect	10.0.20.1		PSM	[Connect] [...]
-	PSMConnect	10.0.20.1		PSM	[Connect] [...]
⌚	root10	10.0.0.20	Test	Test	[Connect] [...]
⌚ ⚡	BindAccount	dc01.cyber-ark-demo.local	WinDomain	VaultInternal	[Connect] [...]
⌚ ⚡	bindAccount	dc01.cyber-ark-demo.local	WinDomain	VaultInternal	[Connect] [...]

4. Click on the **Activities** tab to view the detailed activities log for this account.



The screenshot shows the CyberArk PVWA interface. On the left, there is a sidebar titled 'Accounts' with a search bar above it. The main content area displays a table of accounts with columns for Status, Username, and Address. One row for 'logon01' is selected, showing its details: Platform: Linux via SSH 30, Safe: Linux Finance. Below this, there are tabs for 'Overview', 'Details', 'Activities' (which is highlighted with a red box), and 'Versions'. Under 'Activities', it says '14 Activities for this account' and lists several entries from today, including actions by 'PasswordManager' and 'vaultadmin01' such as 'Change Password' and 'Delete File Category'.

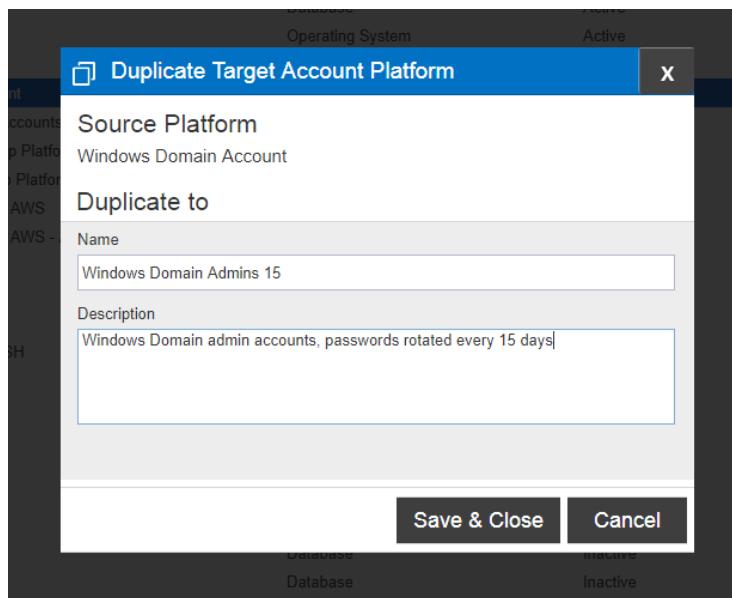
5. Sign out of the **PVWA**.

Managing Windows Domain Accounts

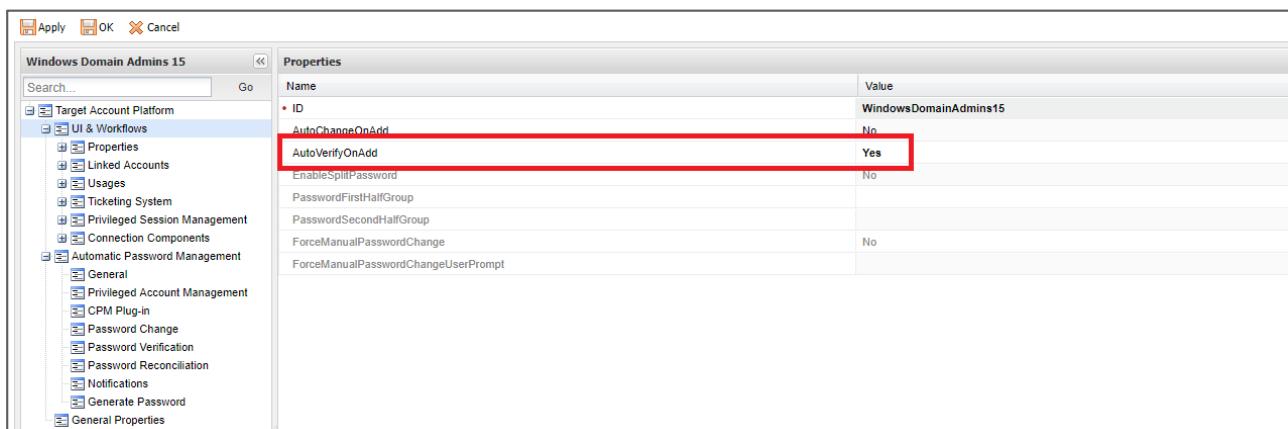
In this section, we will be performing the tasks for managing a Windows domain account. We will again duplicate an appropriate platform (though one adapted to managing Windows domain accounts), add a safe, and then add the account.

Duplicating a Platform

1. Using LDAP authentication, login to the **PVWA** as **vaultadmin01**.
2. Go to the **Administration** page and click **Platform Management**.
3. Highlight the *Windows Domain Account* platform and press **Duplicate**.
4. Enter as the name *Windows Domain Admins 15* (optionally you can give it a meaningful description) and then press **Save & Close**.



5. Select the *Windows Domain Admins 15* platform and press the **Edit** button.
6. Click on **UI & Workflows**.
7. Change *AutoVerifyOnAdd* from *No* to *Yes*.



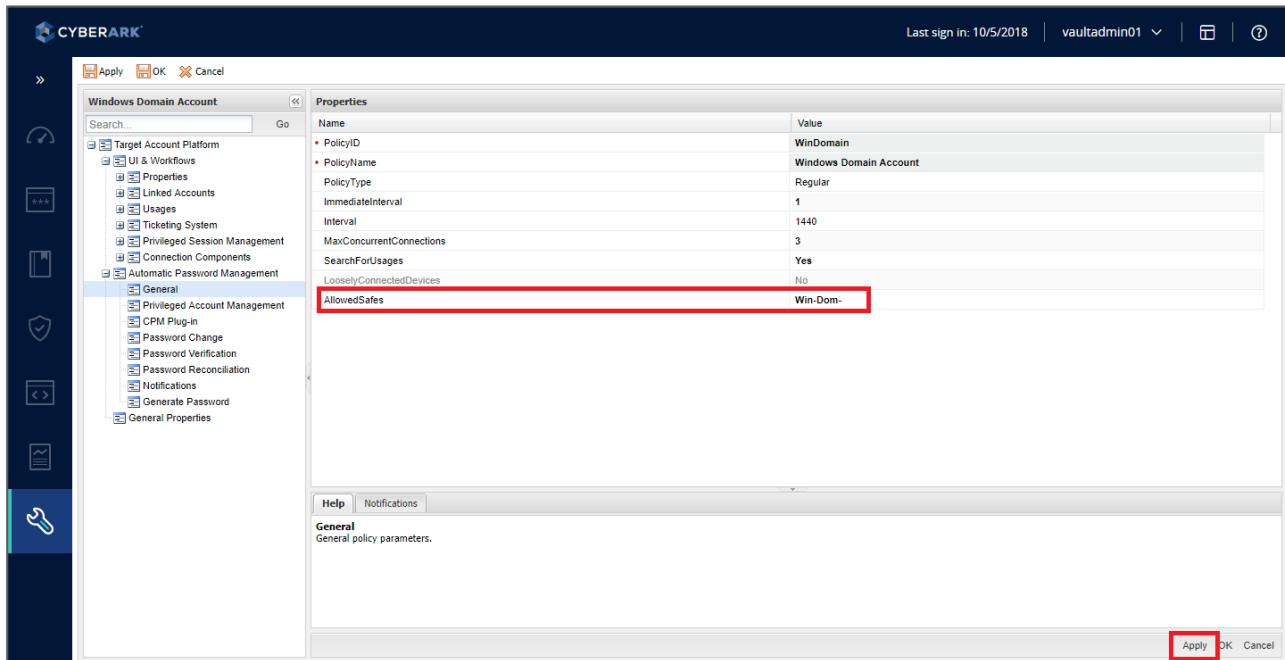
Note: This setting will prompt the **CPM** to automatically verify the password whenever a new account assigned to this platform is added.

8. Press **Apply**.
9. Go to **Automatic Password Management > General** and set *ImmediateInterval* to 1 (as we did in the first platform).
10. Enter **Win-Dom-** in the *AllowedSafes* field (this is case sensitive).



Reminder: This setting restricts the safes to which this platform can be applied to those safes with the string “Win-Dom-” included in the name. This field is case sensitive.

11. Press **Apply**.



12. Go to **Password Change** and set *PerformPeriodicChange* to **Yes**.
13. Go to **Password Verification** and set *VFPerformPeriodicVerification* to **Yes**.
14. Finally, go to **Generate Password**. Here, we are going to modify the password length and complexity to give us more secure passwords for our domain admin accounts. Set the values as follows:

<i>PasswordLength</i>	15
<i>MinUpperCase</i>	1
<i>MinLowerCase</i>	1
<i>MinDigit</i>	1
<i>MinSpecial</i>	1

Note: The sum of the various complexity parameters must be less than or equal to *PasswordLength* in order for password change to function. However, the system does not check the values for you.



15. Press **Apply** and **OK** to close the platform.

Note: Best practice would suggest that we deactivate the default *Windows Domain Account* platform now that we have duplicated it. We can always reuse it later if we need to, but if it is deactivated, no one will use it by mistake.

Creating a Safe

Now you will create a safe in which to store Windows domain accounts.

1. Go to **POLICIES > Access Control (Safes)**.
2. Click **Add Safe**.

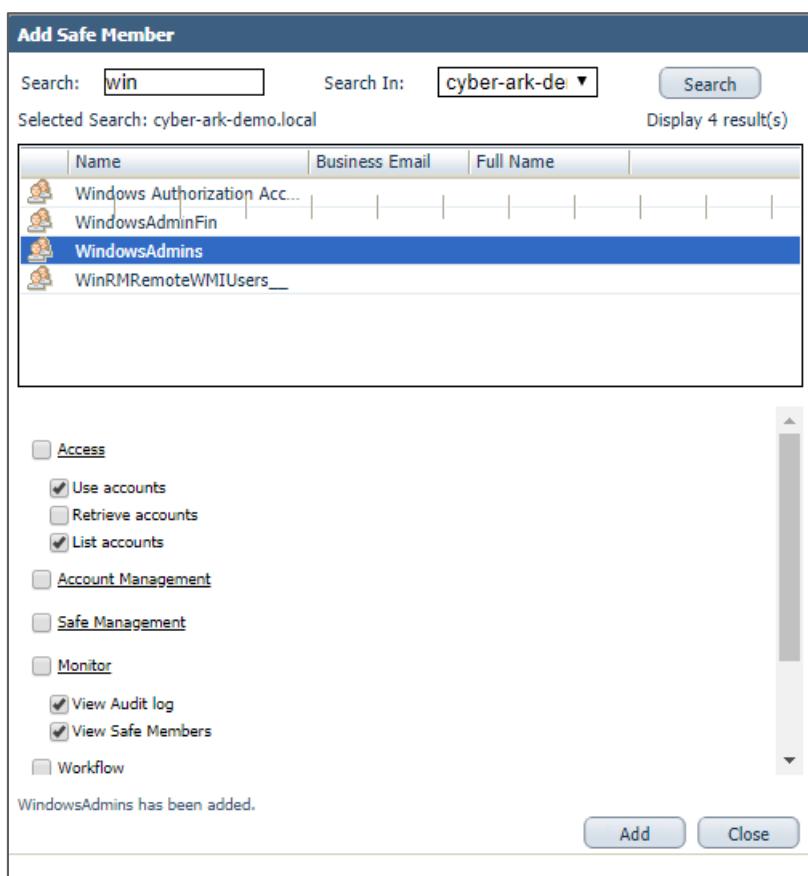
The screenshot shows the CyberArk Policies interface. On the left, there's a sidebar with icons for Policies, Master Policy, Policy by Platform, and Access Control (Safes). The 'Access Control (Safes)' icon is highlighted with a red box. The main panel shows a list of safes: AccountsFeedADAccounts, AccountsFeedDiscoveryLogs, Linux Finance, Notification Engine, PasswordManager, and DequeuedManager Pending. A search bar is at the top right. In the top right corner, there's a message 'Last sign in: 6/13/' and a red box around the '+ Add Safe' button.

3. Enter **Win-Dom-Admins** the Safe name. You can provide a meaningful description. Leave the other values at their defaults and press **Save**.

The screenshot shows the 'Add Safe' dialog box. It has fields for 'Safe name' (set to 'Win-Dom-Admins'), 'Description' (set to 'For Windows domain admin accounts only. Restricted to authorized domain administrators'), 'Saved accounts' (radio buttons for 'Save the last [] account versions' and 'Save account versions from the last [] days' are shown, with the second option selected), and 'Assigned to CPM' (a dropdown menu set to 'PasswordManager'). At the bottom are 'Save' and 'Cancel' buttons.

4. On the *Safe Details* page, click the **Add Member** button to grant other users access to this safe.
5. Enter *win* in the **Search** field, select *cyber-ark-demo.local* in the **Search In** field, and click **Search**.

6. Select *WindowsAdmins*, uncheck the box for *Retrieve accounts*.



7. Press **Add**, then **Close**.

Adding a Windows Account

In this section, we are going to add an account that already exists in Active Directory and that we will use as our reconcile account.

Please note that the account is named *cybrreconcile* (that is *cybr*, without the “e”).

1. Go to the **ACCOUNTS** tab and press the **Add Account** button.
2. Enter the following and then press **Add**:

Store in Safe:	Win-Dom-Admins
System Type:	Windows
Platform Name:	Windows Domain Admins 15
Address:	cyber-ark-demo.local
User Name:	cybrreconcile

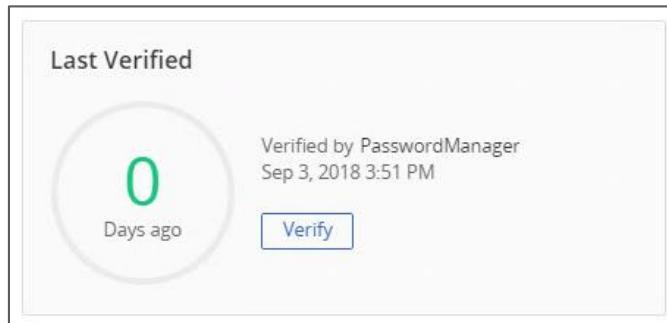
Logon To:	cyber-ark-demo (Click the Resolve link after checking the “Logon To.” box)
Password:	Cyberark1
Confirm Password:	Cyberark1

Add Account

<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Select system type Windows <input checked="" type="checkbox"/> Assign to platform Windows Domain Admins 15 <input checked="" type="checkbox"/> Store in Safe Win-Dom-Admins <p>4 Define properties</p>	<p>4. Define account properties</p> <p>Primary properties</p> <p>Address cyber-ark-demo.local</p> <p>Username cybrreconcile</p> <p>Password (optional)</p> <p>Confirm Password</p> <p><input type="checkbox"/> Customize account name <small>?</small></p> <p>Additional properties</p> <p>Logon To (optional) CYBER-ARK-DEMO <input type="button" value="Resolve"/></p>
<input type="button" value="Cancel"/> <input type="button" value="< Back"/> <input type="button" value="Add"/>	

Note: Because *AutoVerifyOnAdd* was set to **Yes**, the account will be scheduled for immediate verification.

3. Press **Refresh** every few minutes until the account is verified.



4. Select the newly created account from the list and then click on **Additional details & actions in classic interface** to open the account in the classic interface.



The screenshot shows the CyberArk Admin interface for the account 'cybrrreconcile' on the domain 'cyber-ark-demo.local'. The account is part of the 'Win-Dom-Admins' safe. The interface includes tabs for Overview, Details, Activities, and Versions. A red box highlights the 'Additional details & actions in classic interface' button.

- Copy the Safe name and the Name values to Notepad (we'll be using these values in a later exercise).

The screenshot shows the CyberArk Admin interface for the account 'cybrrreconcile'. The 'Safe' field is highlighted with a red box. The 'Name' field is also highlighted with a red box. Other visible fields include Platform Name, Device Type, and various audit logs.

Create a Second Windows Domain Account

We will need another Windows Domain Administrator account for a later exercise – *cybrscan*. Add a second Windows domain account using the information below.

Again, please note that it is CYBR (without the E).

Store in Safe:	Win-Dom-Admins
System Type:	Windows
Platform Name:	Windows Domain Admins 15
Address:	cyber-ark-demo.local
User Name:	cybrscan
Logon To:	cyber-ark-demo (Click the Resolve link after checking the "Logon To:" box)
Password:	Cyberark1
Confirm Password:	Cyberark1



Best Practice: After adding a new account, you should rotate the password so that only CyberArk PAS knows the password. Go ahead and change the passwords for both *cybrreconcile* and *cybrscan*.

Configuring the Master Policy

In this section, we will configure the Master Policy with two objectives in mind:

- Configuring **Privileged Access Workflows** in anticipation of implementing *Dual Control*
- Adding the exceptions for the platforms we created in the section **Password Management – Part 1**

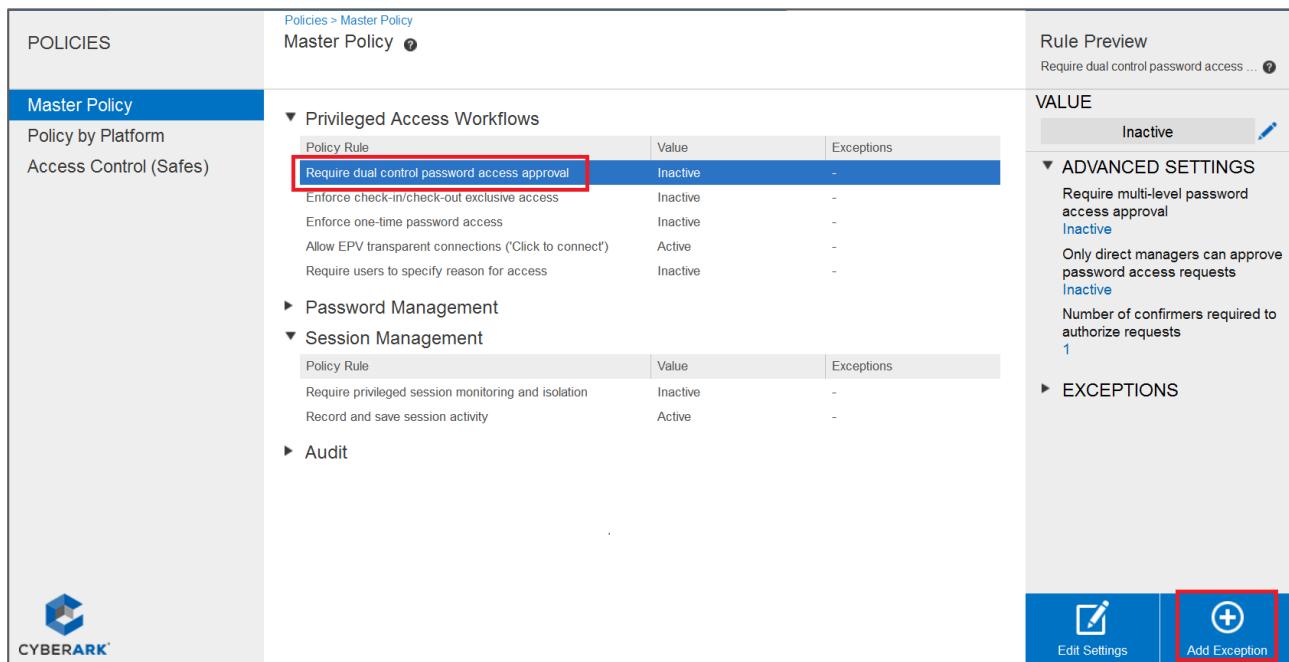
Privileged Access Workflows

In this section we will configure two exceptions to our Master Policy for our platform *Linux via SSH 30*:

- *Require dual control and access approval*
- *Require users to specify reason for access*

Require dual control access approval

1. Go to **POLICIES > Master Policy > Privileged Access Workflows**, select *Require dual control password access approval*, and press **Add Exception**.



Policy Rule	Value	Exceptions
Require dual control password access approval	Inactive	-
Enforce check-in/check-out exclusive access	Inactive	-
Enforce one-time password access	Inactive	-
Allow EPV transparent connections ('Click to connect')	Active	-
Require users to specify reason for access	Inactive	-

Rule Preview
Require dual control password access ... ?

VALUE
Inactive

ADVANCED SETTINGS
Require multi-level password access approval
Inactive
Only direct managers can approve password access requests
Inactive
Number of confirmers required to authorize requests
1

EXCEPTIONS

Edit Settings | **Add Exception**

2. Select *Linux via SSH 30* and press **Next**.

Create Exception

Privileged Access Workflows | Require dual control password access approval

Step 1: Select Platforms > Step 2: Set Exception What's this ?

Name	Device Type	Status
Linux via SSH 30	Operating System	Active
Oracle Database	Database	Active
Unix via SSH Keys	Operating System	Active
Windows Domain Admins 15	Operating System	Active
Windows Server Local Admins 45	Operating System	Active
[Sample Password Group Platform]	Misc	Inactive
[Sample SSH Key Group Platform]	Misc	Inactive
Amazon Web Services - AWS	Cloud Service	Inactive
Amazon Web Services - AWS - Access Keys	Cloud Service	Inactive
AS400	Operating System	Inactive
BMC Remedy	Application	Inactive
Check Point FireWall-1	Security Appliance	Inactive
Check Point GAIa via SSH	Security Appliance	Inactive
Cisco Pix via SSH	Security Appliance	Inactive
Cisco Pix via Telnet	Security Appliance	Inactive
Cisco router via SSH	Network Device	Inactive
Cisco router via Telnet	Network Device	Inactive

Back Next Cancel

3. Click **Active**. Review (but do not modify) the other options available. When ready, press **Finish**.

Create Exception

Privileged Access Workflows | Require dual control password access approval | Linux via SSH 30

Step 1: Select Platforms > Step 2: Set Exception What's this ?

Basic Policy Rule

Require dual control password access approval Active Inactive

Advanced Settings

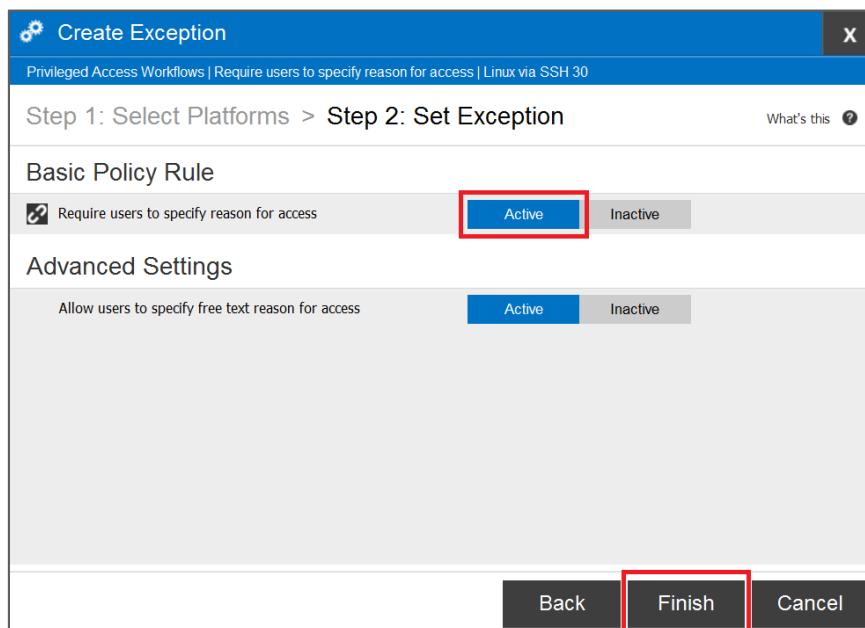
Require multi-level password access approval	Active	Inactive	?			
Only direct managers can approve password access requests	Active	Inactive	?			
Number of confirmers required to authorize requests	1	2	3	All	Other	!

Back Finish Cancel



Require users to specify reason

1. Back in the **Master Policy** page, again under **Privileged Access Workflows**, select the option *Require users to specify reason for access* and press **Add Exception**.
2. Again select *Linux via SSH 30* and press **Next**.
3. Set *Require users to specify reason for access* to **Active**.



4. Press the **Finish** button when you are done.

Password Management

Based on what you have already learned, you should now be able to add **Password Management** exceptions for the two platforms we created in the section **Password Management – Part 1**. Add the following exceptions

Linux via SSH 30	Require password change every 30 days
Windows Domain Admins 15	Require password change every 15 days



Password Management – Part 2

In this section, we are going to continue to explore password management options. Specifically, we will look at:

- Log-on accounts
- Windows server local admin accounts with reconciliation
- Dual control workflow
- Exclusive and one-time passwords
- Unix via SSH keys account (optional)

Configuring a Log-on Account

In this exercise you will add to our CyberArk PAS implementation a Linux privileged account that is prevented by the target platform's security policy from accessing the server via SSH, which is a very common restriction for root accounts. You will then associate a 'logon' account with this new account, allowing you to manage the password despite the SSH restriction. The logon account establishes the connection to the target machine and executes a switch-user operation to the privileged account, and then runs the password change.

Note: In the Unix/Linux world, the account that is typically prevented from connecting to a server remotely is the *root* account. Here in CyberArk training, we are going to use an account named *user01* and we will use the account we created earlier, *logon01*, as the log-on account.

1. Log into the **PVWA** as *vaultadmin01*.
2. Go to the **Accounts** page and press the **Add Account** button.
3. On the **Add Account** screen, enter the following:

System Type:	*NIX
Platform Name:	<i>Linux via SSH 30</i>
Store in Safe:	<i>Linux Finance</i>
Address:	<i>10.0.0.20</i>
User Name:	<i>user01</i>
Password:	<i>Cyberark1</i>
Confirm Password:	<i>Cyberark1</i>

4. Press **Add**.

4. Define account properties

Primary properties

Address
10.0.0.20

Username
user01

Password (optional)
.....

Confirm Password
.....|

Customize account name ?

Allow automatic password management

Cancel < Back Add

5. On the **Account Details** page, press the **Verify** button and select **OK** to the pop up to confirm. The status will appear as '*This account is scheduled for immediate verification*'.

Eventually this will fail because the **CPM** received an 'Access Denied' message due to the restriction on *user01*.

6. Open the account details page using the **Additional details & actions in classic interface** link.

user01 On 10.0.0.20

Platform: Linux SSH 30 Safe: Linux Finance

Additional details & actions in classic interface ? X

Show Copy ... Connect | ▾

Overview Details Activities Versions

7. Press the **Associate** button next to *Logon Account*.



CYBERARK®

CyberArk Privileged Access Security – Administration

Account Details

Search: Leave empty to search all Go

CPM Activities Versions Advanced

The Central Policy Manager failed to verify the password.

Invalid username or bad password. code: 2114 [More details](#)

Logon Account: Associate

Reconcile Account:

Account Group:

Group: [None]

Password

SSH

Platform Name: Linux via SSH 30

Device Type: Operating System

Safe: Linux Finance

Name: Operating System-
LinuxviaSSH30-10.0.0.20-user01

Last verified: N/A

Last modified: vaultadmin01 (5/10/2018 5:38:35 PM)

Last used: vaultadmin01 (5/10/2018 5:38:35 PM)

Username: user01

Address: 10.0.0.20

8. Select the *logon01* account created earlier – you may need to search to see this user – and click **Associate**.

Associate Account

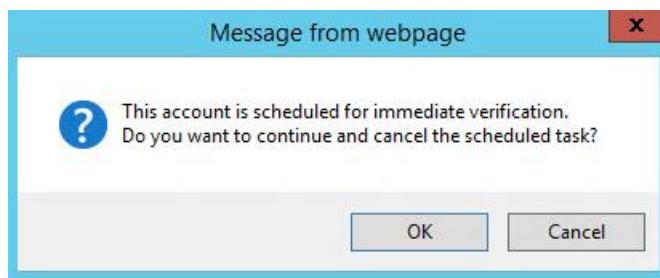
Search: Go

Recently

Username	Address	Safe	Platform ID
admin01	cyber-ark-demo.local	Win-Dom-Admins	WindowsDomainAdmins15
logon01	10.0.0.20	Linux Finance	LinuxviaSSH30
user01	10.0.0.20	Linux Finance	LinuxviaSSH30

Page 1 of 1 | Displaying accounts 1 - 3 of 3

9. Press the **Verify** button and click **OK** to confirm. If you receive the following message, press **OK**.





Note: After a few minutes, the account should be verified. In the background the **CPM** connected to the server as *logon01* and switched to the *user01* account to verify the password.

The screenshot shows the CyberArk Privileged Access Security interface. On the left, there's a sidebar with various icons. The main area is titled 'Accounts' with a search bar. A table lists 60 results for 'All accounts'. One row is selected for 'user01' on '10.0.0.20'. The right side shows detailed information for this account, including its platform (Linux SSH 30) and safe (Linux Finance). It has tabs for 'Overview', 'Details', 'Activities', and 'Versions'. Under 'Overview', there's a 'Compliance Status' section showing 'Compliant' with a '2 Days ago' badge. Below it is a 'Last Verified' section with a '0 Days ago' badge, which is highlighted with a red box. To the right, there's a 'Activities (Last 5)' section listing recent actions like file category changes and updates, and a 'Last Access' section showing activity by 'PasswordManager' today.

Managing a Windows Local Server Account with Reconciliation

In this exercise you will add a Windows local server account for which the correct password is unknown. In order to bring this account under management, you will associate it with a domain administrator account (*cybrreconcile*) that can perform a password change.

Duplicating a Platform

1. Go to **ADMINISTRATION > Platform Management**.
2. Highlight *Windows Server Local Accounts* and click **Duplicate**.
3. Enter *Windows Server Local Admins 45* as the platform name, you may optionally add a description like “Rotate password every 45 days”, and press **Save & Close**.
4. Highlight the newly created platform and press **Edit**.
5. Go to **UI & Workflows**.
6. Change *AutoChangeOnAdd* from **No** to **Yes**. This causes the **CPM** to initiate a password change whenever a new account that uses this policy is created. Select **Apply** to save your change.



The screenshot shows the 'Properties' dialog for a group named 'Windows Server Local Admins 45'. The left pane lists various platform components like Target Account Platform, UI & Workflows, and Automatic Password Management. The right pane displays properties with their values. The 'AutoChangeOnAdd' property is set to 'Yes' and is highlighted with a red box.

Name	Value
ID	WindowsServerLocalAdmins45
AutoChangeOnAdd	Yes
AutoVerifyOnAdd	No
EnableSplitPassword	No
PasswordFirstHalfGroup	
PasswordSecondHalfGroup	
ForceManualPasswordChange	No
ForceManualPasswordChangeUserPrompt	

7. Go to **Automatic Password Management > General** and set both the *Interval* and *ImmediateInterval* to 1.

Note: Once again, we are modifying these values for training purposes only, enabling us to move a little faster. A one-minute immediate interval is suitable for testing but should be set to five in a production environment. The *Interval* parameter should never be set to 1 in a production environment.

8. Enter **Win-Srv-** in the *AllowedSafes* field to limit the accounts with which this platform can be used. Click **Apply** to save your change.

The screenshot shows the 'Properties' dialog for the same group. The 'General' section is selected. The 'ImmediateInterval' field is set to '1' and highlighted with a red box. The 'AllowedSafes' field contains 'Win-Srv-' and is also highlighted with a red box.

Name	Value
PolicyID	WindowsServerLocalAdmins45
PolicyName	Windows Server Local Admins 45
PolicyType	Regular
ImmediateInterval	1
Interval	1440
MaxConcurrentConnections	3
SearchForUsages	Yes
LooselyConnectedDevices	No
AllowedSafes	Win-Srv-

9. Go to **Password Reconciliation** and enter following:

RCAutomaticReconcileWhenUnsynced: Yes

ReconcileAccountSafe: Win-Dom-Admins

**ReconcileAccountName:**

Operating System-
WindowsDomainAdmins15-cyber-ark-demo.local-cybrreconcile
(you can copy this from the notepad file that you created earlier, do NOT copy from this PDF)

Note: The values for the parameters as they appear above assume that you have followed all previous instructions to the letter. If you haven't, then these values will not work. Also, copying and pasting from the PDF into the virtual machine causes problems, so the safest approach is to do as instructed earlier and copy the values from the **PVWA**, paste them into Notepad, and then copy them into the appropriate fields in the Platform.

Name	Value
RCAutoAllowManualReconciliation	Yes
RCAutoReconcileWhenUnsynced	Yes
RCReconcileReasons	2114,2115,2106,2101
RCFromHour	-1
RCToHour	-1
ReconcileAccountSafe	Win-Dom-Admins
ReconcileAccountFolder	Root
ReconcileAccountName	Operating System-WindowsDomainAdmins15-cyber-ark-demo.local-cybrreconcile
RCExecutionDays	
IgnoreReconcileOnMissingAccount	No

Note: Don't forget to enable automatic password change and verification. Also, think about what would be appropriate values for password length and complexity.

10. Press **Apply** and **OK** to close the platform.
11. Log out and exit the **PVWA** browser session.
12. Double-click the **restart-services.bat** on the desktop of your Components server. This will cause the **CPM** server to reload all policies and force your configuration changes to take affect immediately (as well as restarting the **PVWA** and the **PSM**).

Creating a Safe

Now we are going to create a Safe for our Windows server local administrator accounts. To comply with data protection regulation, we are going to organize our safes so that only US admins can access the passwords for US safes.

1. Go to **POLICIES > Access Control (Safes)** and click **Add Safe**.
2. Name the Safe *Win-Srv-Fin-US*. Leave the default values for the rest.



3. Add the AD group **WindowsAdminFin** to the Safe, but remove the check for *Retrieve Accounts* – we don't want our local administrators to view passwords).

The screenshot shows the 'Add Safe Member' dialog box. At the top, there is a search bar with 'Search: win' and a dropdown 'Search In: cyber-ark-de1'. A 'Search' button is to the right. Below the search bar, it says 'Selected Search: cyber-ark-demo.local' and 'Display 4 result(s)'. A table lists four results:

Name	Business Email	Full Name
Windows Authorization Acc...		
WindowsAdminFin		
WindowsAdmins		
WinRMRemoteWMIUsers		

Below the table, there is a sidebar with several sections and checkboxes:

- Access**
 - Use accounts
 - Retrieve accounts
 - List accounts
- Account Management**
- Safe Management**
- Monitor**
 - View Audit log
 - View Safe Members
- Workflow**

At the bottom right are 'Add' and 'Close' buttons.

Adding an Account

Here we will add a local administrator account for your target Windows server. Remember, we don't know what the password is, so you could put anything in the password fields (although they must match).

1. Log in again to the **PWAA** as **vaultadmin01**, go to the **ACCOUNTS** page, and press **Add Account**. Enter the following and press the **Add** button:



Store in Safe:	Win-Srv-Fin-US
System Type:	Windows
Platform Name:	Windows Server Local Admins 45
Address:	vfserver.cyber-ark-demo.local
User Name:	localadmin01
Password:	Cyberark1
Confirm Password:	Cyberark1
Logon To (optional)	<click the <i>Resolve</i> button>

Add Account

4. Define account properties

Primary properties

Address: vfserver.cyber-ark-demo.local

Username: localadmin01

Password (optional):

Confirm Password:

Customize account name: [?](#)

Additional properties

Logon To (optional): VFSERVER

Location (optional):

Note: After adding the account, when you select it you should see a message stating '*The password for this account has been manually scheduled for change.* This is because you set *AutoChangeOnAdd* to **Yes** in the policy. Also note that there is a reconcile account already associated with this new account.

2. Press **Refresh**. Because the password for this account was not *Cyberark1*, **the password change will fail.**



3. Press **Refresh** again and after a short time and you should receive a message saying that the account was successfully reconciled. The first time an account is reconciled it can take a little while, so be patient.

The screenshot shows the CyberArk Privileged Access Security interface for managing accounts. At the top, it displays the account name "localadmin01 On vfserver.cyber-ark-demo.local". Below this, there are status indicators: a yellow lightning bolt icon, "Platform: Windows Server Local Admins 45", and "Safe: Win-Srv-Fin-US". There are also "Connect" and "Show" buttons, and a "..." menu button.

The main interface has tabs for "Overview", "Details", "Activities", and "Versions". The "Overview" tab is selected, showing the "Compliance Status" as "Compliant". A large green circle contains the number "0", indicating "Days ago". Below this, it says "Reconciled by PasswordManager Oct 5, 2018 10:58 AM". There are "Reconcile" and "Change" buttons.

The "Activities" section shows a list of recent actions:

Date	User	Action
Oct 5 10:59:41 AM	vaultadmin01	Retrieve password
Oct 5 10:58:45 AM	PasswordManager	CPM Reconcile Password
Oct 5	PasswordManager	



Configure and Test Dual Control

In this section, we will configure dual control for access to Linux accounts. The ability to receive e-mails is required in order to test the full functionality of dual control.

Dual control is configured in the *Master Policy*. To enable it for Linux machines only, we will add an exception to the *Master Policy* for the appropriate Platform.

Adding a manager to an existing safe

The workflow process is configured through safe membership. We will need to add a manager to the existing safe so that he/she can approve requests. IT Managers will be able to view the passwords and use the passwords to access the safe without approval.

What might be the result if no one has been assigned the responsibility to respond to a workflow request?

