CYBERARK UNIVERSITY

CPM and PVWA

CyberArk Training

OBJECTIVES

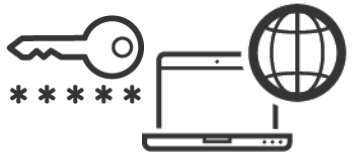
By the end of this lesson, you will be able to:

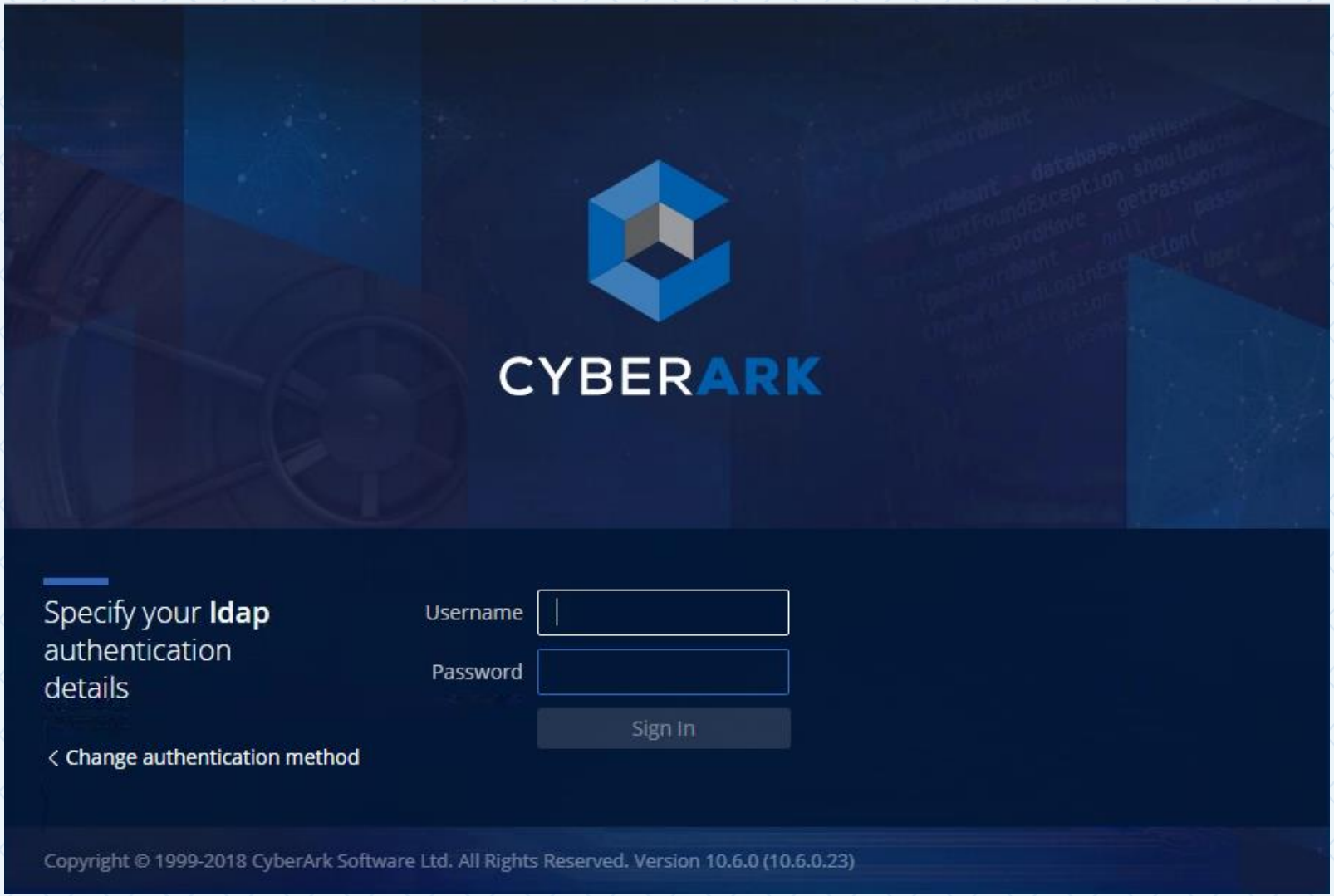
- Describe the main functionality of the CPM and PVWA
- How to Install the CPM and PVWA
- How to Secure and Harden the CPM and PVWA

PVWA AND CPM FUNCTIONALITY

PASSWORD VAULT WEB ACCESS

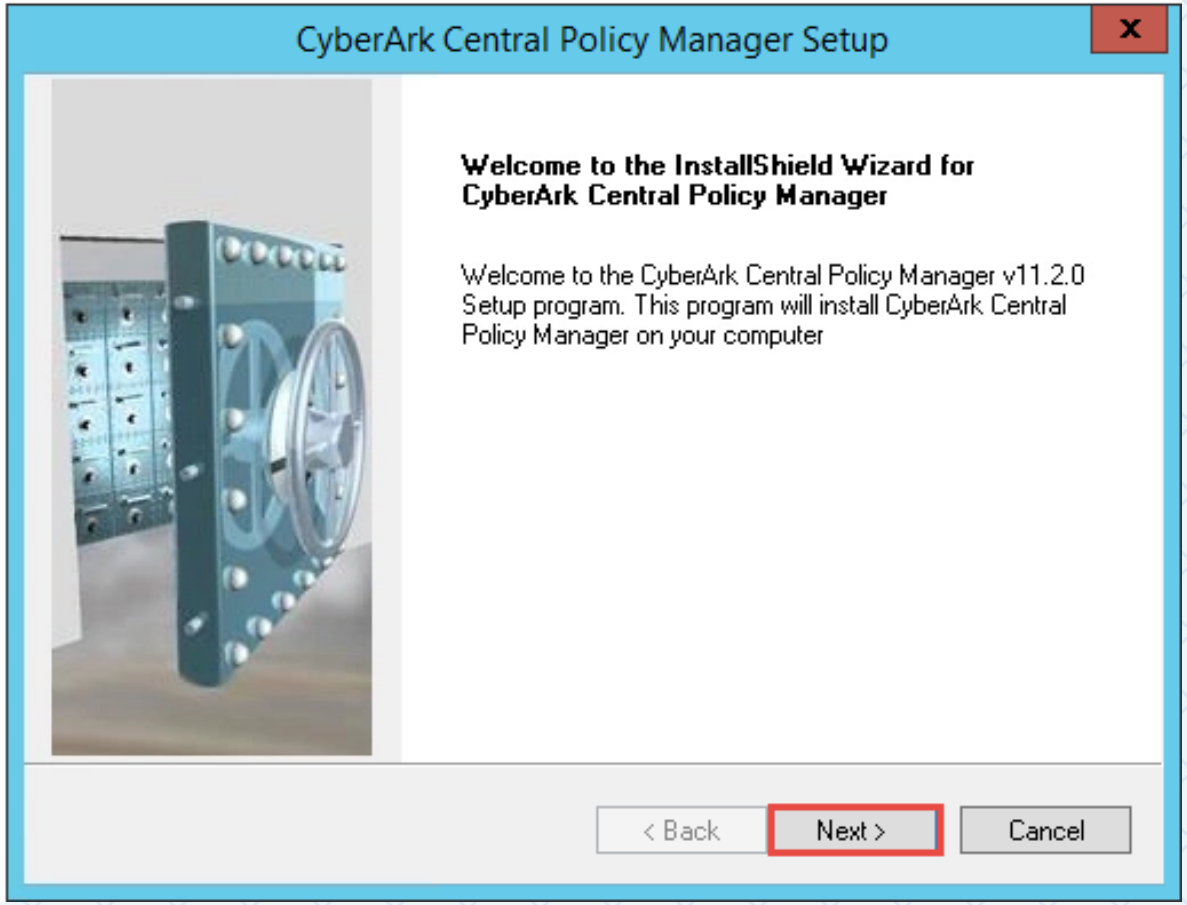
- The **Password Vault Web Access** (PVWA) must be installed first after the Digital Vault
- The **PVWA** enables both end users and administrators to access and manage privileged accounts
- **PAS Component** configurations are accomplished via the **PVWA**



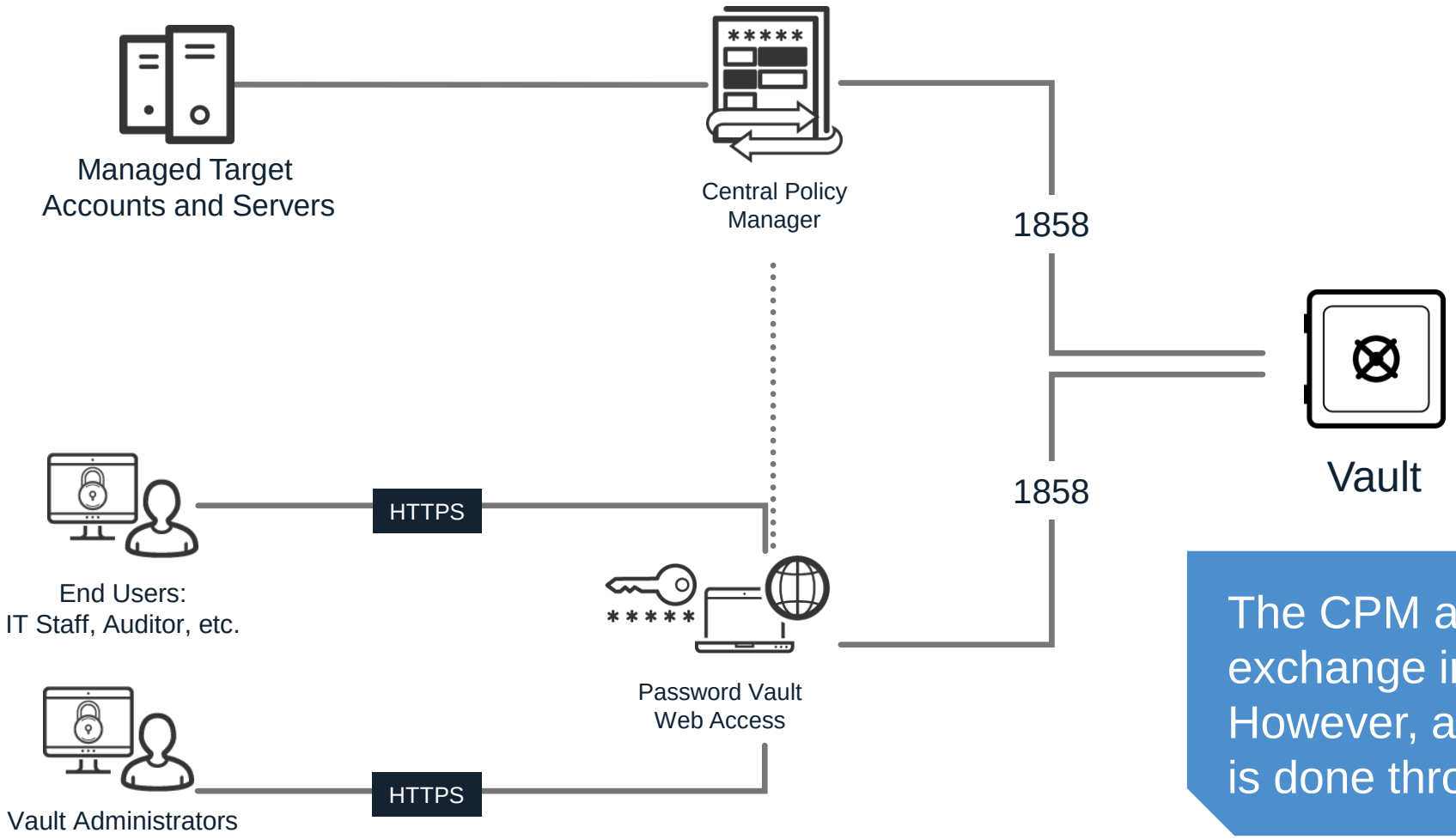


CENTRAL POLICY MANAGER

- The **CPM** is responsible for:
- Password Management Operations
  - Changing and verifying all target account password
  - Enforces Password Policy
- The **CPM** Accounts Feed and Auto-Detection Operations
  - Discovery – Designed to quickly locate critical accounts and credentials
  - Analyze – Provides a view to assess the risk of each account
  - Provision – Accounts can be provisioned in the Vault in a simple and intuitive way



COMPONENT COMMUNICATION – CPM AND PVWA



The CPM and the PVWA exchange information. However, all the communication is done through the Vault.

PVWA INSTALLATION

PRE-INSTALL TASKS

Pre-install tasks	Installation	Post-install tasks	Hardening
Review requirements	Run the PVWA installation script	Check installation log files	Run the hardening script
Close applications & log on	Registration (connect to the Vault)	Check user permissions on web server	Apply post hardening configurations
Run prerequisites script		Add restrictions to credentials file	*Harden server in a Domain environment
		Set API throttling	*Only perform this task if your PVWA server is part of a domain

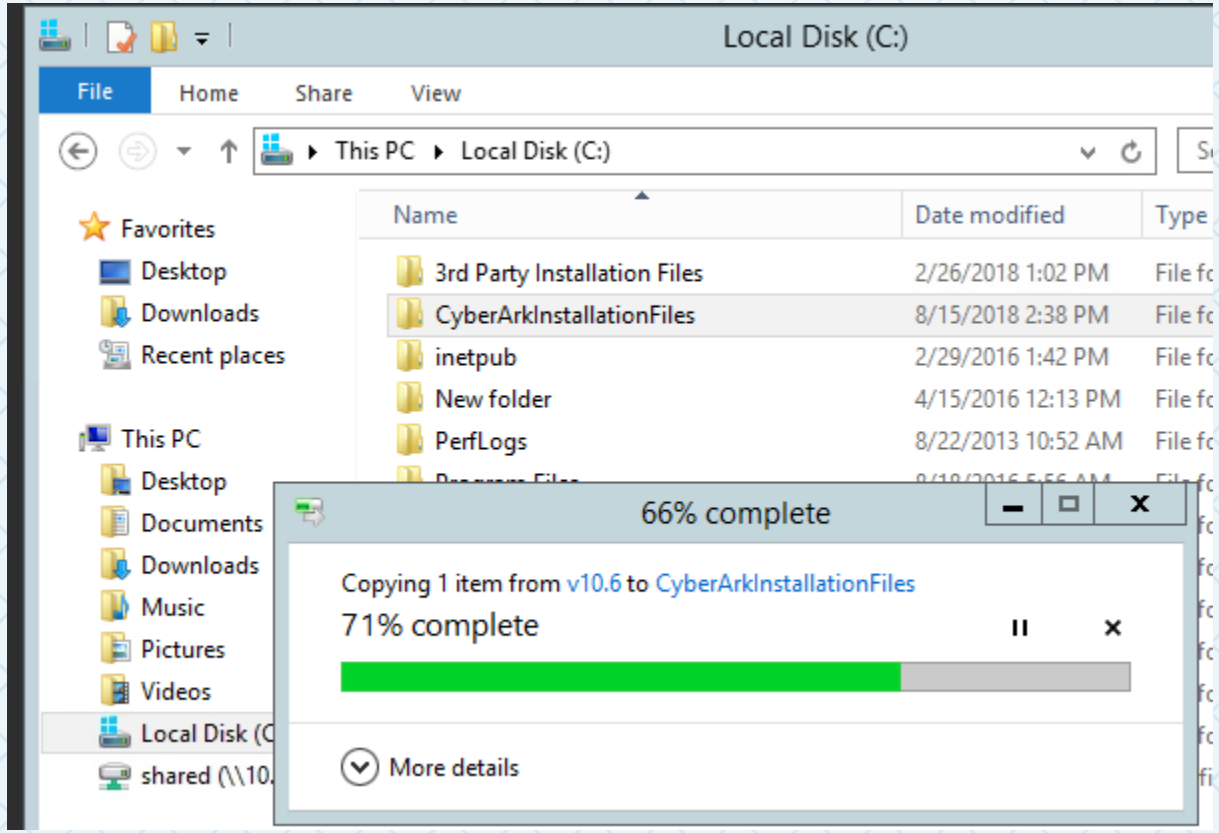
RECOMMENDED PVWA SERVER SPECIFICATIONS

- PVWA must be the first CyberArk PAM component installed after the Digital Vault
- PVWA is supported on the following Windows Platforms
  - Windows 2019
  - Windows 2016
  - Windows 2012 R2
- .NET Framework 4.8 must be installed
- Password Vault Web Access can be installed on virtual hosts such as VMWare, Hyper-V and KVM.
- It is recommended to use the Vault's built-in Administrator to install the PVWA

Small implementation (<1,000 managed passwords)	Mid-range implementation (1,000-20,000 managed passwords)	Large implementation (20,000 – 100,000 managed passwords)	Very large implementation (more than 100,000 managed passwords)
Hardware specifications			
· Quad core processor (Intel compatible) · 8GB RAM · 2X 80GB SATA/SAS hot-swappable drives · RAID Controller · Network adapter (1Gb) · DVD ROM	· 2X Quad core processor (Intel compatible) · 16GB RAM · 2X 80GB SATA/SAS hot-swappable drives · RAID Controller · Network adapter (1Gb) · DVD ROM	· 2X Eight core processors (Intel compatible) · 32GB RAM · 2X 80GB SAS hot-swappable drives · RAID Controller · Network adapter (1Gb) · DVD ROM	· 4X Eight core processors (Intel compatible) · 64GB RAM · 2X 80GB SAS hot-swappable drives · RAID Controller · Network adapter (1Gb) · DVD ROM
Software prerequisites			
· Windows 2019, Windows 2016, Windows 2012 R2 (Standard and Datacenter) · IIS 10.0, 8.5 · .NET Framework 4.8 · Internet Explorer 11.0 · Chrome (any version released in the last six months on Windows and Linux/UNIX) · Firefox (any version released in the last six months on Windows and Linux/UNIX) Not supported for the Monitoring module. · PVWA can be installed on Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platforms			

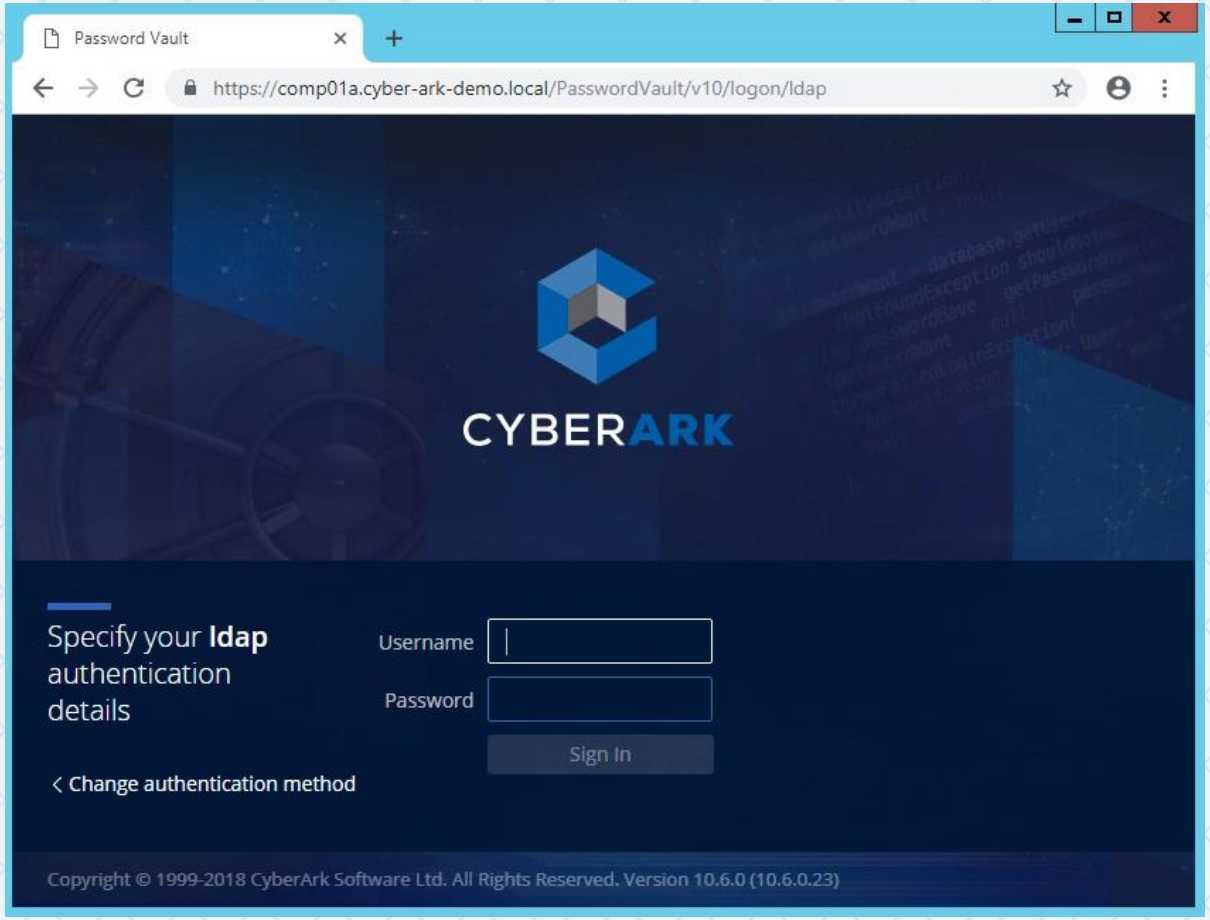
PVWA INSTALL PREPARATION

- Copy all necessary files to the Windows Component Server
- Extract zip files locally and close all applications before running PVWA setup
- Do not attempt to launch the setup or PowerShell scripts from a shared network drive.
- Always launch setup from a local drive.



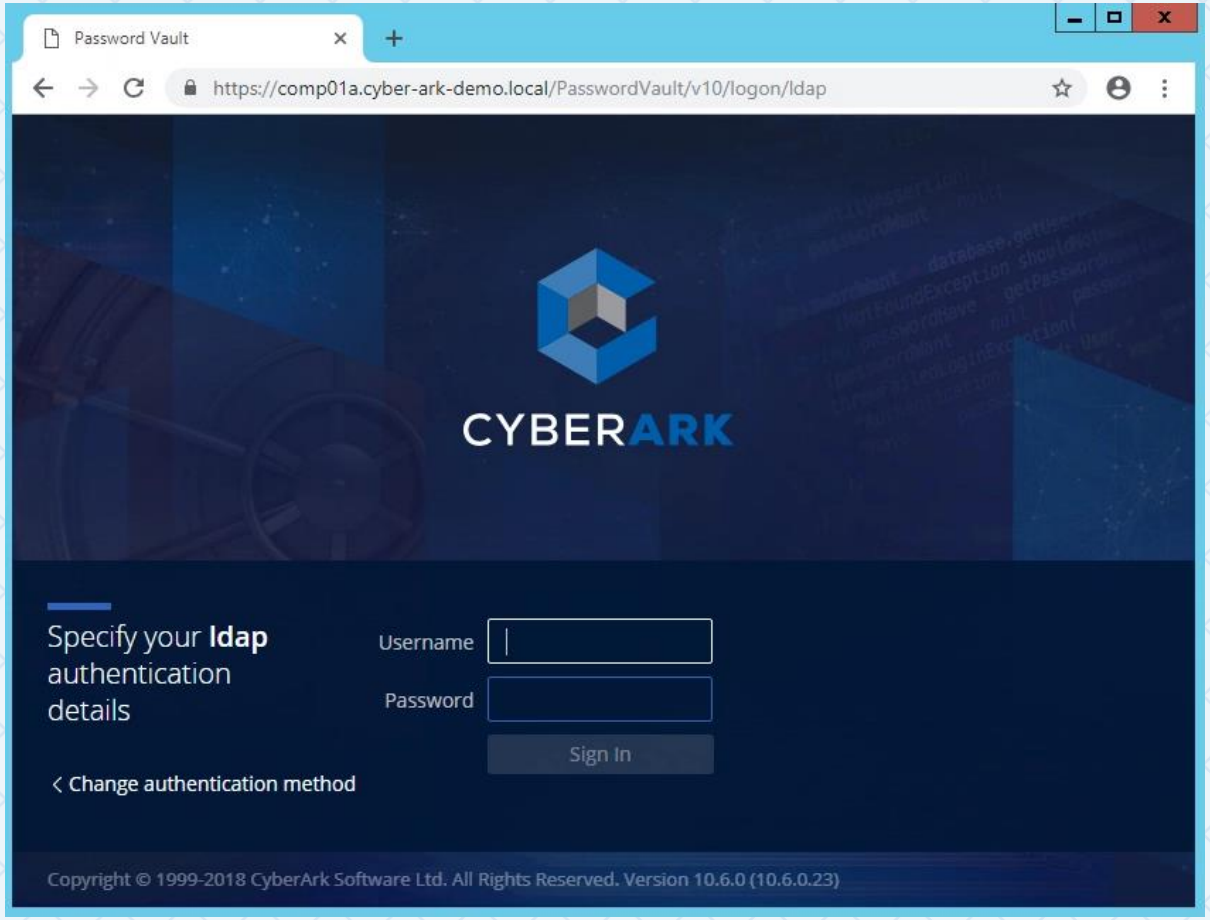
INSTALLATION AUTOMATION

- CyberArk recommends using Installation Automation deployment scripts provided with the installation package to automatically install and configure the Core PAS components servers, according to your organizational requirements
- What do the scripts do?
  - Install Microsoft Internet Information Services (IIS)
  - Install the PVWA component software
  - Implement hardening procedures on the Component Servers
- More information is available online at [PVWA Installation overview]



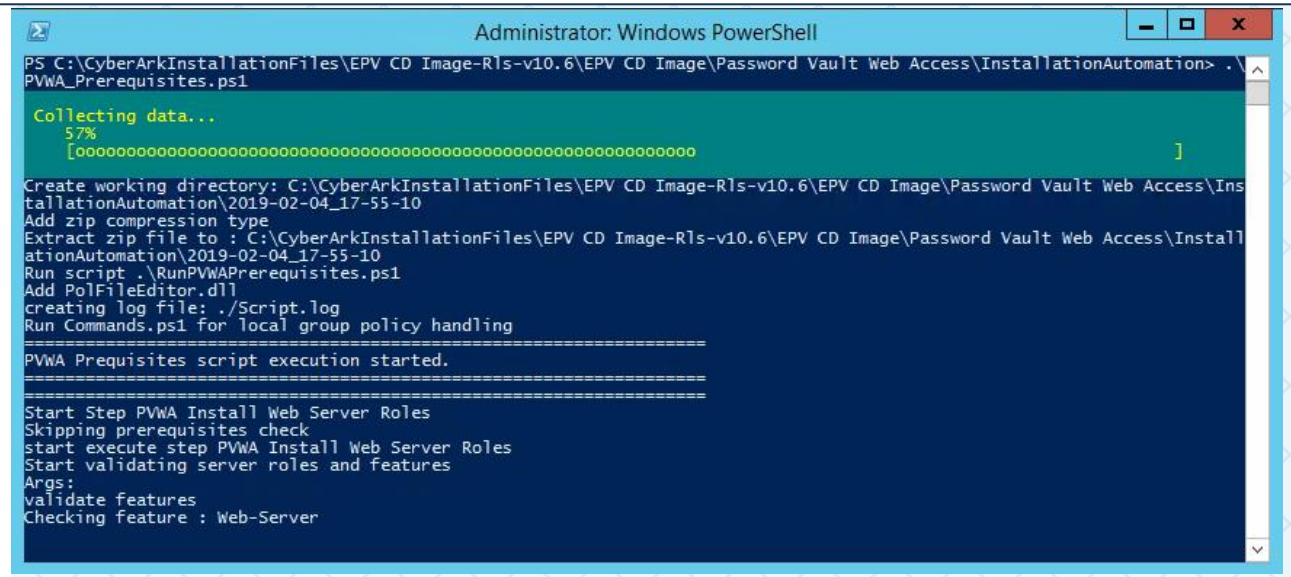
RUN PREREQUISITES SCRIPT

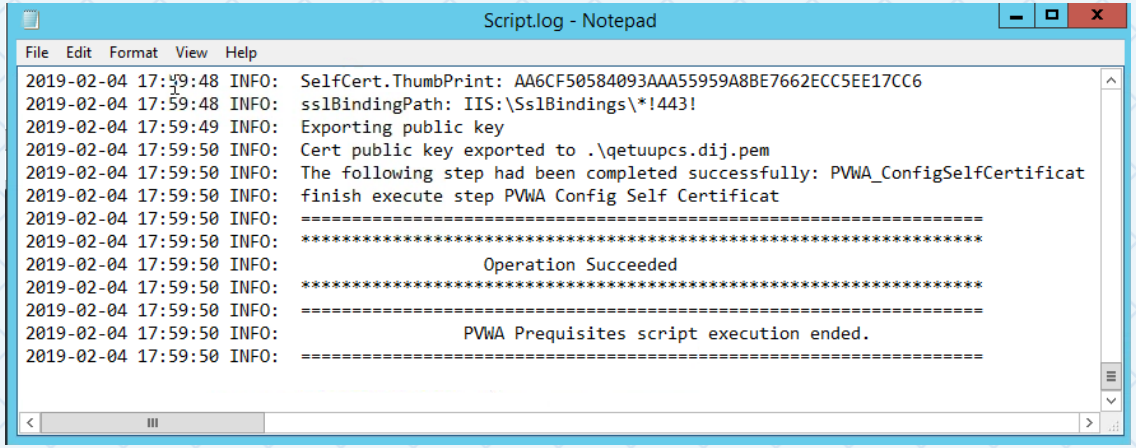
- The PVWA_Prerequisites script automates and performs the following tasks:
  - Verifies .NET version
  - Installs Web server roles, for details, see [Web server roles]
  - Disables IPv6
  - Configures a self signed certificate
  - Sets IIS SSL/TLS configuration
- You can choose which tasks are performed by editing the PVWA_Prerequisites_Config.xml file.



RUN PREREQUISITES SCRIPT

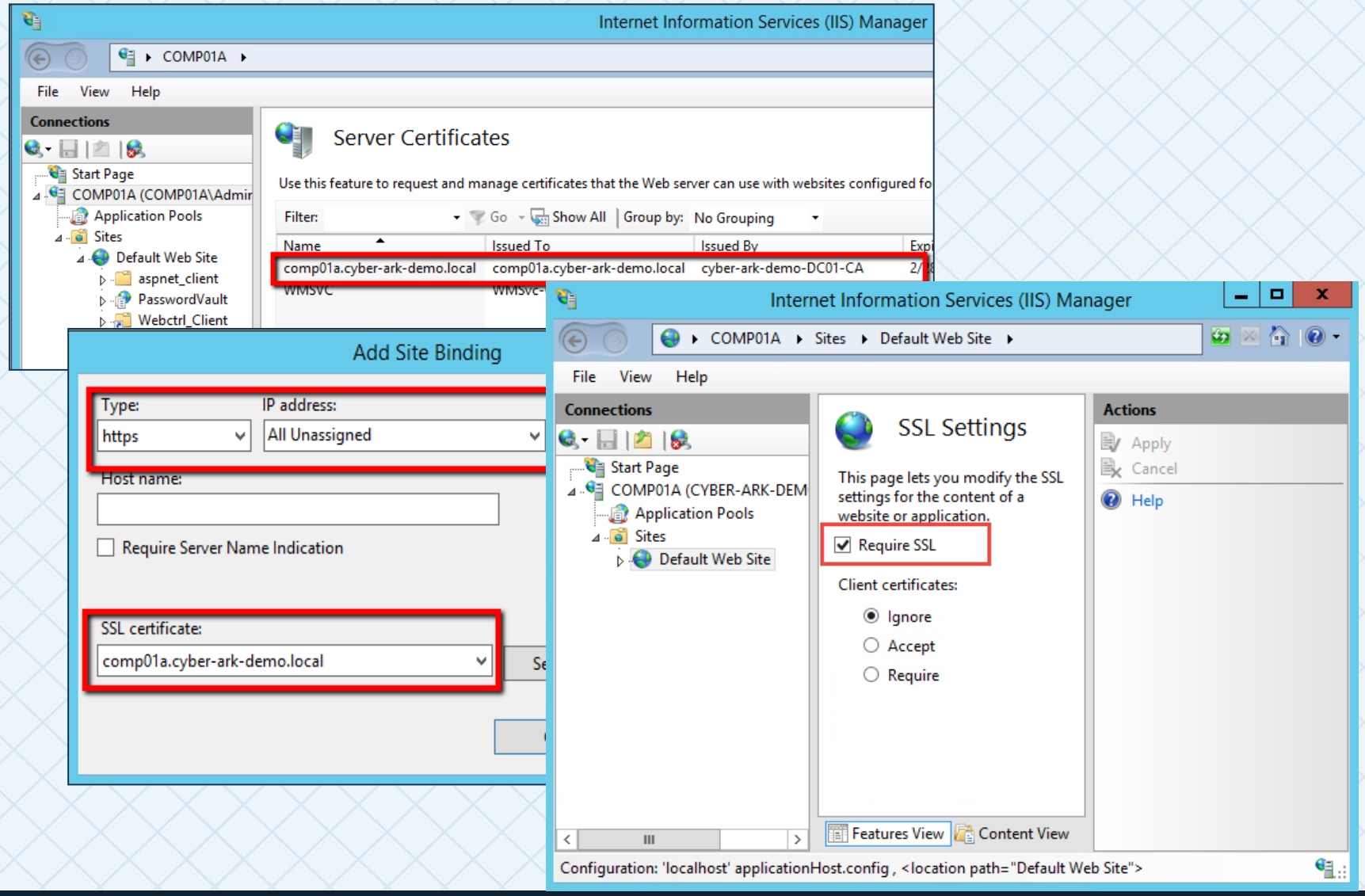
- Launch the Installation Automation PowerShell script from an Administrator: Windows PowerShell
- Allow the script to complete, and review the **script.log** file located in a sub-directory where the script is located.
- Always test the Web Server installation by opening a browser and connecting to the default web site. This is an important test prior to installing the PVWA.