1. Go to **POLICIES > Access Control (Safes)**.
2. Highlight *Linux Finance* and press the **Members** button.

The screenshot shows the CyberArk Admin interface. On the left, there's a sidebar with icons for Policies, Accounts, Notifications, and Audit. The main area is titled 'Policies > Access Control (Safes)' and 'Access Control (Safes)'. It displays a list of safes, with 'Linux Finance' selected and highlighted with a blue bar. To the right, there's a table with columns for 'DESCRIPTION' and 'Members'. At the bottom right of the table, there are three buttons: 'Edit', 'Members' (which is highlighted with a red box), and 'Delete'.

3. Click **Add Member**.
4. Enter *mgr01* in the **Search** field, select *cyber-ark-demo.local* in the **Search In** field, and press **Search**.
5. Select the *mgr01* user.
6. Under **Access**, leave the checks for *Use accounts*, *Retrieve accounts*, and *List account* for this group.



Add Safe Member

Search: Search In: Selected Search: cyber-ark-demo.local Display 1 result(s)

Name	Business Email	Full Name
mgr01	mgr01@cyber-ark...	

Access
 Use accounts
 Retrieve accounts
 List accounts

Account Management

Safe Management

Monitor
 View Audit log
 View Safe Members

Workflow

7. Scroll down and expand the **Workflow** link to access the **Authorize account requests** check box. Check the **Authorize account requests** authorization box with **Level 1** and **Access Safe without confirmation**.



The screenshot shows the 'Add Safe Member' dialog box. At the top, there is a search bar with 'mgr01' entered, a dropdown for 'Search In' set to 'cyber-ark-de', and a 'Search' button. Below the search bar, it says 'Display 1 result(s)'. A table lists one result: 'mgr01' with 'mgr01@cyber-ark...' as the business email. Below the table, there are several sections: 'Monitor' (checkboxes for 'View Audit log' and 'View Safe Members'), 'Workflow' (checkbox for 'Authorize account requests' with 'Level 1' selected), and 'Advanced' (checkbox for 'Membership expires on date'). At the bottom right are 'Add' and 'Close' buttons.

8. Press **Add**.
9. In preparation for a later exercise, please also add the Active Directory group “ITManagers” as a member of this safe with the same rights as *mgr01* for both *Access* and *Workflow*.

Testing Dual Control

Testing this workflow requires us to wear a number of hats. We configured the system as a vault administrator – *vaultadmin01* – now we are going to become ordinary users of the system.

- We will first log in as a user who has the right to use a password, but only with manager approval – *linuxuser01*.
- We will then put on our manager hat and check our email, notice that we have a notification for an approval request pending, log into the **PVWA** as that manager user – *mgr01* – using the link provided, and approve the request.
- Finally, we will return to the **PVWA** as *linuxuser01*, find the approval notification, and access the target system with the password.



Note: Because we will be changing users, you might want to use two browsers or separate browser sessions. You can use incognito mode to open two separate sessions with two separate users.

1. Log out of the **PVWA**.
2. Log back in as the LDAP user *linuxuser01* with the password *Cyberark1*.
3. Leaving the **Search** field blank, click on the magnifying glass icon to search for all accounts.
4. Locate *logon01* and select the **Request Connection** button.

The screenshot shows the CyberArk PVWA interface. At the top, there's a navigation bar with the CyberArk logo, the text "Last sign in: 10/5/2018 | linuxuser01", and various icons. Below this is the "Accounts View" header with a search bar and a "Views" dropdown. On the left, there's a sidebar with sections like "My accounts", "All accounts (default)", "Recently used", "Favorites", and "Checked-out". The main area displays a table of accounts with columns: Star, Status, Username, Address, Platform ID, Safe ↑, Access Request, and Connect with SSH. The account "logon01" is listed with a status of "Failed". The "Access Request" column for "logon01" contains a blue button labeled "Request connection" with a dropdown arrow and three dots. This button is highlighted with a red rectangular box. There are also other accounts listed: "user01" and "logon10", each with their own "Request connection" buttons.

5. Enter a *reason* to access. Activate the **Timeframe** and specify *FROM* the current date in the morning *TO* the end of the last day of the class. Also activate *Multiple access is required* and then press on the **Send Request** button.



Request to connect with Linux via SSH 30-logon01-10.0.0.20

Reason
Need to access this server for training

Timeframe
 Request timeframe

FROM TO
Sep 4, 2018 8:00 AM | ▾ Sep 7, 2018 5:00 PM | ▾
GMT+0100 (GMT Daylight Time)

Multiple access is required

Confirmation
One user must confirm the request
▼ Confirmers List

6. **Sign out of this session** and close the browser, to ensure that the *linuxuser01* session has ended (otherwise the next steps will not work properly). Alternatively, you can use a different browser or a private session.
7. Launch a new browser session and open the email client at <http://cyber-ark-demo.local:8073/webmail/> (there is a short cut in the browser toolbar).
8. Login as *mgr01*. You should have received an e-mail with the new request (if you do not receive an email, make sure the ENE service is running on the **Vault**).

Note: Our email server is currently unable to convert URLs to clickable links, so you will have to copy and paste the URL into your browser's address window. This is not an issue with most commercial email clients.



The screenshot shows an email message in a web-based mail client. The subject of the email is "Notification: Password access request". The message is from "VaultAdmins" to "mgr01@cyber-ark-demo.local". The date is "Today 15:00". The body of the email contains details about a password access request:

CyberArk Enterprise Password Vault
Dear Sir or Madam ,
A password access request is pending your approval.
Request information:
===== Requester name: Requester user: linuxuser01 Requester email: linuxuser01@cyber-ark-demo.local Requester phone: Requester object: Root\Operating System-LinuxviaSSH30-10.0.0.20-logon01 Safe: Linux Finance Request Id: 1 Device User Name: logon01 Device Address: 10.0.0.20 Issued on: 5/11/2018 3:00:24 PM Request start date: 5/11/2018 8:00:00 AM Request end date: 5/15/2018 5:00:00 PM Request type: Multi Reason: Need to access this server for training Ticketing System: N/A Ticket ID: N/A

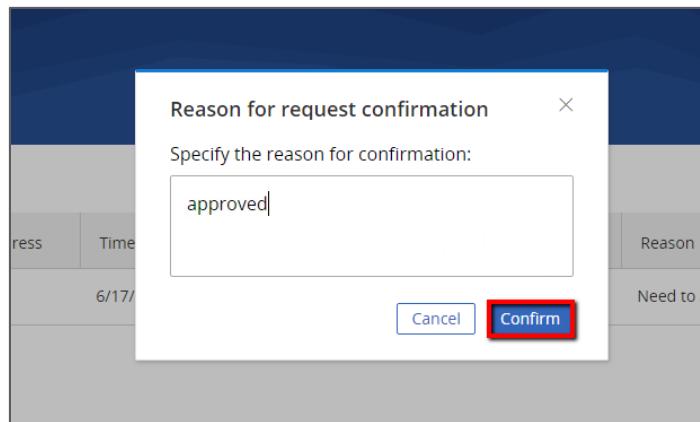
To review the request, click the following link: <http://127.0.0.1/PasswordVault/directaccess.aspx?requestdetails.aspx&RequestId=1&Safe=Linux%20Finance>

This mail has been sent to you through the Enterprise Password Vault Notification Service

9. Login to the **PWVA** as *mgr01* password *Cyberark1*.
10. Go to **Accounts** and select **Incoming Requests**. Locate the incoming request from *linuxuser01* and press the **Confirm** button.

The screenshot shows the "Incoming Requests" page in the CyberArk PWVA. The left sidebar has a "Requests Views" section with options: Pending requests, Pending and confirmed requests, Pending and expired requests, and All requests. The main area shows a table with one result for "Pending requests". The table columns are: Status, Requestor Username, Account Username, Account Address, Time frame, Permission to, Access, Reason, Ticket System Name, and Ticket Number. A row for "linuxuser01" is shown. At the bottom right of the table, there are "Confirm" and "Reject" buttons, both of which are highlighted with a red box.

11. Enter a reason and press **Confirm**.



12. **Sign out, and close the browser** to terminate the *mgr01* session.
13. Browse to the email client at <http://cyber-ark-demo.local:8073/webmail/> and login as *linuxuser01*. You should receive an e-mail stating the request has been confirmed.
14. Login to the **PWVA** as *linuxuser01*, password *Cyberark1* to see the **Account Details** page. Notice the **Status** of the request is now confirmed. You can now use the password and connect to the previously requested account.

Username	Address	Platform ID	Status	Access Request
root02	centos-target01	LinuxSSH30	Linux Finance	
logon01	10.0.0.20	LinuxSSH30	Linux Finance	
user01	10.0.0.20	LinuxSSH30	Linux Finance	
root01	10.0.0.20	LinuxviaKey90	Linux Finance	

15. Sign out of the *linuxuser01* session.

Exclusive Passwords with Automated Release and One-time Use

In this exercise, you will configure the Windows Server Local accounts added earlier for exclusive access with an automatic release based on the Minimum Validity Period.

Adding a Master Policy exception for Exclusive Passwords

Exclusive Passwords are configured in the *Master Policy*.



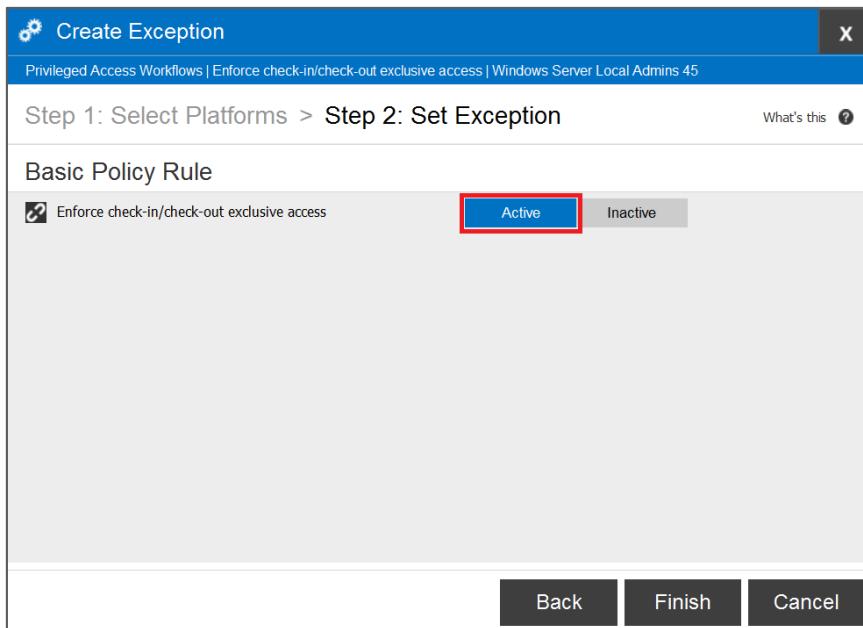
1. Using **PWAA**, login as *vaultadmin01*.
2. Go to **POLICIES > Master Policy** and select *Enforce check-in/check-out exclusive access* and click **Add Exception**.

The screenshot shows the CyberArk Policies interface. On the left, there's a sidebar with icons for Policies, Master Policy (which is selected), Policy by Platform, and Access Control (Safes). The main area is titled 'Policies > Master Policy' and shows a table for 'Privileged Access Workflows'. One row, 'Enforce check-in/check-out exclusive access', is highlighted with a red border. To the right, there's a 'Rule Preview' section showing 'Inactive' and 'None' under 'ADVANCED SETTINGS'.

3. Select *Windows Server Local Admins 45* and press **Next**.

The screenshot shows the 'Create Exception' dialog box. It has a header 'Create Exception' and a sub-header 'Privileged Access Workflows | Enforce check-in/check-out exclusive access'. Below that is a step indicator 'Step 1: Select Platforms > Step 2: Set Exception'. The main area is a table with columns 'Name', 'Device Type', and 'Status'. The table lists numerous platforms, with 'Windows Server Local Admins 45' being the selected item. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

4. Press the **Active** button to enable *Enforce check-in/check-out exclusive access* and click **Finish**.



Adding a Master Policy exception for One-Time Passwords

To allow for an automatic release of a checked-out password, you will need to enable the policy *Enforce one-time password access* for the platform *Windows Server Local Admins 45*.

1. Highlight *Enforce one-time password access* and press **Add Exception**.
2. Select *Windows Server Local Admins 45* and press **Next**.
3. Press **Active** to enable one-time password access for this platform and then click **Finish**.

Reducing the Minimum Validity Period

Note: This next step is for testing/training purposes only and should not be used in a production environment.

We will set the *Minimum Validity Period* to 5 minutes, so that we can see our results more quickly. The *MinValidityPeriod* parameter is configured in the Platform.

1. Go to **ADMINISTRATION > Platform Management**, select *Windows Server Local Admins 45*, and click **Edit**.
2. Go to **Automatic Password Management > Privileged Account Management**.
3. Set *MinValidityPeriod* to **5**.



The screenshot shows the 'Properties' dialog box for a group named 'Windows Server Local Admins 45'. The left pane lists various policy categories. The 'Privileged Account Management' category is selected. The right pane displays properties for this category, including:

Name	Value
MinValidityPeriod	5
DoNotExtendMinValidityPeriod	No
PasswordLevelRequestTimeframe	Yes
ResetOveridesMinValidity	Yes
ResetOveridesTimeFrame	Yes
Timeout	30
UnlockIfFail	No
UnrecoverableErrors	2121,2103,2105
MaximumRetries	5
MinDelayBetweenRetries	90
LogonAccountSafe	

A note below the table states: 'PasswordLevelRequestTimeframe: Whether or not request timeframe in password level is enabled. This parameter is not relevant if the policy is of type group.'

4. Press **Apply** and **OK** to close the Platform and then sign out of the **PVWA**.

Testing Exclusive Passwords

In this section, we will test our configuration of exclusive passwords with automatic release. We will use the user *bill*. Bill is a member of the Active Directory group *WindowsAdminsFin*.

1. Double-click the **restart-services.bat** on the desktop of your components server. This will cause the **CPM** server to reload all policies and force your configuration changes to take affect immediately.
2. Login to the **PVWA** as the **LDAP** user '*bill*' with the password *Cyberark1*.
3. Go to **ACCOUNTS** and press the magnifying glass to search for all accounts.
4. Click on the *localadmin01* account and click the **Connect** button. Bill has now checked out the password.

The screenshot shows the 'Accounts' page in the PVWA. It displays a single result for the account 'localadmin01'. The account details are as follows:

Star icon	Status	Username	Address	Platform ID	Safe ↑	Access Request	Connect with RDP
Star icon	⚡	localadmin01	vfserver.cyber-ark-dem...	WindowsServerLocalAd...	Win-Srv-US	-	Connect

5. Launch the RDP session to the target Windows server. This will check out the account and lock it. Leave the RDP session open.



Note: Bill or an admin can release the account manually by using the “Check-in” option, however we will not use this option as we want to see the system release it automatically at the end of the Minimum Validity Period.

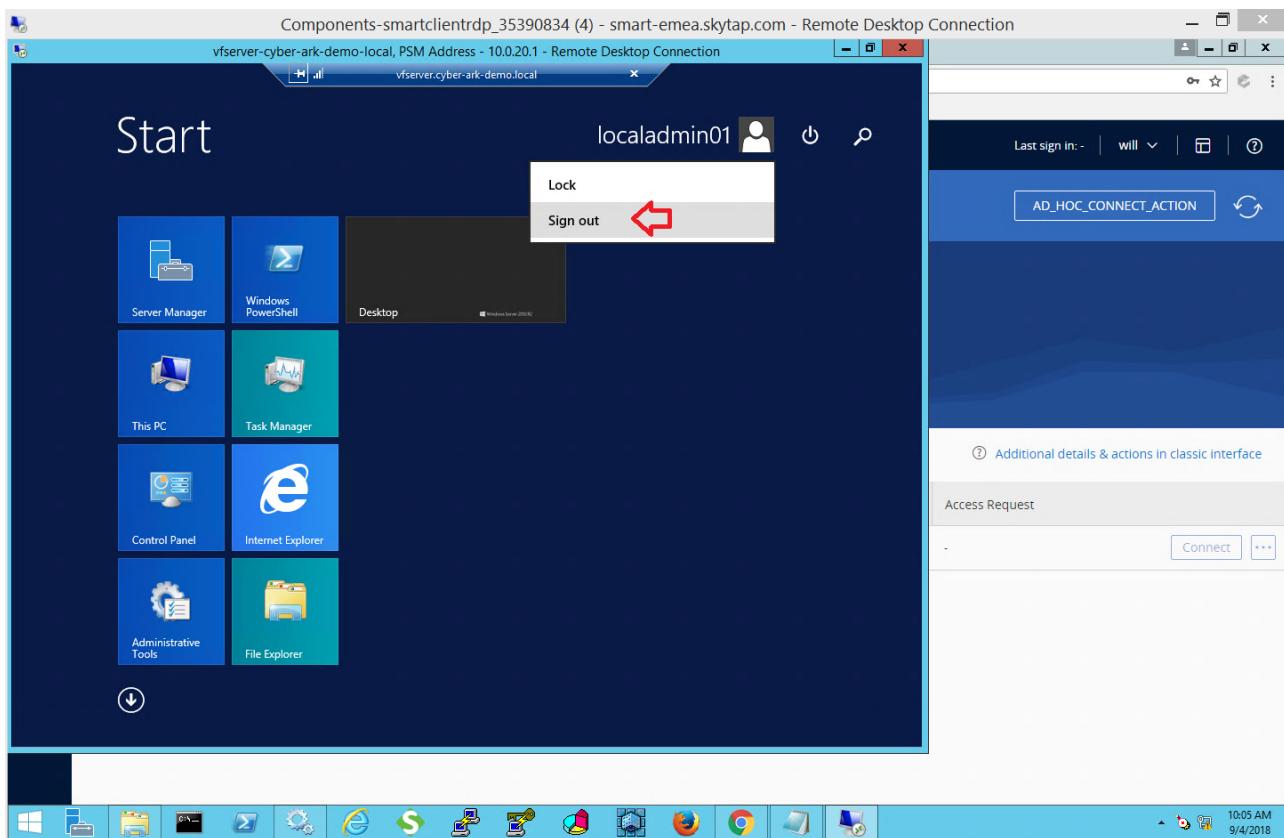
6. Log out out of the **PWVA** and log back in as *vaultadmin01*. You should notice a lock icon next to the *localadmin01* account.
7. Hover over the lock icon, it should say “The account is checked-out by bill”.

The screenshot shows the 'Accounts View' page. At the top, there's a search bar and navigation links for 'Views', 'Recent', and 'Saved'. On the left, a sidebar lists 'My accounts' with options like 'All accounts (default)', 'Recently used', 'Favorites', and 'Checked-out'. On the right, a 'Status' section shows 'Disabled by CPM', 'Failed', 'Newly added', and 'Disabled by user'. Below this, a message says '1 results for: All accounts'. A table lists one account: 'localadmin01' from 'vfserver.cyber-ark-dem...' with platform ID 'WindowsServerLocalAd...' and location 'Win-Srv-Fin-US'. The 'Status' column for this account shows a lock icon with a red border, indicating it is 'Disabled by user'. A tooltip above the lock icon says 'This account is checked-out by bill'. There are also icons for 'Star', 'Lock', and 'Flash'.

8. If you press **Show**, you will receive an error message.

After several minutes (remember the minimum validity period was set to 5 min), the *vaultadmin01* user will be able to access the password and the **CPM** will have changed the password.

If the account is not released after several minutes, run the *restart.bat* file and check again.



Managing an Oracle Account

In this section, we will configure CyberArk to manage an Oracle DBA account. As in previous exercises, we will create a Safe, duplicate a Platform, and then add the account.

Creating a Safe

1. Log in as **vaultadmin01** and go to **POLICIES > Access Control (Safes)**.
2. Press the **Add Safe** button.
3. Enter **Oracle Finance** as the **Safe name** and press **Save**.

Add Safe

Safe name:	Oracle Finance
Description:	<input type="text"/>
<input type="checkbox"/> Enable Object Level Access Control Saved accounts: <input type="radio"/> Save the last <input type="text" value="5"/> account versions <input checked="" type="radio"/> Save account versions from the last <input type="text" value="7"/> days	
Assigned to CPM:	<input type="text" value="PasswordManager"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

4. Add the Active Directory group *OracleAdmins* to the safe with default permissions.

Duplicating a Platform

In this section, we are going to create a Platform dedicated to managing accounts used to access Oracle databases, such as a DBA account.

1. Go to **ADMINISTRATION > Platform Management**.
2. Choose *Oracle Database* and press **Duplicate**.
3. Enter *Oracle DBA 30* and press **Save & Close**.

Duplicate Target Account Platform

Source Platform	Oracle Database
Duplicate to	
Name	<input type="text" value="Oracle DBA 30"/>
Description	<input type="text" value="For Oracle DBA accounts, rotate password every 30 days"/>
<input type="button" value="Save & Close"/> <input type="button" value="Cancel"/>	

4. Select *Oracle DBA 30* and press **Edit**.



The screenshot shows the CyberArk Platform Management interface. On the left, a sidebar titled 'ADMINISTRATION' has a 'Platform Management' section selected. The main area is titled 'Platform Management' and shows a table of 'Target Account Platforms'. The table includes columns for Name, Device Type, and Status. One row, 'Oracle DBA 30', is highlighted. To the right, a 'Platform Preview' panel displays detailed information for the selected platform, including its name ('Oracle DBA 30'), description ('Oracle DBA accounts platform, rotate every 30 days'), and status ('Active').

Name	Device Type	Status
Linux via SSH 30	Operating System	Active
Oracle DBA 30	Database	Active
Windows Domain Admins 15	Operating System	Active
Windows Server Local Admins 45	Operating System	Active
[Sample Password Group Platform]	Misc	Inactive
[Sample SSH Key Group Platform]	Misc	Inactive
Amazon Web Services - AWS	Cloud Service	Inactive
Amazon Web Services - AWS - A...	Cloud Service	Inactive
AS400	Operating System	Inactive
BMC Remedy	Application	Inactive
Check Point FireWall-1	Security Appliance	Inactive
Check Point GAiA via SSH	Security Appliance	Inactive

Note: Take a good look at the image above. You may notice that the only active platforms are those that we have created. This image illustrates why it is a good idea to deactivate unused platforms. Furthermore, the inactive platforms are not shown when adding accounts, so you don't have to scroll through a long list to find the one you want (and possibly make a mistake).

5. Go to **UI & Workflows** and set *AutoChangeOnAdd* to **Yes**.
6. Go to **Automatic Password Management > General**.
7. Set *ImmediateInterval* to **1**.
8. Set *AllowedSafes* to **Oracle**.
9. Press **Apply**.



10. In the **Generate Password** section, add the equal sign character ('=' without the quotes) to the *PasswordForbiddenChars* field. Make sure you add the new character without deleting any of the existing characters.

The screenshot shows the CyberArk Platform's configuration interface for the Oracle DBA 30 target account. The left sidebar lists various management modules like Target Account Platform, UI & Workflows, and General. The main panel displays the properties for Oracle DBA 30, specifically focusing on the 'Generate Password' settings. The 'PasswordForbiddenChars' field is highlighted with a red border, containing the value '%@#:\$00!\$>~!#%'. Other visible properties include PasswordLength (8), MinUpperCase (2), MinLowerCase (2), MinDigit (1), MinSpecial (1), PasswordEffectivelength, PreventSameCharPerPrevPassPosition (No), and PreventRepeatingCharacters (No). Buttons for Apply, OK, and Cancel are at the bottom right.

11. Click **OK** to save the changes and close the Platform.

Adding an Account

1. Go the **ACCOUNTS** tab, click **Add Account** and enter the following:

Store in Safe:	Oracle Finance
Device Type:	Database
Platform Name:	Oracle DBA 30
User Name:	dba01
Address:	10.0.0.20
Password:	Cyberark1
Confirm Password:	Cyberark1
Port:	1521
Database:	xe

2. Press **Add**.



4. Define account properties

Primary properties

Username: dba01

Address (optional): 10.0.0.20

Password (optional):

Confirm Password:

Customize account name:

Additional properties

DSN (ODBC) (optional):

Port (optional): 1521

Database (optional): xe

Account management

Allow automatic password management:

Cancel | < Back | Add

Note: Because the policy was set to *AutoChangeOnAdd=Yes*, the account will be set for immediate change.

3. Press refresh and you will see the message: '*The password for this account has been manually scheduled for change*'.
4. After a minute or two, press the **Show** button to display the new password.

Note: If you want to test the new account, you can log in to the **PVWA** as the user *larry*, who is a member of the *OracleAdmins* group in Active Directory.

OPTIONAL: Managing a Linux Account with SSH Key

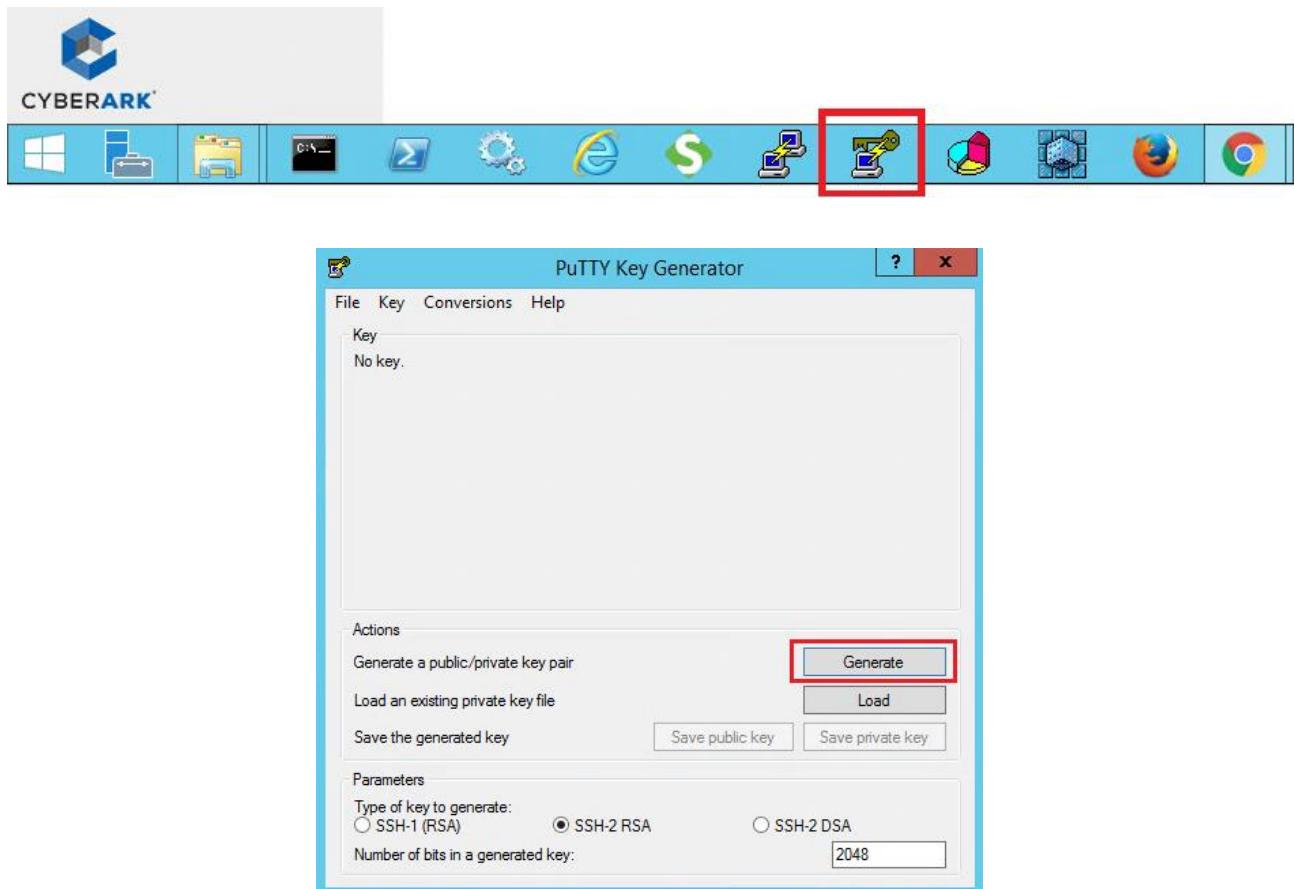
Note: Not all organizations use SSH keys with their *nix servers, while others have only Windows machines. As such, if you feel that this particular exercise is not relevant to your work, feel free to skip it.

In this section, we will perform the tasks required to manage a Linux account that connects to its target server with a public-private key-pair.

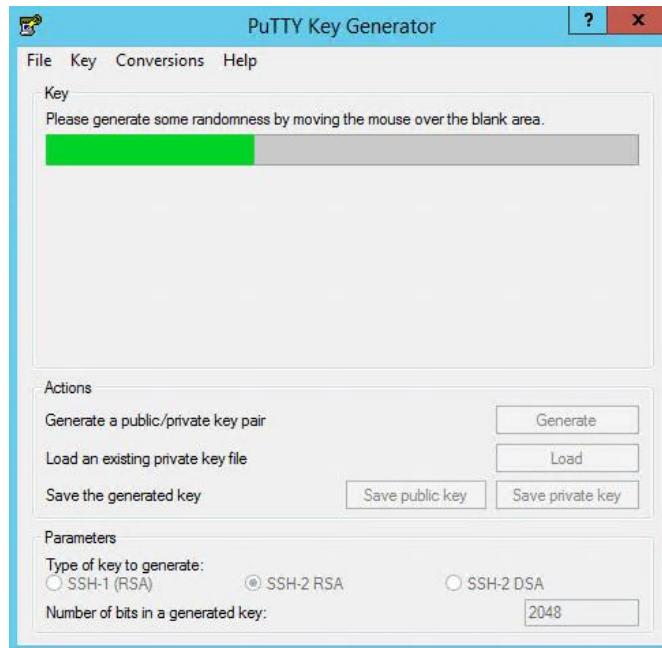


Generating a Key-Pair

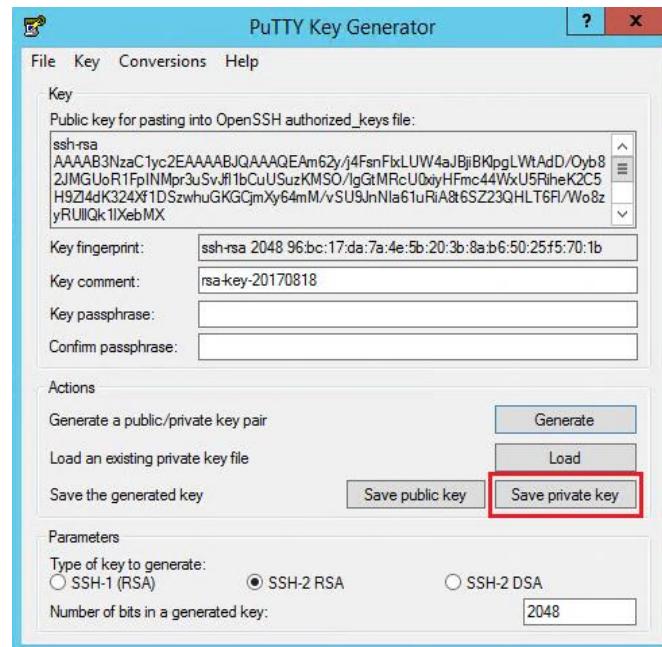
1. On the **Components** server launch **puttygen** from the Taskbar and click **Generate**.



2. As instructed, you need to make mouse movements in the blank area to generate random data for the key.



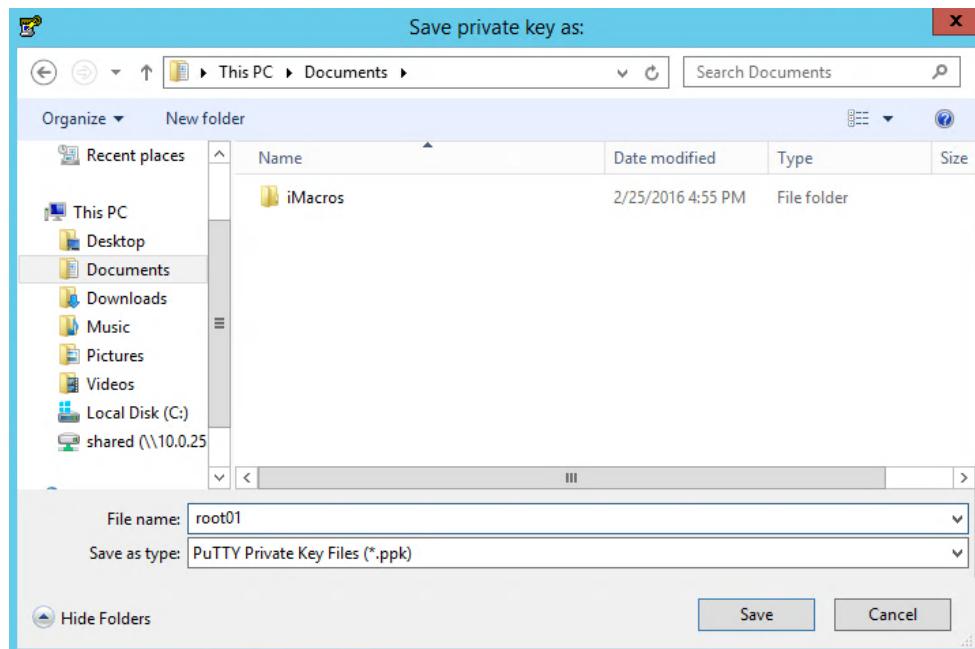
- When the key is generated click **Save Private Key**.



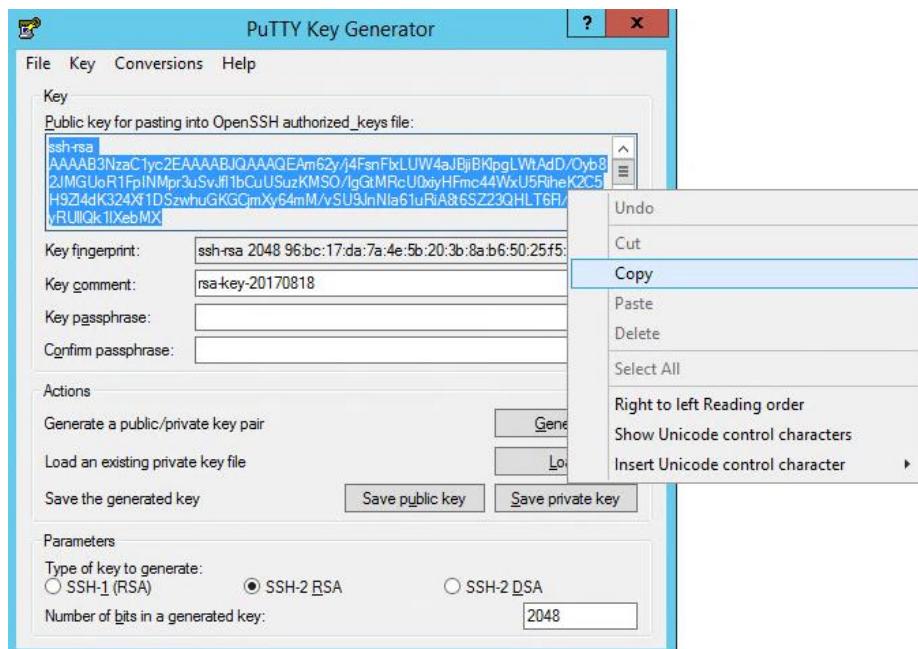
- Click **Yes** to store they key without a passphrase. The **CPM** does not support private keys with passphrases.



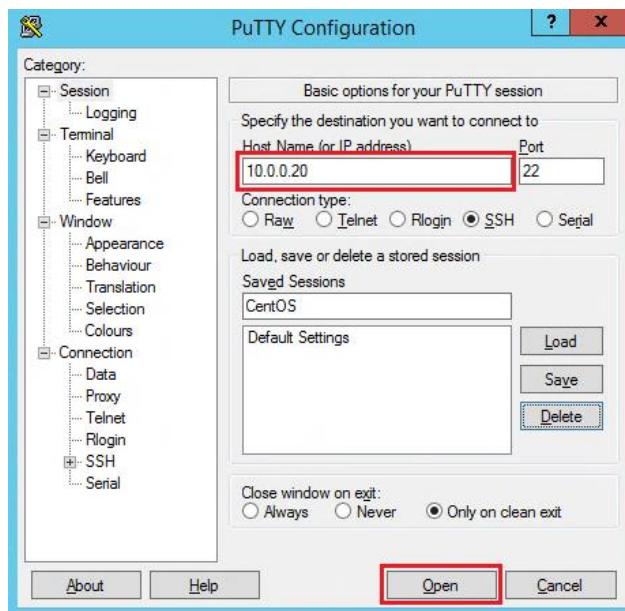
5. Name the key **root01.ppk** and save it to your **Documents** directory.