INSTALL A SIGNED SSL CERTIFICATE

- Replace the self-signed certificate created by Installation Automation script with a web certificate issued by a trusted certificate authority
- The IIS server must be configured to only accept HTTPS connections. This is a manual step
- The PVWA should be a dedicated IIS server. No other web applications should be allowed

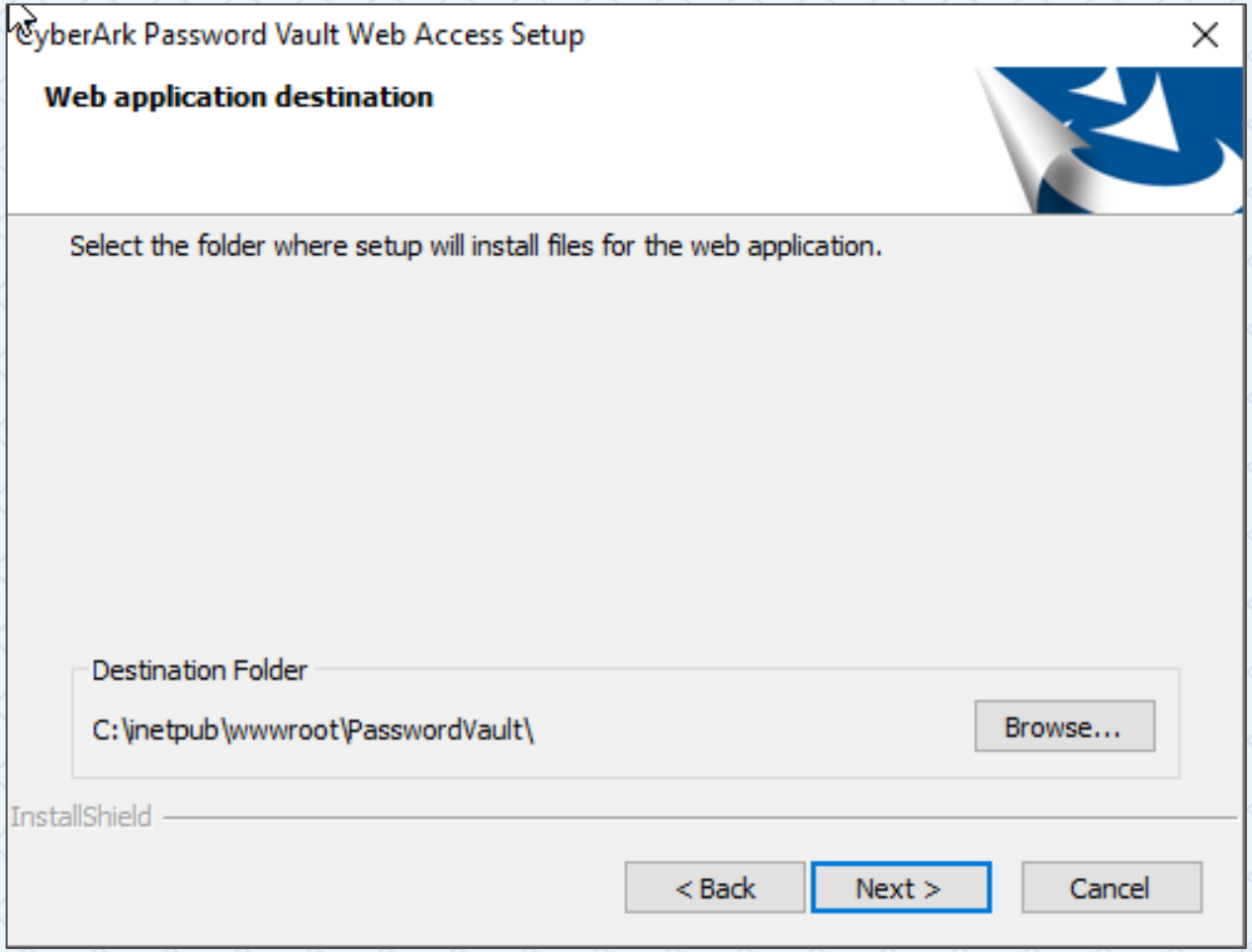


PVWA INSTALLATION

Pre-install tasks	Installation	Post-install tasks	Hardening
Review requirements	Run the PVWA installation script	Check installation log files	Run the hardening script
Close applications & log on	Registration (connect to the Vault)	Check user permissions on web server	Apply post hardening configurations
Run prerequisites script		Add restrictions to credentials file	*Harden server in a Domain environment
		Set API throttling	*Only perform this task if your PVWA server is part of a domain

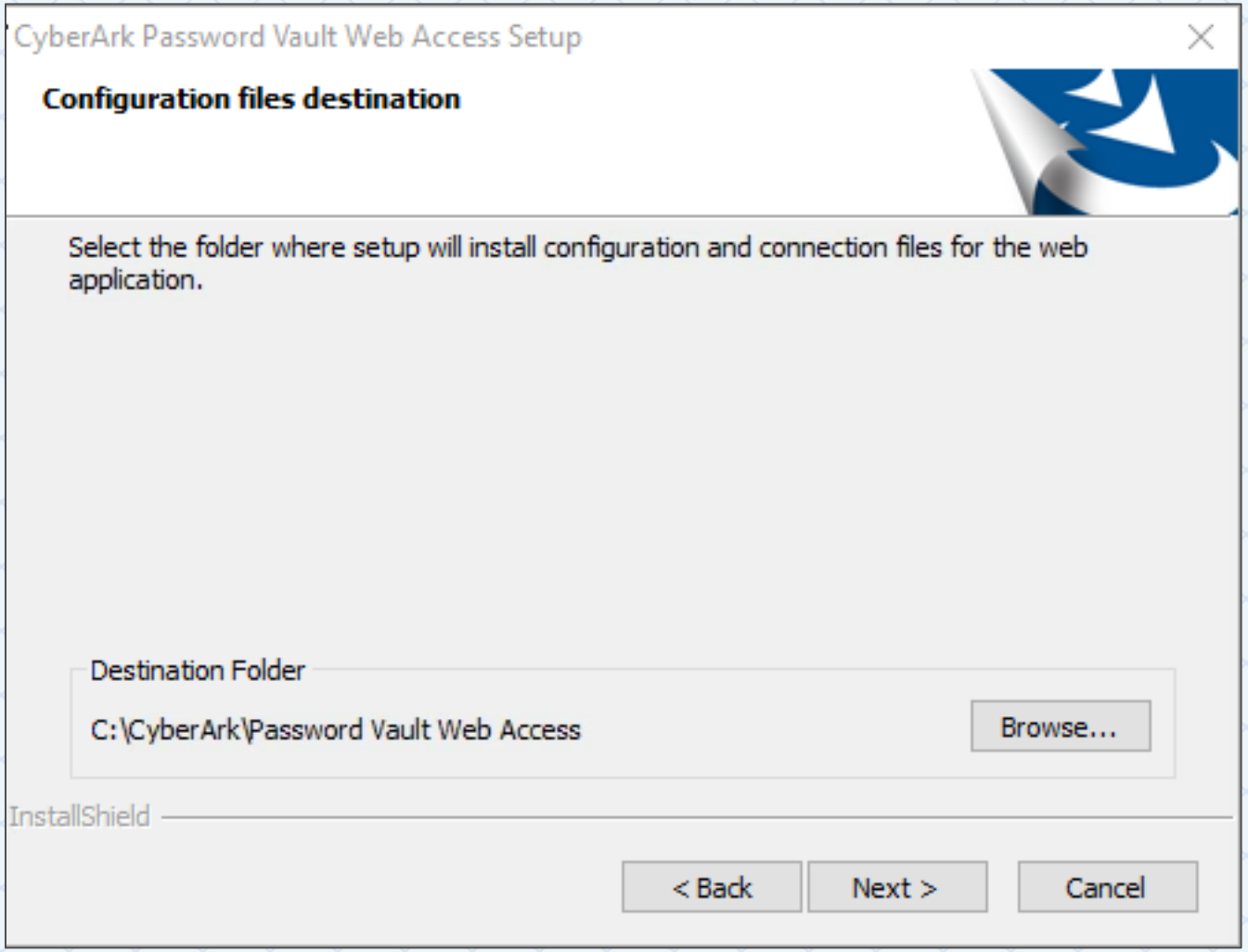
WEB APPLICATION DESTINATION

- After running setup.exe, you will be asked to specify the destination location for the web application
- Because Microsoft installs IIS on “C:\” accept the default destination folder for the PasswordVault virtual directory



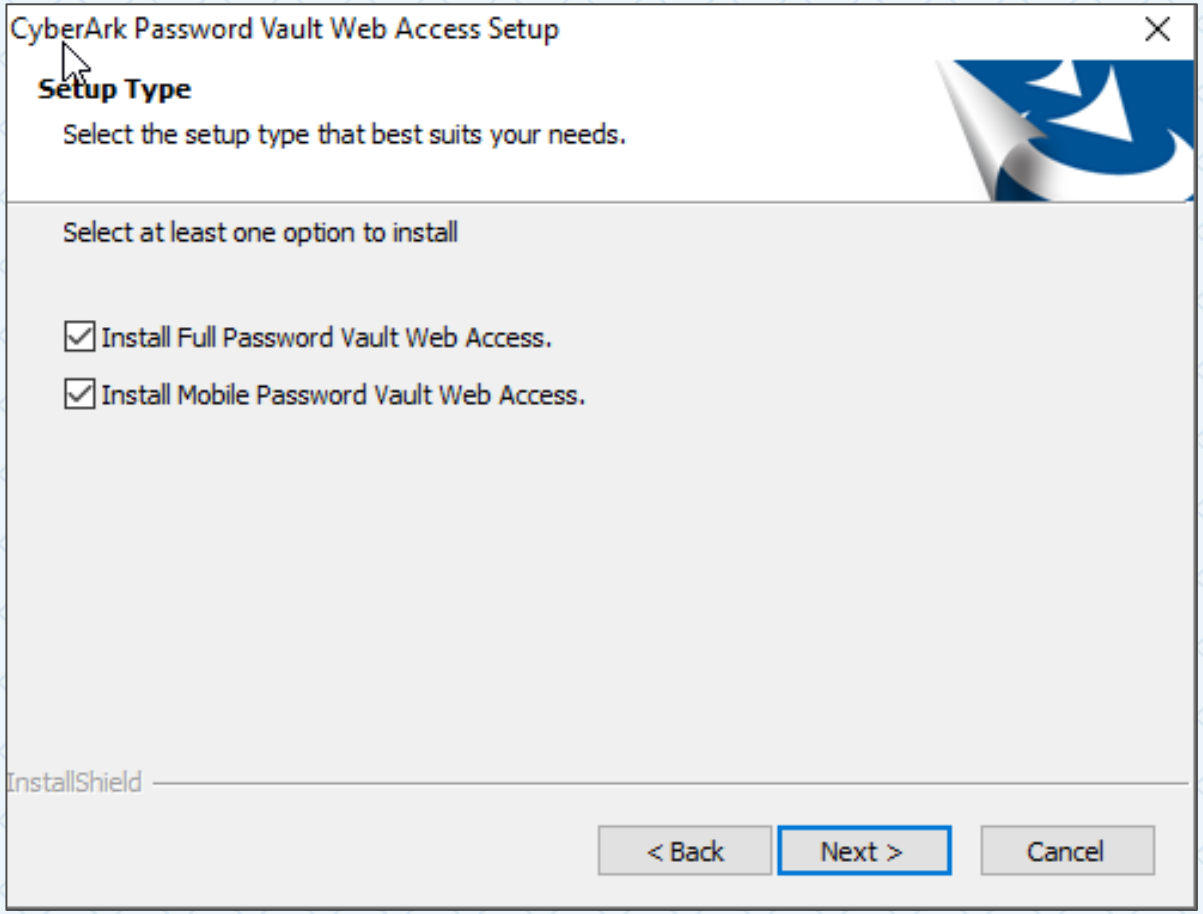
CONFIGURATION FILES DESTINATION

- Select the destination folder for the PVWA configuration files
- If needed, the Configuration Files destination folder can be changed to an alternate drive letter



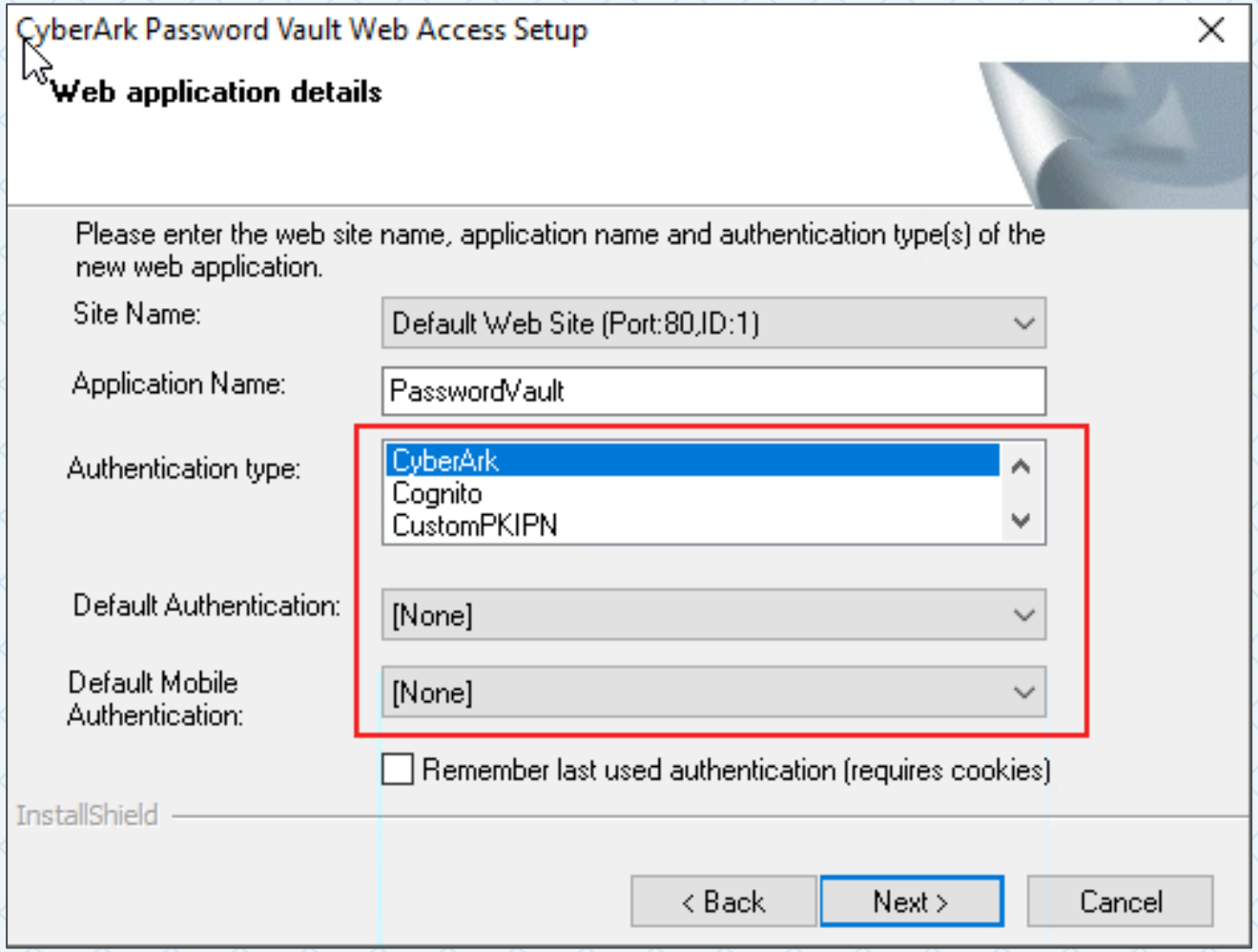
SETUP TYPE

- Full Password Vault Web Access option installs the PVWA for desktop browsers
- Mobile Password Vault Web Access option installs a PVWA interface that is specifically designed for mobile devices
- Select whether to install the full PVWA server, mobile version or both



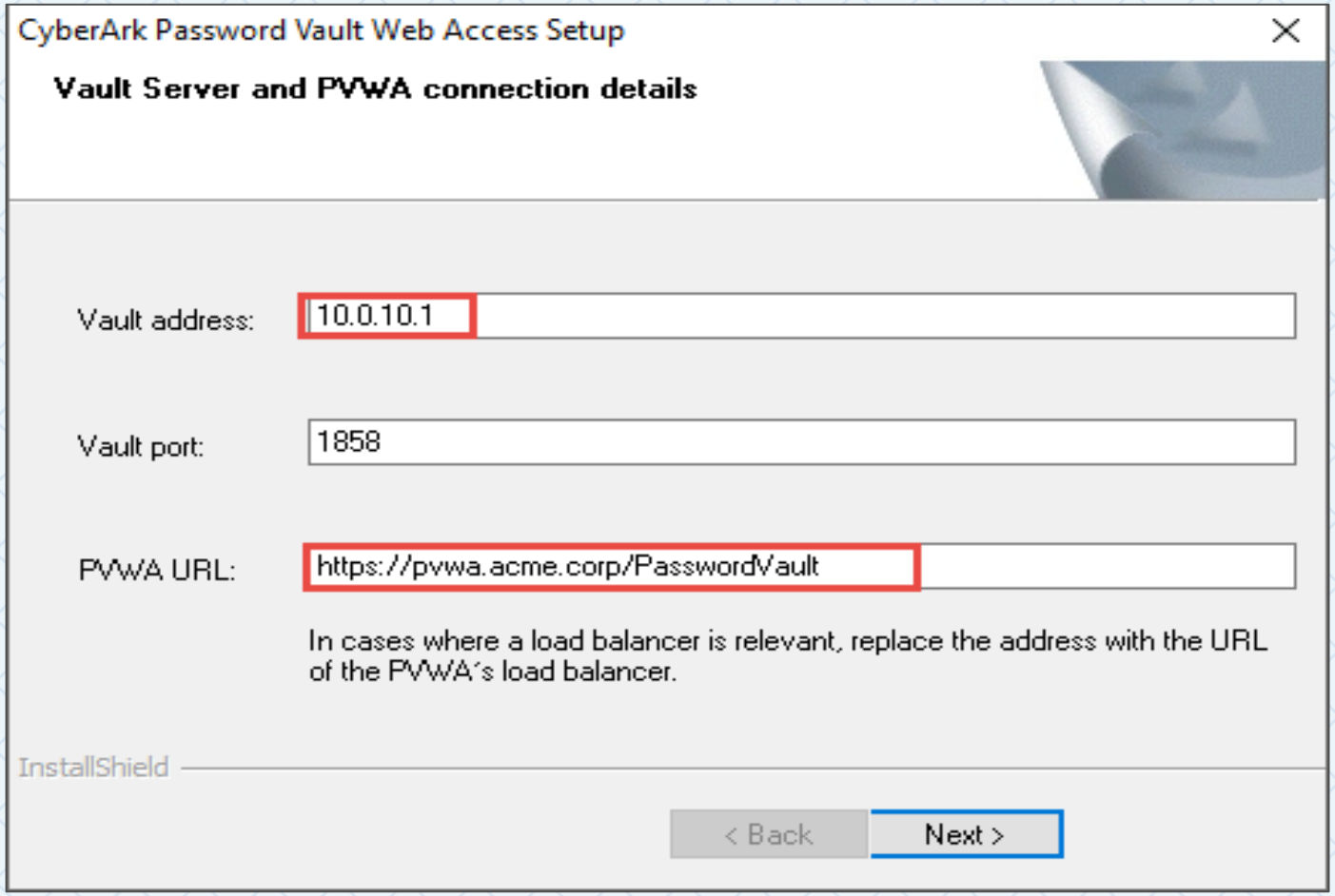
WEB APPLICATION DETAILS

- Select the authentication types that will be enabled on the PVWA
- If no authentication type is selected a user will be unable to authenticate to the Vault using the PVWA
- Default authentication types can be selected here or at a later stage



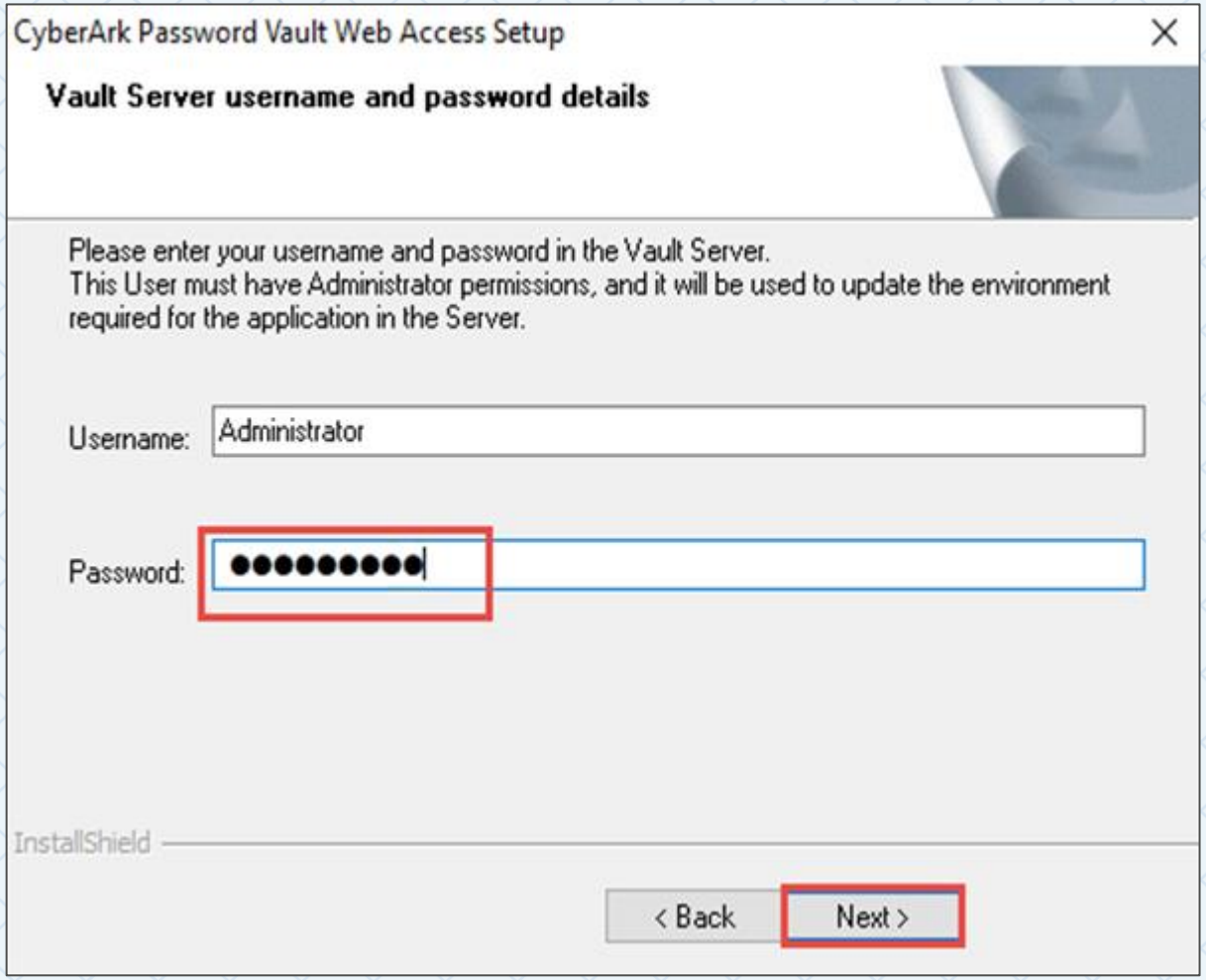
VAULT CONNECTION DETAILS

- Enter the IP **Address** of your Vault server
- The default Vault port is tcp_*1858*
- The PVWA URL is automatically populated with the local host URL
- When Load Balancing PVWA servers update the PVWA URL: field with the Load Balancers URL



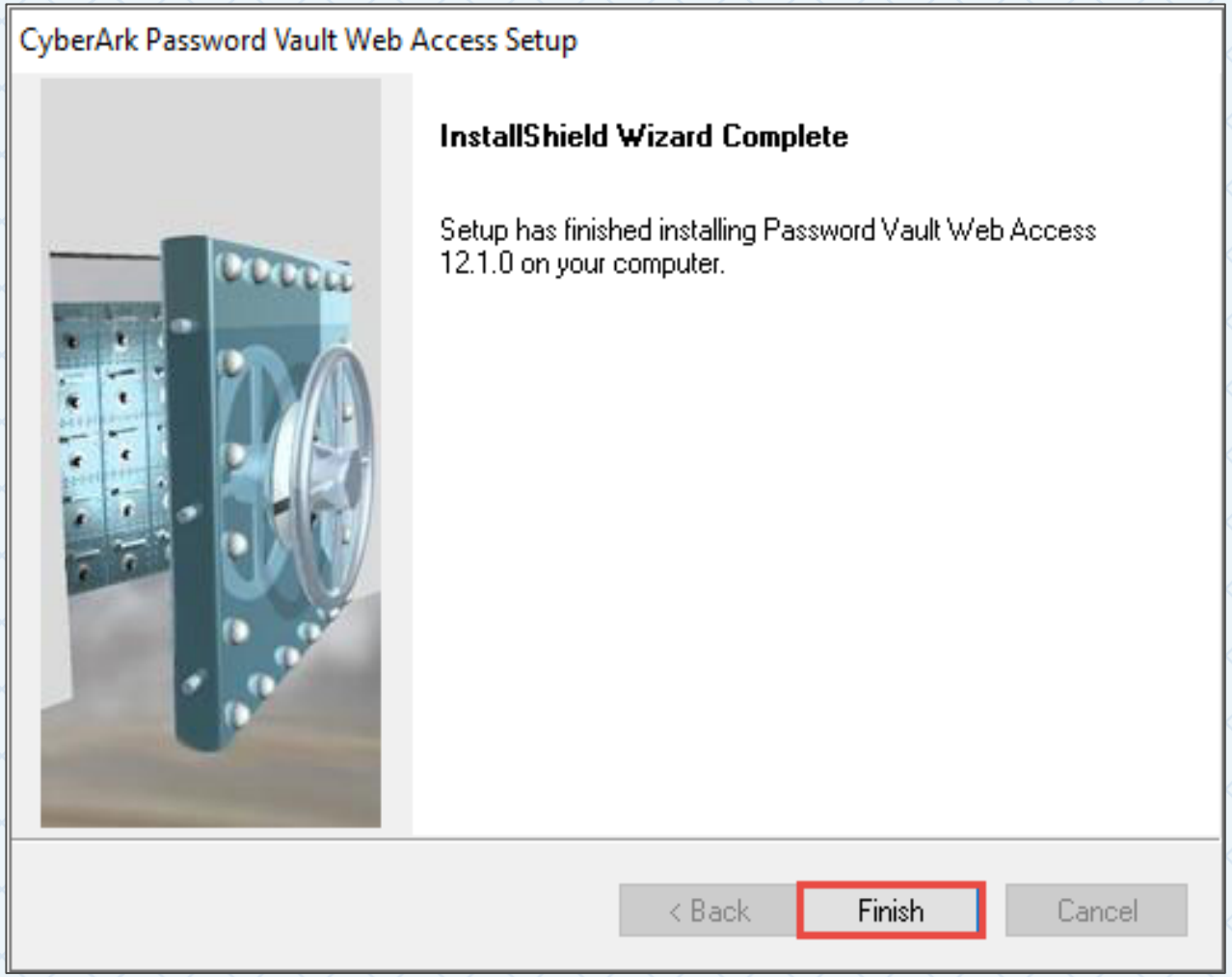
VAULT USERNAME AND PASSWORD DETAILS

- Enter the username and password of the Vault user that will be used to create the CPM environment on the Vault
- Typically, the built-in Administrator is used for installing CyberArk PAM component software



FINISH

- Press the **Finish** button to complete the installation
- There is no need for a reboot

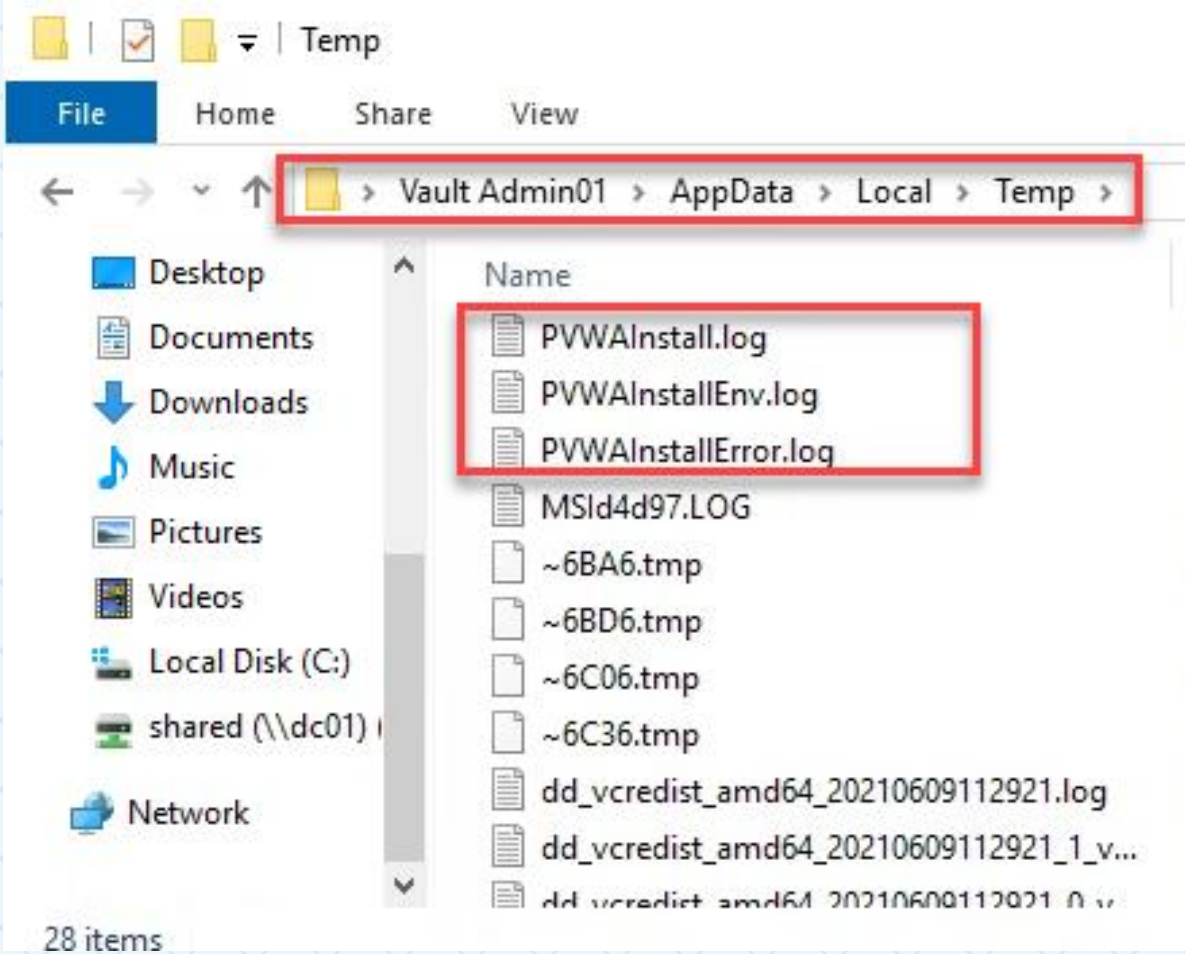


PVWA POST-INSTALLATION TASKS

Pre-install tasks	Installation	Post-install tasks	Hardening
Review requirements	Run the PVWA installation script	Check installation log files	Run the hardening script
Close applications & log on	Registration (connect to the Vault)	Check user permissions on web server	Apply post hardening configurations
Run prerequisites script		Add restrictions to credentials file	*Harden server in a Domain environment
		Set API throttling	*Only perform this task if your PVWA server is part of a domain