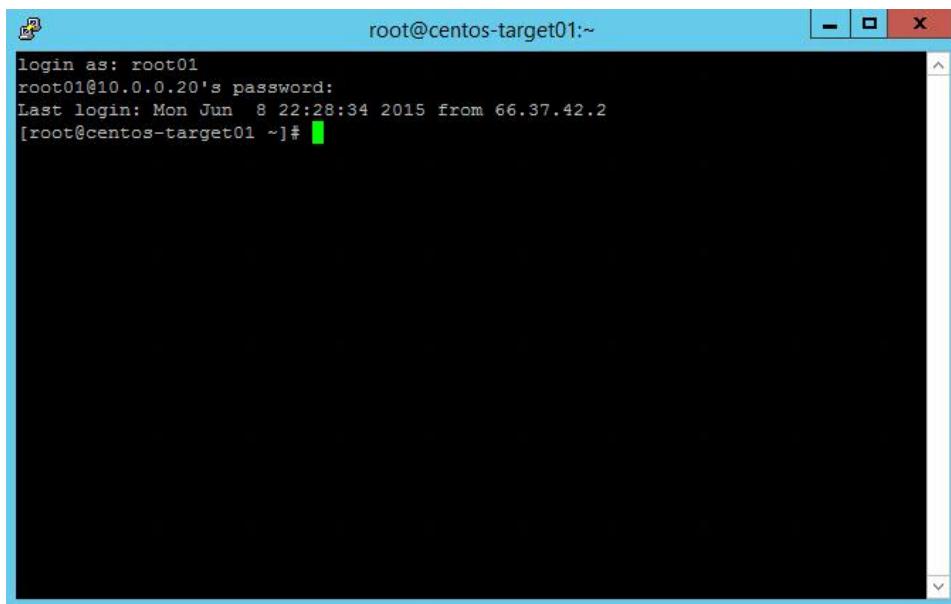
6. Select all the text in the 'Public key for pasting into Open SSH authorized keys file' box and **copy** it to your clipboard.



7. Use putty to connect to 10.0.0.20.



8. Log in as root01 with the password Cyberark1.

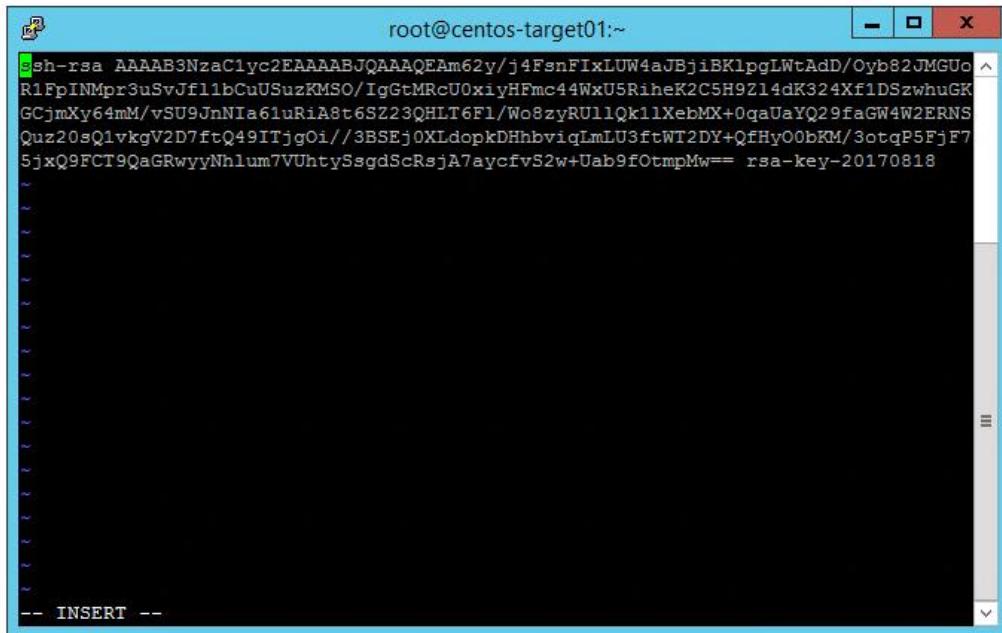


```
root@centos-target01:~
login as: root01
root01@10.0.0.20's password:
Last login: Mon Jun  8 22:28:34 2015 from 66.37.42.2
[root@centos-target01 ~]#
```

9. Edit your authorized key file with vi.

```
vi ~/.ssh/authorized_keys
```

10. Press **i** (or the **Insert** button on your keyboard) to enter insert mode.
 11. Right click inside the editor to paste the key. Verify that the key pasted correctly.



```
root@centos-target01:~
ssh-rsa AAAAB3NzaC1yc2EAAAQEA...rsa-key-20170818
-- INSERT --
```

Warning! It can be a bit tricky to copy and paste into a terminal window. Make sure that your key text begins with the string “ssh-rsa” and that it ends with “rsa-key-**date**” where **date** is today’s date.



12. Press **ESC** and then enter :**wq** -- (colon) (w) (q)
13. Press **ENTER** to exit and save.
14. Make sure the Key appears in the *authorized_keys* file (and that all characters were pasted properly) by using the *cat* command:

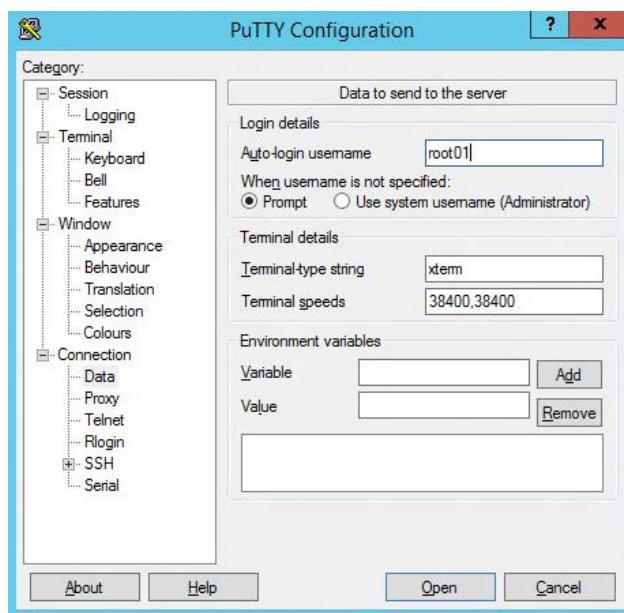
```
cat ~/.ssh/authorized_keys
```
15. Exit your **putty** session.

Note: If you need help with the **vi** editor, you can read the tutorial at:
<http://www.tutorialspoint.com/unix/unix-vi-editor.htm>

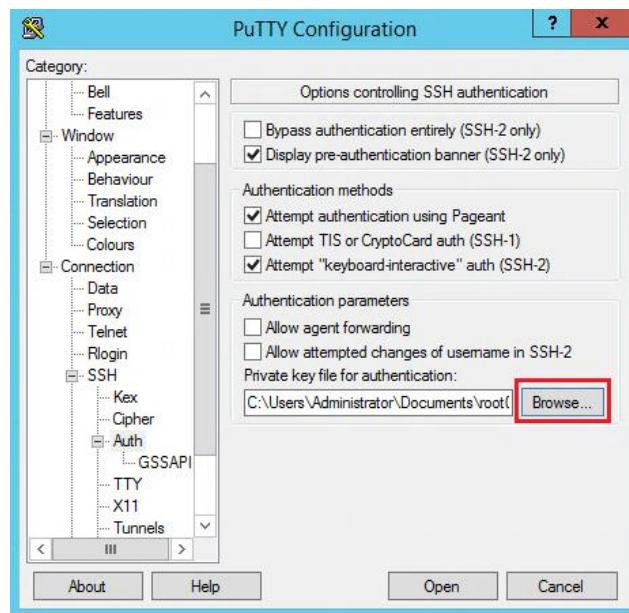
Verify You Are Able to Log in with the Private Key

Now we will test that we are able to authenticate with the private key.

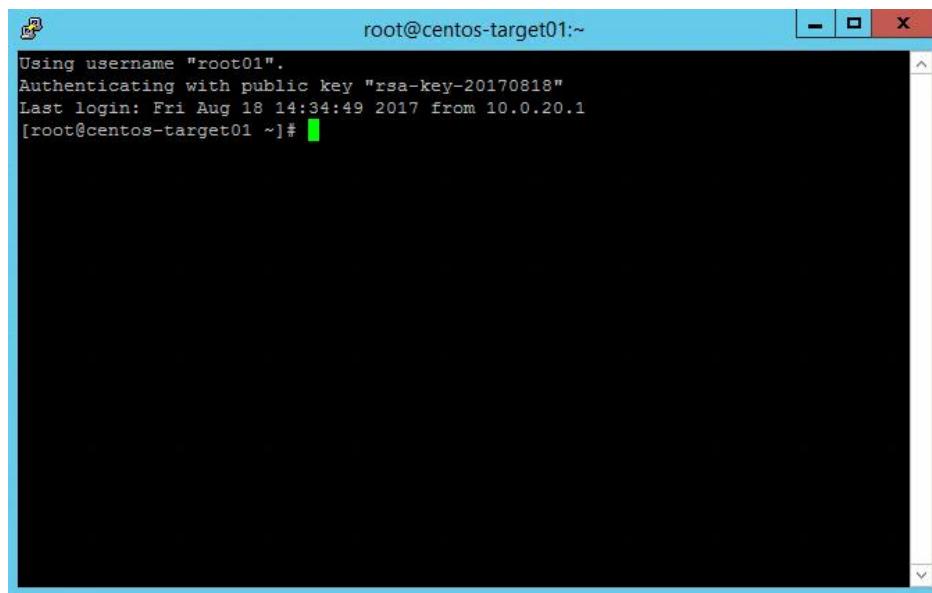
1. Open **putty** again.
2. Type **10.0.0.20** in the **Host Name** box, but do not connect yet. Navigate to **Connection > Data**.
3. Enter **root01** in the **Auto-login username** field.



4. Navigate to **Connection > SSH > Auth**.
5. Click **Browse** and browse to the *ppk* file you created earlier.



- Now click **Open** and verify that you are able to log on without supplying a username and password.



```
root@centos-target01:~  
Using username "root01".  
Authenticating with public key "rsa-key-20170818"  
Last login: Fri Aug 18 14:34:49 2017 from 10.0.20.1  
[root@centos-target01 ~]#
```

Duplicating a Platform

- Login to **PVWA** as **vaultadmin01** and go to **ADMINISTRATION > Platform Management**.
- Highlight **Unix via SSH Keys** (make sure that you choose the “**Unix via SSH Keys**” platform, not the “**Unix via SSH**” platform).
- Press **Duplicate**.



Name	Device Type	Status
test	Operating System	Active
Unix via SSH	Operating System	Active
Unix via SSH Keys	Operating System	Active
VMWare ESX Account	Operating System	Active
VMWare vCenter Personal	Application	Active
VMWare vCenter Shared Accounts	Application	Active
Windows Desktop Local Accounts	Operating System	Active
Windows Domain Admins 15	Operating System	Active
Windows Server Local Accounts	Operating System	Active
Windows Server Local Admins 45	Operating System	Active
[Sample Password Group Platform]	Misc	Inactive
[Sample SSH Key Group Platform]	Misc	Inactive
AS400	Operating System	Inactive
BMC Remedy	Application	Inactive
Check Point FireWall-1	Security Appliance	Inactive
Check Point GAA via SSH	Security Appliance	Inactive
Cisco Pix via SSH	Security Appliance	Inactive

4. Name your platform **Linux via Key 90** and click **Save & Close**. We won't make any modifications to this platform.

Duplicate Target Account Platform

Source Platform
Unix via SSH Keys

Duplicate to

Name
Linux via KEY 90

Description
Linux servers via SSH keys, rotate keys every 90 days|

Save & Close Cancel

Add an Account with an SSH key

1. Using the classic interface, go to the **ACCOUNTS** tab and click the **Add SSH Key** button.



2. Add an account with the following properties. If you do not see the SSH Key configuration area, you may have duplicated the wrong platform.

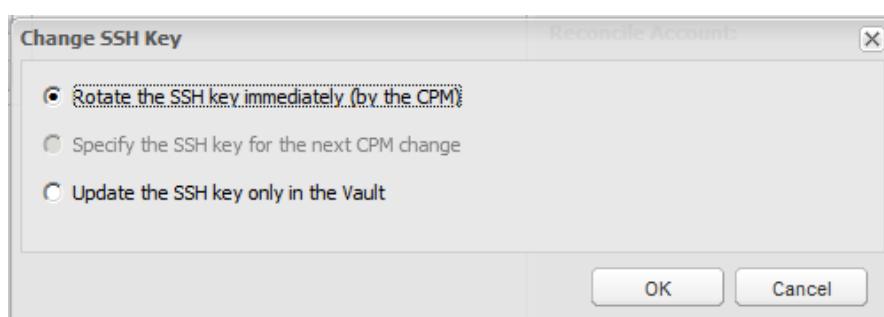


Store in Safe:	Linux Finance
Device Type:	Operating System
Platform Name:	Linux via Key 90
Address:	10.0.0.20
Username	root01
Private Key:	Browse to find the <i>root01.ppk</i> file you created earlier.

3. Click **Save**.

The screenshot shows the 'Add SSH Key' dialog box. It includes fields for 'Store in Safe' (set to 'Linux Finance'), 'Device Type' (set to 'Operating System'), and 'Platform Name' (set to 'Linux via Key 90'). Under 'Required Properties', 'Address' is set to '10.0.0.20' and 'Username' is set to 'root01'. In the 'Optional Properties' section, there is a 'Comment' field. The 'SSH Key' section has a radio button for 'Select SSH key file' which is selected, and a 'Choose File' button pointing to 'root01.ppk'. There is also a 'Paste SSH key' option. Below these, there are fields for 'Name' (with radio buttons for 'Auto-generated' or 'Custom') and 'Disable automatic management for this account' with a 'Reason' input field. At the bottom are 'Save' and 'Cancel' buttons.

4. Click **Change** and select *Rotate the SSH key immediately (by the CPM)*.
5. Click **OK**. This process can take a few minutes.



6. Once the change completes verify that you are NOT able to connect with **putty** using the SSH key.

Onboarding Accounts

In the following exercises you will use the **Accounts Feed** feature as well as the **Password Upload Utility** to onboard accounts to the system.

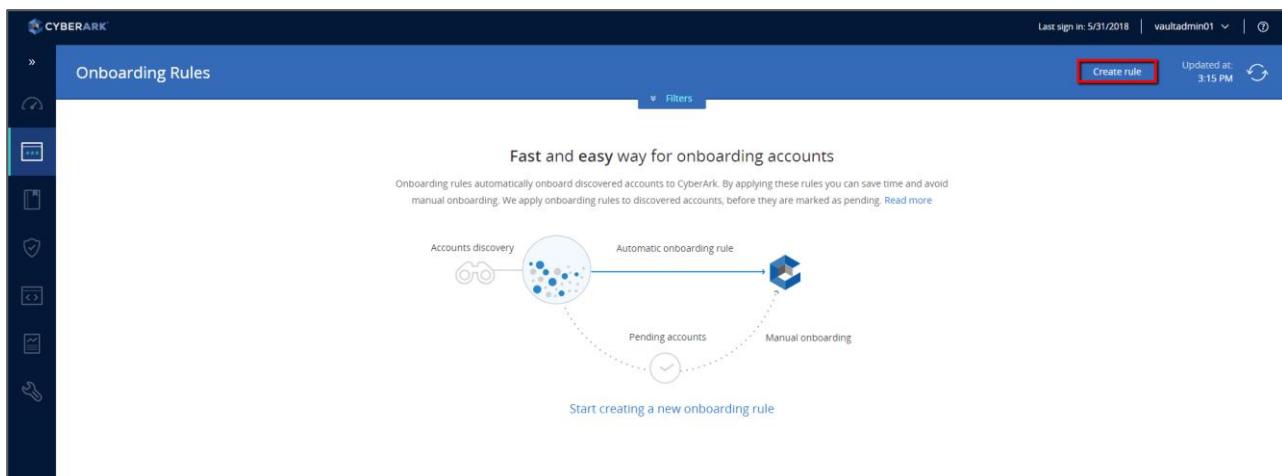
Accounts Feed

In the next exercise you will configure rules for automatically onboarding accounts discovered using the Accounts Feed feature and then run a Windows Discovery to discover and automatically onboard accounts.

Configure Automatic Onboarding Rules

In this section, you will configure Onboarding Rules in order to add newly discovered accounts to the **Vault** without any human intervention.

1. On the **Components** server, open Chrome and go to the **PWVA**.
2. Go to **Accounts > Accounts Feed > Onboarding Rules** and click on **Create rule**.



3. In **Select system type** select **Windows**.



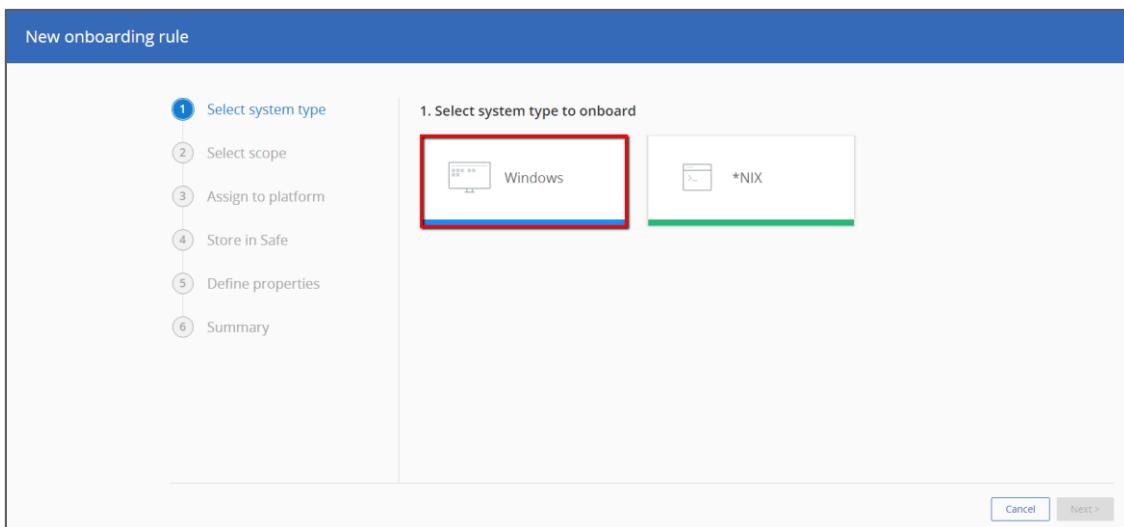
New onboarding rule

1. Select system type to onboard

① Select system type
② Select scope
③ Assign to platform
④ Store in Safe
⑤ Define properties
⑥ Summary

Windows *NIX

Cancel Next >



4. In **Select Scope** select the following:

Machine Type:	Server
Account Type:	Local
Account Category:	Any
Privileged Account Type:	Any
Username (begins...):	discovery

New onboarding rule

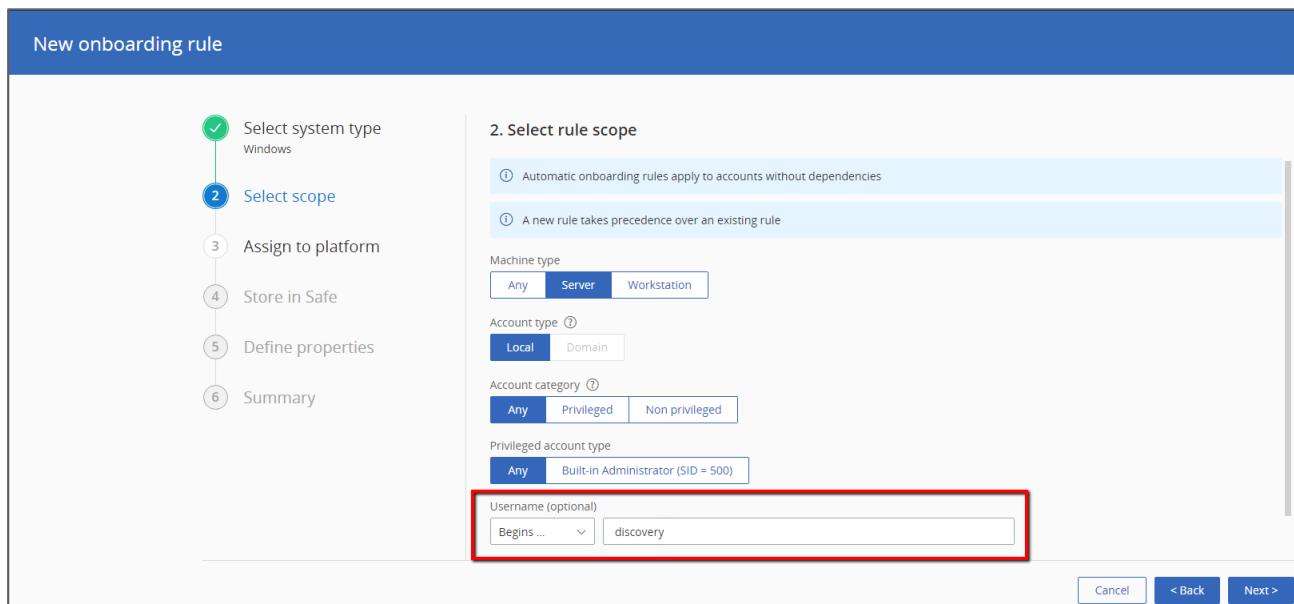
1. Select system type
Windows

2. Select rule scope

Automatic onboarding rules apply to accounts without dependencies
A new rule takes precedence over an existing rule

Machine type: Any Server Workstation
Account type: Local Domain
Account category: Any Privileged Non privileged
Privileged account type: Any Built-in Administrator (SID = 500)
Username (optional): Begins ... discovery

Cancel < Back Next >



5. Click **Next**.

6. In **Assign to platform** select *Windows Server Local Admins 45*.



The screenshot shows the 'New onboarding rule' wizard. Step 3, 'Select platform', is displayed. A list of platforms includes 'Windows Desktop Local Accounts', 'Windows Domain Account', 'Windows Domain Admins 15', 'Windows Server Local Accounts', and 'Windows Server Local Admins 45'. The last item, 'Windows Server Local Admins 45', is highlighted with a red box. On the left, a vertical navigation bar shows steps 1 through 6, with steps 1, 2, and 3 completed (indicated by green checkmarks) and steps 4 through 6 still pending (indicated by blue circles).

7. In **Store in Safe** select *Win-Srv-Fin-US*.
8. In **Define rule properties** enter the following name: *Discovery users*.

The screenshot shows the 'New onboarding rule' wizard at step 6, 'Summary'. The summary details are as follows:

Rule scope	
System type Windows	Account category Any
Machine type Any	Privileged account type Any
Account type Local	Username Begins with: discovery

Destination	
Platform Windows Server Local Admins 45	Safe Win-Srv-Fin-US

Rule properties	

On the left, a vertical navigation bar shows steps 1 through 6, all completed (green checkmarks). At the bottom right, there are buttons for 'Cancel', '< Back', and 'Create rule'.

9. Review your rule and if everything seems to be in order click on **Create rule**.

Configure and Run Windows Accounts Discovery

The Accounts Discovery process requires an account to log in to the domain and scan the individual machines. You can use the existing *cybrscan* account.

1. Go to **Accounts > Pending & Discovery > Discovery Management** and click **New Windows Discovery**.



ACCOUNTS Accounts > Discovery Management
Discovery Management

New Unix Discovery New Windows Discovery

Back to Accounts
Accounts Discovery
Pending Accounts
Discovery Management

To discover accounts, click 'New Windows Discovery' or 'New Unix Discovery'

Introduction to Accounts Discovery Management
This page displays the Accounts Discovery processes that were created in the system. Accounts Discovery processes are listed here including associated details and statuses.
Click 'New Windows Discovery' or 'New Unix Discovery' to easily initiate a new Accounts Discovery process. Accounts identified during a Discovery process will be listed in the Pending Accounts view.

2. Enter *cyber-ark-demo.local* in the **Domain** field.
3. Use the **Click to select an account from the Vault** link and select the *cybrscan* account.

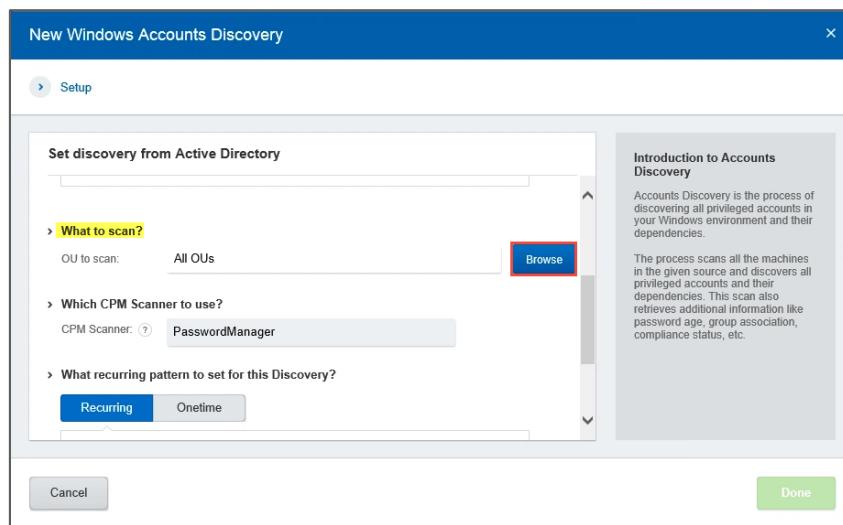
Note: The user **cybrscan** is an Active Directory account created especially for the purposes of running Accounts Discovery scans. It is a member of the Domain Admins AD group.



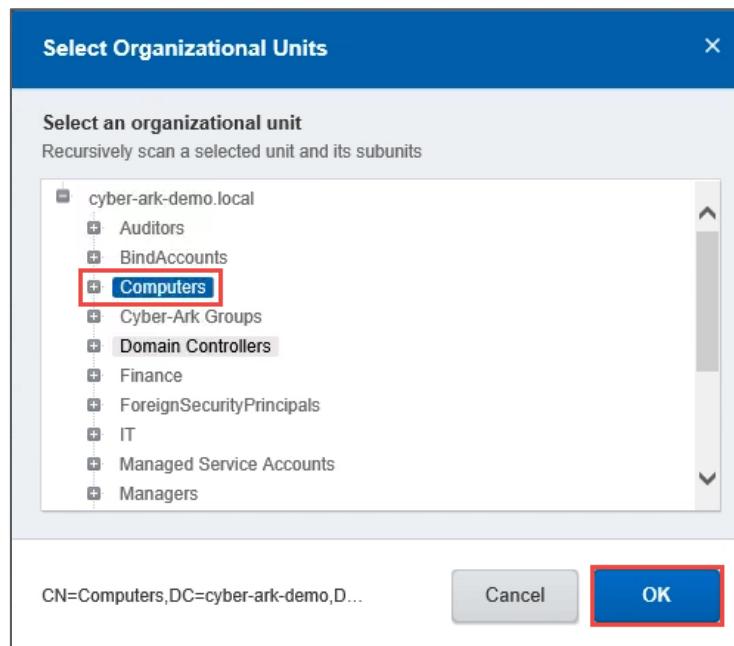
CYBERARK®

CyberArk Privileged Access Security – Administration

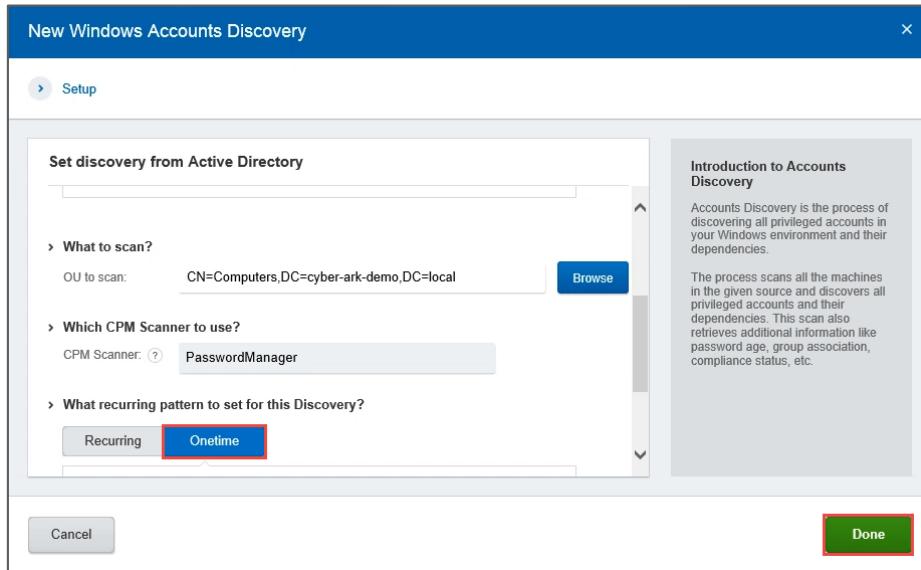
4. In the *What to scan?* section, click **Browse**.



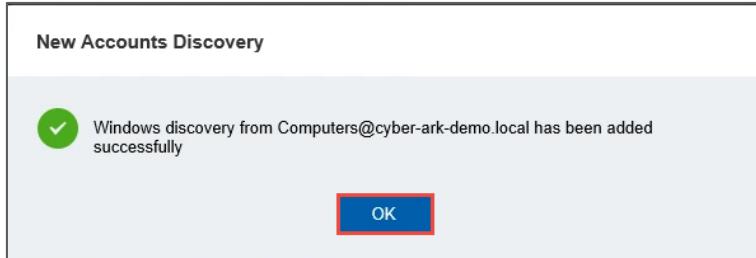
5. Select the *Computers* container and press **OK**.



6. Under **What recurring pattern to set for this Discovery?** Select **Onetime**, then click **Done**.



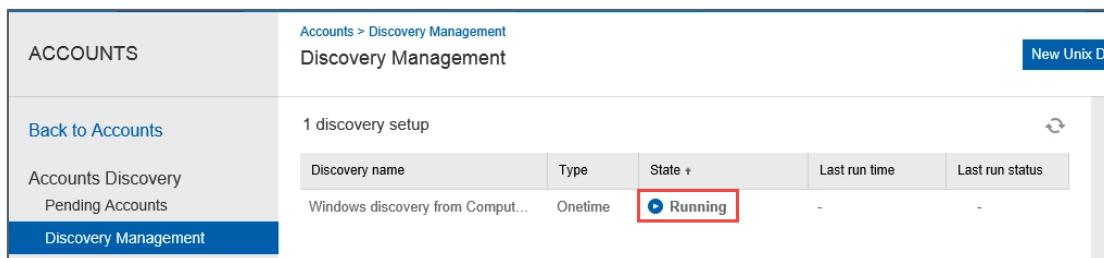
7. You will receive a message saying that the Windows discovery has been added. Press **OK**.



8. Press the **Refresh** icon to update the status. You may need to back out of the window and go back in to see the state change. This can take a few minutes.

ACCOUNTS	Accounts > Discovery Management	New Unix D
Discovery Management		
Back to Accounts	1 discovery setup	
Accounts Discovery	Discovery name	Type
Pending Accounts	Windows discovery from Comput...	Onetime
Discovery Management	State +	Last run time
	(Pending)	-
		-

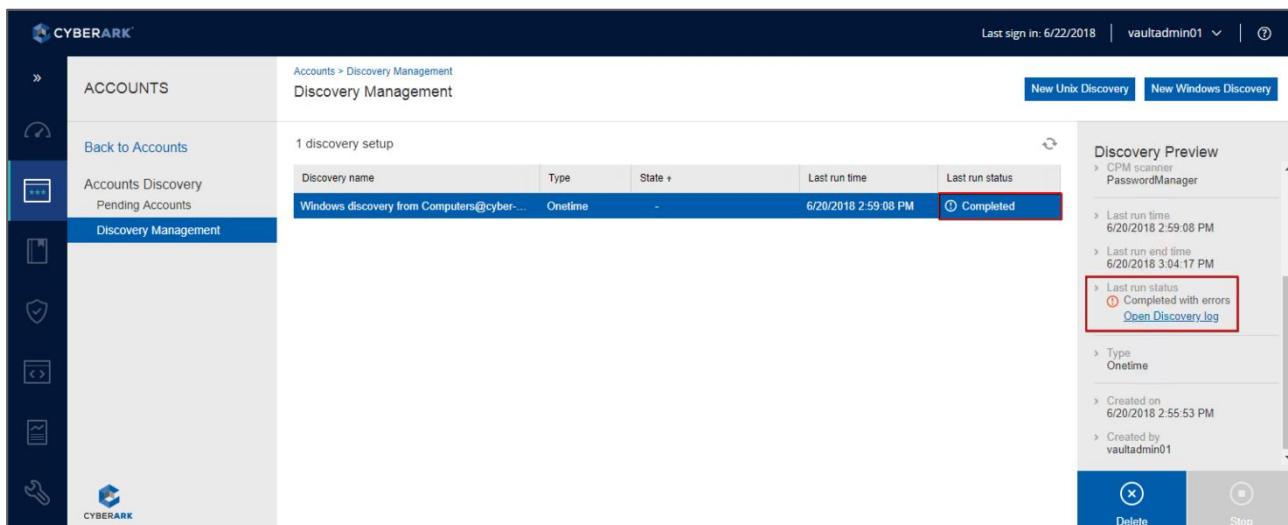
9. You should see the status change from *Pending* to *Running*.



Discovery name	Type	State +	Last run time	Last run status
Windows discovery from Comput...	Onetime	Running	-	-

10. After several minutes, the process should appear as *Completed*.

Note: You will get an error message - Because some of the machines in the lab environment are **not** running (or don't exist at all), the Accounts Discovery will fail to access them and will return an error. However, the machines that we need should be available and successfully scanned.



Discovery name	Type	State +	Last run time	Last run status
Windows discovery from Computers@cyber...	Onetime	Completed	6/20/2018 2:59:08 PM	Completed with errors

Discovery Preview

- > CPM scanner
- > PasswordManager
- > Last run time
6/20/2018 2:59:08 PM
- > Last run end time
6/20/2018 3:04:17 PM
- > Last run status
Completed with errors
[Open Discovery.log](#)
- > Type
Onetime
- > Created on
6/20/2018 2:55:53 PM
- > Created by
vaultadmin01

Verify Automatically Onboarded Accounts

1. Go to **Accounts > Accounts View**. If you configured your automatic rules properly, you should be able to see all the “discoveryXX” accounts in the accounts view. If you assigned a reconcile account to the platform, the accounts added should also be scheduled for immediate reconciliation.



Manually onboard discovered accounts

In this section, we will manually onboard an account that was discovered but for which there was no automatic onboarding rule.

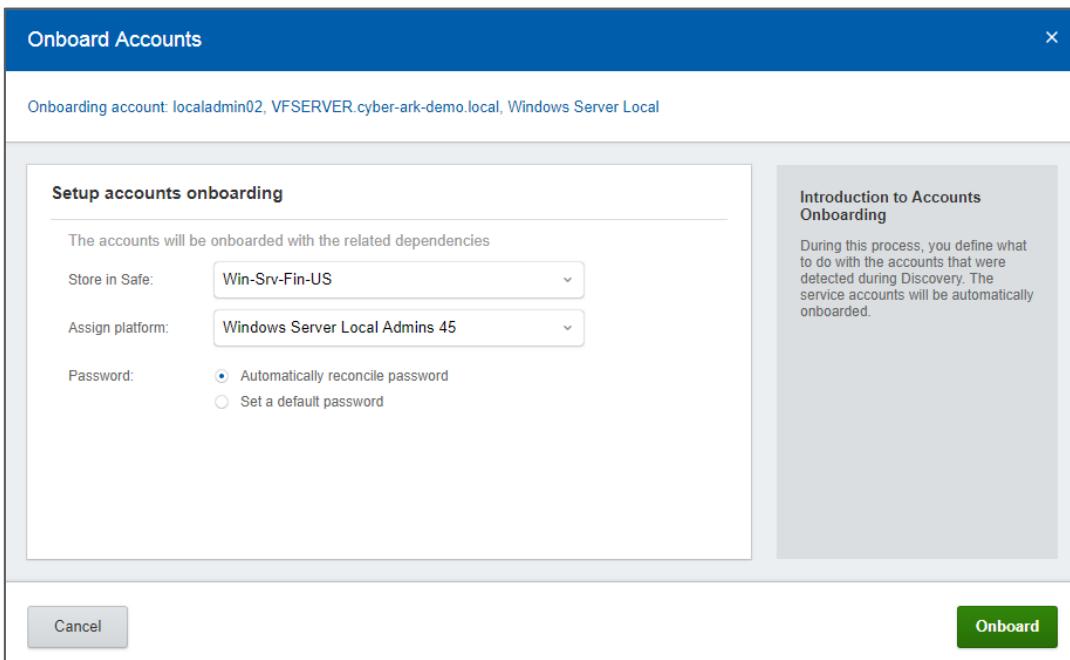
1. Go to the **Pending Accounts** list, enter *localadmin02* in the **Keywords** field and run a search.
2. Select the resulting *localadmin02* account and press the **Onboard Accounts** button

3. In the **Onboard Accounts** window, enter the following:

Store in Safe	<i>Win-Srv-Fin-US</i>
----------------------	-----------------------

Assign platform	<i>Windows Server Local Admins 45</i>
Password	<i>Automatically reconcile password (this will only be available if the assigned platform contains a reconcile account)</i>

4. Press **Onboard**.



The dialog box is titled "Onboard Accounts". It shows the onboarding account as "localadmin02, VFSERVER.cyber-ark-demo.local, Windows Server Local". The main section is titled "Setup accounts onboarding" and contains the following fields:

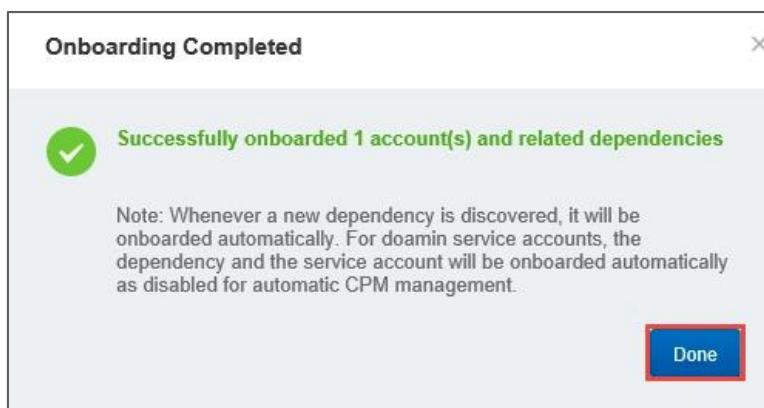
- Store in Safe: Win-Srv-Fin-US
- Assign platform: Windows Server Local Admins 45
- Password: Automatically reconcile password Set a default password

To the right, there is an "Introduction to Accounts Onboarding" panel with the following text:

During this process, you define what to do with the accounts that were detected during Discovery. The service accounts will be automatically onboarded.