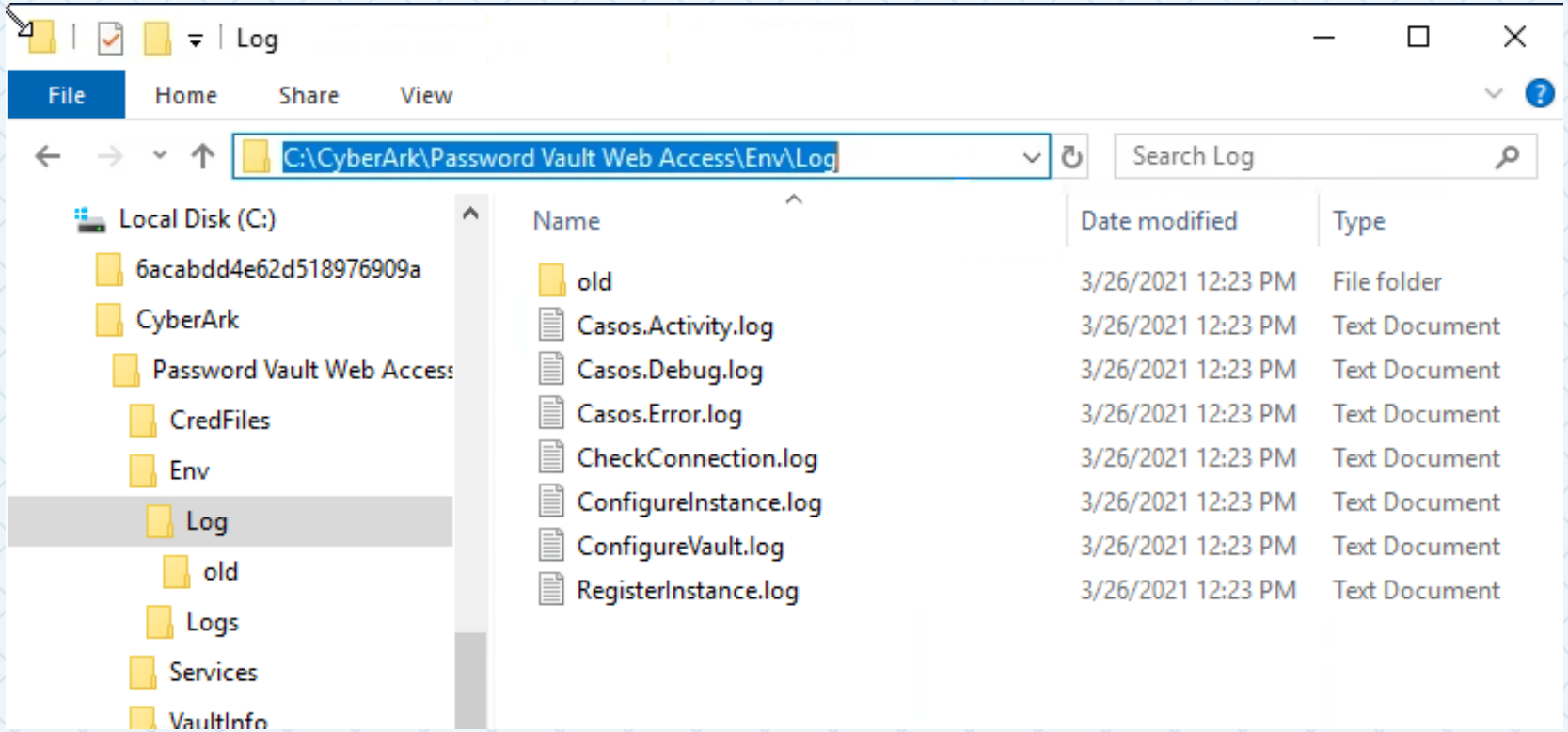
CHECK INSTALLATION LOG FILES

- The following log files contain information about the installation procedure:
  - PVWAInstall.log
  - PVWAInstallEnv.log
  - PVWAInstallError.log
  - PVWAInstallErrorEnv.log
- The log files are located in C:\Users\Administrator\AppData\Local\Temp



ADDITIONAL LOG FILES

- Additional log files are created in the Env\Log subfolder of the PVWA configuration folder.
- These files contain important information about the Vault connection configuration and the PVWA environment set up in the Vault



CHECK THE USER PERMISSIONS ON THE WEB SERVER

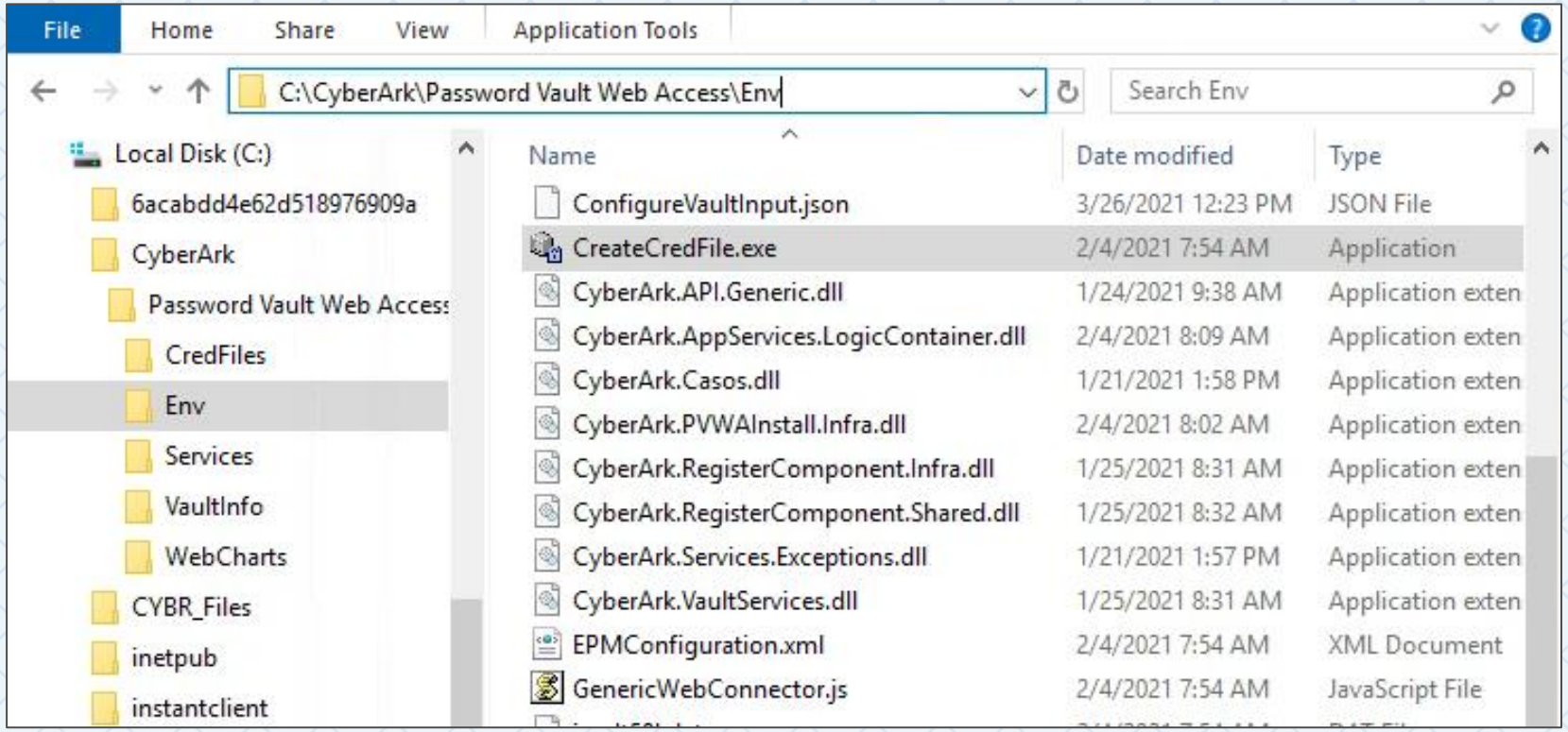
- During PVWA installation, a set of folders are created on the web server in the default location, C:\CyberArk\Password Vault Web Access, or in the location that you specified during installation
- There may be inherited permissions not listed in this table. CyberArk recommends removing inherited permissions for these folders

Folder	User/Group	Permission
CredFiles	Administrators	Full control
	Application pool's dedicated user: • IIS AppPool\PasswordVaultWebAccessPool	Full control
VaultInfo	Administrators	Full control
	Application pool's dedicated user: • IIS AppPool\PasswordVaultWebAccessPool	Full control
WebCharts	Administrators	Full control
	Application pool's dedicated user: • IIS AppPool\PasswordVaultWebAccessPool	Full control
	Internet Guest user[1] (IIS_IUSR)	Read & Execute
<Windows folder>\Temp	Administrators	Full control
	Application pool's dedicated user: • IIS AppPool\PasswordVaultWebAccessPool	Full control

ADD RESTRICTIONS TO CREDENTIALS FILE

Add restrictions to the protected credentials file

- During installation, a credentials file is created to enable the PVWA user to log on to the Vault
- To enhance the security of the credentials file, use the CreateCredFile utility in the Env folder to create a protected credentials file
- For more information, see "*User credential files*" on docs.cyberark.com

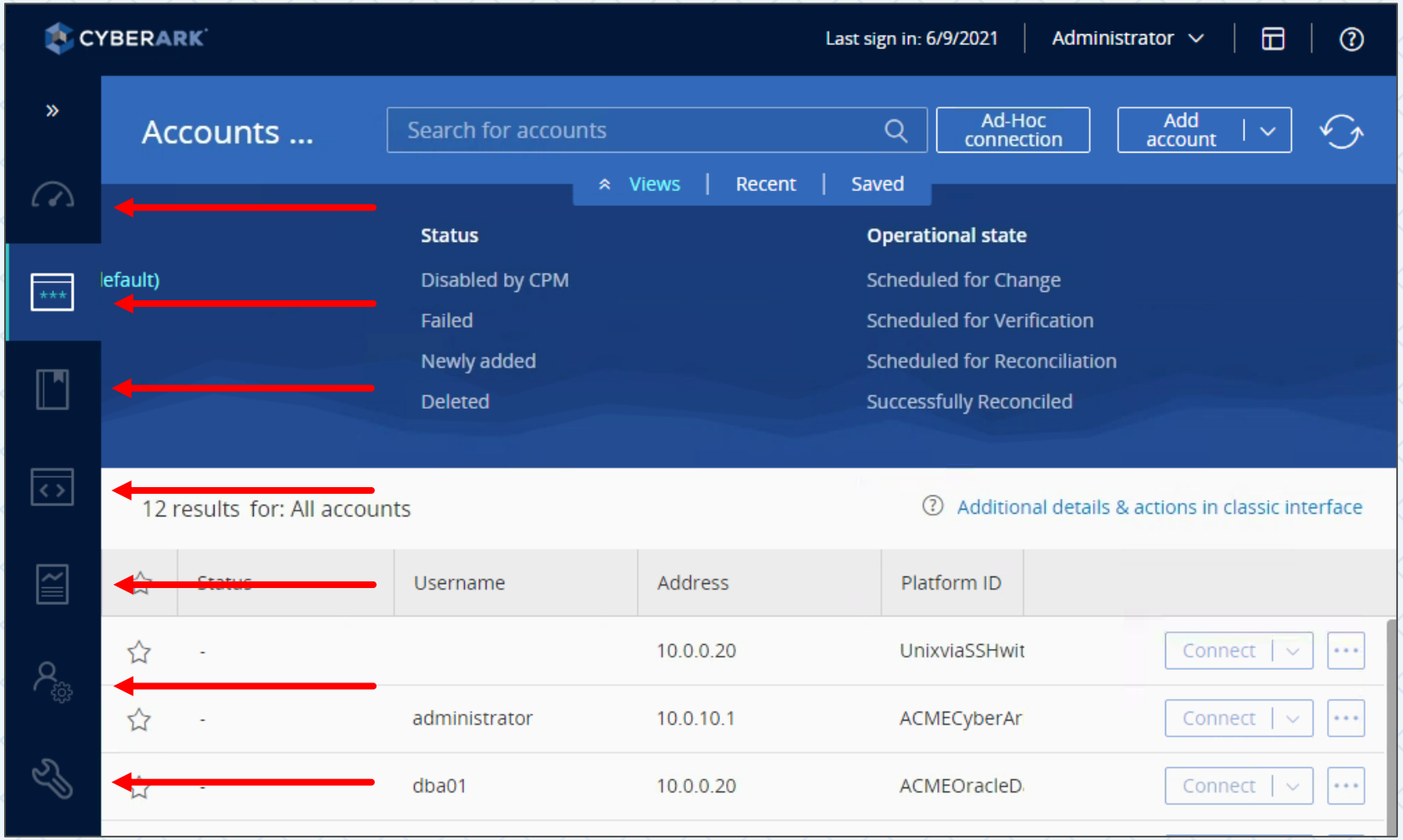


VALIDATE PVWA OPTIONS

Sign in to the PVWA as Administrator to confirm a successful installation

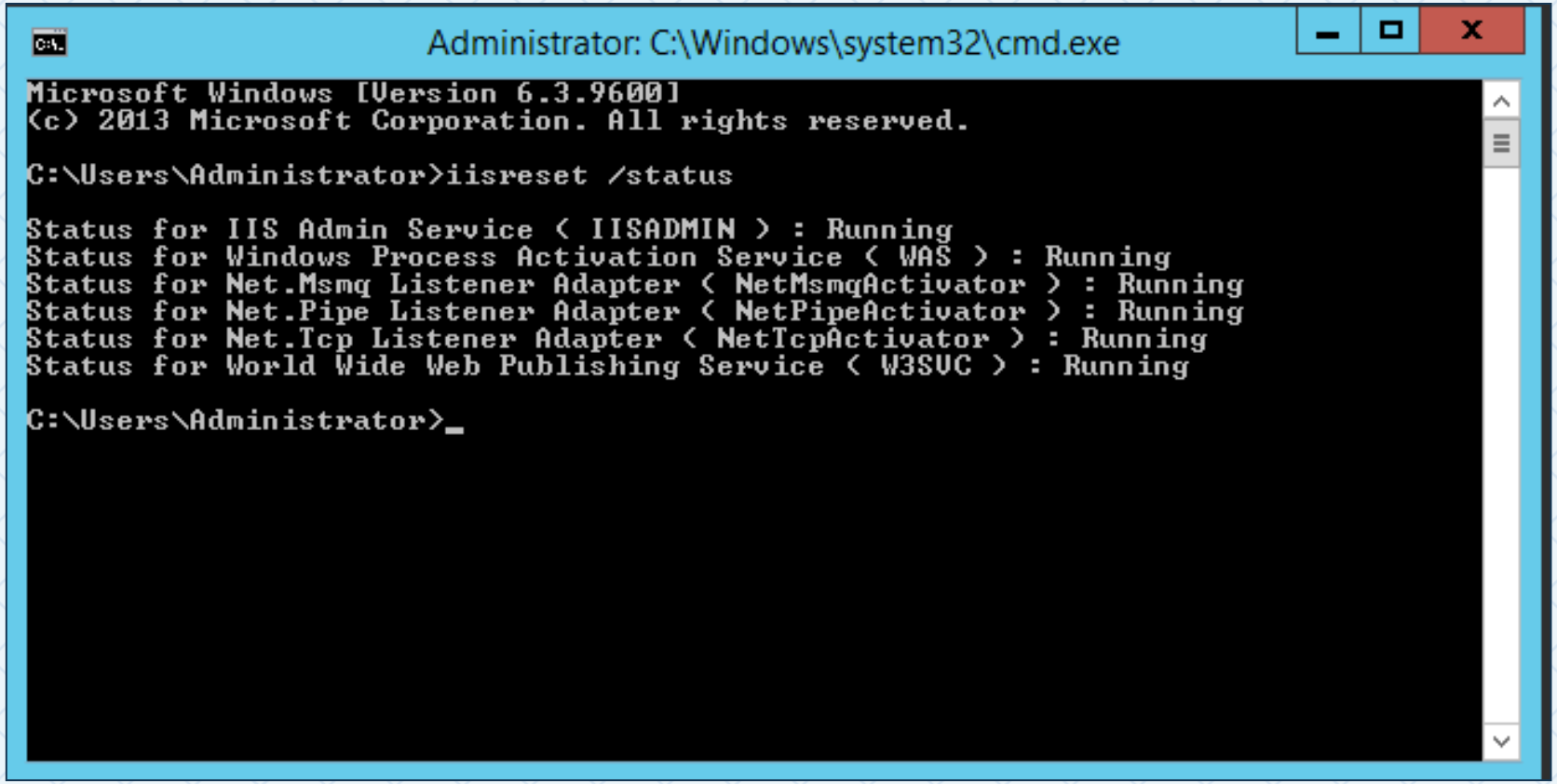
An Administrator should have access to the following options

- System Health
- Accounts
- Policies
- Applications
- Reports
- User Provisioning
- Administration



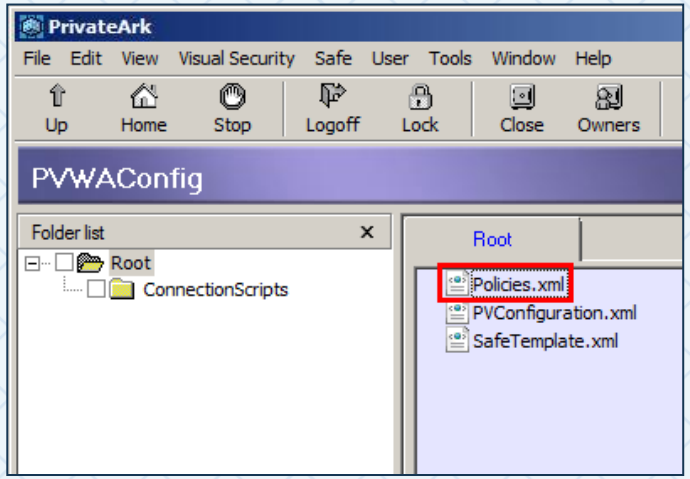
PVWA SERVICE (IIS SERVICES)

- The PVWA should be a dedicated server with no other applications, specifically web applications installed
- PVWA services status can be viewed or restarted using the IISRESET command at an Administrative Command prompt
- IISRESET with the /Status option will display the status for all relevant services as shown



PVWACONFIG SAFE - POLICIES.XML

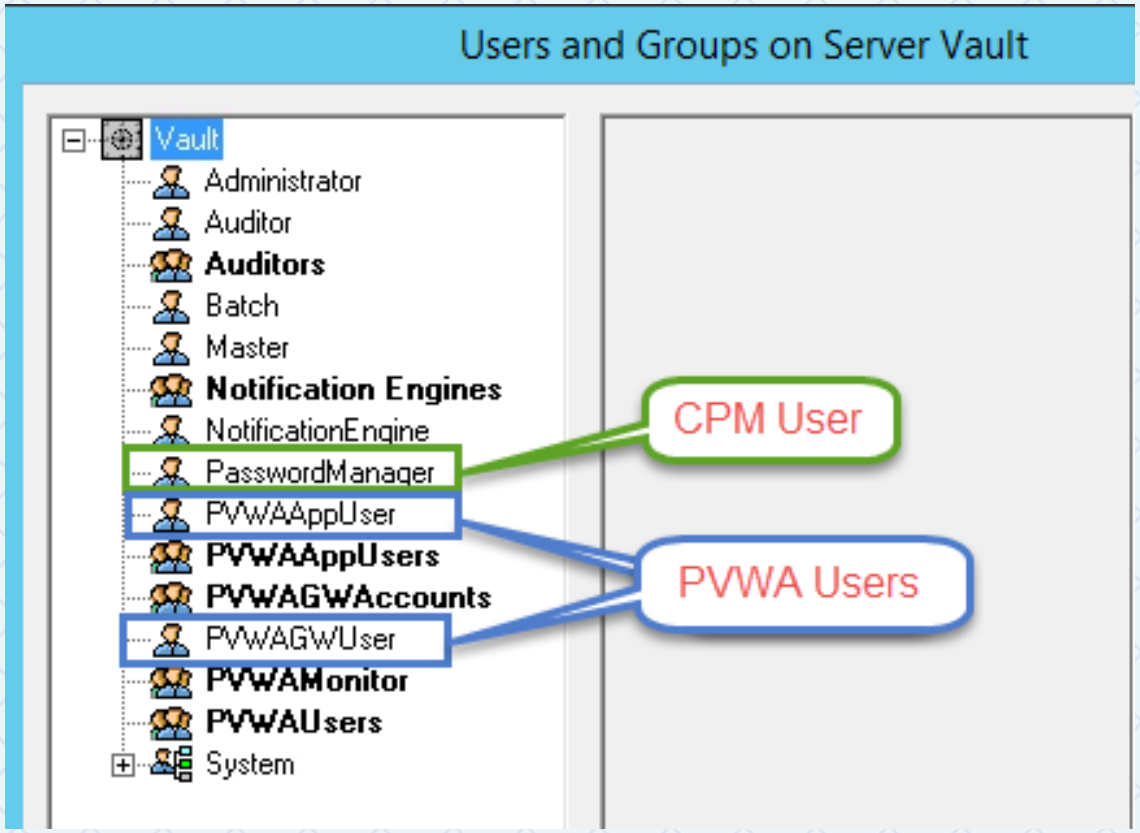
- The Policies.xml contains the “UI & Workflow” settings for all platforms
- The PlatformBaseID, ties the platforms listed in the Policies.xml with the platforms contained in the PasswordManagerShared safe




```
    <TicketingSystem ValidateTicketNumber="No" EnterTicketingInfo="No"/>
  </Policy>
- <Policy PlatformBaseProtocol="SSH" PlatformBaseType="Unix" PlatformBaseID="UnixSSH" AutoVerifyOnAdd="No"
  AutoChangeOnAdd="No" ID="Lin-Prd-PCI">
    - <Properties>
        - <Required>
              <Property Name="Address"/>
              <Property Name="Username"/>
          </Required>
          <Optional/>
      </Properties>
    - <LinkedPasswords>
          <Link Name="LogonAccount" PropertyIndex="1"/>
          <Link Name="ReconcileAccount" PropertyIndex="3"/>
      </LinkedPasswords>
      <TicketingSystem ValidateTicketNumber="No" EnterTicketingInfo="No"/>
    - <PrivilegedSessionManagement Enable="Yes">
          <SSHProxy/>
      </PrivilegedSessionManagement>
    - <ConnectionComponents>
          <ConnectionComponent Id="PSM-SSH"/>
          <ConnectionComponent Id="SSH"/>
          <ConnectionComponent Id="PuTTY" Enable="No"/>
          <ConnectionComponent Id="PSM-WinSCP"/>
      </ConnectionComponents>
    - <OnDemandPrivilegesManager>
          <Commands/>
          <Defaults/>
          <Authentication/>
        - <CommandsGroups>
            - <CommandsGroup Name="SHELLS">
```

PVWA VAULT USERS AND GROUPS

- **PVWAAppUser** is used by the Password Vault Web Access for internal Processing
- **PVWAGWUser** impersonates the logged-on user to the Vault

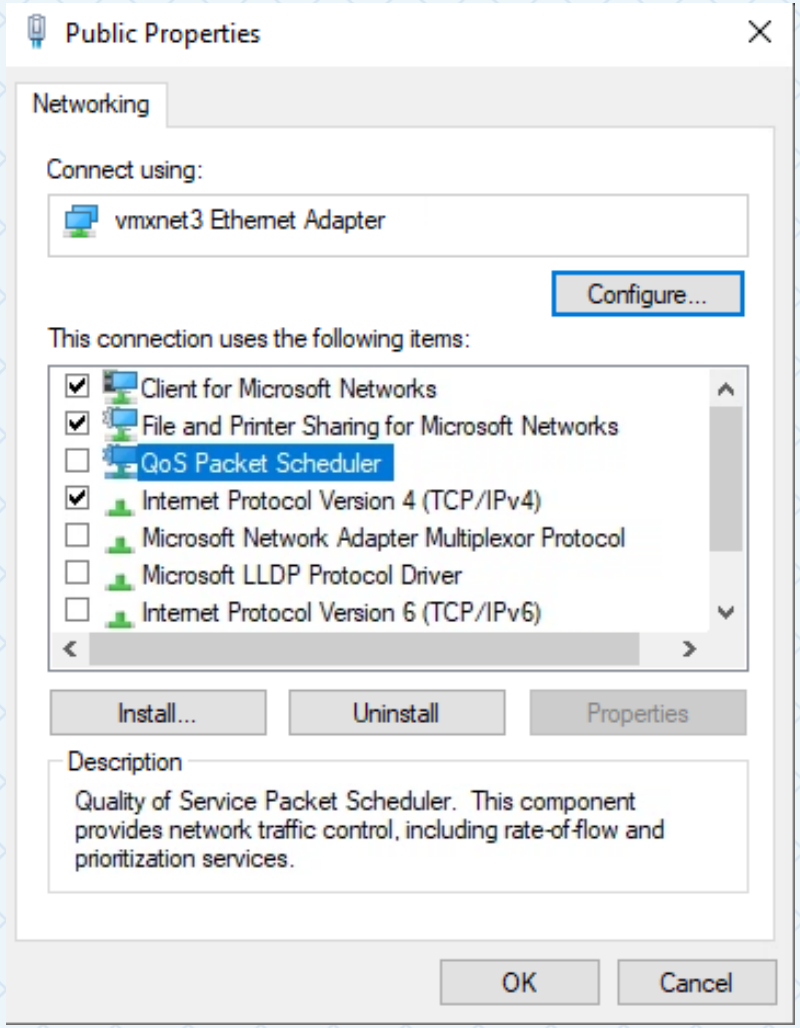


PVWA HARDENING

Pre-install tasks	Installation	Post-install tasks	Hardening
Review requirements	Run the PVWA installation script	Check installation log files	Run the hardening script
Close applications & log on	Registration (connect to the Vault)	Check user permissions on web server	Apply post hardening configurations
Run prerequisites script		Add restrictions to credentials file	*Harden server in a Domain environment
		Set API throttling	*Only perform this task if your PVWA server is part of a domain

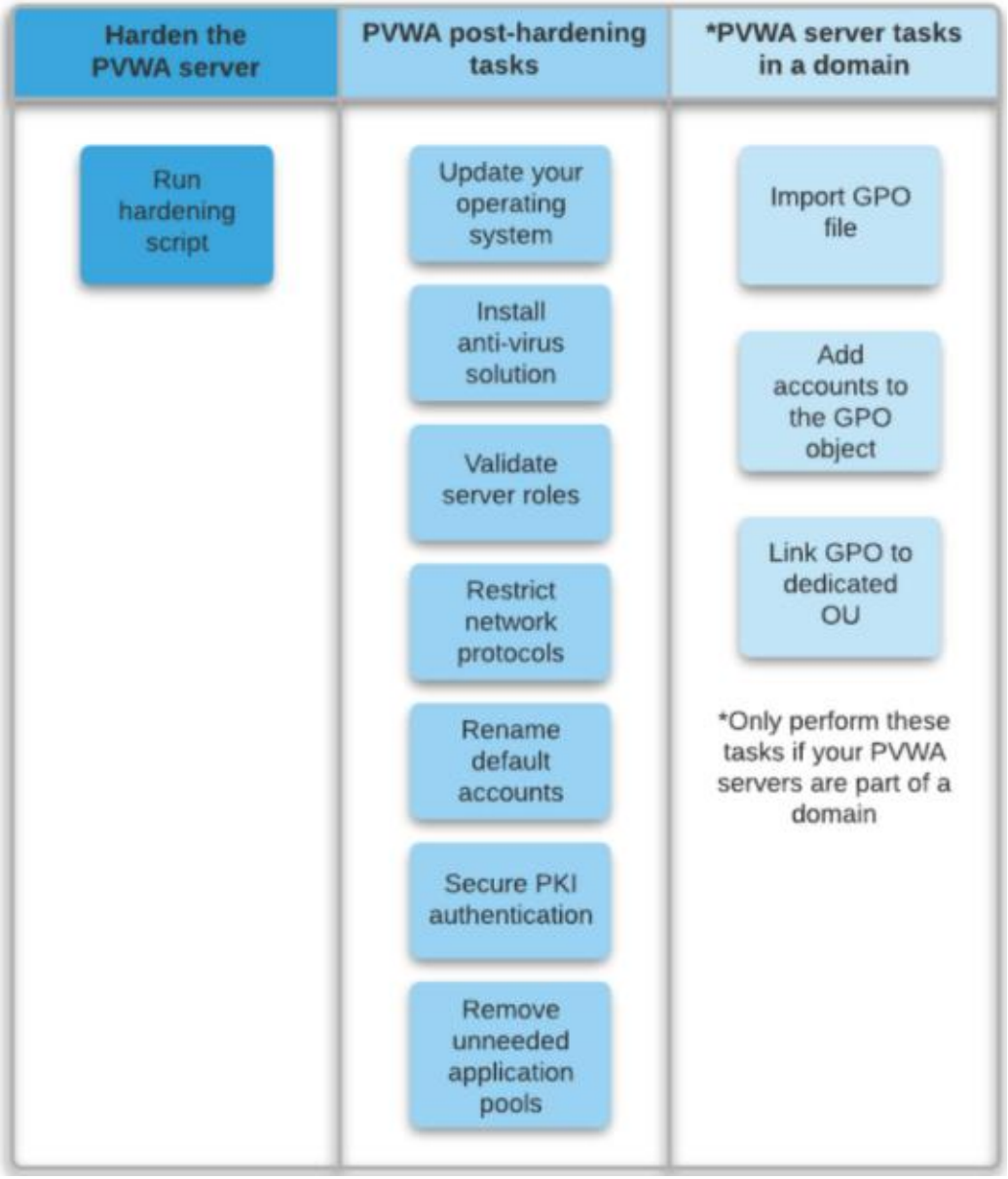
PVWA HARDENING – MANUAL PROCEDURES

- Only the following network protocols, services or clients are required for a CPM and or PVWA Component Server:
  - Client for Microsoft Network
  - File and Printer Sharing for Microsoft Network
  - Internet Protocol Version 4 (TCP/IPv4)
- Disable all other default protocols, services and clients



PVWA HARDENING

- The PVWA hardening process is a series of tasks that enhance security on the Windows Server machine. Hardening is performed after PVWA installation.



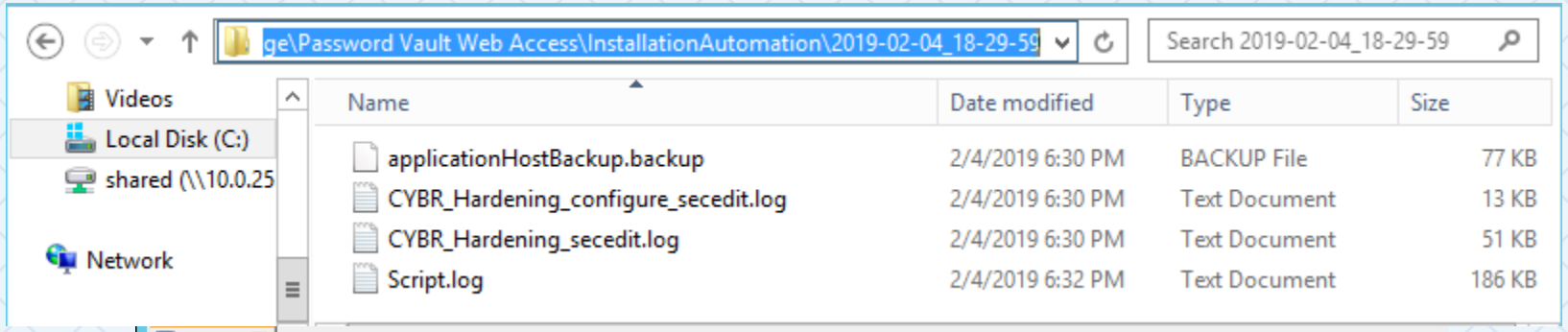
RUN THE HARDENING SCRIPT

YOU CAN HARDEN THE PVWA SERVER AUTOMATICALLY USING A SCRIPT FILE. THE HARDENING SCRIPT FILE PERFORMS THE FOLLOWING TASKS:

- Imports the INF configuration (Workgroup)
- Validates server roles
- Enables IIS Anonymous authentication
- Disables IIS Registry shares
- Disables IIS Directory browsing
- Disables IIS WebDAV
- Removes unnecessary IIS Mime types
- IIS SSL/TLS settings
  - Updates IIS SSL\TLS settings
  - Configures ciphers suites
- Policy configuration
  - Enables screen saver policies
  - Configures advanced audit policies
  - Configures Remote Desktop Services policies
- General auditing, registry, and file system configuration
  - Registry audits
  - Registry permissions
  - FileSystem permissions
  - FileSystem audit
- Disables services

PVWA INSTALLATION AUTOMATION - HARDENING

- PVWA Installation Automation PS script.log can be found in a subfolder of **\InstallationAutomation** ***Date_Time***
- The Script.log file provides detail on the status of the changes