At the bottom are "Cancel" and "Onboard" buttons.

5. You should receive a message saying “Successfully onboarded 1 account(s) and related dependencies. Press **Done**.





6. Go to the **ACCOUNTS** page and search (**press the magnifying glass icon top right**) for the newly created account. Because the platform was configured for automatic reconciliation, you will see that the account has been successfully reconciled.

Password Upload Utility

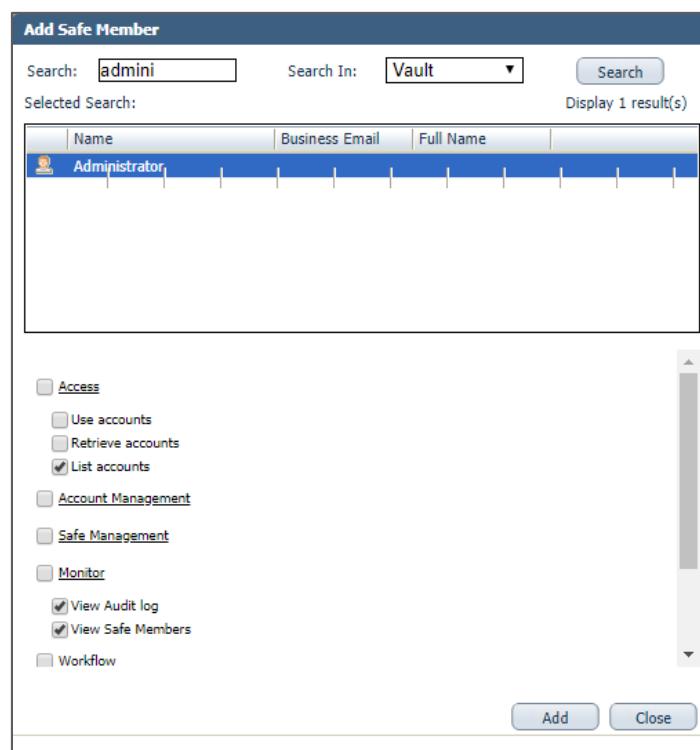
In this exercise, we are going to run the **CyberArk Password Upload Utility** (or PUU for short), a command-line tool for performing bulk uploads of accounts into the system. For convenience, we will run the **Password Upload Utility** using the CyberArk *administrator* account.

We will be adding the new accounts to a new Safe that we create with the PUU – **LinuxPU**.

The *administrator* does not have any custom safe authorizations and so cannot even see the safes that we have created so far. We want to use our existing **Linux Finance** safe as a *template safe* (basically a standard safe that provides parameters not given during the execution of the PUU), so we just need to add the *administrator* to the **Linux Finance** safe as a member before starting the Password Upload Utility process.

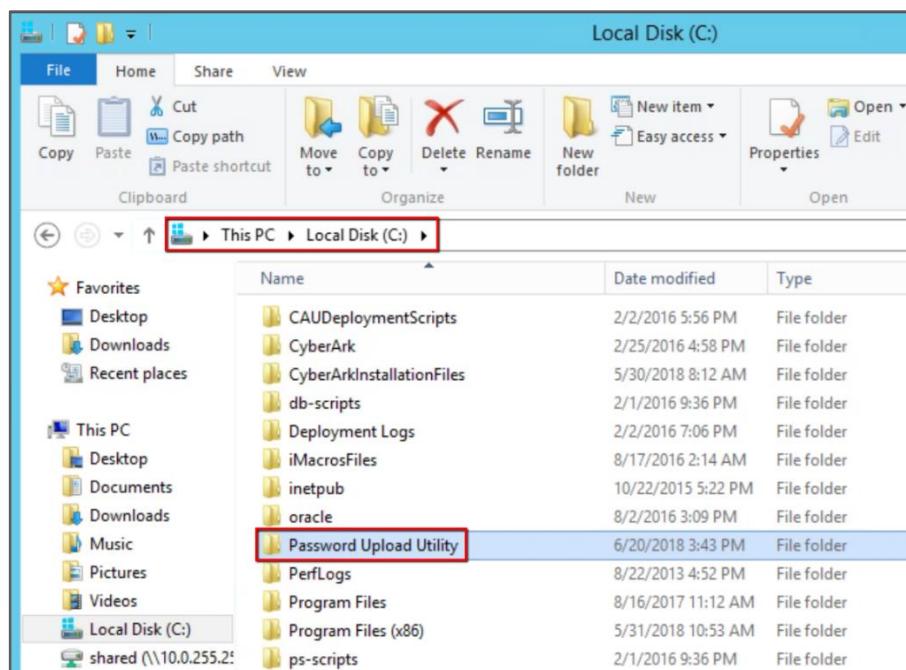
Add the Administrator as a member of template safe

1. Login to the **PVWA** via LDAP as *vaultadmin01*.
2. Go to **POLICIES > Access Control (Safes)**.
3. Select *Linux Finance* and click the **Members** button.
4. Click **Add Member**.
5. Enter *admin* in the search field, **leave Vault** as the option for **Search In**, and press the **Search** button. If you search in *cyber-ark-demo*, you will also find an *Administrator* account. **That account will not work.**
6. Select **Administrator (NOT Administrators)**, uncheck the options for *Use accounts* and *Retrieve accounts*, click **Add**, and then **Close**.

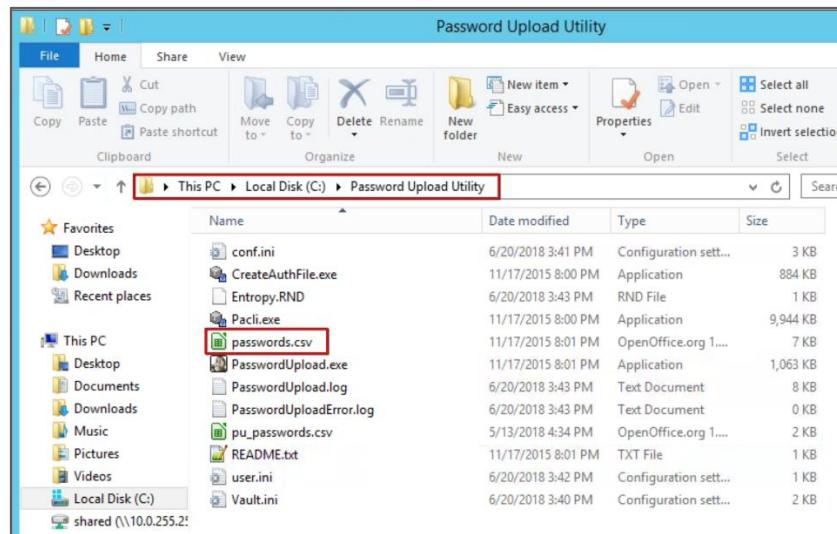


Configure and run PUU

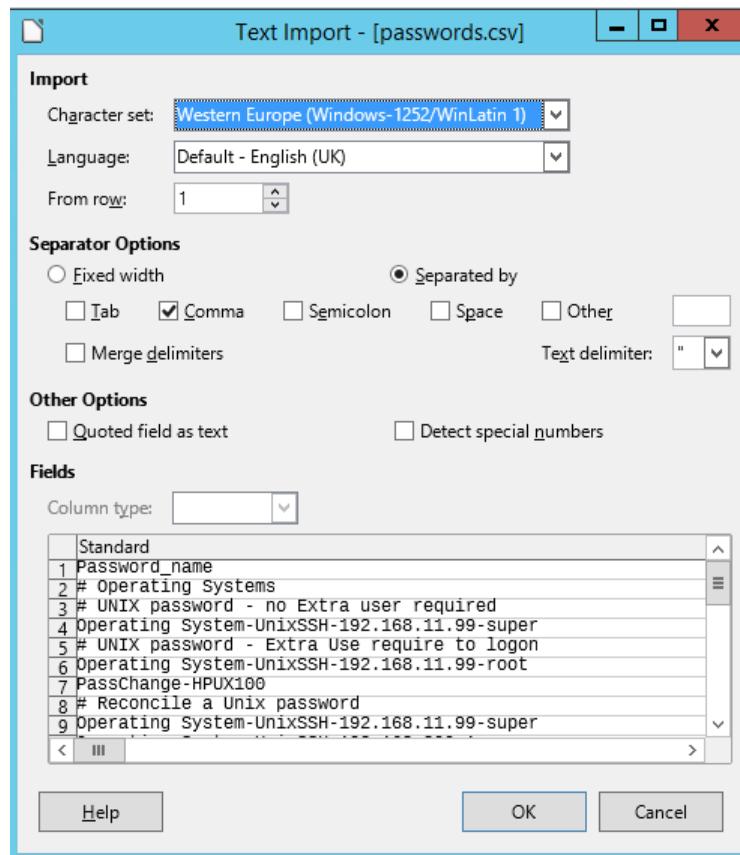
1. Go to the C:\Password Upload Utility directory.



2. First let's look at the sample file provided with the PUU. Double-click the **passwords.csv** file.



3. On the *Text Import* screen make sure that the file is only *Separated by...Comma*.
4. Press **OK**.

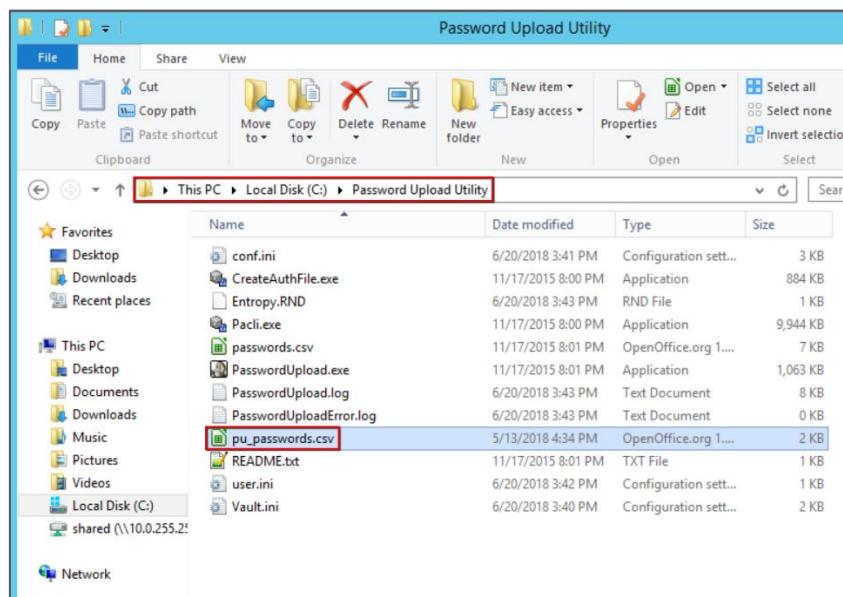


5. Review the contents of this file to see the options available for uploading accounts.



	A	
1	Password_name	Template
2	# Operating Systems	
3	# UNIX password - no Extra user required	
4	Operating System-UnixSSH-192.168.11.99-super	Unix Pas
5	# UNIX password - Extra Use require to logon	
6	Operating System-UnixSSH-192.168.11.99-root	
7	PassChange-HPUX100	
8	# Reconcile a Unix password	
9	Operating System-UnixSSH-192.168.11.99-super	
10	Operating System-UnixSSH-192.168.200.1-super	
11	# Reconcile a Unix password where the target & reconcile accounts require an extra password object to log on	
12	Operating System-UnixSSH-192.168.11.99-super	
13	Operating System-UnixSSH-192.168.200.1-super	
14	Operating System-192.168.200.1-UnixSSH-LoginUser	
15	# Verify a Unix password now	
16	Operating System-UnixSSH-192.168.11.99-super	
17	# Change a Unix password now	
18	Operating System-UnixSSH-192.168.11.99-super	

6. Close the file when you are done (we will use a preformatted file to perform the actual import).
7. In the same folder, double-click the **pu_passwords** file.



8. Make sure that the file is Separated by...Comma and press **OK**.



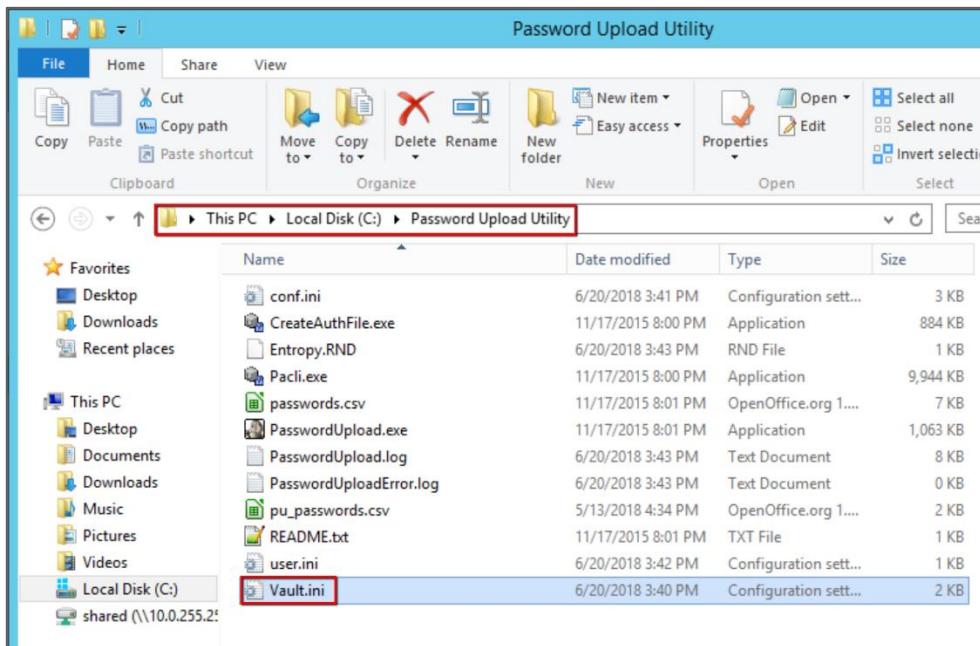
	A	B	C	D	E	F	G	H	I	J	K
1	Password_name	TemplateSafe	CPMUser	Safe	Folder	Password	DeviceType	PolicyID	Address	UserName	
2	Operating System-LinuxviaSSH30-10.0.0.20-logon21	Linux Finance	PasswordManager	LinuxPU	Root	Cyberark1	Operating System	LinuxviaSSH30	10.0.0.20	logon21	
3	Operating System-LinuxviaSSH30-10.0.0.20-logon22	Linux Finance	PasswordManager	LinuxPU	Root	Cyberark1	Operating System	LinuxviaSSH30	10.0.0.20	logon22	
4	Operating System-LinuxviaSSH30-10.0.0.20-logon23	Linux Finance	PasswordManager	LinuxPU	Root	Cyberark1	Operating System	LinuxviaSSH30	10.0.0.20	logon23	
5	Operating System-LinuxviaSSH30-10.0.0.20-logon24	Linux Finance	PasswordManager	LinuxPU	Root	Cyberark1	Operating System	LinuxviaSSH30	10.0.0.20	logon24	
6	Operating System-LinuxviaSSH30-10.0.0.20-logon25	Linux Finance	PasswordManager	LinuxPU	Root	Cyberark1	Operating System	LinuxviaSSH30	10.0.0.20	logon25	
7	Operating System-LinuxviaSSH30-10.0.0.20-logon26	Linux Finance	PasswordManager	LinuxPU	Root	Cyberark1	Operating System	LinuxviaSSH30	10.0.0.20	logon26	
8	Operating System-LinuxviaSSH30-10.0.0.20-logon27	Linux Finance	PasswordManager	LinuxPU	Root	Cyberark1	Operating System	LinuxviaSSH30	10.0.0.20	logon27	
9	Operating System-LinuxviaSSH30-10.0.0.20-logon28	Linux Finance	PasswordManager	LinuxPU	Root	Cyberark1	Operating System	LinuxviaSSH30	10.0.0.20	logon28	
10	Operating System-LinuxviaSSH30-10.0.0.20-logon29	Linux Finance	PasswordManager	LinuxPU	Root	Cyberark1	Operating System	LinuxviaSSH30	10.0.0.20	logon29	
11	Operating System-LinuxviaSSH30-10.0.0.20-logon30	Linux Finance	PasswordManager	LinuxPU	Root	Cyberark1	Operating System	LinuxviaSSH30	10.0.0.20	logon30	
12											
13											
14											
15											
16											
17											
18											
19											
20											
21											

Note: This is a pre-formatted file with all the necessary information to upload into CyberArk.

- If you would like to experiment, you can add a line or two to the file. Adding the information below would add a single new account in a separate Safe named **LinuxPU2**.

Password_name:	<i>linuxadmin01</i>
TemplateSafe:	<i>Linux Finance</i>
Folder:	<i>Root</i>
CPMUser:	<i>PasswordManager</i>
Safe:	<i>LinuxPU2</i>
Password:	<i>Cyberark1</i>
DeviceType:	<i>Operating System</i>
PolicyID:	<i>LinuxviaSSH30</i>
Address:	<i>10.0.0.20</i>
UserName:	<i>linuxadmin01</i>

- Save and close the file when done. **Be sure to maintain the same CSV format.**
- Double-click the *Vault.ini* file

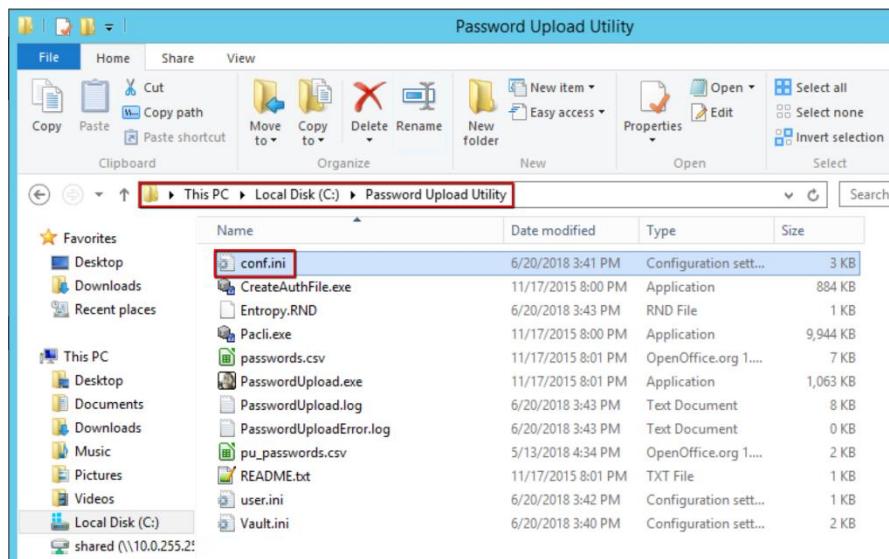


12. In the **address** field, enter the **IP address** your vault server (make sure you use the IP address of **your Vault Server**).

```
VAULT = "My Vault".
ADDRESS=10.0.10.1
PORT=1858
#-----
# Additional parameters (optional)
#-----
```

13. Save and close the file.

14. Double-click the *conf.ini* file.





15. Scroll down to **bottom** of the file to the second *Mandatory parameters* section, enter the following:

PasswordFile:	<i>pu_passwords.csv</i>
DefaultTemplateSafe:	<i>Linux Finance</i>

16. Open a command prompt. Change directories to *c:\Password Upload Utility*.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd "c:\Password Upload Utility"
```

17. Enter **dir** to display the contents of the folder.

```
c:\Password Upload Utility>dir
Volume in drive C has no label.
Volume Serial Number is F023-6DFF

Directory of c:\Password Upload Utility

02/01/2013 11:04 AM <DIR> .
02/01/2013 11:04 AM <DIR> ..
02/01/2013 11:16 AM 2,798 conf.ini
10/25/2012 04:01 PM 905,216 CreateAuthFile.exe
10/25/2012 04:01 PM 10,182,656 Pacli.exe
10/25/2012 04:01 PM 6,846 passwords.csv
10/25/2012 04:01 PM 1,088,378 PasswordUpload.exe
02/01/2013 11:04 AM 2,348 pu_passwords.csv
10/25/2012 04:02 PM 504 README.txt
02/01/2013 11:12 AM 2,049 Vault.ini
               8 File(s)    12,190,795 bytes
               2 Dir(s)   7,044,616,192 bytes free
```

18. Run the following:

```
C:\Password Upload Utility> CreateAuthFile.exe user.ini
Enter CyberArk Vault username [None]: administrator
Enter CyberArk Vault password : Cyberark1
```

```
c:\Password Upload Utility>CreateAuthFile.exe user.ini
Enter CyberArk Vault username [None]:administrator
Enter CyberArk Vault password :*****
Credentials file has been created/updated successfully.

c:\Password Upload Utility>
```

19. Run the following command:

```
 PasswordUpload.exe conf.ini
```

```
c:\Password Upload Utility>PasswordUpload.exe conf.ini
```



20. If configured correctly, you will see messages indicating that each password is being stored.

21. When complete, you will receive a message displaying the total number of passwords uploaded or updated.

```
Updating property: "username" Value: "TrainingUser01"
Adding CPM user: "PasswordManager" as owner to Safe: "Training"
Sharing Safe: "Training" with GW account(s): PWAGWUser
=====
Total password objects in file: 22
Total password objects loaded/updated: 22
=====
Password Upload Utility ended: 01/02/2013 11:46:20 with 0 errors
c:\Password Upload Utility>
```

22. Log in to the **PWAA** as **Administrator** using CyberArk authentication.

23. Go to the **ACCOUNTS** view and search for all accounts to verify that the new users have been added.

The screenshot shows the CyberArk PWAA interface. On the left, there's a sidebar with various icons and a navigation tree. The main area is titled 'ACCOUNTS' and shows a table of accounts. The table has columns for Username, Address, Safe, Platform ID, and several action icons. A red box highlights the 'Username' column header. The table data is as follows:

Username	Address	Safe	Platform ID
logon01	10.0.0.20	Linux Finance	LinuxSSH30
logon21	10.0.0.20	LinuxPU	LinuxviaSSH30
logon22	10.0.0.20	LinuxPU	LinuxviaSSH30
logon23	10.0.0.20	LinuxPU	LinuxviaSSH30
logon24	10.0.0.20	LinuxPU	LinuxviaSSH30
logon25	10.0.0.20	LinuxPU	LinuxviaSSH30
logon26	10.0.0.20	LinuxPU	LinuxviaSSH30
logon27	10.0.0.20	LinuxPU	LinuxviaSSH30
logon28	10.0.0.20	LinuxPU	LinuxviaSSH30
logon29	10.0.0.20	LinuxPU	LinuxviaSSH30
logon30	10.0.0.20	LinuxPU	LinuxviaSSH30
root01	10.0.0.20	Linux Finance	LinuxviaKEY90
root02	centos-target01	Linux Finance	LinuxSSH30
user01	10.0.0.20	Linux Finance	LinuxSSH30

24. Sign out of the **PWAA** session.



Privileged Session Management

In this section, we will perform a number of tests to see the various privileged session management options that are available with CyberArk Core PAS.

First, we will disable the **PSM** globally and then activate it for specific platforms using exceptions.

We will then perform a number tests to ensure that privileged session management is functioning properly using the various connection methods available:

- Privileged Session Manager (PSM)
- Privileged Session Manager for SSH (PSM for SSH)
- Privileged Session Manager for Windows (PSM for Windows)

Privileged Session Manager

This method allows users to connect securely via the PSM to all types of systems and applications through the unified PVWA web portal user interface

Enabling PSM

The **PSM** is enabled through the **Master Policy**. PSM can be enabled either globally for all platforms or disabled globally and only activated through exceptions, which is what we will test here.

If your PSM is *Active*, switch it to *Inactive* before performing this exercise.

1. Login to the **PVWA** as **vaultadmin01** using LDAP authentication.
2. Go to **POLICIES > Master Policy**.
3. In the **Session Management** section, highlight *Require privileged session monitoring and isolation* and deactivate it.
4. Once deactivated, with *Require privileged session monitoring and isolation* still selected, press **Add Exception**.

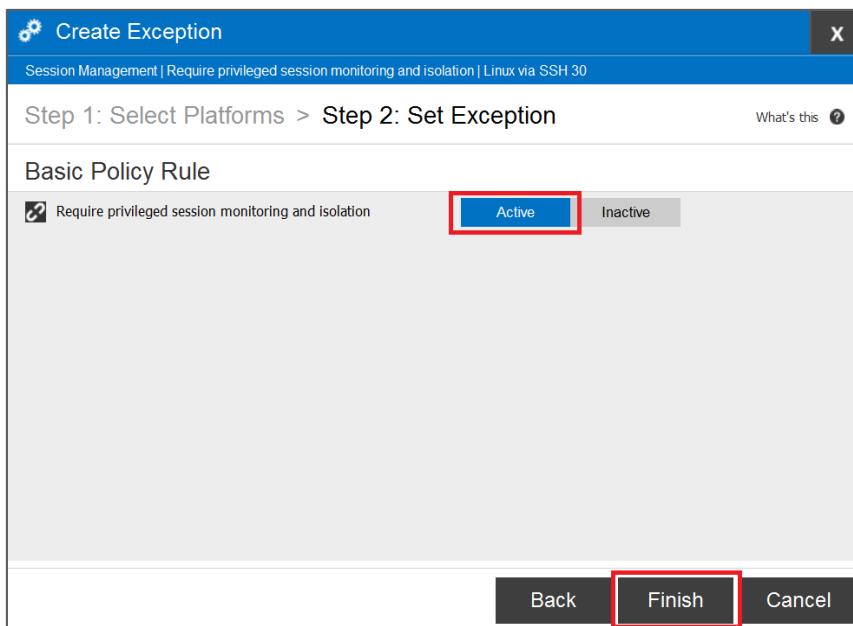


The screenshot shows the CyberArk Admin interface with the 'Master Policy' selected. The 'Session Management' section is expanded, displaying two policy rules: 'Require dual control password access approval' and 'Require privileged session monitoring and isolation'. The second rule is highlighted with a red box. The 'Exceptions' column for this rule shows three entries: 'Inactive' (value 1), 'Inactive' (value 1), and 'Active' (value 3). On the right side, there are sections for 'Rule Preview' (showing 'Require privileged session monitoring...'), 'ADVANCED SETTINGS' (set to 'None'), and 'EXCEPTIONS (3)' (with a red box around it). At the bottom right, there are 'Edit Settings' and 'Add Exception' buttons.

5. Select **Linux via SSH 30** and press **Next**.

The screenshot shows the 'Create Exception' dialog box. It has two steps: 'Step 1: Select Platforms' and 'Step 2: Set Exception'. The 'Select Platforms' step is active, showing a table of platforms. The platform 'Linux via SSH 30' is selected and highlighted with a red box. The table columns are 'Name', 'Device Type', and 'Status'. Other platforms listed include 'Linux via KEY 90', 'Oracle DBA 30', 'Windows Domain Admins 15', 'Windows Server Local Admins 45', '[Sample Password Group Platform]', '[Sample SSH Key Group Platform]', 'Amazon Web Services - AWS', 'Amazon Web Services - AWS - Access Keys', 'AS400', 'BMC Remedy', 'Check Point FireWall-1', 'Check Point GAIa via SSH', 'Cisco Pix via SSH', 'Cisco Pix via Telnet', 'Cisco router via SSH', and 'Cisco router via Telnet'. The 'Status' column shows various values like 'Active' and 'Inactive'. At the bottom of the table are 'Back', 'Next', and 'Cancel' buttons. A red arrow points from the text 'Step 2: Set Exception' to the 'Next' button.

6. Press the **Active** button and press **Finish**.



Now, add an exception for the *Oracle DBA 30* platform.

7. Press **Add Exception** again. Select *Oracle DBA 30* and press **Next**.
8. Select **Active** and press **Finish**.

Note: Prior to testing **PSM**, you can choose to wait approximately 20 minutes for all components to refresh their configurations or you can restart all the **CyberArk** services so that the **PSM** and **PVWA** will see all the configuration changes immediately.

9. Sign out of the **PVWA**, and double-click the *restart-services* batch file on the desktop of the components server.

Connect with a Linux Account

We will first test securely connecting to a Linux machine using SSH via the PSM. In this exercise, you will connect to the PSM using RDP, and the PSM will run PutTTy to connect you to the target Linux machine

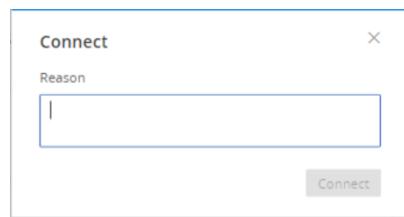
1. After restarting the services, login as *vaultadmin01*.
2. Go to the **ACCOUNTS** page and locate *user01*. Press the **Connect** button.



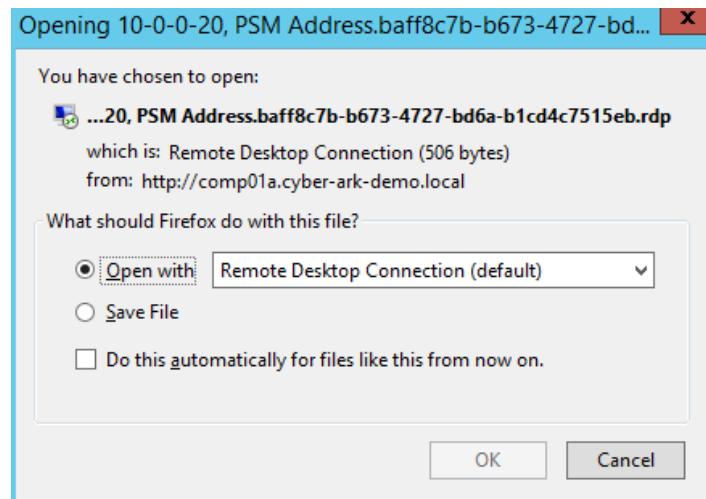
The screenshot shows the CyberArk Accounts interface. A search bar at the top contains 'user01'. Below it, there are sections for 'Status' and 'Operational state'. A table lists one result for 'user01' with columns: Username, Address, Platform ID, Safe ↑, Status, and Access Request. The 'Access Request' column for this user has a red box around the 'Connect' button.

Note: You should be prompted to enter a reason for the connection.

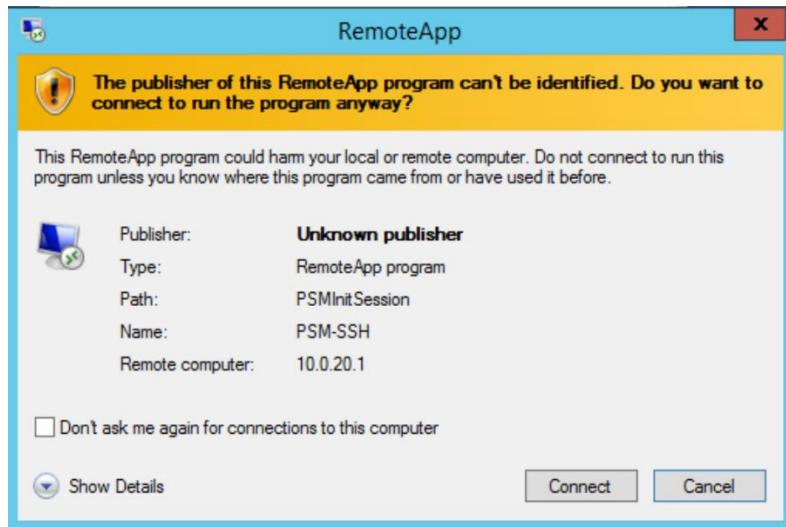
3. If you are, enter something in the box provided.



4. After pressing **OK**, you will notice an RDP file has been downloaded to your desktop. Choose to open it with *Remote Desktop Connection (default)* and press **OK**.



5. At the **Remote Desktop Connection** window, press the **Connect** button



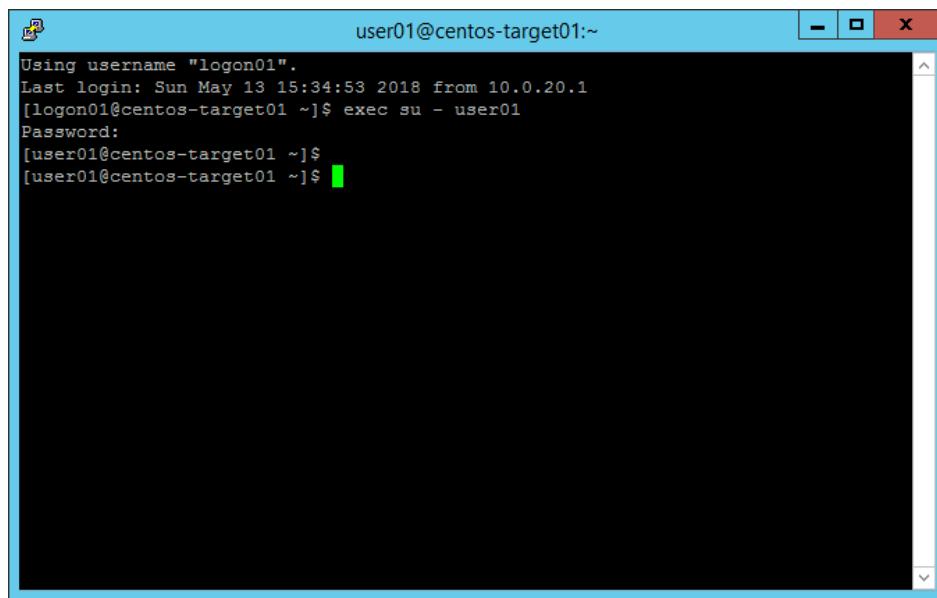
You may receive the following pop-up error messages. Clear the pop-ups and retry the connection component.



If everything was configured correctly, you should see a message that your session is being recorded.



6. Press **Yes** to accept the host key.



```
user01@centos-target01:~$ Using username "logon01".
Last login: Sun May 13 15:34:53 2018 from 10.0.20.1
[logon01@centos-target01 ~]$ exec su - user01
Password:
[user01@centos-target01 ~]$ [user01@centos-target01 ~]$ 
```

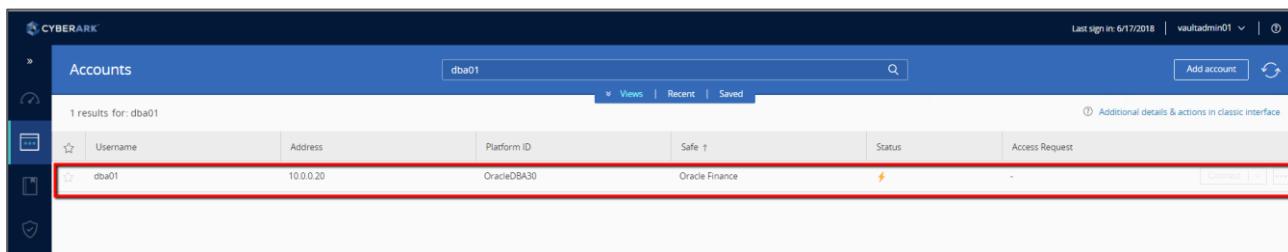
Optionally, run some Linux commands. In the example below the user is running:

```
cat /var/log/messages
mkdir user16
rm -R user16
```

7. Type **Exit** to end this session.

Connect with an Oracle Account

1. Press the **Back** button to return to the main **Accounts** window.
2. At the **ACCOUNTS** page, select *dba01*.



Username	Address	Platform ID	Status	Access Request
dba01	10.0.0.20	OracleDBA30	Oracle Finance	-

3. Press the **Connect** button.

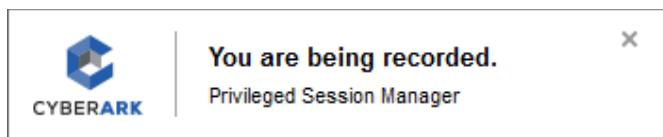


The screenshot shows the CyberArk Privileged Access Security interface. At the top, it displays 'dba01 On 10.0.0.20', 'Platform: Oracle DBA 30', and 'Safe: Oracle Finance'. Below this, there are four tabs: 'Overview' (which is selected), 'Details', 'Activities', and 'Versions'. In the top right corner, there are buttons for 'Show', 'Copy', '...', and 'Connect' (which is highlighted with a red box). The main area is divided into three sections: 'Compliance Status' (Compliant, 3 days ago, last changed by PasswordManager Jun 13, 2018 11:20 PM, with 'Reconcile' and 'Change' buttons), 'Activities (Last 5)' (listing vaultadmin01's PSM Disconnect, SQL Command, and multiple SQL Commands from Jun 14 at various times), and 'Last Access' (by vaultadmin01 on Jun 14, 2018 12:43 AM).

4. On the **Remote Desktop Connection** window, press **Connect**.
5. You should see a message stating that your session is being recorded.

If you receive a Remote Desktop Connect pop-up, “Your Remote Desktop Services session has ended”, retry the connection component. You may have to connect a couple of times before seeing the message.

Note: You may see an additional prompt.



Later in the lab exercise, you will be logging in as an auditor and looking for any sessions that issued commands with the word salary.

Note: The commands below will not produce any results because the table “scott.salary”, does not exist. The purpose of this step is to allow the auditor to see someone tried to access a salary table.

6. Run the following commands:

```
select * from dual;
create table psm01 (id01 int, psm01 varchar(40));
select * from scott.salary;
```



```
update scott.salary set salary ='1,000,000' where id01 =1;
```

7. Type **exit** to end the session.

Connect via HTML5 Gateway

In this exercise you will configure the PSM to provide secure remote access to a target machine through an HTML5 gateway. The HTML5 gateway tunnels the session between the end user and the PSM proxy machine using a secure WebSocket protocol (port 443). This eliminates the requirements to open an RDP connection from the end user's machine. Instead, the end user only requires a web browser to establish a connection to a remote machine through PSM.

Note: in this environment the HTML5 Gateway has already been installed for you. The HTML5GW is installed on the same Linux machine as the PSM for SSH.

1. First, login to the **PWVA** as **vaultadmin01**, go to **ADMINISTRATION > Configuration Options > Options**
2. Next, go to **Privileged Session Management > Configured PSM Servers > PSMServer > Connection Details > PSM Gateway**
3. Set the *Enable* parameter to Yes and click **OK**.

Name	Value
ID	PSMGW
Enable	Yes

4. Go back to the **ACCOUNTS** page and locate **user01**. Press the **Connect** button. This time, instead of downloading an RDP file, you should be able to see the secure connection being established in a new tab in the Chrome browser.



IF you can't connect but instead see a white screen, connect to the PSMP/PSMGW VM in your environment. Run **service tomcat stop and then service tomcat start.** To manually startup the service.

Note: Press **Yes** to accept the host's RSA key if asked

```
Using username "logon01".
Last login: Tue Dec  4 13:34:08 2018 from comp01a.cyber-ark-demo.local
[logon01@centos-target01 ~] $ exec su - user01
Password:
[user01@centos-target01 ~] $
[user01@centos-target01 ~] $ 
```

5. You may leave the HTML5 GW enabled or disable it in order to return to the previous method of downloading an RDP file.

Connect using PSM Ad-Hoc Connection

Next, you will configure a **PSM Ad-Hoc Connection** (previously known as Secure Connect), which allows you to launch a **PSM** connection using unmanaged accounts.

1. First, logged into the **PWVA** as *vaultadmin01*, go to **ADMINISTRATION > Platform Management**.
2. Select *PSM Secure Connect* and activate it.
3. Go to **POLICIES > Master Policy**.
4. In the *Session Management* section, select *Require privileged session monitoring* and press **Add Exception**.
5. Select *PSM Secure Connect* and press **Next**.
6. Select *Active* and press **Finish**.
7. Go to the **ACCOUNTS** page and click on **Ad-Hoc connection**.



CYBERARK®

CyberArk Privileged Access Security – Administration

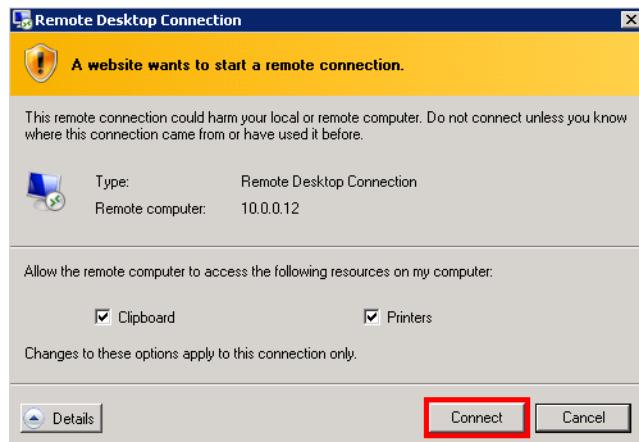
The screenshot shows the CyberArk Accounts View interface. At the top, there's a search bar labeled "Search for accounts" and several navigation buttons: "Views", "Recent", "Saved", "Ad-Hoc connection" (which is highlighted with a red box), "Add account", and a refresh icon. Below this, there's a section titled "My accounts" with categories like "All accounts (default)", "Recently used", "Favorites", and "Checked-out". To the right of these categories are columns for "Status" and "Operational state". A table below lists 71 results for "All accounts", including columns for "Status", "Username", "Address", "Platform ID", "Safe", "Access Request", and "Actions" (with "Connect" and "More" buttons). A note at the bottom right says "Additional details & actions in classic interface".

8. Enter the following:

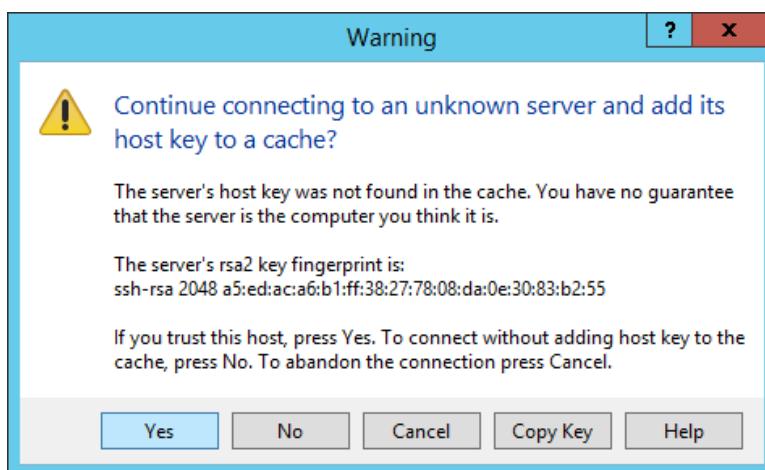
Client:	WinSCP
Address:	10.0.0.20
User Name:	root01
Password:	Cyberark1
Map Local Drives:	Checked (scroll down)

9. Press Connect.

The dialog box is titled "Ad-Hoc connection". It contains fields for "Client" (set to "PSMSecureConnect"), "Address" (set to "10.0.0.20"), "Username" (set to "root01"), and "Password" (represented by a series of asterisks). At the bottom are "Cancel" and "Connect" buttons.

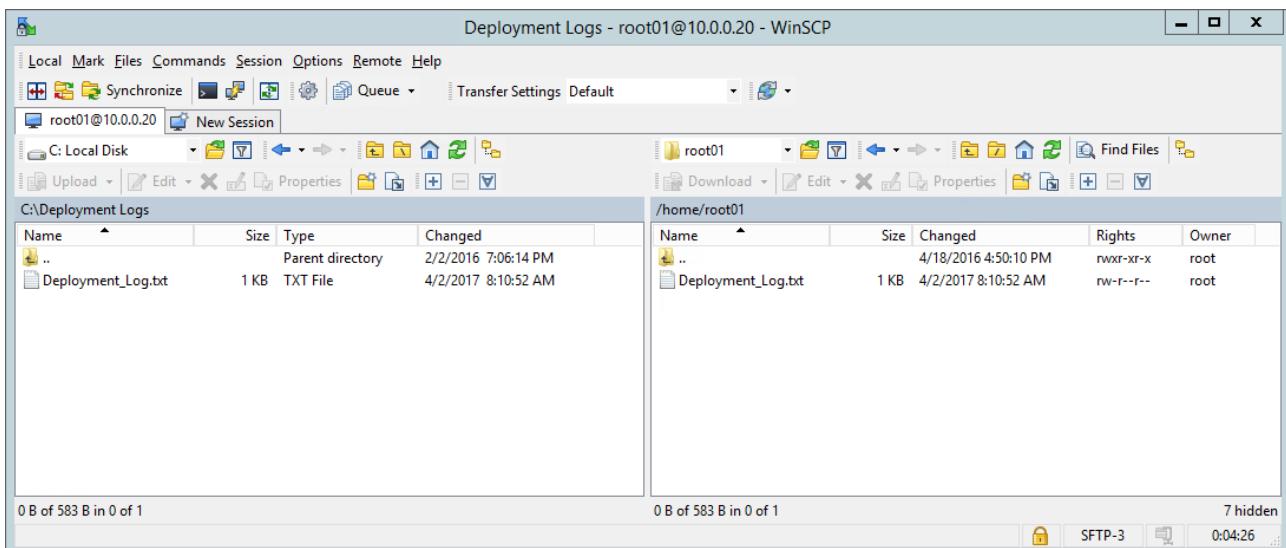


10. Press **Yes** to accept the host's RSA key if asked.



11. **Optional:** When you have connected to WinSCP, copy a file from the PSM server to target machine the local client.

Suggestion: C:\Deployment Logs\Deployment_Logs.txt.



12. Press **F10** to exit and quit the application.

Privileged Session Manager for Windows

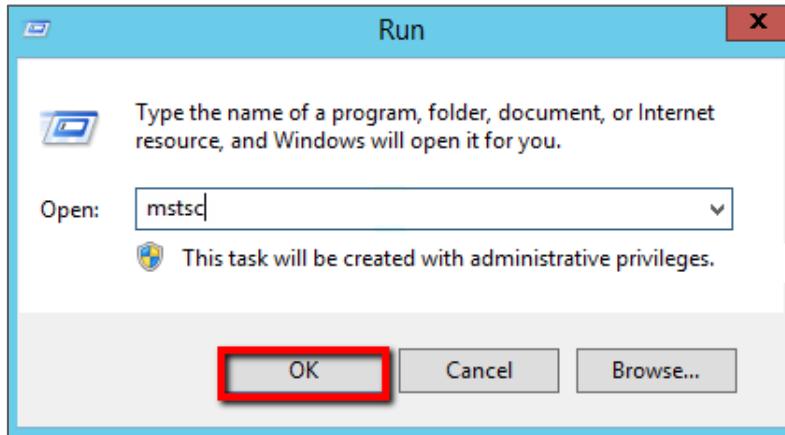
PSM for Windows (previously known as “RDP Proxy”) enables users to connect through PSM to any remote target securely with a standard remote desktop client application like mstsc or a connection manager.

Note: Prior to testing PSM for Windows make sure the PSM is enabled in the Master Policy for all the relevant platforms you test.

Make sure “Require users to specify reason” is disabled for all relevant platforms you test.

Make sure “Require dual control password access approval” is disabled for all platforms you test.

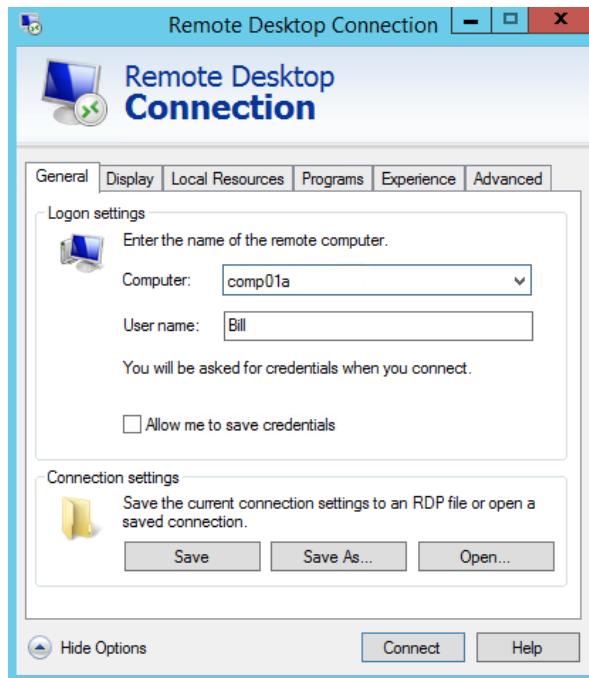
1. First, use run to launch mstsc.exe





2. Click on *Show Options* and specify the following under *General*

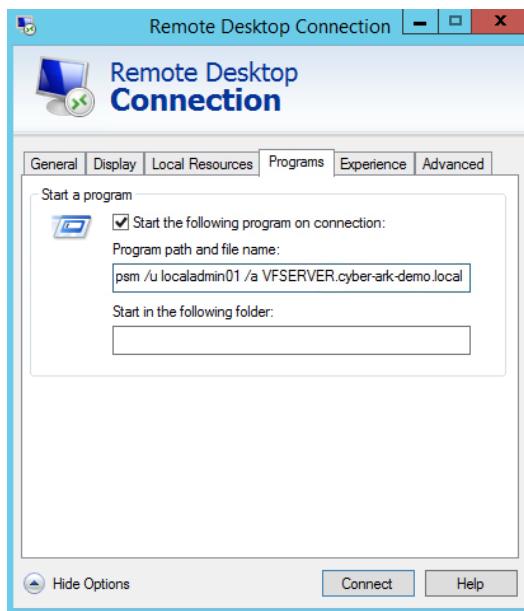
Computer:	Comp01a
User name:	Bill



3. Next, go to Programs and specify the following command:

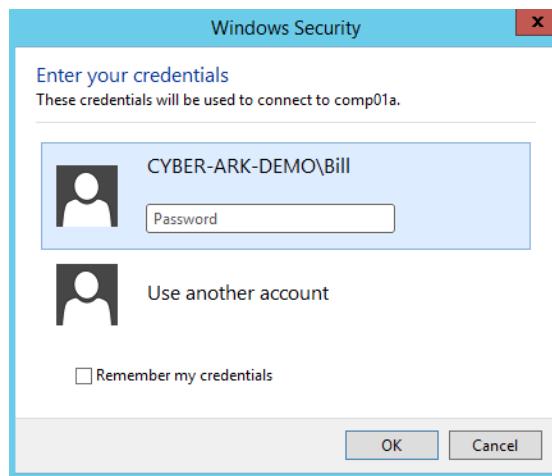
```
psm /u localadmin01 /a VFSERVER.cyber-ark-demo.local /c PSM-RDP
```

Note: the above command instructs the PSM to launch an RDP connection to the VFSERVER target machine, using the localadmin01 account.

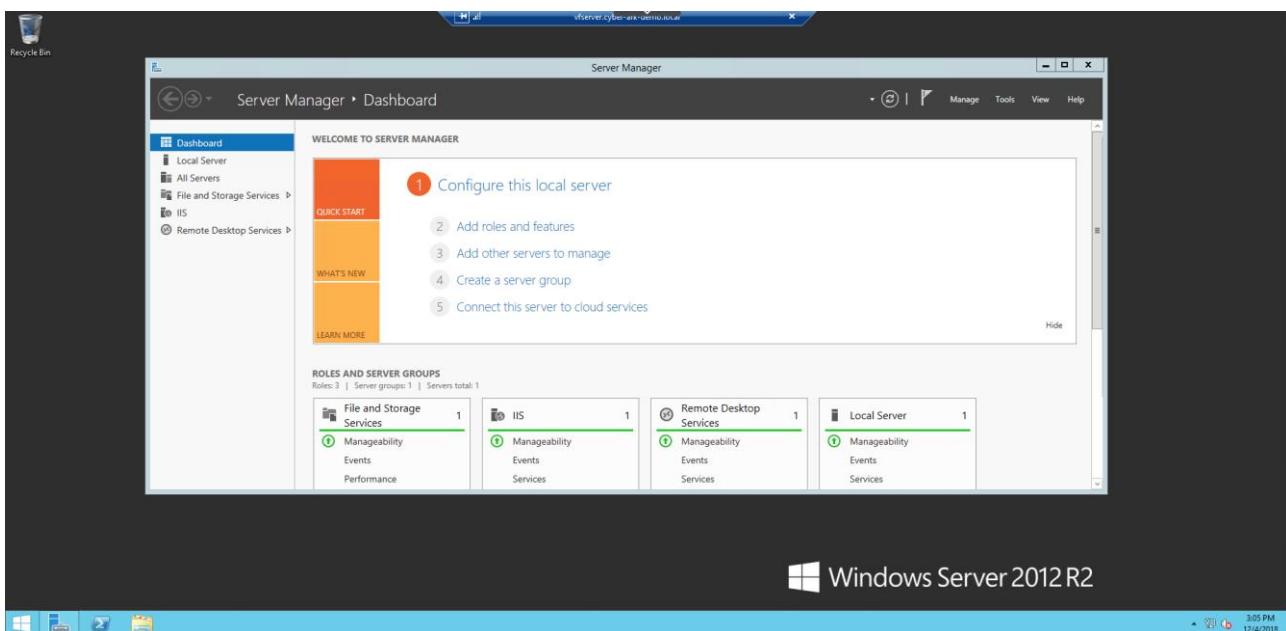


Make sure the platform associated with the localadmin01 account (*Windows Server Local Admins 45*) has an exception added in the Master Policy for Require privileged session monitoring.

4. When prompted, authenticate as Bill (password is Cyberark1).



5. If everything was configured correctly, you should be able to see a secure RDP connection established to the target Windows Machine where you are logged in as localadmin01.



Privileged Session Manager for SSH

PSM for SSH (previously known as PSM SSH Proxy or PSMP) is designed to provide a native Unix/Linux user experience, connecting to any SSH target.

- Note:** in this environment the PSM for SSH has already been installed for you. The PSM for SSH is installed on the same Linux machine as the HTML5 Gateway
- Note:** Prior to testing PSM for SSH make sure “Require dual control password access approval” is disabled for all platforms you test.

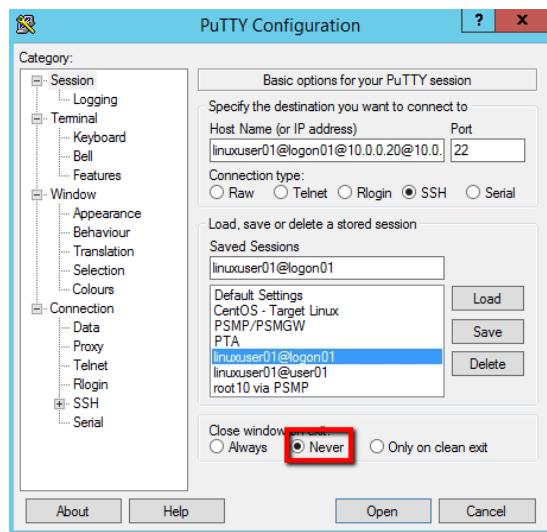
1. On the Components server, open PuTTY. You can find a shortcut for PuTTY in the task bar.



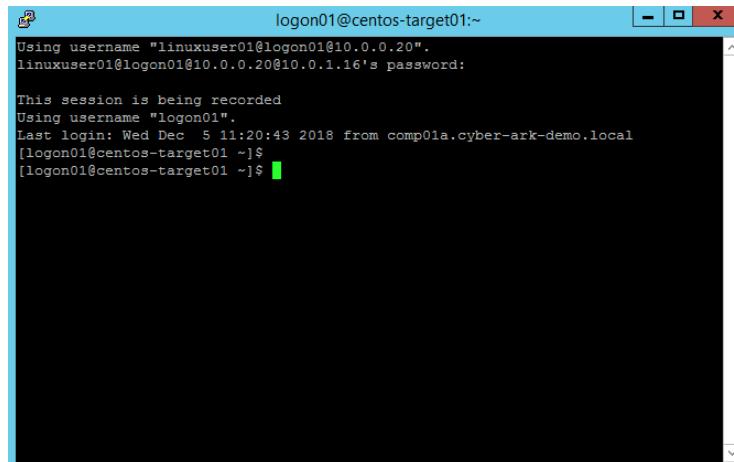
2. Use the following connection string to connect to the Target Linux machine using the *logon01* account where the Vault user is *linuxuser01*.

```
linuxuser01@logon01@10.0.0.20@10.0.1.16
```

Hint: to be able troubleshoot easily, make sure you mark “Never” under “Close window on exit”



- When prompted for a password, enter the password for *linuxuser01* (password: *Cyberark1*)



Auditing user activity in the PSM (Monitoring)

In this section, we are going to look at some of the audit information that was gathered by **CyberArk PAS** during our **PSM** testing. To do so, we will need to connect as a user who is a member of the **Auditors** group – *auditor01*.

Monitor Active Sessions

- Login to the **PWVA** as *Bill* and open a privileged session using the *localadmin01* account via the PSM.
- Logout of the **PVWA** and log back in via LDAP as *auditor01*.
- Go to the **MONITORING** pane.



4. Go to **Active Sessions** and locate the session opened by *Bill* and click on **Monitor**. You should now be able to monitor *Bill's* session as it happens.

The screenshot shows the CyberArk Monitoring interface. At the top, there are filters for 'Sessions properties' and 'Sessions activities'. Below that is a search bar and date/time controls ('From Dec 7, 2018 12:00 AM' and 'To Dec 9, 2018 11:59 PM'). An 'Apply' button is located at the top right. The main area displays a table of active sessions. The first row in the table is highlighted with a red box around the 'More' icon. The table columns are: Risk, User, From IP, Client, Account User Name, Account Address, Account Policy ID, and Start. The data for the first row is: Bill, 10.0.20.1, RDP, localadmin01, vserver.cyber-ark-demo.lo..., WindowsServerLocalAdmi..., 12/9/2018 3:23 PM.

5. As *auditor01*, try to *Suspend*, *Resume* and ultimately *Terminate* the session.

This screenshot is identical to the one above, showing the CyberArk Monitoring interface with the same session details for user Bill. However, a red box highlights the 'More' icon in the session table, which has expanded to show three additional options: 'Suspend', 'Resume', and 'Terminate'.

Monitor Recordings

6. As *auditor01*, verify that you can see the recordings related to your prior sessions and try to play some of these recordings. Note that recordings related to PSM for SSH are presented in the classic UI.



Last sign in: 12/6/2018 | auditor01 | ?

Monitoring

Sessions properties ? Sessions activities ? Filters

From: Dec 3, 2018 12:00 AM To: Dec 9, 2018 11:59 PM Apply

Recordings Active sessions

31 results for: From: 12/3/2018 12:00 AM , To: 12/9/2018 11:59 PM Clear all filters Additional details & actions in classic interface

Risk	User	Client	Account User Name	Account Address	Account Policy ID	Start ↴	Duration	Video Size	Action
-	Bill	RDP	localadmin01	vfservr.cyber-ark-de...	WindowsServerLocalA...	12/9/2018 3:23 PM	00:06:07	372 KB	D Play
-	Linus	SSH	root02	centos-target01	Linuxvia55H30	12/6/2018 3:52 PM	00:36:38	42 KB	D Play
-	Linus	SSH	root02	centos-target01	Linuxvia55H30	12/6/2018 3:48 PM	00:01:03	35 KB	D Play
-	vaultadmin01	SSH	user01	10.0.0.20	Linuxvia55H30	12/6/2018 1:10 PM	02:41:32	116 KB	D Play
-	vaultadmin01	SSH	user01	10.0.0.20	Linuxvia55H30	12/6/2018 1:00 PM	00:01:22	26 KB	D Play

7. You can also search recordings by activities in a privileged session. For example, Enter **salary** in the **Session activities** field and press **Apply**. Once you locate the SQL recording, click on **Play**.

Last sign in: 6/16/2018 | auditor01 | ?

Monitoring

Sessions properties ? Sessions activities ? Filters

From: To: Apply

Recordings Active sessions

1 results for: Sessions activities: salary Clear all filters Additional details & actions in classic interface

Risk	User	Client	Account User Name	Account Address	Account Policy ID	Start ↴	Duration	Video Size	Action
-	vaultadmin01	SQL*Plus	dba01	10.0.0.20	OracleDBA30	6/14/2018 12:43 AM	00:04:16	32 KB	D Play

8. Review the recording. Click **Close** when you are done.



The screenshot shows the CyberArk Monitoring interface. On the left, there's a sidebar with icons for Monitoring, Risk, and Session History. The main area displays a timeline of database activity for session 14.6 on Thursday, June 14, 2018, from 12:44:00 AM to 12:48:00 AM. The session details are as follows:

- 12:44:00 AM: BEGIN DBMS_OUTPUT.DISABLE;
- 12:44:00 AM: SELECT USER FROM DUAL;
- 12:44:00 AM: BEGIN DBMS_OUTPUT....
- 12:44:00 AM: SELECT ATTRIBUTE,SC...
- 12:44:00 AM: SELECT CHAR_VALUE F...
- 12:44:00 AM: BEGIN DBMS_APPLICA...

To the right of the timeline is a terminal window titled "C:\oracle\instantclient11g\plsql.exe" showing the Oracle SQL*Plus prompt. The session history at the bottom of the interface shows the command "BEGIN DBMS_OUTPUT.DISABLE;".

- Click on the session line for more detail and find the command “select * from scott.salary”. Note that the recording will now start at the command selected.

This screenshot shows the same monitoring session as the previous one, but with a specific command highlighted. The command "select * from scott.salary" is highlighted with a blue box and a "Play" button next to it. The rest of the session history and the terminal window are identical to the first screenshot.



Privileged Threat Analytics

In this section, we will be looking at the CyberArk Privileged Threat Analytics component. Both the target CentOS and Windows servers have been configured to forward security information to the PTA.

We will be looking at:

- Unmanaged Privileged Access
- Suspected Credential Theft and Automatic Password Rotation
- Suspicious Password Change and Automatic Reconciliation
- Suspicious activities in a session and automatic suspension
- Security Rules Exceptions

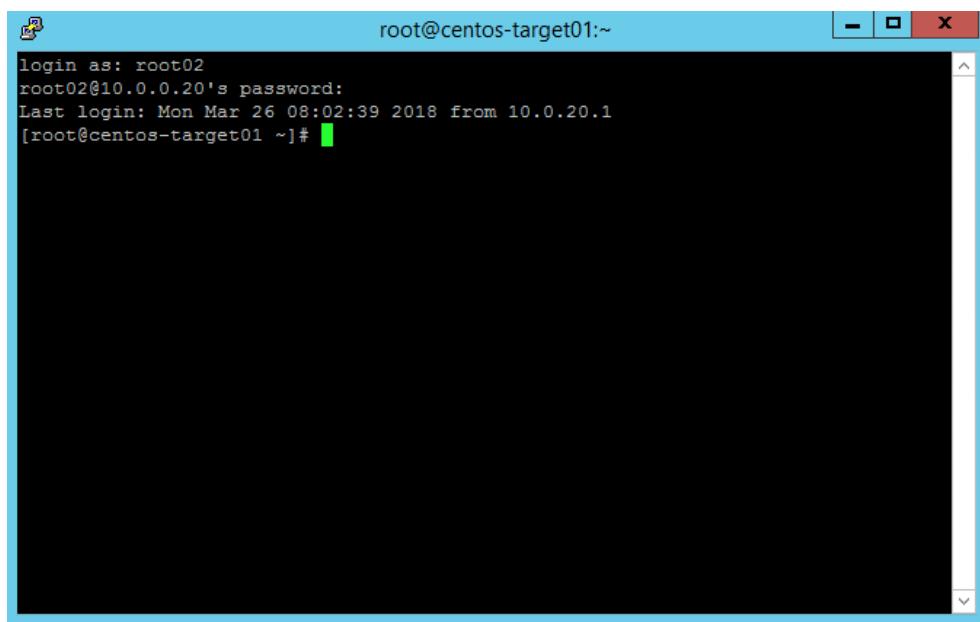
Unmanaged Privileged Access

Note: Because the PTA server can become unpredictable in the Skytap environment if it gets suspended, it has been configured not to start automatically. To perform these next steps, you will need to start your PTA server manually in Skytap.

In this section you will observe how the **PTA** detects when privileged accounts are being used and then check if they are being managed by **CyberArk**. If the account is not managed, the **PTA** will generate a security alert and add the account to the list of **Pending Accounts**. The Vault Administrator can then onboard the account to the relevant safe. Automatic Onboarding Rules can also be applied starting from v10.4.

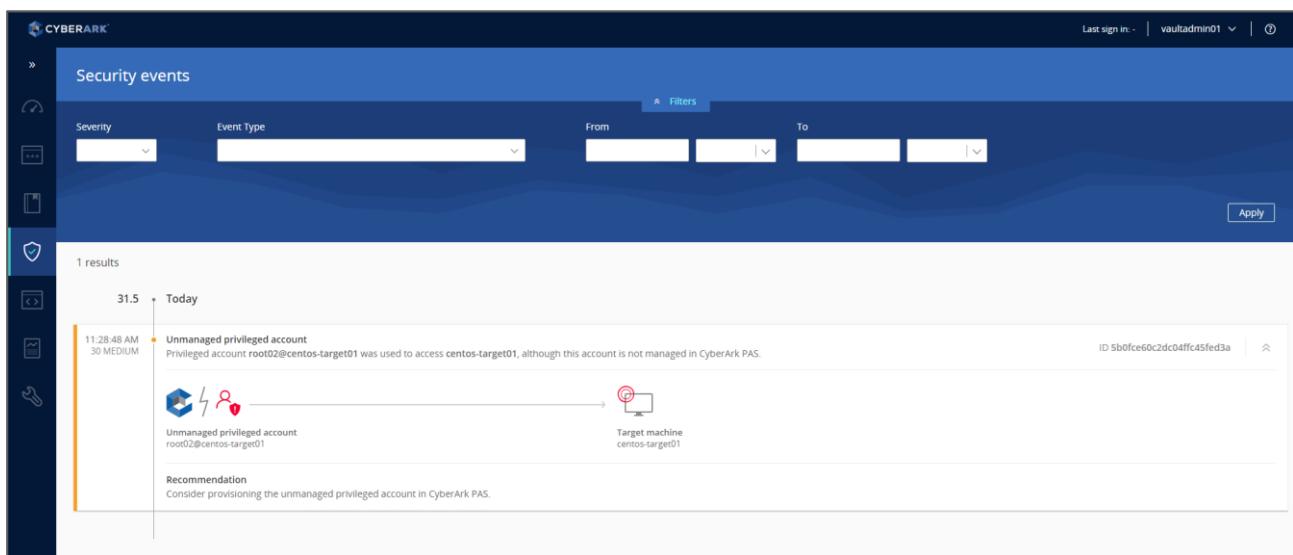
First, we need to establish an SSH session to the target Linux server to create an alert on the **PTA**, which we will review using the new **Security** pane in the **PVWA**.

1. Open **PuTTY** from the **Components** server and open an SSH session to 10.0.0.20 as *root02* (password: *Cyberark1*).



```
root@centos-target01:~  
login as: root02  
root02@10.0.0.20's password:  
Last login: Mon Mar 26 08:02:39 2018 from 10.0.20.1  
[root@centos-target01 ~]#
```

2. Login to the **PWAA** as **vaultadmin01** and go to **Security > Security Events** and verify that you can see the “Unmanaged privileged account” alert related to *root02*.



The screenshot shows the CyberArk PWAA interface under the 'Security events' section. It displays a single result for an 'Unmanaged privileged account' event. The event details are as follows:

- Severity:** 31.5 (MEDIUM)
- Event Type:** Unmanaged privileged account
- Description:** Privileged account root02@centos-target01 was used to access centos-target01, although this account is not managed in CyberArk PAS.
- ID:** 5b0fce60c2dc04ffca5fed3a
- Timestamp:** 11:28:48 AM Today
- Target machine:** centos-target01
- Recommendation:** Consider provisioning the unmanaged privileged account in CyberArk PAS.

3. Go to **Accounts Feed > Pending Accounts**. Select *root02* from the list (use “Refine By” to search for the account if needed) and click on **Onboard Accounts**.



The screenshot shows the 'Pending Accounts' section of the CyberArk PAS interface. On the left, there's a sidebar with 'Back to Accounts', 'Accounts Discovery', 'Pending Accounts' (which is selected and highlighted in blue), and 'Discovery Management'. Below that is a 'Refine by' section with a 'Keywords' input field containing 'root02', a 'Clear' button, and an 'Apply' button. The main area shows a table with one result for 'root02'. The table has columns: Username, Address +, Platform, Dependen, Age (days), and Account category. The row for 'root02' is highlighted with a red border. To the right of the table is an 'Account Preview' pane with expandable items like 'Username', 'Address', 'Platform', 'Age (days)', 'Last set', 'Last login date', and 'Account category'. At the bottom right of the preview pane is a blue button labeled 'Onboard Accounts' with a white icon, which is also highlighted with a red box.

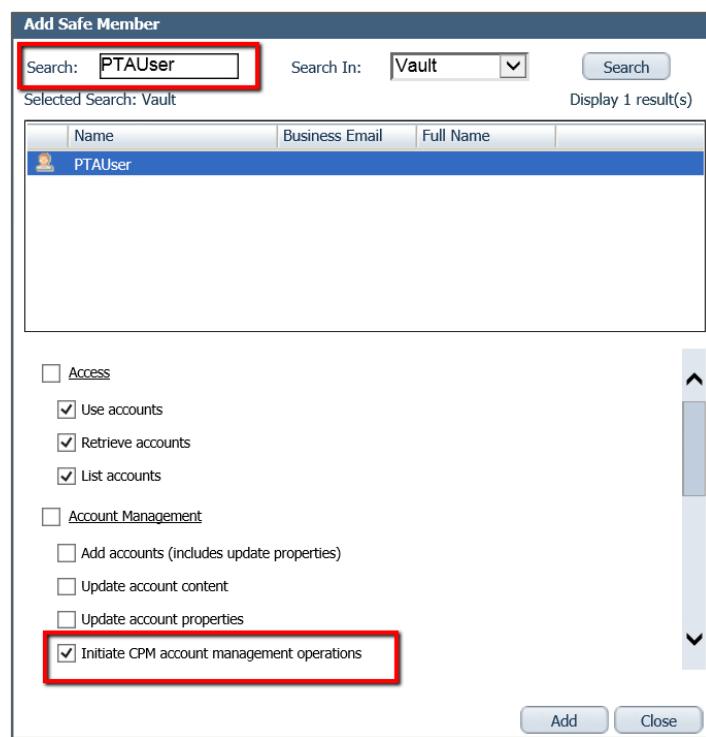
4. Onboard the account to the **Linux Finance** safe and associate the account with the **Linux via SSH 30** platform.
5. Enter “Cyberark1” as the default password.

Note: “root.*” is defined by default as a privileged user in the PTA. You can add other usernames (using regular expressions) that should also be detected by the **PTA** as privileged accounts which should be managed by CyberArk PAS. To add additional usernames login to the **PTA** administrative interface and go to **SETTINGS > Privileged Groups and Users**.

Suspected Credential Theft and Automatic Password Rotation

In this section you will configure the **PTA** to detect when privileged accounts are being used without first retrieving the password from PAS, and trigger the **CPM** to initiate a password change.

1. Login to the **PVWA** as *vaultadmin01* and go to **POLICIES > Access Control (Safes)**. Select the *Linux Finance* safe and click on **Members**.
2. Click on **Add Member** and search for the *PTAUser* in the Vault. Select the *PTAUser*. Keep the default permissions and expand **Account Management**. Select “Initiate CPM account management operations” and click on **Add**.



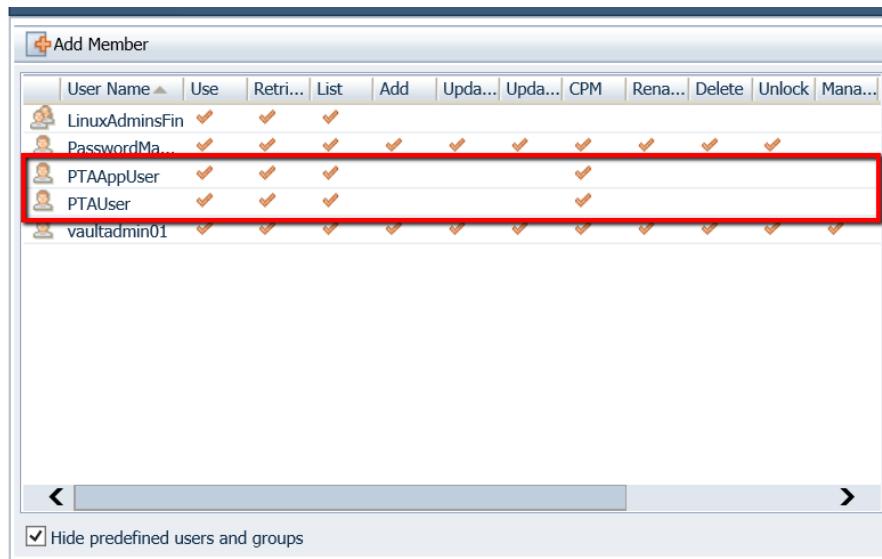
Add Safe Member

Search: Search In: Search
Selected Search: Vault Display 1 result(s)

Name	Business Email	Full Name
PTAUUser		

Access
 Use accounts
 Retrieve accounts
 List accounts
 Account Management
 Add accounts (includes update properties)
 Update account content
 Update account properties
 Initiate CPM account management operations

3. Repeat the above step to add the *PTAAppUser* to the *Linux Finance* safe as well (including the “Initiate CPM account management operations” permission).



Add Member

User Name	Use	Retri...	List	Add	Upda...	Upda...	CPM	Rena...	Delete	Unlock	Mana...
LinuxAdminsFin	✓	✓	✓								
PasswordMa...	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
PTAAppUser	✓	✓	✓			✓					
PTAUUser	✓	✓	✓			✓					
vaultadmin01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Hide predefined users and groups

4. Close and exit from your putty session to 10.0.0.20 if it is still open.
5. Once again, open **PutTY** from the **Components** server and open an SSH session to 10.0.0.20 as *root02* (password: *Cyberark1*).
6. Login to the **PWVA** as *vaultadmin01* and go to **Security > Security Events** and verify that you can see the “**Suspected Credentials Theft**” alert related to *root02*.



CYBERARK®

CyberArk Privileged Access Security – Administration

The screenshot shows the CyberArk PVWA interface under the 'Security events' tab. It displays 17 results for today, specifically a 'Suspected credentials theft' event at 4:50:41 PM. The event details show a privileged account from 'centos-target01' accessed 'centos-target01' with a password not retrieved from CyberArk PAS. A diagram illustrates the flow from 'Source machine comp01a.cyber-ark-de...' through 'Cyberark PAS' to 'Target machine centos-target01'. A recommendation states: 'Password change request was initiated. Ensure that your organizational policy and PAS controls are not bypassed, and that your managed accounts are controlled.'

7. In the **PVWA**, go to the *root02* account and verify that the **CPM** changed the password.
8. Open the **Activities** tab to verify that the **CPM** changed the password after the **PTA** detected the suspected credential theft alert and under **Activities** added the relevant file category for *Immediate Change*.

The screenshot shows the CyberArk PVWA interface for the 'root02 On centos-target01' account. The 'Activities' tab is selected, displaying a list of recent actions:

Date	User	Action
May 31 11:42:01 AM	>PasswordManager	CPM Change Password
May 31 11:40:36 AM	PTAUser	Add File Category
May 31 11:40:36 AM	PTAApUser	Privileged Threat Analytics Event
May 31 11:36:59 AM	vaultadmin01	Add File Category
May 31 11:36:59 AM	vaultadmin01	Add File Category

Note: To detect *Suspected Credential Theft*, the PTA compares the login time on the target machine with the last time the password was retrieved from the Vault. By default, the PTA creates a *Suspected Credential Theft* event if the password was not retrieved within the last 8 hours. For the purpose of this lab, we have configured the PTA to raise an alert if the password was not retrieved within the last 5 minutes.



Suspicious Password Change and Automatic Reconciliation

In this section you will configure the **PTA** to detect when a password is being changed manually, bypassing the **CPM**, and have the **PTA** trigger the **CPM** to reconcile the password.

For this exercise to work, you must associate a reconcile account with *root02*.

- Note:** If you performed the optional exercise on SSH key, you can use the *root01* account you created previously. If you have not already added the *root01*, do so now, creating it as a normal password account (exactly like *logon01*, page 35).
- Note:** If you configured SSH Command Access Control to block the **passwd** command, disable SSH Command Access Control in the *Linux via SSH 30* platform before performing this exercise and then restart the PSM service.

1. Login to the **PWAA** as *vaultadmin01* and go to **Accounts > Accounts View** and select the *root02* account. Using the classic UI, associate *root01* as the reconcile account for *root02*.

Last sign in: 6/22/2018 | vaultadmin01 | ?
Search: Leave empty to search all | Go
Add SSH Key | Add Account | Customize

Account Details

Logon Account: This account was successfully reconciled by the CPM at 6/20/2018 5:06 PM. More details

Reconcile Account: Linux via KEY 90-root01-10.0.0.20

Account Group

Group: [None] | Modify | Create New

Platform Name: Linux SSH 30
Device Type: Operating System
Safe: Linux Finance
Name: centos-target01-root02-c2eb5d4c-3d3a-4109-beef-0f0d852cb6c6
Last verified: 6/20/2018 4:52:12 PM
Last modified: PasswordManager (6/20/2018 5:06:51 PM)
Last used: vaultadmin01 (6/20/2018 5:05:31 PM)
Username: root02
Address: centos-target01

2. Go to **Accounts > Accounts View** and select *root02* again and launch an SSH connection via the PSM.
3. Type the following command to change the password of *root02* back to *Cyberak1*:

```
passwd root02
```



```
root@centos-target01:~  
Using username "root02".  
Last login: Thu May 31 13:11:56 2018 from comp01a.cyber-ark-demo.local  
[root@centos-target01 ~]# [root@centos-target01 ~]# passwd root02  
Changing password for user root02.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@centos-target01 ~]#
```

4. Go back to the **PWVA** as **vaultadmin01** and go to **Security > Security Events**. You should be able to see two new alerts. One for a “**Suspicious activities detected in a privileged session**”, and one for “**Suspicious password change**”.
5. Verify that you can see the “**Suspicious password change**” alert and that an automatic password reconciliation was initiated.

The screenshot shows the CyberArk PWVA interface with the 'Security events' page selected. The alert in question is highlighted with a red box:

1:21:33 PM HIGH Suspicious password change Initiated remediation
Privileged account root02@centos-target01 password was changed outside of CyberArk PAS.

Below the alert, a timeline diagram shows the password change process:

- Source machine unknown
- Cyberark PAS
- Privileged account root02@centos-target01

A recommendation is provided: "Password reconciliation request was initiated. Ensure that your organizational policy and PAS controls are not bypassed, and take control over the managed accounts."

6. Go to **Accounts > Accounts View** and select **root02**. Verify that **root02** was indeed reconciled by the **CPM**.



root02 On centos-target01

Platform: Linux SSH 30 Safe: Linux Finance

Overview Details Activities Versions

Compliance Status Compliant
Reconciled by PasswordManager... May 31, 2018 1:22 PM
Reconcile Change

Last Verified Never Verified Created 2 hours ago Verify

Activities (Last 5)

- May 31 1:22:32 PM PasswordManager CPM Reconcile Password
- May 31 1:21:55 PM PTAAppUser Privileged Threat Analytics Event
- May 31 1:21:55 PM PTAUser Delete File Category
- May 31 1:21:55 PM PTAUser Delete File Category
- May 31 1:21:55 PM PTAUser Update File Category

Last Access by PasswordManager Today

Suspicious activities in a session and automatic suspension

In this section you will configure the **PTA** to detect when a risky command is used in a privileged session and to suspend the session automatically.

1. Login to the **PWA** as **vaultadmin01** and go to **Security > Security Configurations > Privileged Session Analysis and Response**. Find the SSH **passwd** command (the command is used to change the password manually) and click on **Edit**.

Security Configurations					
Assign a risk score and automatic response to high-risk activities detected during recorded user sessions.					
Category	Pattern	Score	Description	Response	Status
SSH	(.*history{,*})	70	Represents a set of commands that may indicate a user clear...	None	Active
SSH	(.*authorized_keys{,*})	60	Manipulation of SSH keys on the machine. Could indicate an at...	None	Active
SSH	(.*sudoers{,*})	80	Manipulation of the sudoers file. Could indicate an attacker gr...	None	Active
SSH	(.*passwd{,*})	80	Access to passwd files exposes sensitive user details such as h...	None	Active
SSH	(.*)(DENIED .)	90	An indication of a restricted command execution trial.	None	Active
Windows titles	Registry Editor{,*}	65	Indication of access to the operating system registry.	None	Active
Windows titles	Windows Firewall with Advance...	70	Modification of the security configuration. Could indicate an at...	None	Active
Windows titles	Internet Properties	60	Modification of the network configuration. Could indicate an a...	None	Active
Windows titles	Network{,*}	60	Modification of the network configuration. Could indicate an a...	None	Active
Windows titles	Add .*Credential	60	Change user password. All privileged user passwords should b...	None	Active
Windows titles	Credential Manager{,*}	60	Change user password. All privileged user passwords should b...	None	Active

2. Configure the risk to a score of 90 and the response to “**Suspend Session**”. Click on **Save**.



Edit Rule

Category	Pattern
SSH	(.*)passwd(.*)
Description (optional)	
Access to passwd files exposes sensitive user details such as home directory, user ID, and more.	
Session response	Score
<input checked="" type="radio"/> Suspend	Set score (1 - 100) 90
<input type="radio"/> Terminate	Status
<input type="radio"/> None	Active
Scope	
This rule will apply to all Vault users, accounts, and machines.	
<input type="button" value="Cancel"/> <input type="button" value="Save"/>	

3. Go to **Accounts > Accounts View** and select the **root02** account. Launch a privileged session by clicking on the connect button. (If the session does not open, make sure the **Cyber-Ark Privileged Session Manager** service is running).
4. After the session opens, try to run the **passwd root02** command again. The session should be suspended immediately and a message should appear letting the user know the session is suspended.

```
root@centos-target01:~  
Using username "root02".  
Last login: Thu May 31 13:41:28 2018 from comp01a.cyber-ark-demo.local  
[root@centos-target01 ~]# [root@centos-target01 ~]# passwd root02  
Changing password for user root02.  
New password: [REDACTED]
```

5. Login to the **PWAA** as **auditor01**. Go to **Security > Security Events** and verify you can see the “**Suspicious activities detected in a privileged session**” alert. Verify that the session got a score of 90.



6. Click on **Resume** to resume the suspended session.

The screenshot shows the CyberArk Security events interface. A green banner at the top right indicates "Session resumption initiated successfully". The main area displays a list of security events with a red box highlighting the timestamp "1:44:46 PM 90 HIGH". Below this, a detailed view of a session is shown: "Active session Suspicious activities detected in a privileged session" initiated by "Vault user vaultadmin01" on "centos-target01" with activity "passwd root02". The session ID is "ba281107-1d72-4c15-be70-9ca41422f904". The diagram shows the flow from "Vault user vaultadmin01" through "Cyberark PAS" to the "Target service centos-target01". A red box highlights the "Resume" button on the right.

7. Click on the session link and verify that it takes you to the session details in the **Monitoring** pane. If the session is still in progress, you should see the options to terminate or monitor the session. If you already closed the session, you should be able to play the recording.

The screenshot shows the CyberArk Monitoring pane. It displays a session log for "vaultadmin01 connected as root02 on centos-target01" starting at "5/31/2018 1:44 PM" with a duration of "00:10:51". The "Activities" tab is selected, showing a single activity: "passwd root02" at "1:44:46 PM". On the right, there are "Terminate" and "Monitor" buttons, both highlighted with a red box. A note above the buttons says "Additional details & actions in classic interface".

Note: Auditor01 has access to the **Security** pane as it was added manually by us to the **Security Admins** and **Security Operators** groups. Auditor01 was able to resume the session as it was added manually by us to the **PSMLiveSessionTerminators** group.

Security Rules Exceptions

In this section, we will tweak the rule we created in the last section so that if a designated user needs to execute **passwd** during a session, their session will not be suspended out.



1. Go back to **Security > Security Configurations**, select the *passwd* rule and click the **Edit** button.
2. To create an exception to the rule, click on **Change scope**.

Category: SSH
Pattern: (*.passwd(.*))
Description (optional): Access to passwd files exposes sensitive user details such as home directory, user ID, and more.
Session response:
 Suspend
 Terminate
 None
Score: Set score (1 - 100): 80
Status: Active (checked)
Scope:
This rule will apply to all Vault users, all accounts and all machines
Change scope »
Cancel Save

3. Enter the user name *Linus* in the field, hit **Enter**, and then click the **Change scope** button. You will then be returned to **Edit Rule** dialogue. Click **Save** to close the dialogue.

Change scope
Vault users Accounts Machines
Exclude Include only
Linus
The following rule will apply to all Vault users, except for the selected ones
Cancel Change Scope



4. To test the rule, you can log in to the **PVWA** as the user *Linus* and connect using any of the accounts in the *Linux Finance* safe. Your session should not be suspended.

Note: As Linus is a member of the *ITManagers* Active Directory group, he does not have to submit a request to access the accounts.

Connect to the PTA Administration Interface

The **PTA** has a separate administration interface that is used for initial configuration and can be used to monitor threats and run reports.

In our environment, you can access the **PTA** Administration interface with the following:

Address:	https://10.0.0.1:8443/login
User name:	administrator
Password:	CyberArk123!

The screenshot shows the CyberArk Privileged Threat Analytics (PTA) sign-in interface. The page has a modern design with a large blue abstract graphic on the left side. On the right, there's a 'Sign In' form with the following details:

- User name:** administrator
- Password:** CyberArk123!

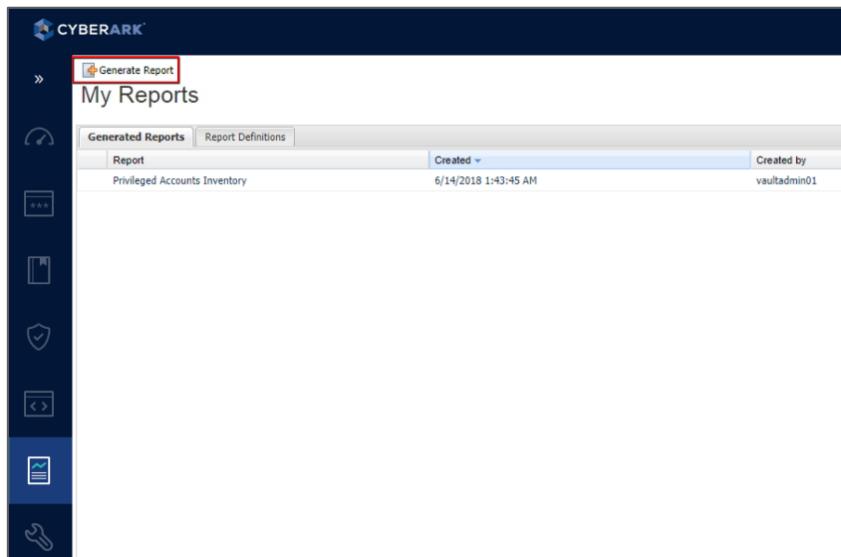
A blue 'Sign In' button is located at the bottom of the form. The CyberArk logo is in the top left corner of the page.

Reports

In this section you will be asked to create three types of reports.

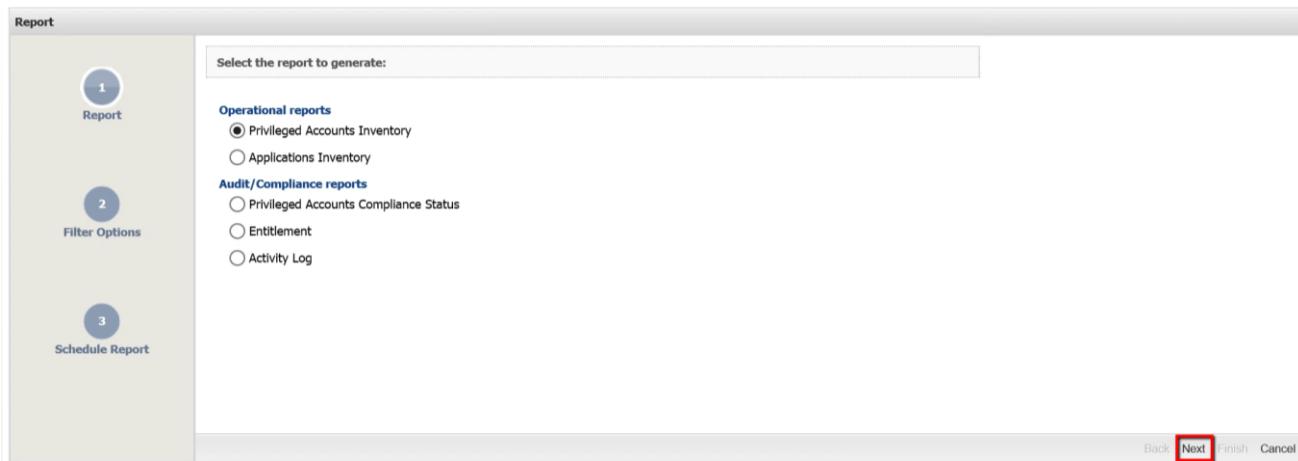
Generate “Privileged Accounts Inventory” report

1. Login to the **PVWA** as **vaultadmin01**, go to the **Reports** tab, and then click on **Generate Report**.



Report	Created	Created by
Privileged Accounts Inventory	6/14/2018 1:43:45 AM	vaultadmin01

2. Click **Next** to generate the “Privileged Accounts Inventory” report.



3. Review the options to filter the report but keep the default values, then click **Next**.



CYBERARK®

CyberArk Privileged Access Security – Administration

Filter Options

1 Report 2 Filter Options 3 Schedule Report

Specify filter options for Privileged Accounts Inventory report:

Report name: Privileged Accounts Inventory

General

Free search: []

Safe: []

Account name: []

Device type: []

Platform ID: []

Group: []

Include Service Accounts

Automatic Management Status

No filter

Back Next Finish Cancel

4. Click **Finish** generate the report.

Schedule Report

1 Report 2 Filter Options 3 Schedule Report

Report Recurrences

Generate

Generate and save report definitions

Schedule

Subscribers

Add

User Name	Success Notification
vaultadmin01	[]

Back Next Finish Cancel

5. Select the refresh icon  at the bottom of the page until the report status shows “Done”. Open the report by clicking on the **Excel** icon.
6. Click **OK** to open with the default **LibreOffice Calc**.

Generate Report Customize

My Reports

Generated Reports Report Definitions

Report	Created	Created by	Status	Records	Size	Actions
Privileged Accounts Inventory	5/9/2016 2:39:44 AM	vaultadmin01	Done	17	8KB	  
Applications Inventory	5/5/2016 5:46:43 AM	vaultadmin01	Done	1	1KB	  
Role Based Entitlement	5/5/2016 4:21:59 AM	vaultadmin01	Done	7784	3.96MB	  
Privileged Accounts Inventory	5/5/2016 3:48:24 AM	vaultadmin01	Done	17	8KB	  

Page 1 of 1 |    Displaying Reports 1 - 4 of 4

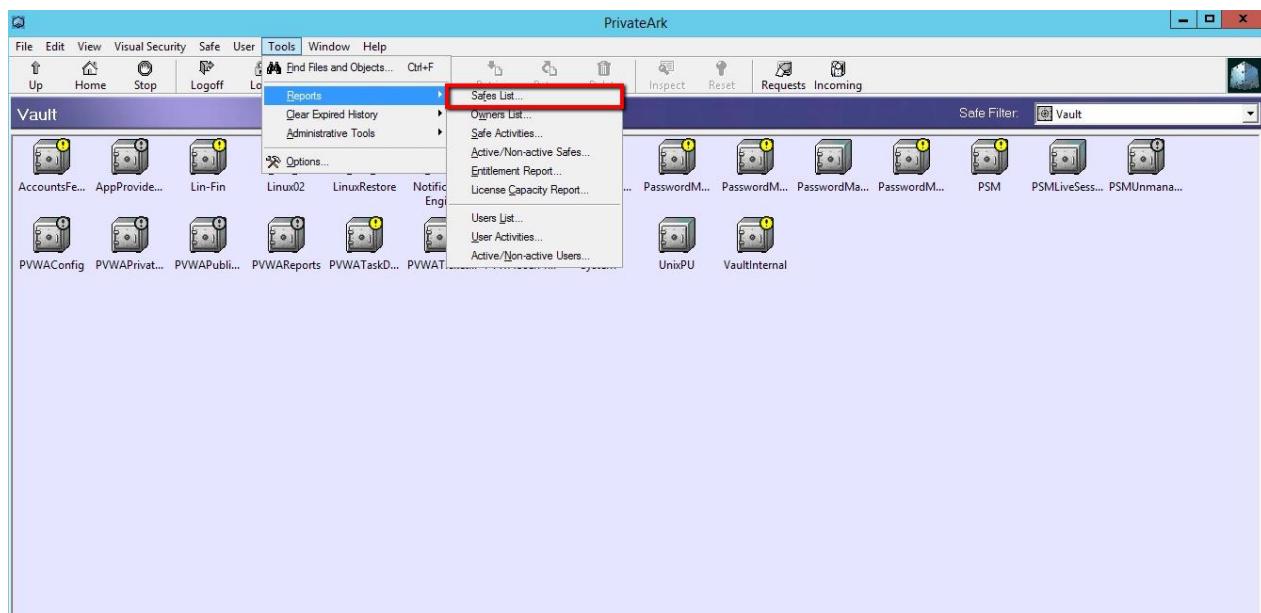


7. After going over the report, save the new report to the desktop of the Components server. If you are asked if you want to save the document in its current format, click **Keep Current Format**.

D	E	F	G	H	I	J	K	L
Target system address	Target system user name	Group name	Last accessed date	Last accessed by	Last modified date	Last modified by	Change failure	Verification failure
10.0.0.2	BindAccount			01/05/2016 00:00:00	vaultadmin01	21/04/2016 00:00:00	Administrator	No
10.0.0.20	logon01			25/04/2016 00:00:00	vaultadmin01	24/04/2016 00:00:00	PasswordManager	No
cyber-ark-demo.local	admin01			01/05/2016 00:00:00	vaultadmin01	25/04/2016 00:00:00	vaultadmin01	Yes
10.0.0.20	user01			01/05/2016 00:00:00	vaultadmin01	25/04/2016 00:00:00	vaultadmin01	No
10.0.0.20	dba01			01/05/2016 00:00:00	vaultadmin01	25/04/2016 00:00:00	PasswordManager	No
10.0.0.20	root01			01/05/2016 00:00:00	vaultadmin01	25/04/2016 00:00:00	PasswordManager	No
10.0.10.50	localadmin01			01/05/2016 00:00:00	vaultadmin01	25/04/2016 00:00:00	PasswordManager	No
VFSERVER.cyber-ark-den	discovery01					25/04/2016 00:00:00	PasswordManager	No
VFSERVER.cyber-ark-den	discovery04					25/04/2016 00:00:00	PasswordManager	No
VFSERVER.cyber-ark-den	discovery02						sswordManager	No
VFSERVER.cyber-ark-den	discovery03						sswordManager	No
VFSERVER.cyber-ark-den	discovery05						sswordManager	No
VFSERVER.cyber-ark-den	discovery06						sswordManager	No
cyber-ark-demo.local	Admin11						sswordManager	No
10.0.0.20	root01b						ultadmin01	Yes
10.0.1.15	root01b						ultadmin01	No
10.0.0.20	linuxusr01						ultadmin01	Yes

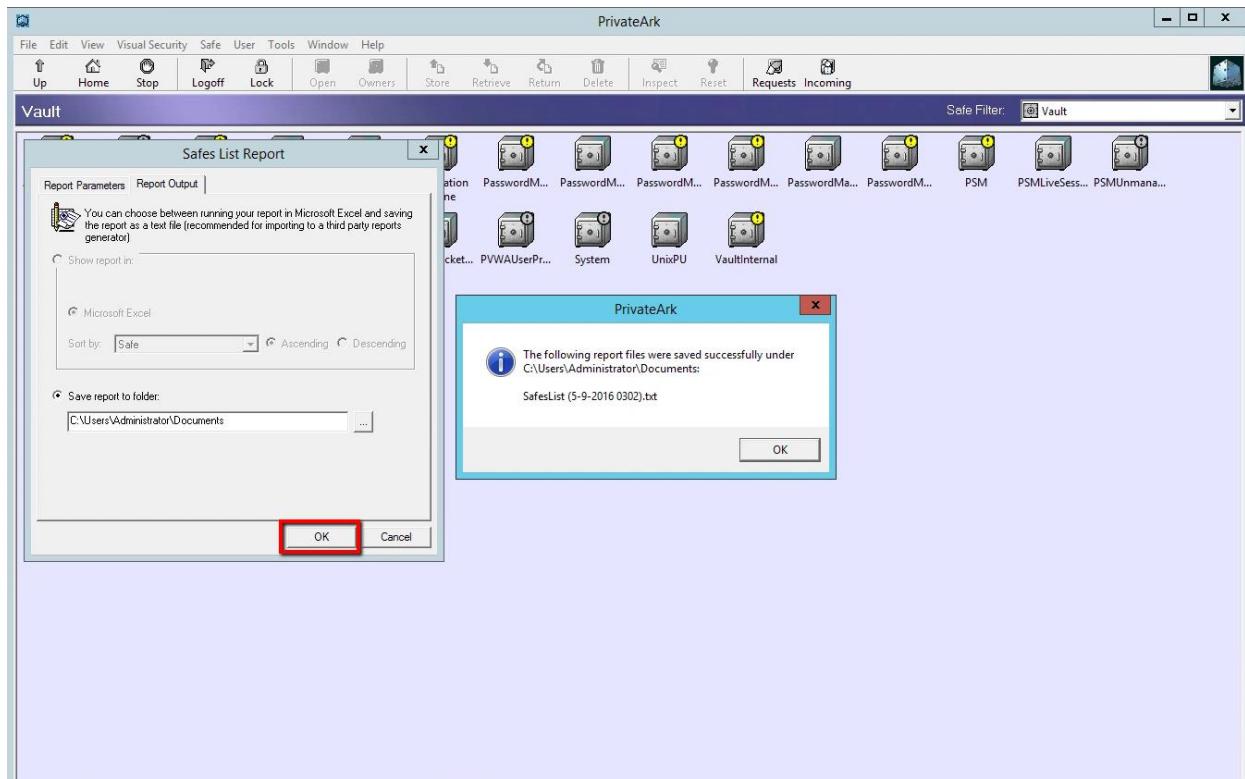
Generate “Safes List” Report and “Users List” report

1. On the **Components** server, open the **PrivateArk Client** and login as **Administrator**
2. Under **Tools > Reports**, click on **Safes List** to generate a safes list report

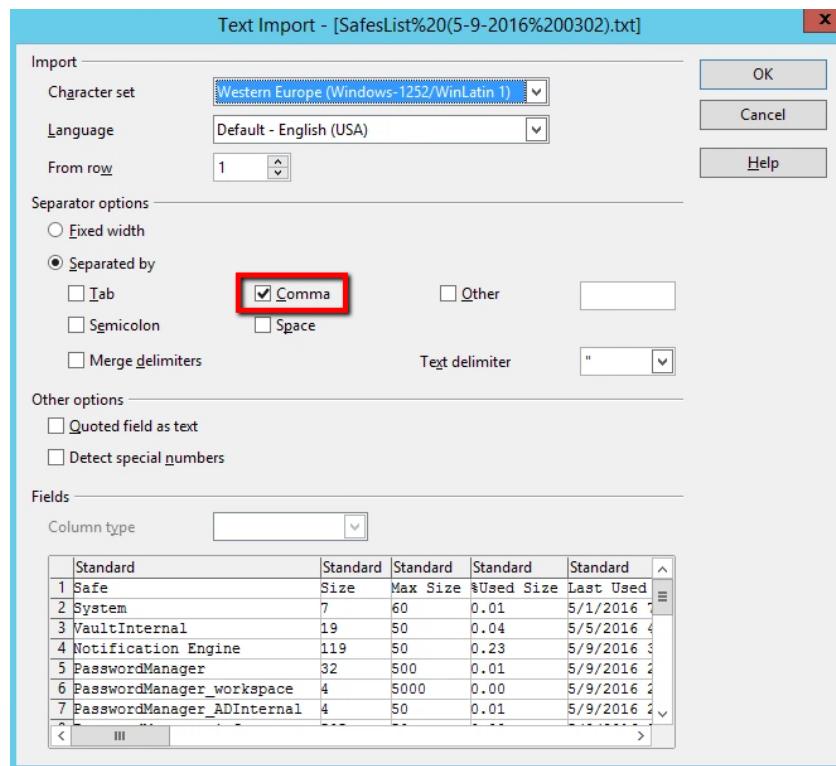




3. Click **Report Output** and save the new report to the desktop of the Components server.



4. Right click on the report and open with **LibreOffice Calc**.
5. Under “Separator options” choose **Separated by: Comma**
6. Click **OK**.



7. After reviewing the report, save a copy of the report to the desktop of the Components server.
8. Select *Keep Current Format*.
9. Repeat these steps creating a **Users List** report and copy the report to the desktop of the Components server.
10. By the end of this exercise you should have 3 reports on the desktop. These reports are **“Privileged Accounts Inventory”**, **“Safes List”** and **“Users List”**.

Common Administrative Tasks

Backup and Restore

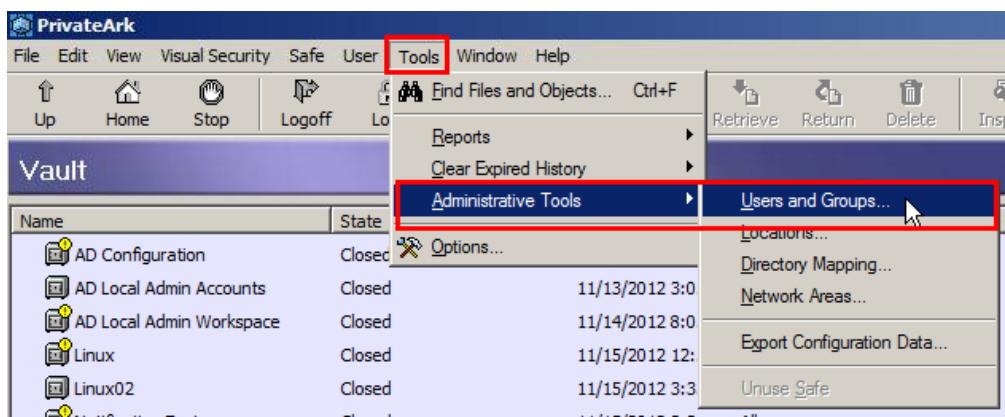
Again, for the sake of convenience, we will be using our *Administrator* account to perform a number of tasks during backup and restore.

We will begin by enabling two additional CyberArk accounts: *Backup*, which we will use to execute the back up; and *DR*, the disaster recovery account that has authority to restore objects, create Safes, etc.

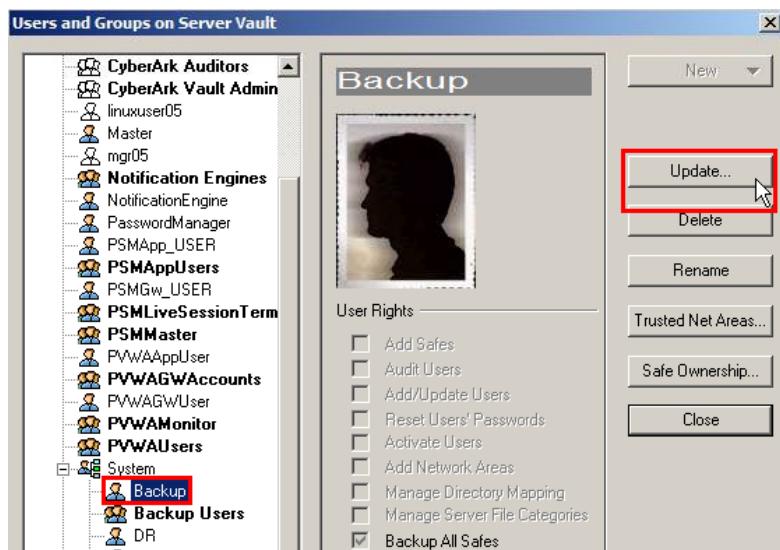
Enabling the Backup and DR users

For this section of the exercise, you will log in to the **PrivateArk Client** on the **Components** server in order to enable the users required to run a backup.

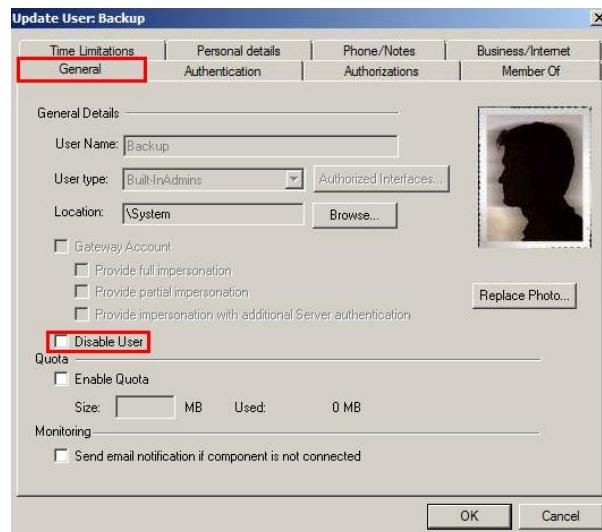
1. Use the **PrivateArk Client** to log into the **Vault** as *administrator*.
2. Go to **Tools > Administrative Tools > Users and Groups**.



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



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

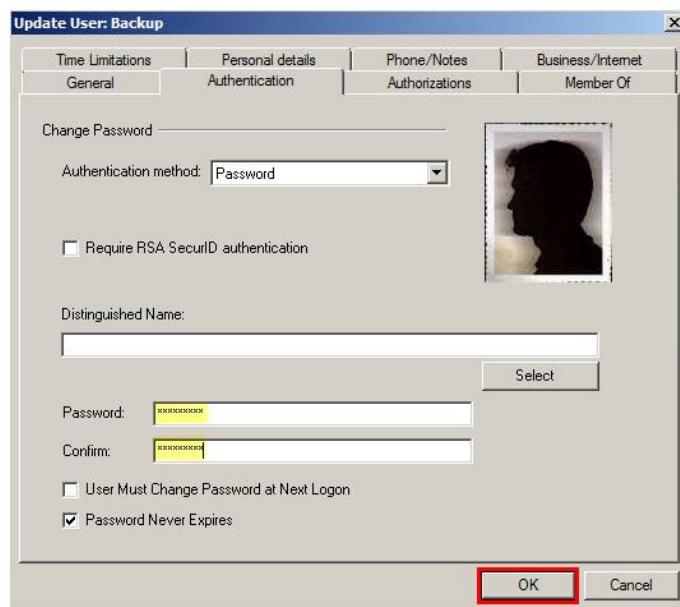


5. On the **Authentication** tab enter **Cyberark1** in the **Password** and **Confirm** fields.
6. Press **OK**.



CYBERARK®

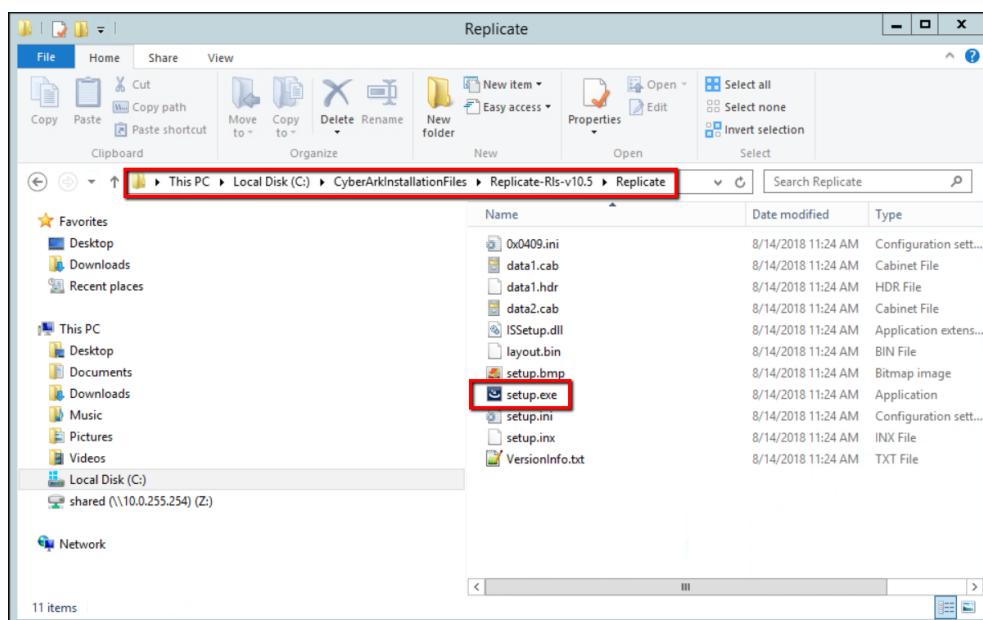
CyberArk Privileged Access Security – Administration



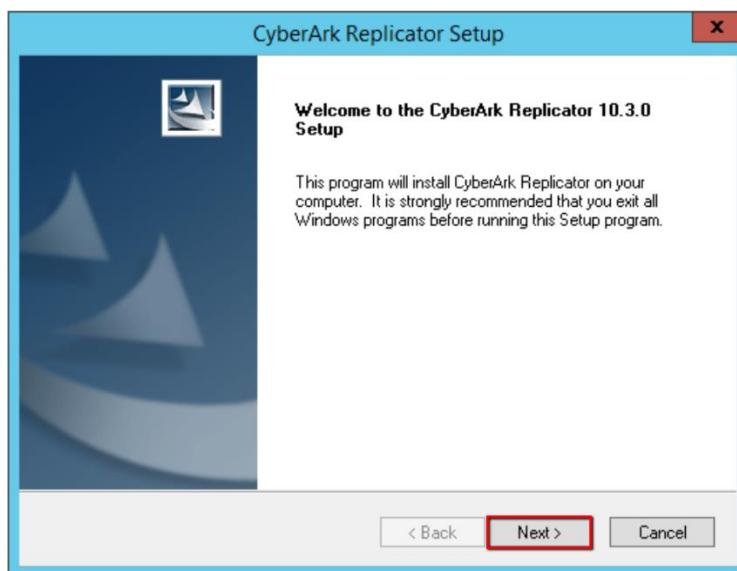
7. Repeat the above steps in order to enable the **DR** user as well. For convenience, the **DR** user will be used to restore the safes.
8. Log out of **PrivateArk Client**.

Installing the PrivateArk Replicator

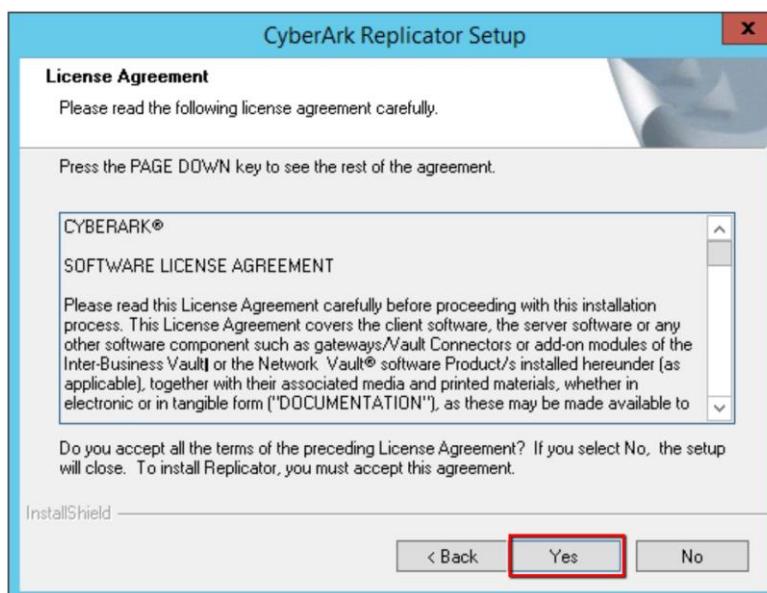
1. On the **Component Server**, open Windows **File Explorer** and go to C:\CyberArk\InstallationFiles\Replicate.
2. Double-click **setup.exe**.



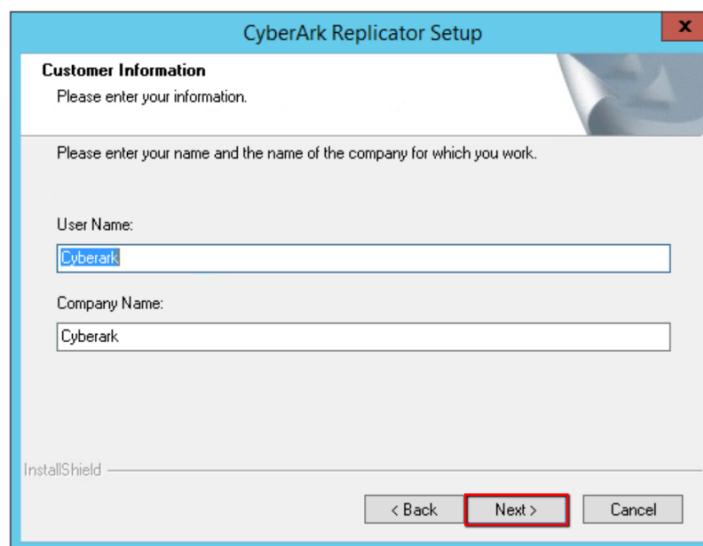
3. On the first screen enter **Next**.



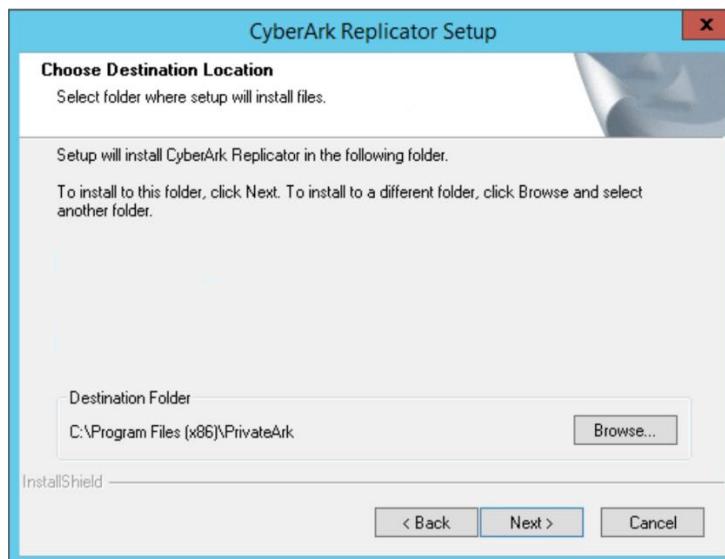
4. Click **Yes** to accept the license agreement.



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



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

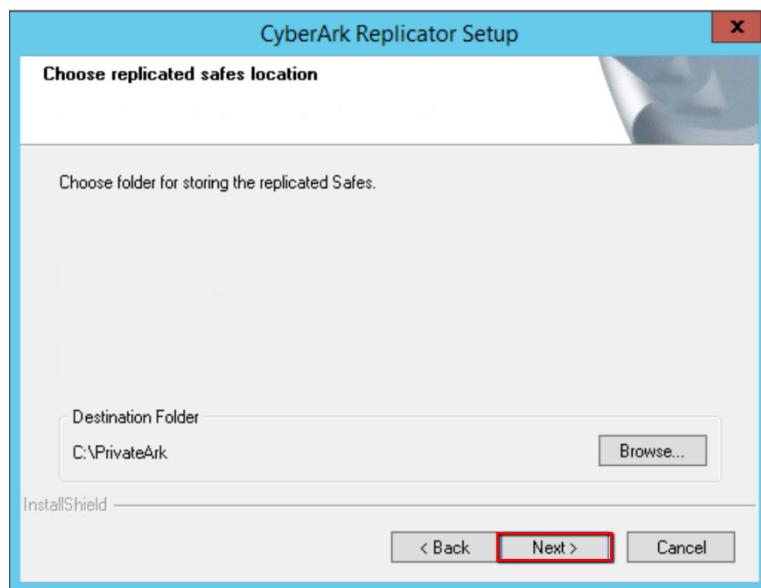


7. Press **Next** to accept the default safes location.

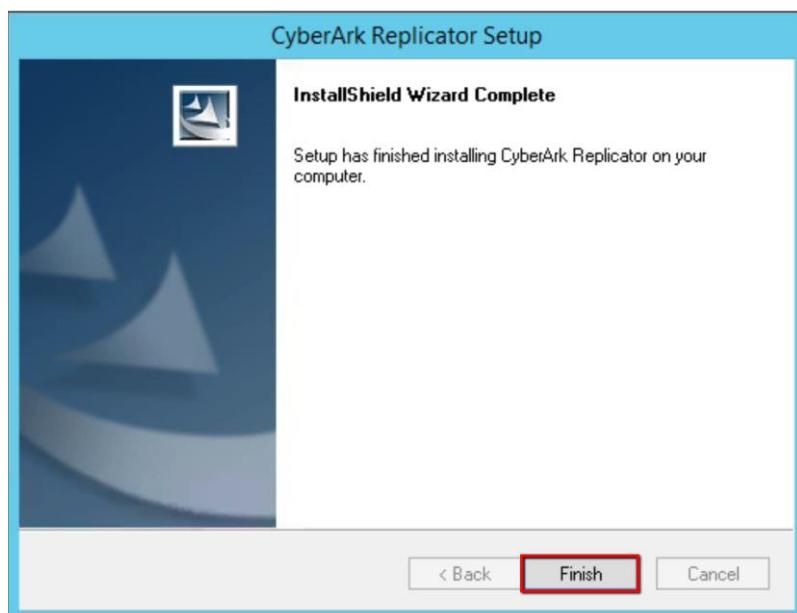


CYBERARK®

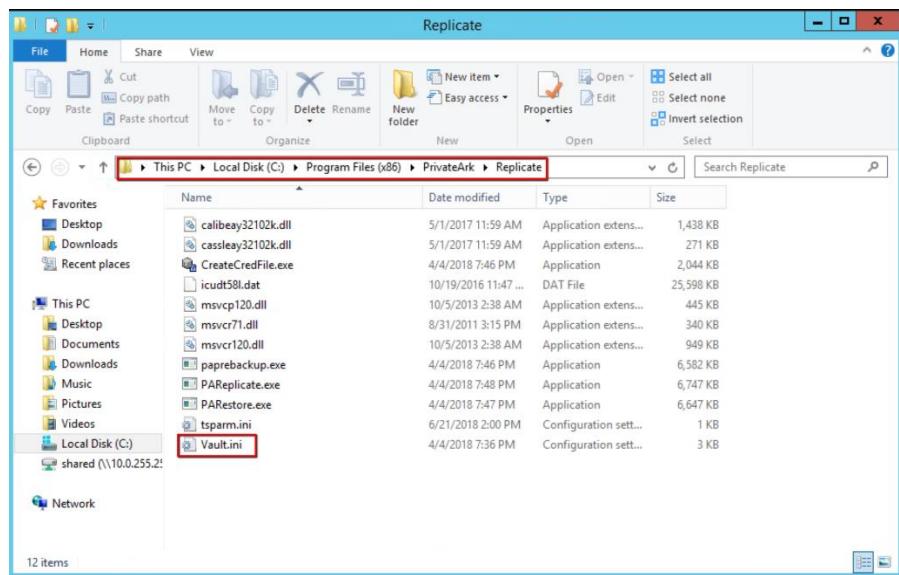
CyberArk Privileged Access Security – Administration



8. Click the **Finish** button.



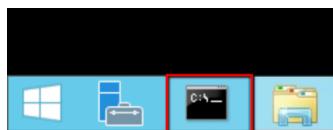
9. In Windows **File Explorer** go to *C:\Program Files (x86)\PrivateArk\Replicate*.
10. Double-click the *Vault.ini* file.



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: **10.0.10.1**

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

13. Save and close the file.
14. Open a Command Prompt.



15. Enter `cd c:\Program Files (x86)\PrivateArk\Replicate`.