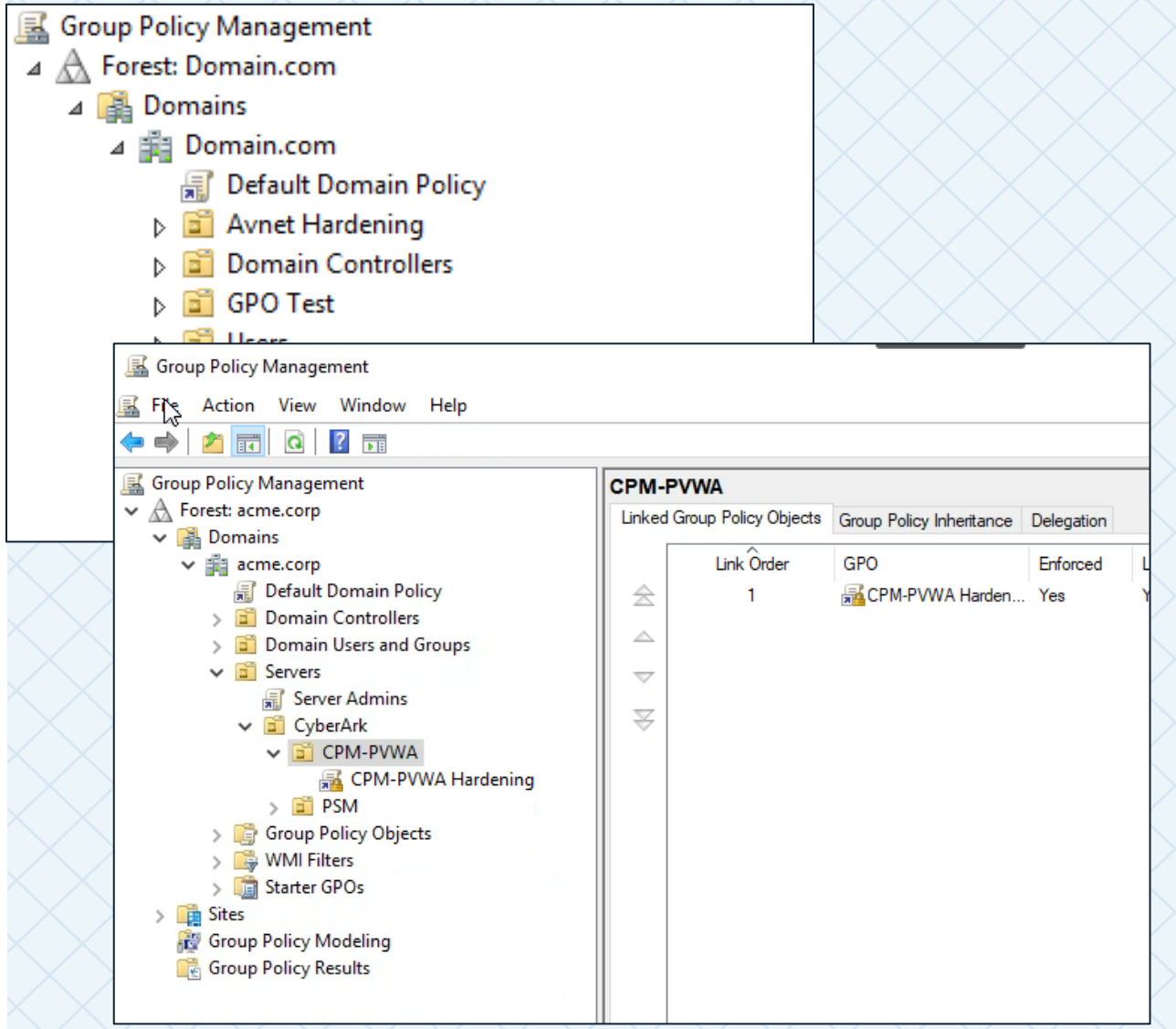


Script.log

```
2019-02-04 18:32:25 INFO:  ==================================================================
2019-02-04 18:32:25 INFO:  Start Step PVWA Post Installation
2019-02-04 18:32:25 INFO:  Skipping prerequisites check
2019-02-04 18:32:25 INFO:  start execute step PVWA Post Installation
2019-02-04 18:32:25 INFO:  Start PVWA_PostInstallation
2019-02-04 18:32:25 INFO:  Log credentials file security warning
2019-02-04 18:32:25 WARNING:  To enhance the security of the PVWA credentials file, we recommend to
2019-02-04 18:32:25 INFO:  Log credentials file security warning finish
2019-02-04 18:32:25 INFO:  Redirect HTTP requests To HTTPS
2019-02-04 18:32:25 INFO:  set LOCAL_FQDN: comp01a.cyber-ark-demo.local
2019-02-04 18:32:25 INFO:  set redirectPage: https://comp01a.cyber-ark-demo.local/PasswordVault
2019-02-04 18:32:27 INFO:  Disable HTTP requests for inner web site
2019-02-04 18:32:28 INFO:  Redirect HTTP requests To HTTPS finish
2019-02-04 18:32:28 INFO:  Finish PVWA_PostInstallation successfully
2019-02-04 18:32:28 INFO:  The following step had been completed successfully: PVWA_PostInstallation
2019-02-04 18:32:28 INFO:  finish execute step PVWA Post Installation
2019-02-04 18:32:28 INFO:  ==================================================================
2019-02-04 18:32:28 INFO:  ******************************************************************
2019-02-04 18:32:28 ERROR:          The following Step failed : FileSystemPermissions
2019-02-04 18:32:28 INFO:  ******************************************************************
2019-02-04 18:32:28 INFO:  start IIS service
2019-02-04 18:32:30 INFO:  Start CyberArk Scheduled Tasks service
2019-02-04 18:32:42 INFO:  ==================================================================
2019-02-04 18:32:42 INFO:                  PVWA_Hardening script execution ended.
2019-02-04 18:32:42 INFO:  ==================================================================
```

PVWA HARDENING TASKS IN A DOMAIN

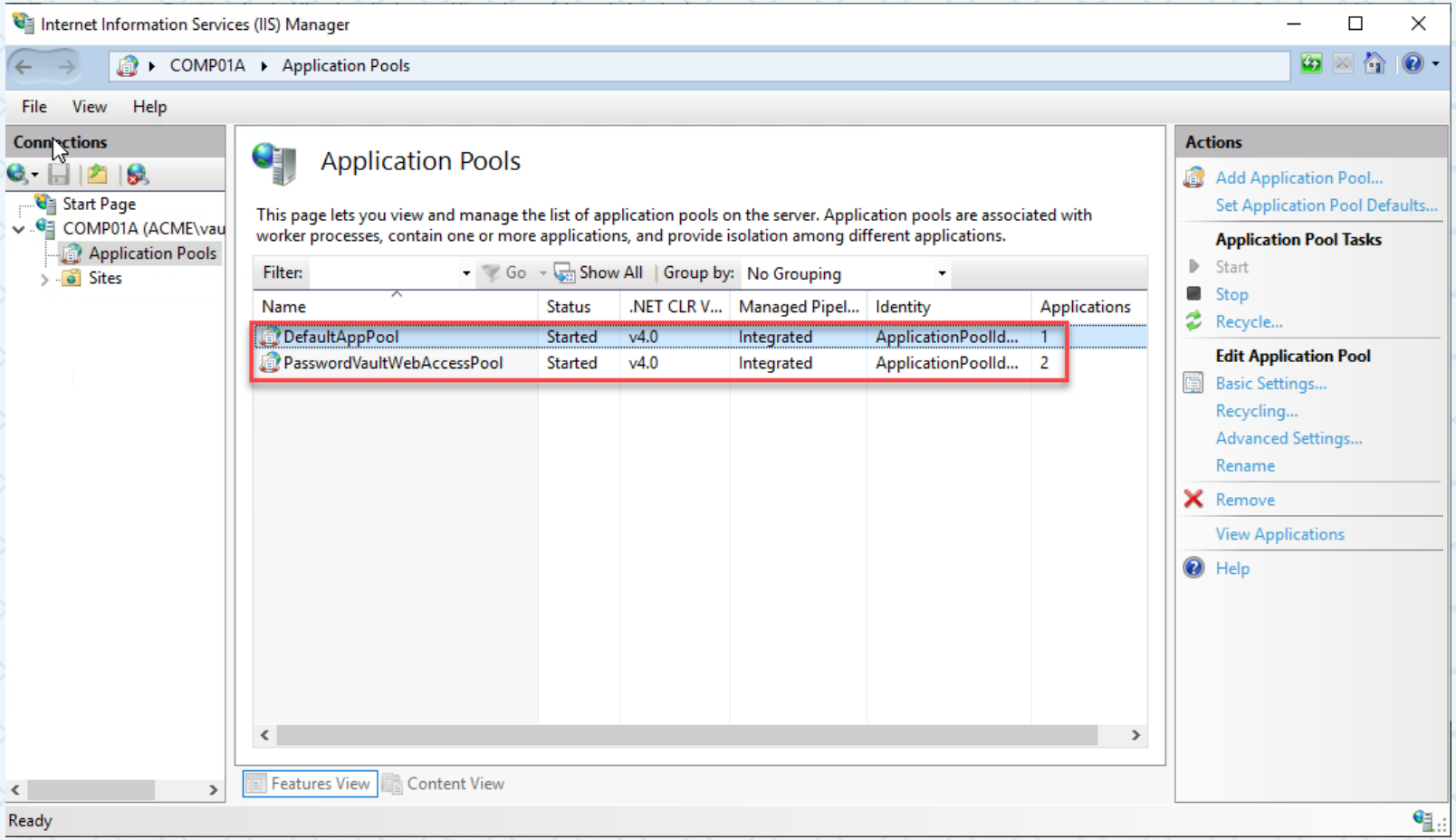
- When the PVWA is installed on a Domain Joined Windows Server, a GPO is provided for policy enforcement
- Use Group Policy Management Console (GPMC.MSC) to import GPO settings provided by CyberArk
- Add applicable accounts to the GPO object if service accounts require “Logon as a service” right
- Link and Enforce the new GPO to the Organizational Unit where the PVWA is located



MANUALLY REMOVE UNNEEDED IIS APPLICATION POOLS

Keep the following application pools only and delete all others:

- Default AppPool
- PasswordVaultWebAccessPool



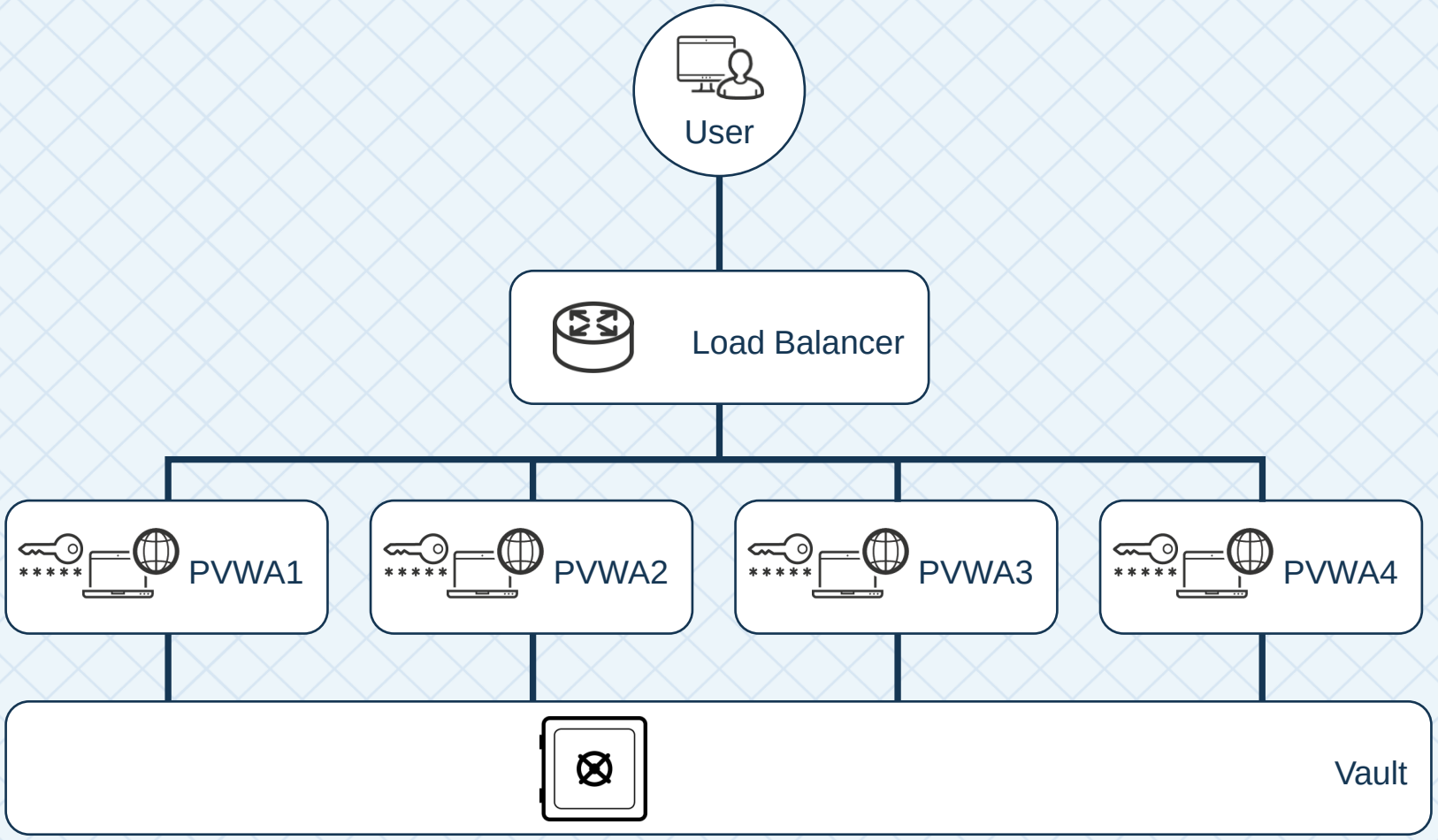
MULTIPLE PVWAS

USE CASES

- Fault Tolerance and Disaster Recovery in the Web Interface
- Additional capacity for heavy end user traffic
- Reduction of web traffic over WAN lines for remote site users
- To provide a second less privileged web interface for external users (vendors or contractors).

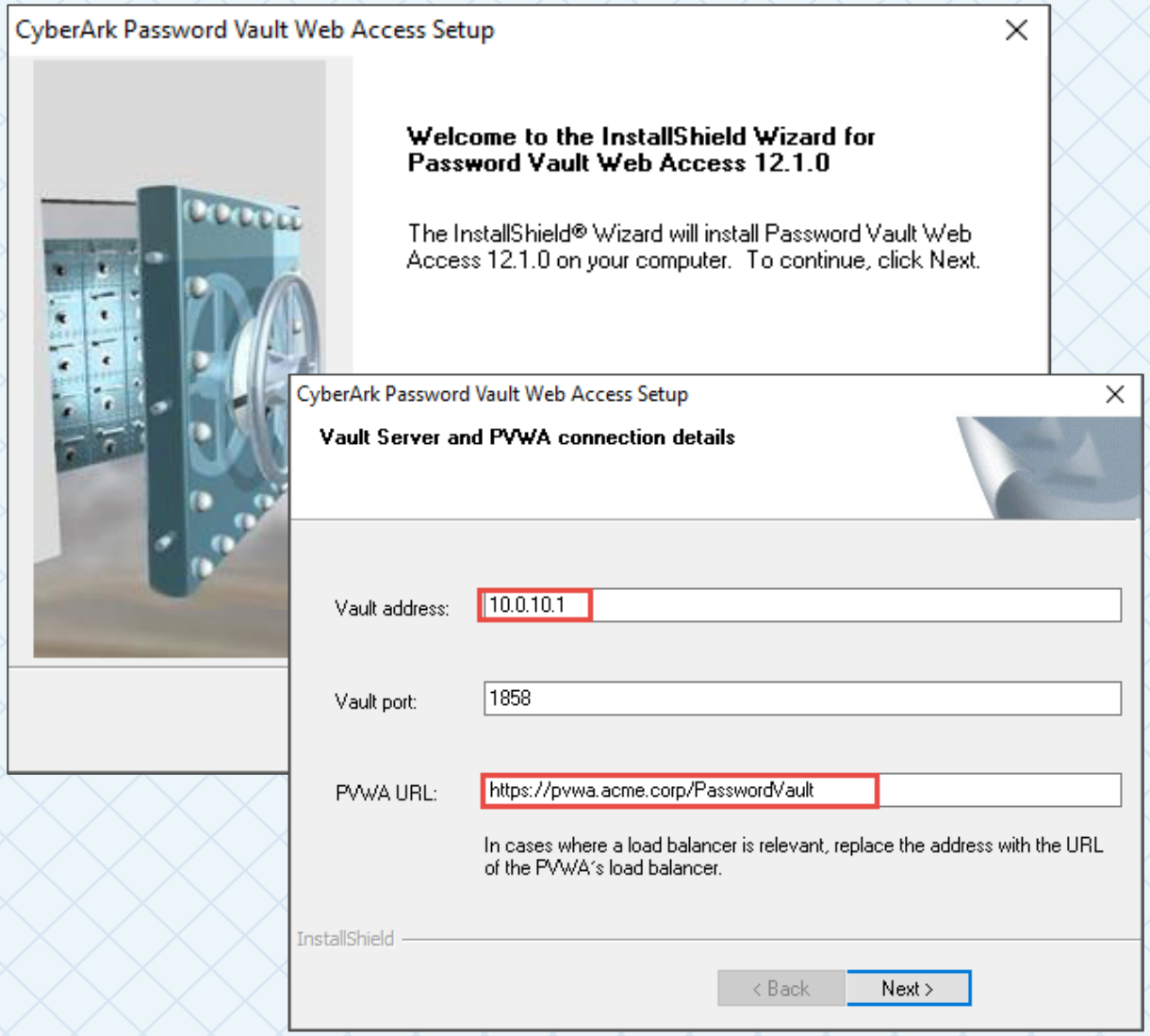
ARCHITECTURE

- A naming convention is usually irrelevant since PVWAs are all active and all serve the same role
- PVWAs can be load balanced with an external hardware load balancer
- In a load balanced configuration, each component server must be identically configured, e.g., operating system, CyberArk PAS version and installation directories