```
Administrator: Command Prompt  
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 as they are not relevant in our environment.

```
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>
```

Create a Safe and an Account to test Backup

Log in to the **PVWA** as *Administrator* (don't forget to choose *CyberArk authentication*). First we will create a Safe and an account that we will later delete in order to test the restore process.

1. Go to the **POLICIES > Access Control (Safes)**.
2. Press **Add Safe**. Enter *Linux02* as the **Safe Name** and press **Save**.

Add Safe

Safe name:	<input type="text" value="Linux02"/>
Description:	<input type="text"/>
<input type="checkbox"/> Enable Object Level Access Control	
Saved passwords:	<input checked="" type="radio"/> Save the last <input type="text" value="5"/> password versions <input type="radio"/> Save password versions from the last <input type="text" value="7"/> days
Assigned to CPM:	<input type="text" value="PasswordManager"/>
Save Cancel	

3. Using the classic interface, go to the **Accounts** page and click **Add Account**.
4. Enter the following:

Store in Safe:	<i>Linux02</i>
Device Type:	<i>Operating System</i>

Platform Name:	<i>Linux via SSH 30</i>
Address:	<i>10.0.0.21</i>
User Name:	<i>root</i>
Password:	<i>Cyberark2</i>
Confirm Password:	<i>Cyberark2</i>
Name (Custom):	<i>root.backup.test</i>

Note: The target machine **10.0.0.21** does not exist. This is just a dummy account to test Back-up and Restore.

5. Press **Save** and logout of the **PWVA**.

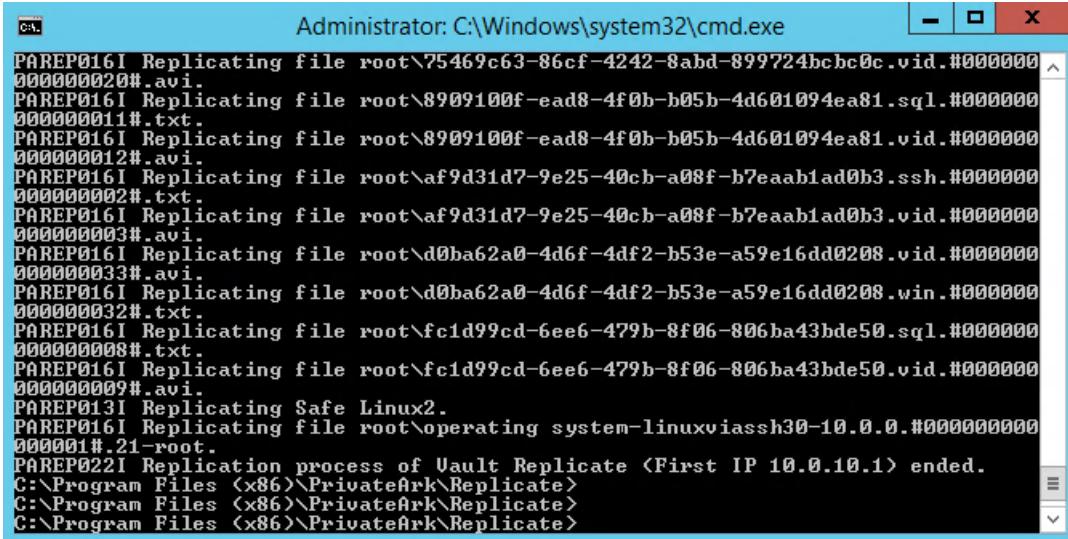
Running a Backup

To perform a backup, run the following command from the Replicate installation folder:

```
PAREPlicate.exe vault.ini /logonfromfile 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.

If the replicate was successful, proceed to the next steps. If not, verify the configuration information and try again.



```

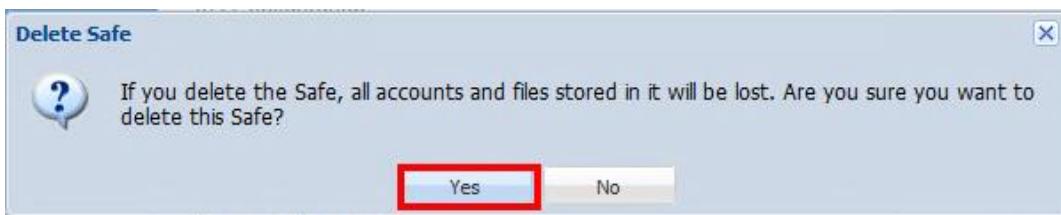
Administrator: C:\Windows\system32\cmd.exe
PAREP016I Replicating file root\75469c63-86cf-4242-8abd-899724bcbc0c.vid.#00000000000000000000000000000000.avi
PAREP016I Replicating file root\8909100f-ead8-4f0b-b05b-4d601094ea81.sql.#00000000000000000000000000000000.txt
PAREP016I Replicating file root\8909100f-ead8-4f0b-b05b-4d601094ea81.vid.#00000000000000000000000000000000.avi
PAREP016I Replicating file root\af9d31d7-9e25-40cb-a08f-b7eaab1ad0b3.ssh.#00000000000000000000000000000000.txt
PAREP016I Replicating file root\af9d31d7-9e25-40cb-a08f-b7eaab1ad0b3.vid.#00000000000000000000000000000000.avi
PAREP016I Replicating file root\d0ba62a0-4d6f-4df2-b53e-a59e16dd0208.vid.#00000000000000000000000000000000.avi
PAREP016I Replicating file root\d0ba62a0-4d6f-4df2-b53e-a59e16dd0208.win.#00000000000000000000000000000000.txt
PAREP016I Replicating file root\fc1d99cd-6ee6-479b-8f06-806ba43bde50.sql.#00000000000000000000000000000000.txt
PAREP016I Replicating file root\fc1d99cd-6ee6-479b-8f06-806ba43bde50.vid.#00000000000000000000000000000000.avi
PAREP0131 Replicating Safe Linux2.
PAREP016I Replicating file root\operating system-linuxviassh30-10.0.0.#00000000000000000000000000000000.21-root.
PAREP022I Replication process of Vault Replicate <First IP 10.0.10.1> ended.
C:\Program Files (<x86>)\PrivateArk\Replicate>
C:\Program Files (<x86>)\PrivateArk\Replicate>
C:\Program Files (<x86>)\PrivateArk\Replicate>
```

Delete the *Linux02* Safe

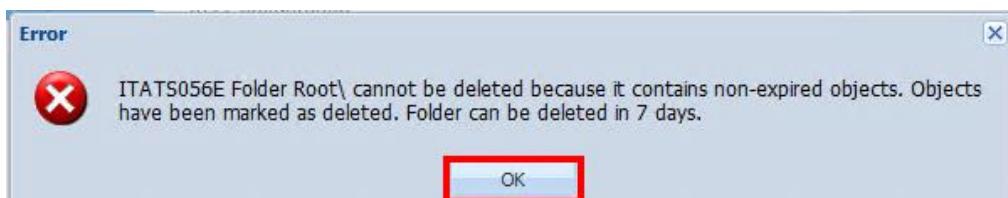
- Making sure you are logged into the **PWVA** as the *administrator* user, go to **POLICIES > Access Control (Safes)**.



2. Highlight *Linux02* and click the **Delete** button.
3. Press **Yes** to confirm that you would like to delete the safe and contents.



4. 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.



5. To confirm that the contents of the *Linux02* safe have been deleted go to the **Accounts** page.
6. Enter *root* in the search box and press the **Search** button.
7. The *root* account that you created earlier in this exercise using address *10.0.0.21*, should not appear.

Running a Restore

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

```
PARestore.exe vault.ini dr /RestoreSafe Linux02 /TargetSafe  
LinuxRestore.
```

You will be prompted for the password for the **DR** user, which should be *Cyberark1*.

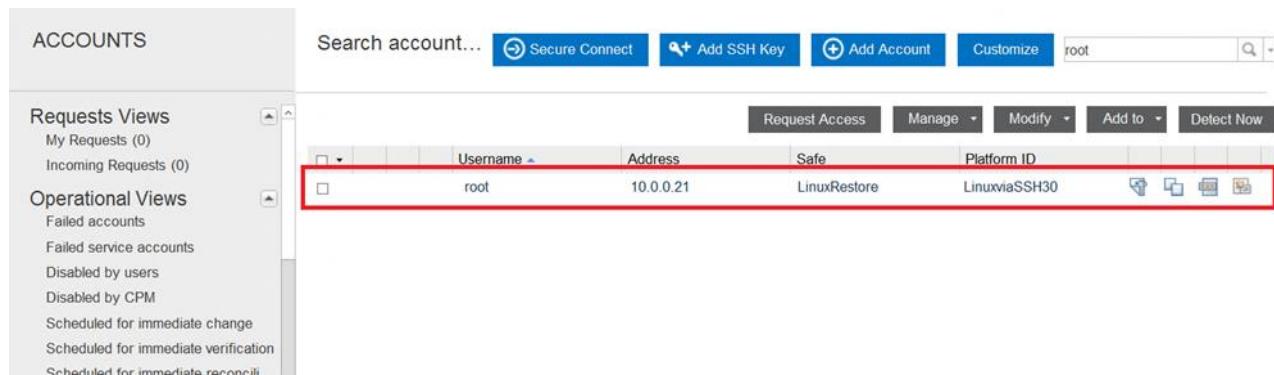
2. You will receive a message stating that the restore process has ended.

Administrator: C:\Windows\system32\cmd.exe

```

C:\>Program Files (<x86>)\PrivateArk\Replicate>
C:\>Program Files (<x86>)\PrivateArk\Replicate>PARestore.exe vault.ini dr /restoresafe Linux02 /targetsafe LinuxRestore
Password: *****
PARST011I Restore process of Vault Restore <10.0.10.1> started at Sun May 13 20:18:14 2018
PARST021I Restoring Metadata file backup-dump.sql.gz.
PARST009I Restoring file backup-dump.sql.gz.
PARST021I Restoring Metadata file cfg.backup-enecredfile.ini.gz.
PARST009I Restoring file cfg.backup-enecredfile.ini.gz.
PARST021I Restoring Metadata file cfg.backup-replicationuser.pass.gz.
PARST009I Restoring file cfg.backup-replicationuser.pass.gz.
PARST019I 1 out of 1 dump files restored successfully.
PARST020I 0 out of 0 Binary Logs restored successfully.
PARST027I 2 out of 2 Configuration files restored successfully.
PARST025E Could not find a source data directory for Safe Linux02.
PARST003E PARestore ended with errors.
PARST012I Restore process of Vault Restore <10.0.10.1> ended at Sun May 13 20:18:31 2018
C:\>Program Files (<x86>)\PrivateArk\Replicate>
```

3. Go back to the **PWAs** and search for root again.
4. You should now see the *root* account using address **10.0.0.21**, residing in safe **LinuxRestore**.



	Username	Address	Safe	Platform ID
<input type="checkbox"/>	root	10.0.0.21	LinuxRestore	LinuxviaSSH30

Note: The Target Safe (**/LinuxRestore**) is the name of the restored Safe to create. The restore process does not overwrite an existing Safe – it creates a new one. Therefore, this name must not correspond with an existing Safe.

Remote Control Client

Configuring the Remote Control Client on the Vault:

1. Logon to the **Vault** server with the local user **Administrator** and password **Cyberark1**.
2. Navigate to the **Vault** server **Conf** folder (By default: **C:\Program Files (<x86>)\PrivateArk\Server\Conf**).

3. Open the *PARagent.ini* file and add the IP address of your Components server to the “RemoteStationIPAddress” parameter. (10.0.20.1) and save the file.
4. Open a command line window from this location. You can do this by holding the *Shift* key and right-clicking in a blank space in the folder, then selecting “Open command window from here”.
5. Move up one directory level and run:

```
PARagent.exe setpassword Cyberark1
```

6. You should now have a new file in the *\Conf* directory called: *paragent.pass*.
7. Go to the **Services** window in the **Server Manager** and restart the *PrivateArk Remote Control Agent Service*:

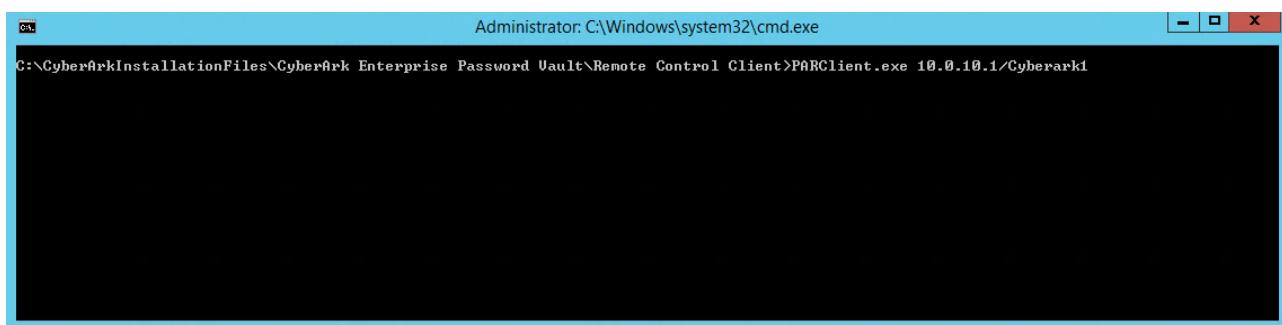
Connecting with the Remote Control Client from the Components server:

1. Logon to the **Components server** and navigate to:

```
C:\CyberArk\InstallationFiles\ Remote Control Client
```

2. Open a command line window from this location. You can do this by holding the *Shift* key and right clicking in a blank space in the folder, then selecting “Open command window from here”. You may need to expand the window to find a large enough blank space.
3. Run the following command:

```
PARClient.exe 10.0.10.1/Cyberark1
```



4. After the DLLs have loaded you should see the **PARCLIENT** prompt:



```
Administrator: C:\Windows\system32\cmd.exe - PARClient.exe 10.0.10.1/Cyberark1
C:\CyberArkInstallationFiles\CyberArk Enterprise Password Vault\Remote Control Client>PARClient.exe 10.0.10.1/Cyberark1
Cyber-Ark Remote Administration Client <9.80.3.0>
Working with agent on: 10.0.10.1
Loaded component from [C:\CyberArkInstallationFiles\CyberArk Enterprise Password Vault\Remote Control Client\PARClusterVaultClient.dll]
Loaded component from [C:\CyberArkInstallationFiles\CyberArk Enterprise Password Vault\Remote Control Client\PARDRClient.dll]
Loaded component from [C:\CyberArkInstallationFiles\CyberArk Enterprise Password Vault\Remote Control Client\PARNEClient.dll]
Loaded component from [C:\CyberArkInstallationFiles\CyberArk Enterprise Password Vault\Remote Control Client\PARVaultClient.dll]

PARCLIENT>
```

- Run the following command to see the status of the Vault

```
status Vault
```

- Run the following command to set the debug level of the Vault:

```
SetParm Vault DebugLevel=PE(14) /Immediate
```

- Type **exit** to quit PARClient

Create a password file for the Remote Agent

You can also connect to the Remote Agent using a password file instead of typing the password in clear text.

- Run the following command in order to create a password file:

```
PARClient.exe /createpassfile pass.pwd
```

- Enter the same password you used before (*Cyberark1*) and confirm.

```
Administrator: C:\Windows\system32\cmd.exe
C:\CyberArkInstallationFiles\CyberArk Enterprise Password Vault\Remote Control Client>PARClient.exe /createpassfile pass.pwd
Cyber-Ark Remote Administration Client <9.80.3.0>
Working with agent on:

Loaded component from [C:\CyberArkInstallationFiles\CyberArk Enterprise Password Vault\Remote Control Client\PARClusterVaultClient.dll]
Loaded component from [C:\CyberArkInstallationFiles\CyberArk Enterprise Password Vault\Remote Control Client\PARDRClient.dll]
Loaded component from [C:\CyberArkInstallationFiles\CyberArk Enterprise Password Vault\Remote Control Client\PARNEClient.dll]
Loaded component from [C:\CyberArkInstallationFiles\CyberArk Enterprise Password Vault\Remote Control Client\PARVaultClient.dll]

Enter password for password file creation.
New password: *****
Confirm new password: *****
Password file created successfully.

C:\CyberArkInstallationFiles\CyberArk Enterprise Password Vault\Remote Control Client>
```

- In order to connect to the **PARAgent** on the Vault Server using the newly created password file, run the following command:



```
PARClient.exe <IP Address of Vault Server> /usepassfile  
<filename>
```

```
Administrator: C:\Windows\system32\cmd.exe - PARClient.exe 10.0.10.1 /usepassfile pass.pwd
C:\CyberArkInstallationFiles\CyberArk Enterprise Password Vault\Remote Control Client>
C:\CyberArkInstallationFiles\CyberArk Enterprise Password Vault\Remote Control Client>PARClient.exe 10.0.10.1 /usepassfile pass.pwd
Cyber-Ark Remote Administration Client <9.80.3.0>
Working with agent on: 10.0.10.1
Loaded component from [C:\CyberArkInstallationFiles\CyberArk Enterprise Password Vault\Remote Control Client\PARClusterVaultClient.dll]
Loaded component from [C:\CyberArkInstallationFiles\CyberArk Enterprise Password Vault\Remote Control Client\PARDCRClient.dll]
Loaded component from [C:\CyberArkInstallationFiles\CyberArk Enterprise Password Vault\Remote Control Client\PARNECClient.dll]
Loaded component from [C:\CyberArkInstallationFiles\CyberArk Enterprise Password Vault\Remote Control Client\PARVaultClient.dll]
PARCLIENT>
```

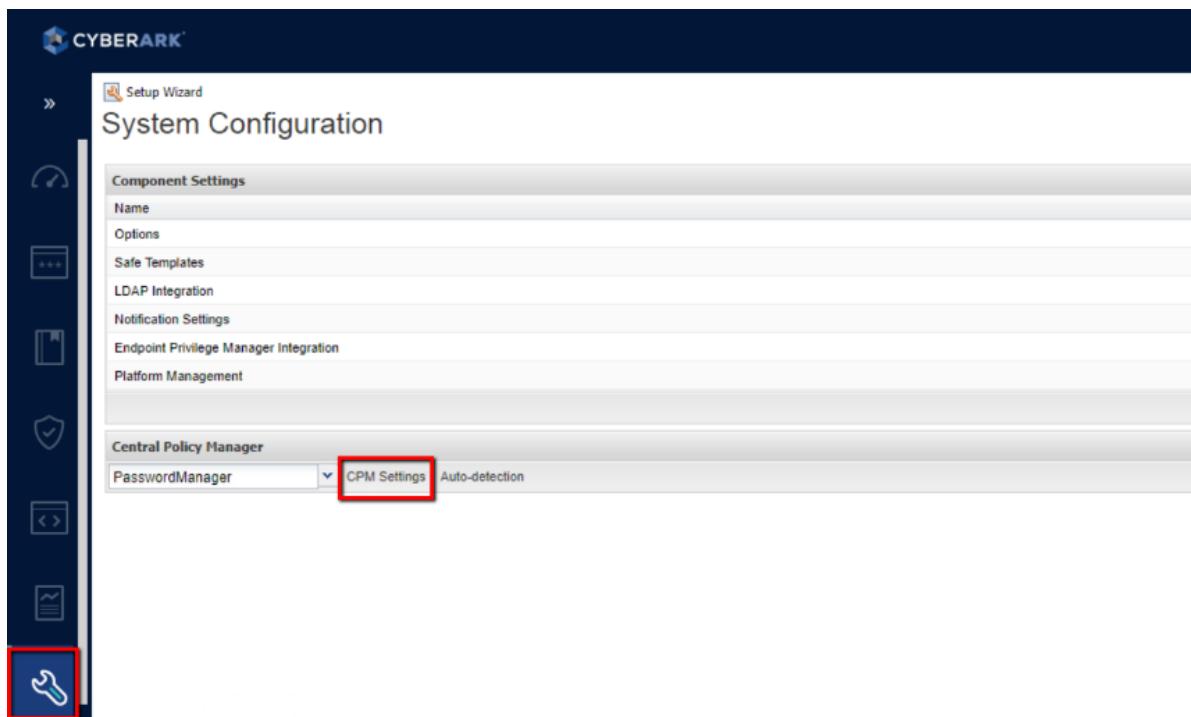
Verify the changes made with the Remote Control Client

1. Connect to your **Vault** server.
2. Click on the **PrivateArk Server** icon.
3. Examine the ITA log and verify the Debug level settings have been applied.

Rotating CPM Logs

The **CPM** log files can be automatically uploaded to a Safe in the **Vault** according to a predefined period of time in the **CPM** parameters file. Each time a log file is uploaded to the **Vault**, it is copied to the *History* subfolder in the *Log* folder, and the **CPM** begins writing to a new log file.

1. Log into the **PWVA** as *vaultadmin01*.
2. On the **ADMINISTRATION** tab, you should see that *PasswordManager* is already selected as the **CPM**. If there were multiple CPMs you would select the appropriate CPM from the pulldown list
3. Click **CPM Settings**.



4. Select **Configuration > General** and scroll down to set the following parameters.

LogCheckPeriod:	1
LogSafeName:	CPM_Logs

5. Click **OK**.
6. Create a safe called **CPM_Logs** and assign **PasswordManager** as the assigned **CPM**.
7. Modify the *Members* list to add the *Vault Admins* group.
8. Grant the *Vault Admins* group **all** safe permissions.
9. The *Vault Admins* group will now be able to access the **CPM** logs.

Log in with Master

There are some cases where you will need to log in to the **Vault** with the *Master* user. This can be in the event of an emergency or to give permissions to a user for safe when there are no active users with the necessary permissions.



In order to use the Master user, the dbparm.ini file must point to the location of the Recovery Private Key. By default, this is the CD-ROM drive of the server.

1. On the **Vault** server, open *C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini*.
2. Because we do not have a CD-ROM drive (we are using VMs for our lab exercises), you will need to point it to the relevant location.
3. Update the *RecoveryPrvKey* parameter to point to the location of the file called **recprv.key** in the **Master CD** folder:

```
RecoveryPrvKey=C: \CyberArk Installation Files \Master CD\recprv.key
```

4. Restart the **Vault** service (using the **PrivateArk Server** console with the stop light) as any change to the *dbparm.ini* file requires a restart of the service.
5. Open the **PrivateArk Client** from the **Vault** server machine.
6. In the *User name* field, enter: *Master*.
7. In the *Password* field enter the password that was configured during the installation process (*Cyberark1*).

Question: How many safes are listed?

8. Close the **PrivateArk Client** session.
9. Open the **PrivateArk Client** session and login as *Administrator*

Question: How many safes are listed?

10. You should notice that there are many more safes displayed when you were logged in as the *Master* user.

Optional Exercises

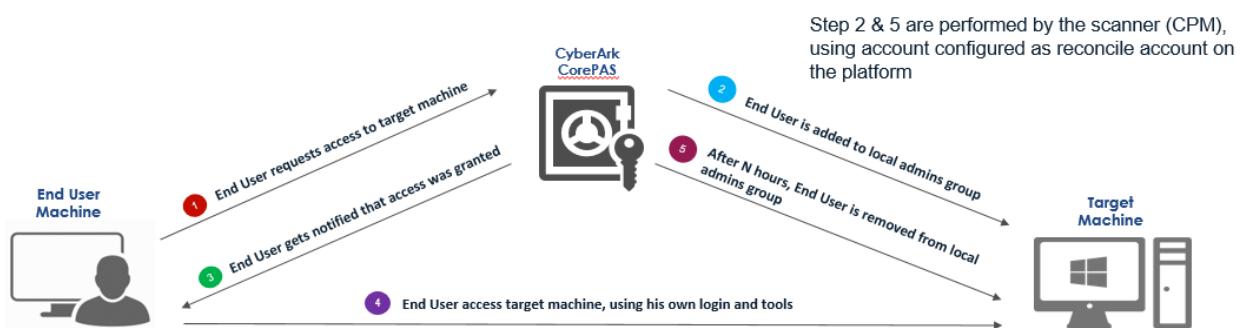
Ad Hoc Access

A major step in the Privilege Access Security program is to secure the Windows local administrators. This is essential to reduce the risk of lateral movement. CyberArk enables securing local administrator credentials, as well as using PSM to access those accounts.

There are cases, however, where managing the local administrator passwords is not possible at the initial stage of deployment, whether because of objection from the IT users, or other reasons. Ad hoc access allows you to smoothen out your local administrators' security. It can be used as an intermediate step towards full implementation of Vaulting the local administrators. You can grant Windows admins on-demand, ad hoc privileged access to Windows targets, for 4 hours.

During this time, domain users can request to access a system as local administrator. If authorized, the system temporarily adds the logged-on Windows users into the target system's local administrator group, without the need to manage the credentials of the local administrator on that target. This allows for a frictionless and lightweight solution that enables your organization to introduce privileged controls and help establish habitual security, before moving into a robust Privileged Access Security program.

The workflow, as exhibited in the following diagram, starts when an end user requests access to a designated ad hoc target machine, and is subsequently added to the local admin groups. The end user is notified that they have been granted access (or not), and once granted, is able to access the target machine using their own login for 4 hours. After this period, the user is automatically removed from the local admin group



In this exercise, you will set up Ad Hoc access for the Windows admin user (Bill), allowing Bill to be added to the local admin group on the target system for 4 hours.



Set up the Ad Hoc Access Platform

1. Log into the **PWAA** as **vaultadmin01**.
2. Go to **ADMINISTRATION > Platform Management**, and duplicate the *Windows Server Local Admins 45* Platform to a new platform called *Windows Servers AdHoc Access*. You may add description stating accounts associated with this platform are not managed by the **CPM**.

Duplicate Target Account Platform

Source Platform
Windows Server Local Admins 45

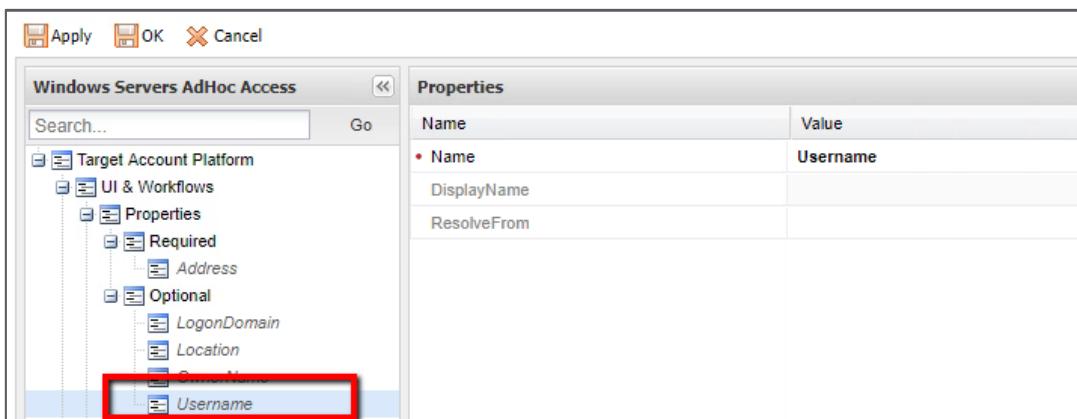
Duplicate to

Name
Windows Servers AdHoc Access

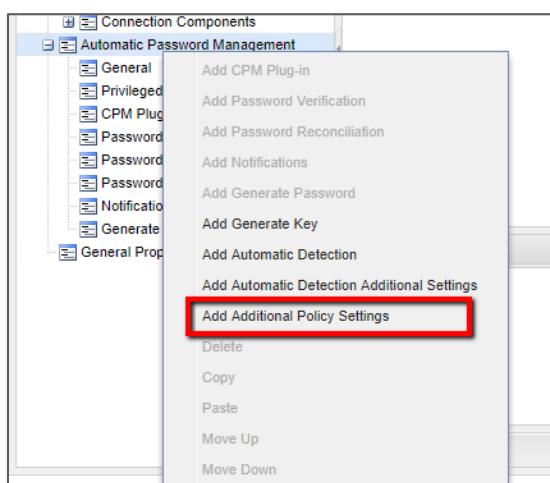
Description
Accounts associated with this platform will not be managed by the CPM

Save & Close Cancel

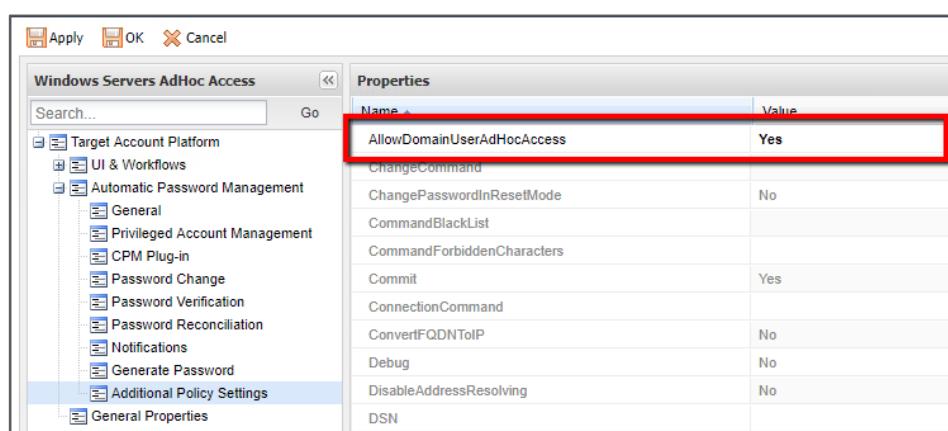
3. Click on **Edit** to edit the new platform. In the new platform set the following parameters to **NO**.
 - AllowManualChange
 - PerformPeriodicChange
 - VFAllowManualVerification
 - VFPerformPeriodicVerification
 - RCAccAllowManualReconciliation
 - RCAutomaticReconcileWhenUnsynced
4. In the new platform, go to **UI & Workflows > Properties**. Remove the *Username* property from *Required*, and add a new property called *Username* under *Optional*.



5. In the new Platform, right-click on **Automatic Password Management**, and select **Additional Policy Settings**.



6. Under **Additional Policy Settings**, set **AllowDomainUserAdHocAccess** to Yes.



Note: For Ad Hoc access, a Domain Account which is used as a reconcile account should be associated with the platform. In our case, this has already been defined in the base platform we duplicated: *Windows Server Local Admins 45*



Note: For security best practice, you need to limit the Safes that are required for ad hoc access, by setting the AllowedSafes parameter with a regular expression that lists the Safes that this platform can be applied to. This too has already been defined in the base platform we duplicated: *Windows Server Local Admins 45*

Add the Local Administrator Account

7. Go to Accounts View and click on Add Account. Add the local administrator account of the Target Windows server:

Store in Safe:	Win-Srv-Fin-US
System Type:	Windows
Platform Name:	Windows Server AdHoc Access
Address:	vfserver.cyber-ark-demo.local
User Name:	Administrator
Password:	Cyberark1
Confirm Password:	Cyberark1
Logon To (optional)	<click the Resolve button>

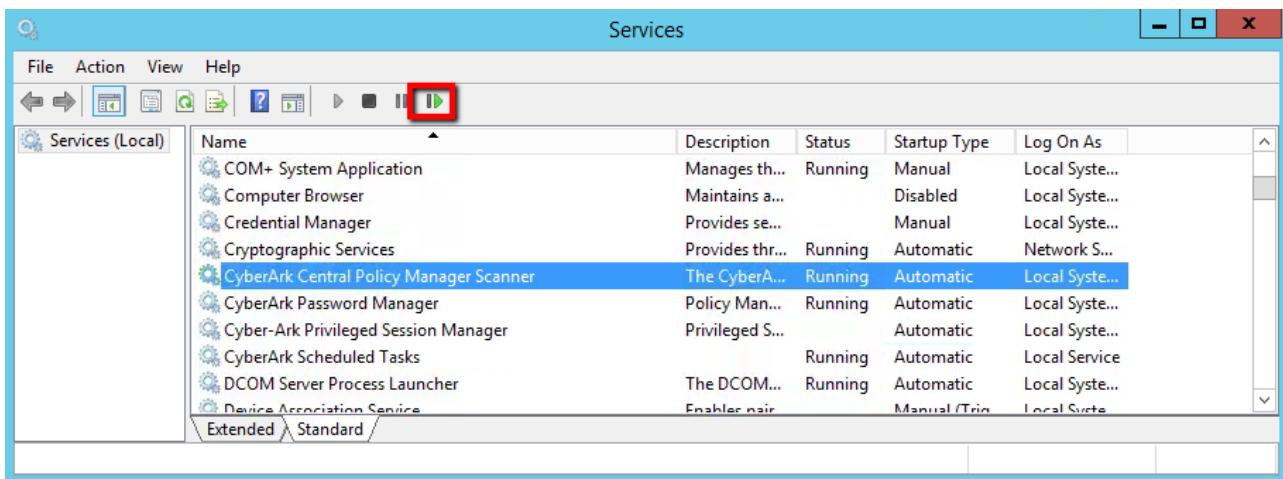
CPM Scanner Configuration

8. On the Comp01A server, navigate to C:\Program Files (x86)\CyberArk\Password Manager\Scanner. Using Notepad++, edit the **CACPMScanner.exe.config** using and add the following line:

- <add key="IsAdHocEnabled" value="true" />

```
1  <?xml version="1.0" encoding="utf-8"?>
2  <configuration>
3      <configSections>
4          <section name="quartz" type="System.Configuration.NameValueSectionHandler, System, Version=1.0.5000.0,Culture=neutral, PublicKeyToken=b03f5f7f1434493e" />
5      </configSections>
6      <quartz>
7          <add key="quartz.scheduler.instanceName" value="ScannerScheduler" />
8          <add key="quartz.threadPool.type" value="Quartz.Simpl.SimpleThreadPool, Quartz" />
9          <add key="quartz.threadPool.threadCount" value="1" />
10         <add key="quartz.jobStore.type" value="Quartz.Simpl.RAMJobStore, Quartz" />
11     </quartz>
12     <appSettings>
13         <add key="IsAdHocEnabled" value="true" />
14         <add key="VaultFile" value="C:\Program Files (x86)\CyberArk\Password Manager\Vault\Vault.ini" />
15         <add key="ConfigurationCredentialFile" value="C:\Program Files (x86)\CyberArk\Password Manager\Vault\User.ini" />
16         <add key="LogFolder" value="C:\Program Files (x86)\CyberArk\Password Manager\Logs\" />
17         <!-- Valid values: "" - use temp folder -->
18         <add key="MultiLingualSupport" value="No" />
19         <!-- DNA configuration -->
20         <add key="MaxThreadNumber" value="10" />
```

9. Save the file and then restart the CPM Scanner service.

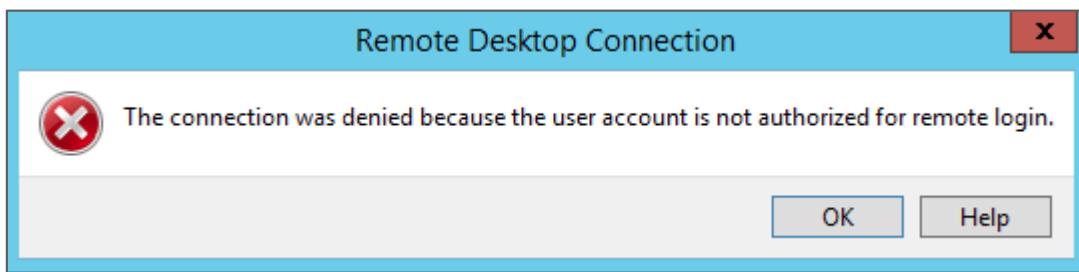


Test Ad Hoc Access

- First, open MSTSC and attempt to connect to the target windows machine as cyber-ark-demo\bill.



- You should receive an error stating that bill is not authorized for remote login:



- Next, login to the PVWA as Bill. Search for the Target Windows local Administrator account and click on **Get Access**. If you configured everything successfully, you should receive a notification saying you've been granted admin access for 4 hours.

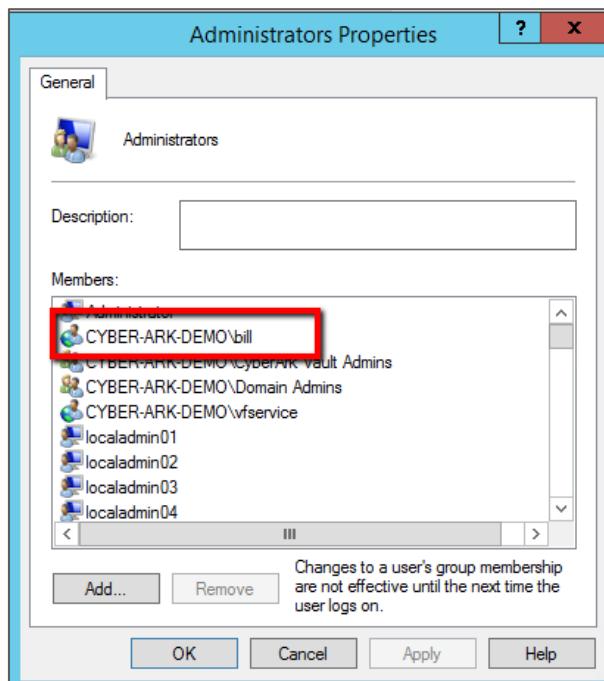


The screenshot shows the CyberArk Accounts View interface. At the top, a green banner displays the message: "You have been successfully granted access on target machine vfserver.cyber-ark-demo.local for 4 hours". Below the banner, the title bar says "Accounts View" and "administrator". The left sidebar has sections for "My accounts", "All accounts (default)", "Recently used", "Favorites", and "Checked-out". On the right, there's a "Status" section showing "Disabled by CPM", "Failed", "Newly added", and "Disabled by user". The main area lists "2 results for: administrator":

Star	Status	Username	Address	Platform ID	Safe	Access Request
Star	⚡	Administrator	vfserver.cyber-ark-demo.local	WindowsServersAdHocAccess	Win-Srv-Fin-US	-
Star	-	localadmin02	VFSERVER.cyber-ark-demo.local	WindowsServerLocalAdmins45	Win-Srv-Fin-US	-

For the first result (Administrator), there are buttons for "Get access", "Connect", and "...". A red box highlights the "Get access" button.

13. Now try to launch another RDP connection to the Target Windows server as cyber-ark-demo\bill. You should be able to login this time.
14. After successfully connecting to the Target Windows server, go to Computer Management > Local Users and Groups > Groups and open the local Administrators group. Verify that cyber-ark-demo\bill was added to the group.



15. Disconnect from the Target Windows server.

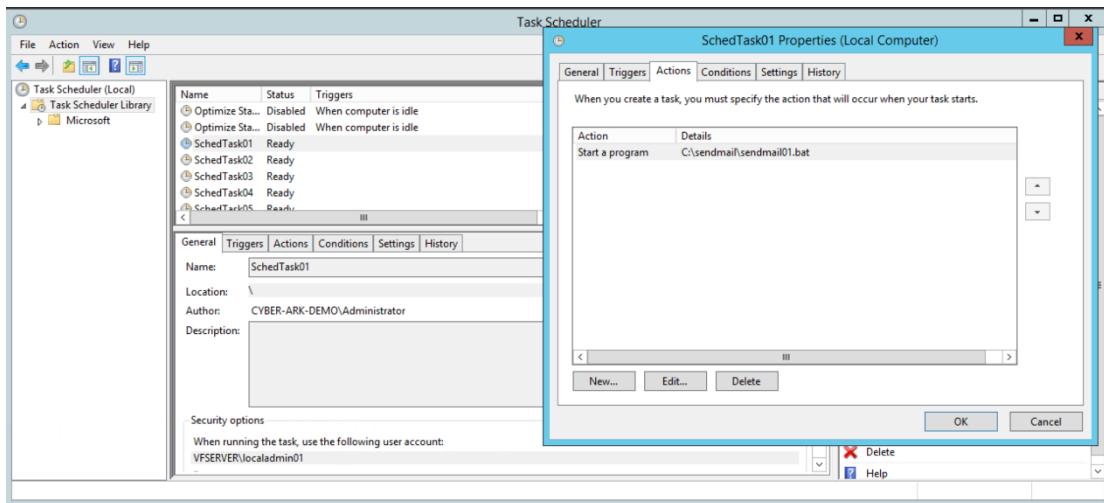


Usages

Manage a Scheduled Task Usage

In this exercise, you will configure a usage, which allows you to manage applications (services, scheduled tasks) that are dependent on the main account.

The virtual machine “Target Windows” (vfserver - 10.0.10.50) server contains a scheduled task, **SchedTask01**. The scheduled task is configured to send an email to the **vaultadmin01** account every time it is run.



We will be using the **localadmin01** account for testing. We will modify the **MinValidityPeriod** setting so that the password does not change while we are trying to use it by resetting it to its default value.

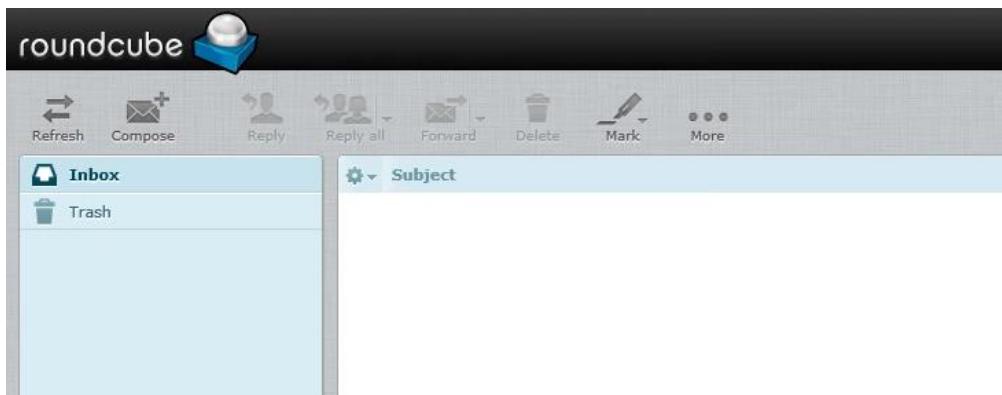
1. Logged in to the **PVWA** as **vaultadmin01**, navigate to **Administration > Platform Management**, select **Windows Server Local Admins 45** platform and press **Edit**
2. Go to **Automatic Password Management > Privileged Account Management** and change **MinValidityPeriod** to **60**.
3. Press **Apply** and **OK**.
4. To test the scheduled task, run the following command from a command prompt.

```
scftasks /run /s 10.0.10.50 /tn SchedTask01
```



```
C:\>Administrator: Command Prompt
C:\>Administrator>
C:\>Administrator>
C:\>Administrator>
C:\>Administrator>
C:\>Administrator>
C:\>Administrator>
C:\>Administrator>
C:\>Administrator>
C:\>Administrator>
C:\>Administrator>sc tasks /run /s 10.0.10.50 /tn SchedTask01
SUCCESS: Attempted to run the scheduled task "SchedTask01".
C:\>Administrator>
```

5. Because the *localadmin01* account password was changed in an earlier exercise without accounting for the associated scheduled task, **the scheduled task will not run properly (even though the return message says “SUCCESS”)**. You can confirm that the schedule task did not complete properly by checking your email client as *vaultadmin01@cyber-ark-demo.local* and seeing that you do not have any messages referring to “scheduled task”.



6. Now, go to the *localadmin01 Account Details* and locate the *Scheduled Task* tab. Press **Add**.



The screenshot shows the CyberArk Privileged Access Security administration interface. On the left, there's a sidebar with various icons. The main area has two tabs: 'Account Details' and 'Scheduled Task'. The 'Account Details' tab is active, showing account information for 'Windows Server Local Admins 45'. The 'Scheduled Task' tab is also visible. At the top right, there are buttons for 'Add SSH Key', 'Add Account', and 'Customize'.

7. Enter **SchedTask01** in the *Task Name* field and enter **vfserver** in the *Address* field. Press **Save**.

Privileged Account Windows Server Local Admins 45-localadmin01
Scheduled Task

Required Properties:

Task Name:	<input type="text" value="SchedTask01"/>
Address:	<input type="text" value="vfserver"/>

Optional Properties:

<input type="checkbox"/> Task Folder:	<input type="text"/>
<input type="checkbox"/> Disable automatic management for this account	<input type="text"/>

Note: Reason:

Buttons: Save | Cancel

8. After pressing **Save**, click on the newly created scheduled task.

Note: The *localadmin01* account cannot update the scheduled task remotely, so you will associate the usage with a domain account that contains the required privileges to act as the logon account.

9. We are now looking at the Account Details for the Scheduled Task. Press the **Associate** button.



The screenshot shows the CyberArk Admin interface. On the left, there's a sidebar with various icons. The main area is titled "Account Details" and shows details for a "Scheduled Task". The "Logon Account" section has three buttons: "Clear", "Associate", and "Create New". The "Associate" button is highlighted with a red box.

10. Select **cybrreconcile** and press **Associate** to associate the scheduled task with the **cybrreconcile** domain account as a logon account.

The screenshot shows the "Associate Account" dialog box. It has a search bar at the top. Below it is a table titled "Recently" with columns: Username, Address, Safe, and Platform ID. The table lists several accounts, including "admin01" which is selected. At the bottom right of the dialog box, the "Associate" button is highlighted with a red box.

Username	Address	Safe	Platform ID
admin01	cyber-ark-demo.local	Win-Dom-Admins	WindowsDomainAdmins15
dba01	10.0.0.20	Oracle Finance	OracleDBA30
localadmin01	vfserver.cyber-ark-demo.local	Win-Srv-US	WindowsServerLocalAdmins45
logon01	10.0.0.20	Linux Finance	LinuxviaSSH30
root	10.0.0.21	Linux2	LinuxviaSSH30
root01	10.0.0.20	Linux Finance	LinuxviaKEY90
root02	centos-target01	Linux Finance	LinuxviaSSH30
user01	10.0.0.20	Linux Finance	LinuxviaSSH30

11. Next, go back to the **localadmin01 Account Details** window and change the **localadmin01** password.
12. Select *Change the password immediately (by the CPM)* and press **OK**.
13. Wait for the **localadmin01** password to change.



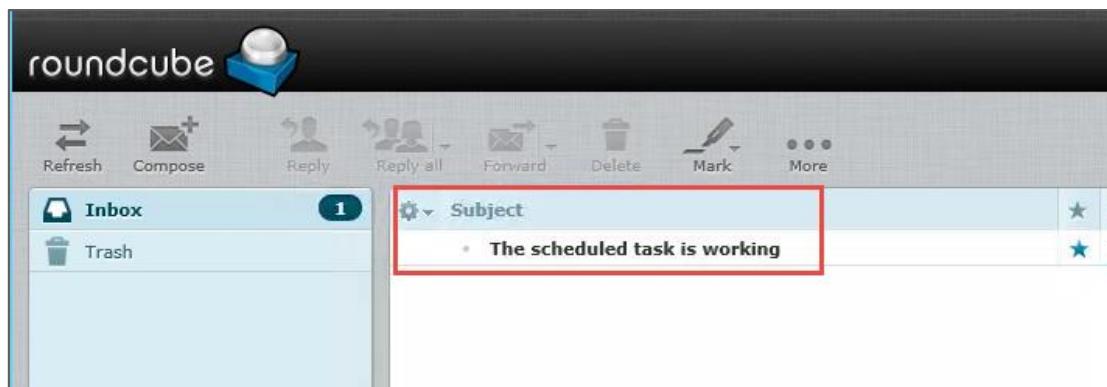
Note: The scheduled task is associated with a different platform than the *localadmin01* account. After the *localadmin01* account has been changed, the flag will be set for the scheduled task to be changed. The entire process could take in excess of 10 minutes to complete.

14. After the Windows password has been changed, select the scheduled task and open the Account Details. You will see that the usage password is now scheduled for immediate change.
15. Wait for the usage password to change and then re-run the scheduled task from the command prompt.

The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The command entered was "schtasks /run /s 10.0.10.50 /tn SchedTask01". The output indicates two successful attempts to run the task: "SUCCESS: Attempted to run the scheduled task "SchedTask01"" and "SUCCESS: Attempted to run the scheduled task "SchedTask01"".

```
C:\>C:\>C:\>C:\>C:\>C:\>C:\>C:\>Administrator>schtasks /run /s 10.0.10.50 /tn SchedTask01
SUCCESS: Attempted to run the scheduled task "SchedTask01".
C:\>Administrator>schtasks /run /s 10.0.10.50 /tn SchedTask01
SUCCESS: Attempted to run the scheduled task "SchedTask01".
C:\>
```

16. Now check your email. You should receive a message stating that “The scheduled task is working”.





Managing a Configuration File Usage

In this exercise you will be using a usage to update a password in a text file whenever the specified account's password is changed.

The file *app01.ini* is located on the Linux server IP address 10.0.0.20 in the */var/opt/app* directory.

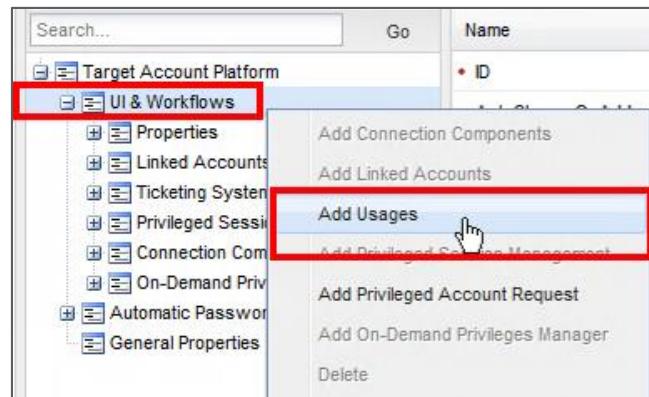
```
[Startup]
Product=App Server
ProductGUID=b1f0850-d1c7-11d3-8e83-0000e8efafe3
CompanyName=Acme
CompanyURL=www.acmeiincv.com
MediaFormat=1
LogMode=1
SmallProgress=N
SplashTime=
CheckMD5=Y
CmdLine=
ShowPasswordDialog=N
ScriptDriven=4

[Languages]
Default=0x0409
Supported=0x0409
RequireExactLangMatch=0x0404,0x0804
RTLLangs=0x0401,0x040d

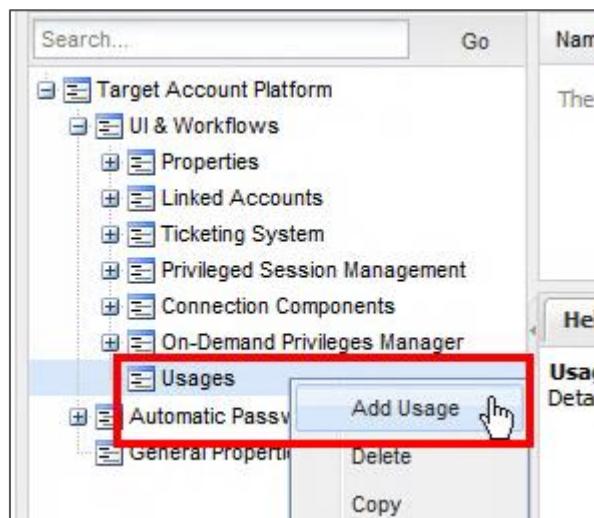
[Server]
Hostname=DBServer01
Password=Cyberark1

[Database]
Db=MySQL
Port=3306
```

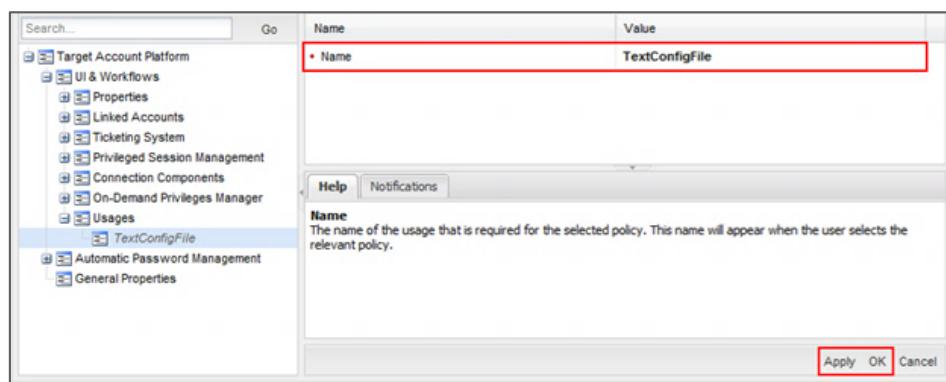
1. On your **Components** server, log in to the **PWAs** as *vaultadmin01*.
2. Navigate to the **ADMINISTRATION** tab and click **Platform Management**.
3. Select *Linux via SSH 30* and press **Duplicate**. Enter *Linux Apps via SSH 90* as the name and click **Save**.
4. Select the newly-created platform and choose **Edit**.
5. Go to **Automatic Password Management > General**, set *SearchForUsages* to Yes and press **Apply**.
6. Right-click **UI & Workflows** and choose **Add Usages**.



7. After selecting **Add Usages**, you will have a new ‘Usages’ entry at the end of the *UI & Workflows* section. Right click **Usages** and select **Add Usage**.



8. Enter *TextConfigFile* as the **Value**. Press **Apply** and **OK**.



9. In the interest of good practice, create a dedicated Safe for this purpose called **Linux Apps**.



10. Go to **ACCOUNTS** and press **Add Account** and enter the following:

Store in Safe:	Linux Apps
Device Type:	Operating System
Platform Name:	Linux Apps via SSH 90
Address:	10.0.0.20
User Name:	app-account01
Password:	Cyberark1
Confirm Password:	Cyberark1

11. Press **Save**.

12. Go to the **Text Config File** tab and press **Add**.

The screenshot shows the CyberArk Admin interface. On the left, the 'Account Details' page is displayed, showing account information such as Address (10.0.0.20), User Name (app-account01), and Platform Name (Linux Apps via SSH 90). On the right, the 'Text Config File' tab is selected in the navigation bar. A red box highlights the 'Add' button in the toolbar of this tab.

Note: This tab is visible because we activated the *TextConfigFile Usage* in the platform with which this account is associated.

13. Enter the following:

Address:	10.0.0.20
File Path:	/var/opt/app/app01.ini
Password Regex	Password=(.*)
Connection Type:	SSH

14. Press **Save**.



Privileged Account Linux Apps via SSH 90-app-account01-10.0.0.20: Add Text Config File

Required Properties:

Address:	10.0.0.20
File Path:	/var/opt/app/app01.ini
Password Regex:	Password=(.*)
Connection Type:	SSH

Optional Properties:

<input type="checkbox"/> Port:	
<input type="checkbox"/> Backup Password File:	[Select]
<input type="checkbox"/> Usage Display Name:	

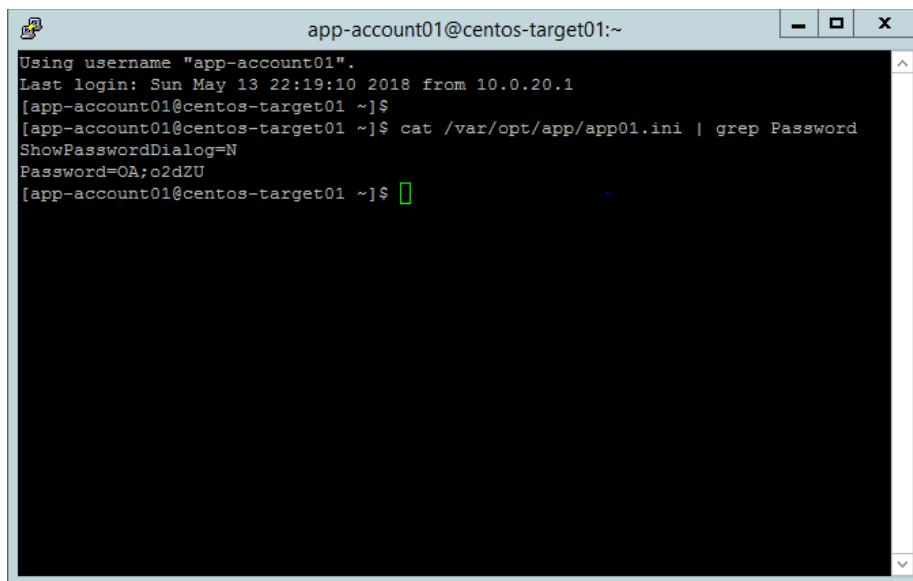
Disable automatic management for this account
Reason:

Buttons: Save Cancel

15. Go to the **Account Details** for the primary account (*app-account01*), click the **Change** button page.

Note: This process can take several minutes to complete. The usage has interval settings, just like the account. When the account changes, it scans the vault for usages, marks those usages for change, and then, according to those intervals, the changes take effect. So it will be a few minutes between when the password changes and the file changes.

16. After the password change is complete, connect to 10.0.0.20 with the *app-account01*.
17. Enter the following:
`cat /var/opt/app/app01.ini | grep Password`
You should see that the password matches the new password in the **Vault**.



```
Using username "app-account01".
Last login: Sun May 13 22:19:10 2018 from 10.0.20.1
[app-account01@centos-target01 ~]$
[app-account01@centos-target01 ~]$ cat /var/opt/app/app01.ini | grep Password
ShowPasswordDialog=N
Password=OA;o2dZU
[app-account01@centos-target01 ~]$
```



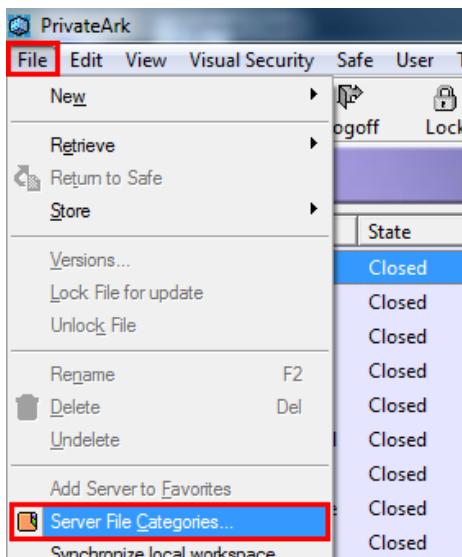
Custom File Categories

File category is the CyberArk term for the attributes or fields available on accounts (Address, User Name, etc.). This section will detail the steps required to create and use custom file categories, allowing you to categorize accounts based on your organization's requirements.

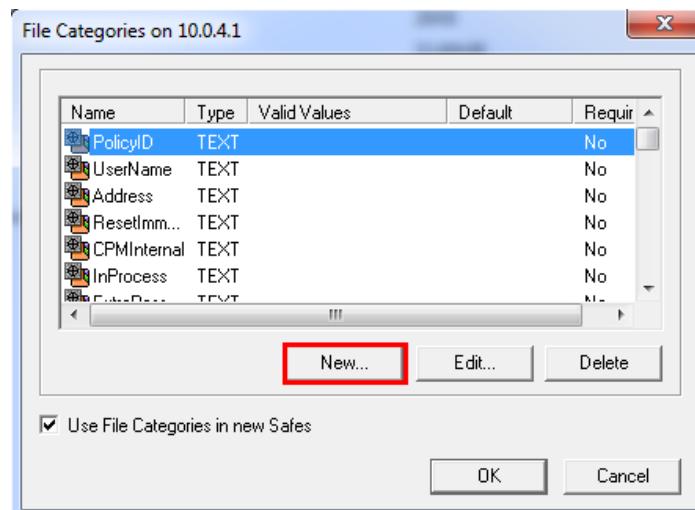
In this final exercise, we will create a custom file category called *BusinessUnit* and provide a list of possible choices: *International*, *Retail*, and *Corporate*. We will then modify our Oracle platform so that when users add new accounts, they will be required to associate the new account with one of these business units. Finally, we will make the new parameter searchable within the **PVWA** and, of course, we will test what we have done.

Creating the Custom File Category

1. Using the **Components** server, from the **PrivateArk Client**, log onto the **Vault** and go to **File > Server File Categories**.



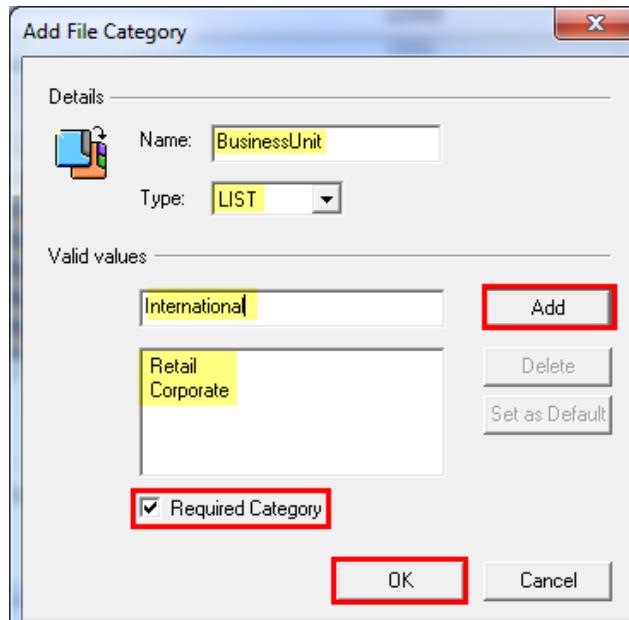
2. Press the **New...** button.



3. In the *Add File Category* window, enter the following:

Name:	<i>BusinessUnit</i>
Type:	<i>List</i>
Valid values:	<i>International, Retail, and Corporate</i>

4. After each value is added, select the *Required Category* checkbox and click **OK**.



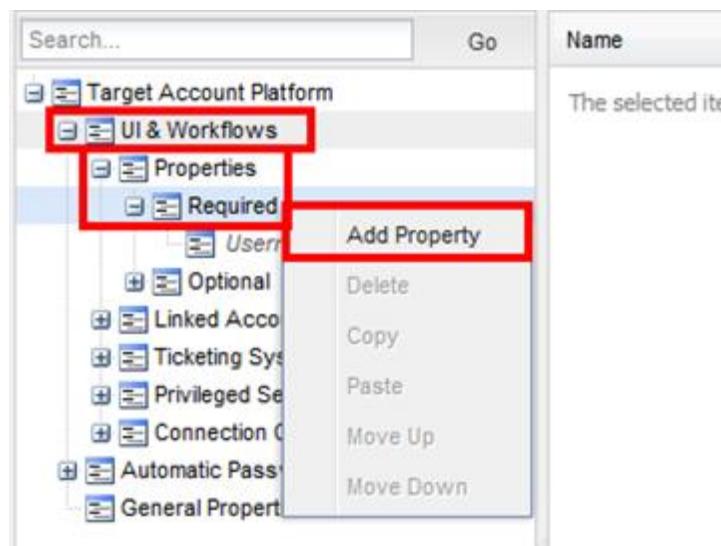
5. Log out of the **PrivateArk Client**.



Adding the Custom File Category to the Platform

Now we'll make the new **BusinessUnit File Category** a required field for accounts assigned to the *Oracle DBA 30* platform.

1. Log into the **PVWA** as *vaultadmin01*.
2. Go to the **ADMINISTRATION** tab and click **Platform Management**.
3. Highlight *Oracle DBA 30* and press **Edit**.
4. Go to **UI & Workflows > Properties > Required**. Right-click and select **Add Property** from the context menu.



5. Enter **BusinessUnit** in the **Name** field and press **Apply** and **OK**. This will make **BusinessUnit** a required field on any accounts attached to the *Oracle DBA 30* policy.



The screenshot shows the CyberArk Admin interface. The top navigation bar has tabs: POLICIES, ACCOUNTS, APPLICATIONS, REPORTS, ADMINISTRATION, and a user dropdown set to 'vaultadmin01'. The main content area is titled 'Oracle DBA 30' with a search bar and a tree view of account properties. A red box highlights the 'Name' field in the 'Properties' table, which contains the value 'BusinessUnit'. Below the table is a help section for 'DisplayName'. At the bottom right are 'Apply', 'OK', and 'Cancel' buttons.

Making the File Categorical Searchable

Now we will make the new *BusinessUnit* file category searchable.

1. Go to **ADMINISTRATION > Options**.
2. Right-click on **Search Properties** and select **Add Property**.

The screenshot shows the CyberArk Admin interface. The top navigation bar has tabs: POLICIES, ACCOUNTS, APPLICATIONS, REPORTS, ADMINISTRATION, and a user dropdown set to 'vaultadmin01'. The main content area is titled 'Options' with a search bar and a tree view of configuration items. A red box highlights the 'Search Properties' item under 'PIM Suite Configuration'. A context menu is open over 'Search Properties', with 'Add Property' highlighted. Other options in the menu include Delete, Copy, Paste, Move Up, and Move Down. To the right is a 'Properties' table with one row: Name (Value: BusinessUnit). A note says 'The selected item exposes no properties. Please choose another item.'

3. Enter *BusinessUnit* in the **Name** field and press **Apply** and **OK**. This will allow the new file category to be searchable.



The screenshot shows the 'Properties' dialog box from the CyberArk PVWA interface. On the left, a tree view lists various properties like DSN, Database, ServiceName, etc. The 'Name' property is selected in the main pane, showing its current value as 'BusinessUnit'. At the bottom right, there are 'Apply', 'OK', and 'Cancel' buttons, with 'OK' being highlighted by a red box.

4. Sign out of the **PVWA** session.
5. Run the restart-services batch file on the **Components** server Desktop.

Testing the New File Category

1. Login to the **PVWA** as **vaultadmin01**, go to the **ACCOUNTS** tab and open the **dba01** account.
2. Click on the **Edit** button. Select *Retail* and press **Save**.

Edit Account: Oracle DBA 30-dba01-10.0.0.20

Store in Safe:	Oracle Finance
Device Type:	Database
Platform Name:	Oracle DBA 30
Required Properties:	
Username:	dba01
Business Unit:	Change to: Retail
Optional Properties:	
<input type="checkbox"/> DSN (ODBC):	Change to: <input type="text"/>
<input checked="" type="checkbox"/> Address:	10.0.0.20
<input checked="" type="checkbox"/> Port:	1521
<input checked="" type="checkbox"/> Database:	xe
Change to: <input type="text"/>	
<input type="checkbox"/> Disable automatic management for this account Reason: <input type="text"/>	

[Show advanced section](#)

Save **Cancel**

3. Enter *retail* in the Search field on the **ACCOUNTS** tab and press **Go**.



	Username	Address	Safe	Platform ID
<input type="checkbox"/>	dba01	10.0.0.20	Oracle Finance	OracleDBA30

4. dba01 should be returned based on the new file category.