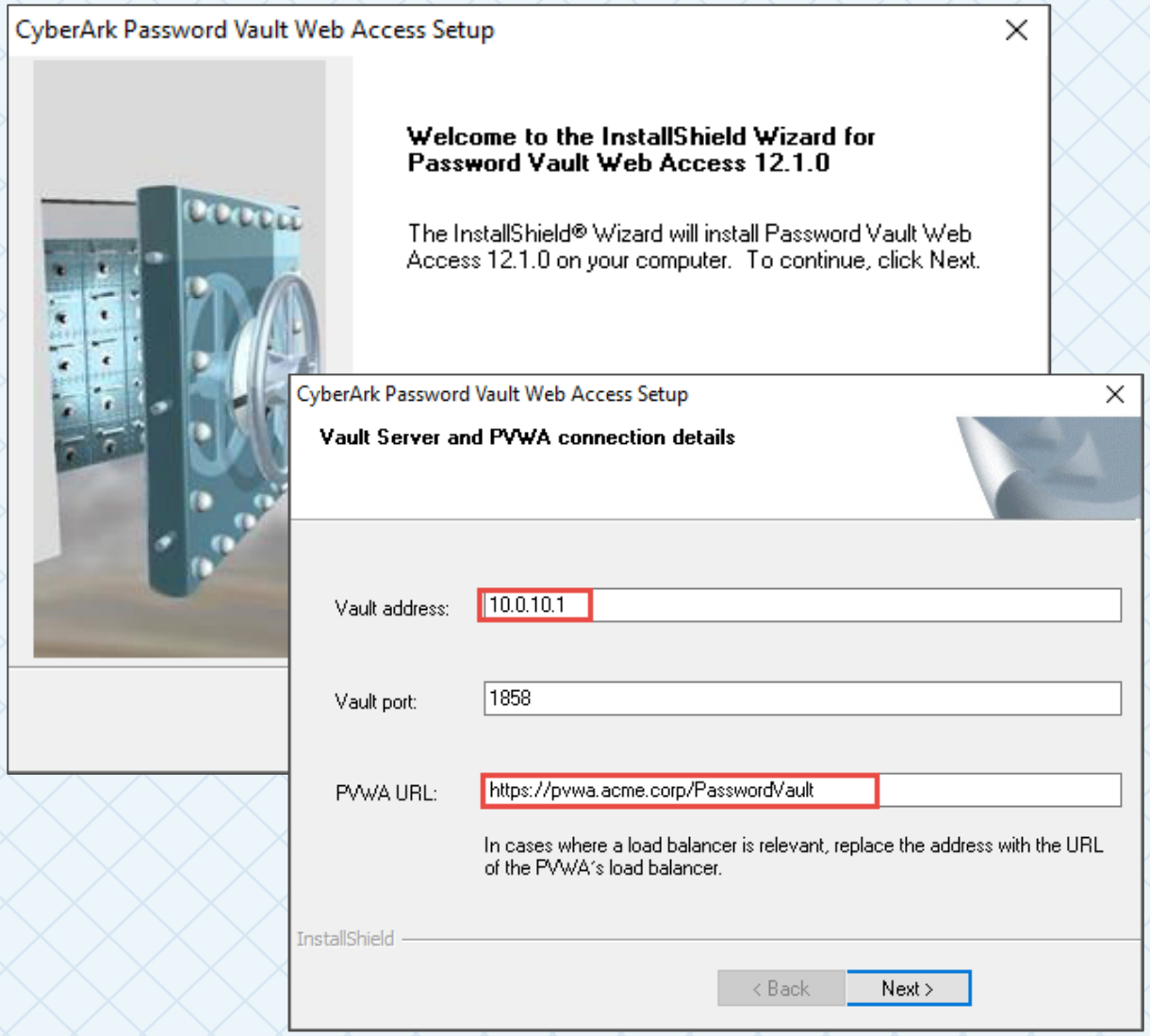
INSTALL MULTIPLE PVWA SERVERS

- Install each PVWA normally. No special configuration required
- Each PVWA server should be installed with the same versions and configured the same for Load Balanced configurations
- Provide the list of PVWA host names to Admin of your External Load Balancer and request a Virtual IP and update the PVWA URL: during installation



LOAD BALANCER REQUIREMENTS

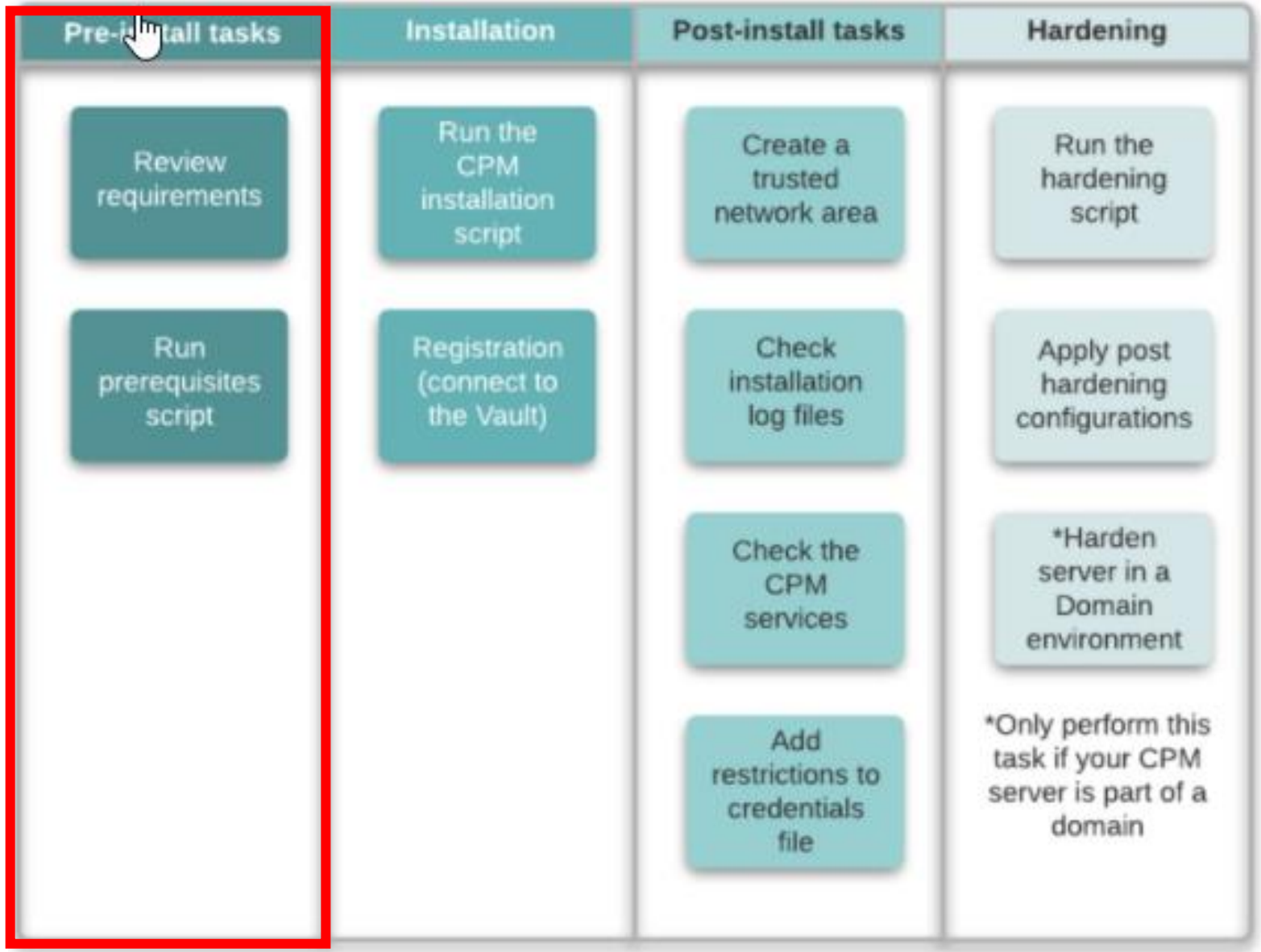
- The load balancer must not alter page content, or it should include a mechanism to prevent pages from being altered
- The load balancer must not alter the application path hierarchy (leave the default application path as it is)
- The load balancer must support 'sticky sessions'
- More information can be found online at docs.cyberark.com. Search for *"Multiple PVWAs in a single Vault environment"*



INTERMISSION

CPM INSTALLATION

PRE-INSTALL TASKS



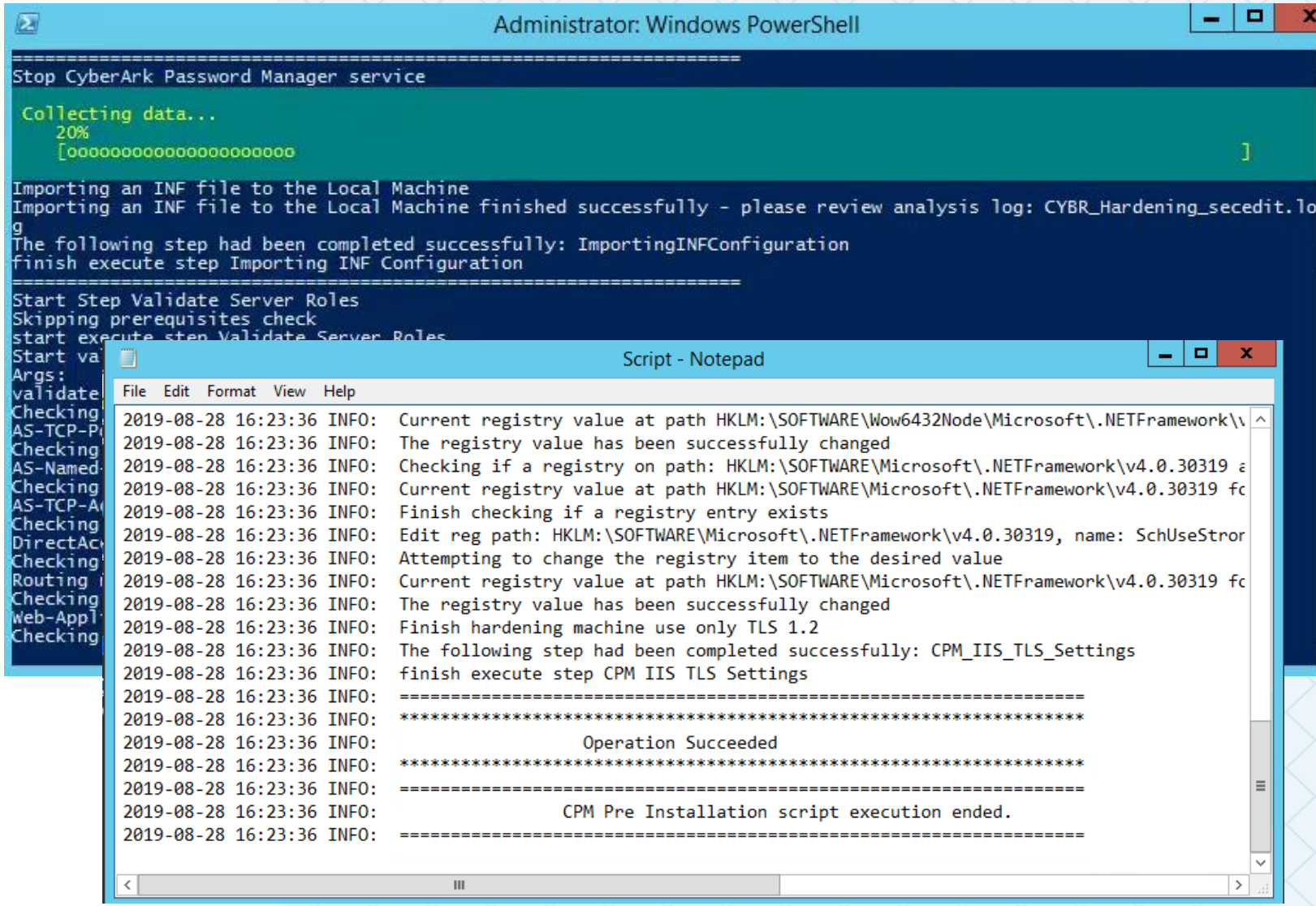
RECOMMENDED CPM SERVER SPECIFICATIONS

- CPM is supported on the following Windows Platforms
  - Windows 2019
  - Windows 2016
  - Windows 2012 R2
- .NET Framework 4.8 must be installed prior to installing CPM
- The CPM should not have access to or be accessible from the Internet.
- At least one PVWA server must be installed prior to installing CPM

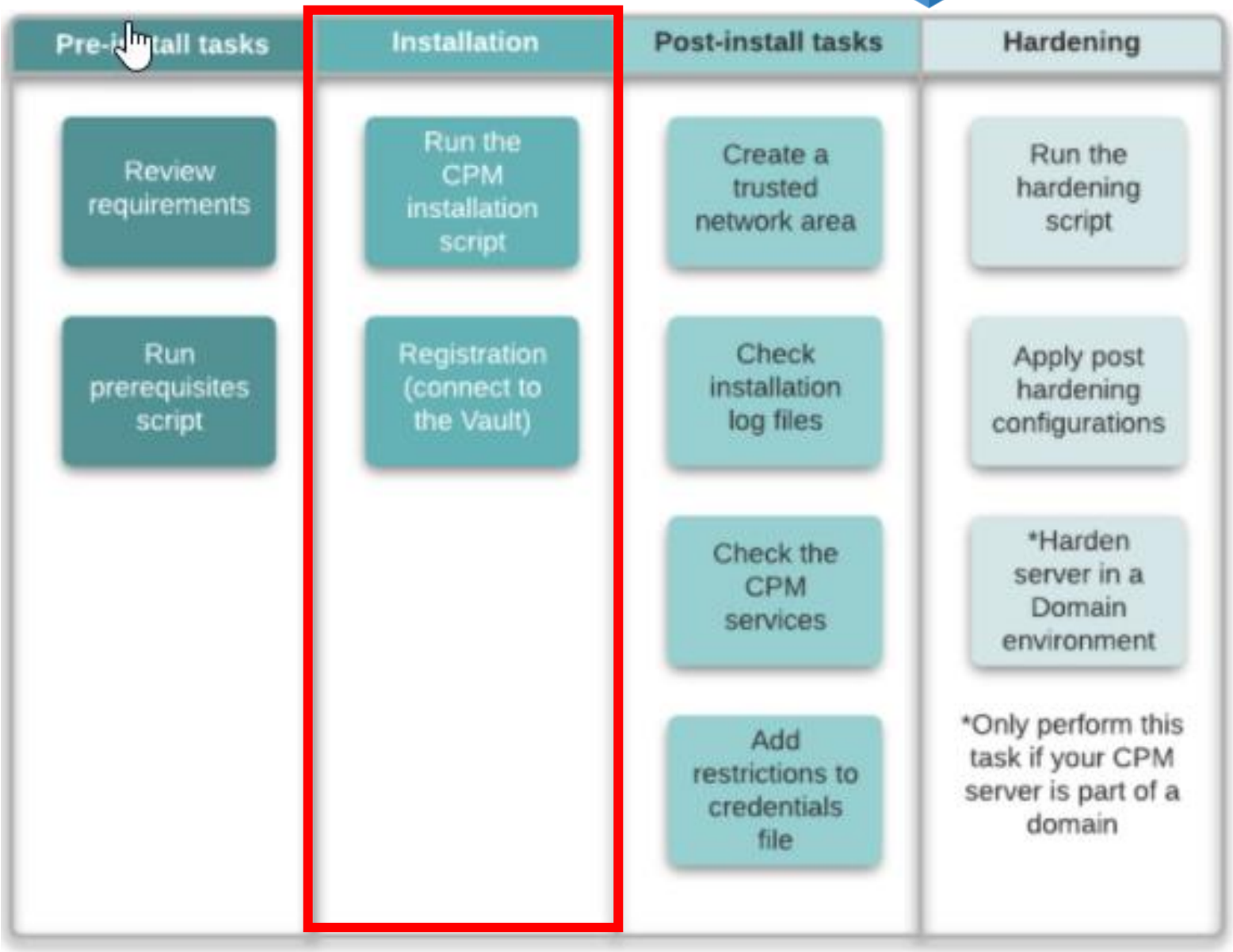
Small implementation (<1,000 managed passwords)	Mid-range implementation (1,000-20,000 managed passwords)	Large implementation (20,000 – 100,000 managed passwords)	Very large implementation (more than 100,000 managed passwords)
Hardware specifications			
• Quad core processor (Intel compatible) • 8GB RAM • 2X 80GB SATA/SAS hot-swappable drives • RAID Controller • Network adapter (1Gb) • DVD ROM	• 2X Quad core processor (Intel compatible) • 16GB RAM • 2X 80GB SATA/SAS hot-swappable drives • RAID Controller • Network adapter (1Gb) • DVD ROM	• 2X Eight core processors (Intel compatible) • 32GB RAM • 2X 80GB SAS hot-swappable drives • RAID Controller • Network adapter (1Gb) • DVD ROM	• 4X Eight core processors (Intel compatible) • 64GB RAM • 2X 80GB SAS hot-swappable drives • RAID Controller • Network adapter (1Gb) • DVD ROM
Software prerequisites			
• Windows 2019, Windows 2016, Windows 2012 R2 (Standard and Datacenter) • .NET Framework 4.8 • CPM can be installed on Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platforms			

INSTALL CPM PREREQUISITES

- If installing the CPM on a dedicated Windows Server, run the CPM_PreInstallation.ps1 script to enable TLS 1.2
- Launch the Installation Automation PowerShell script from an Administrator: Windows PowerShell
- Allow the script to complete and review the **script.log** file located in a sub-directory where the script is located

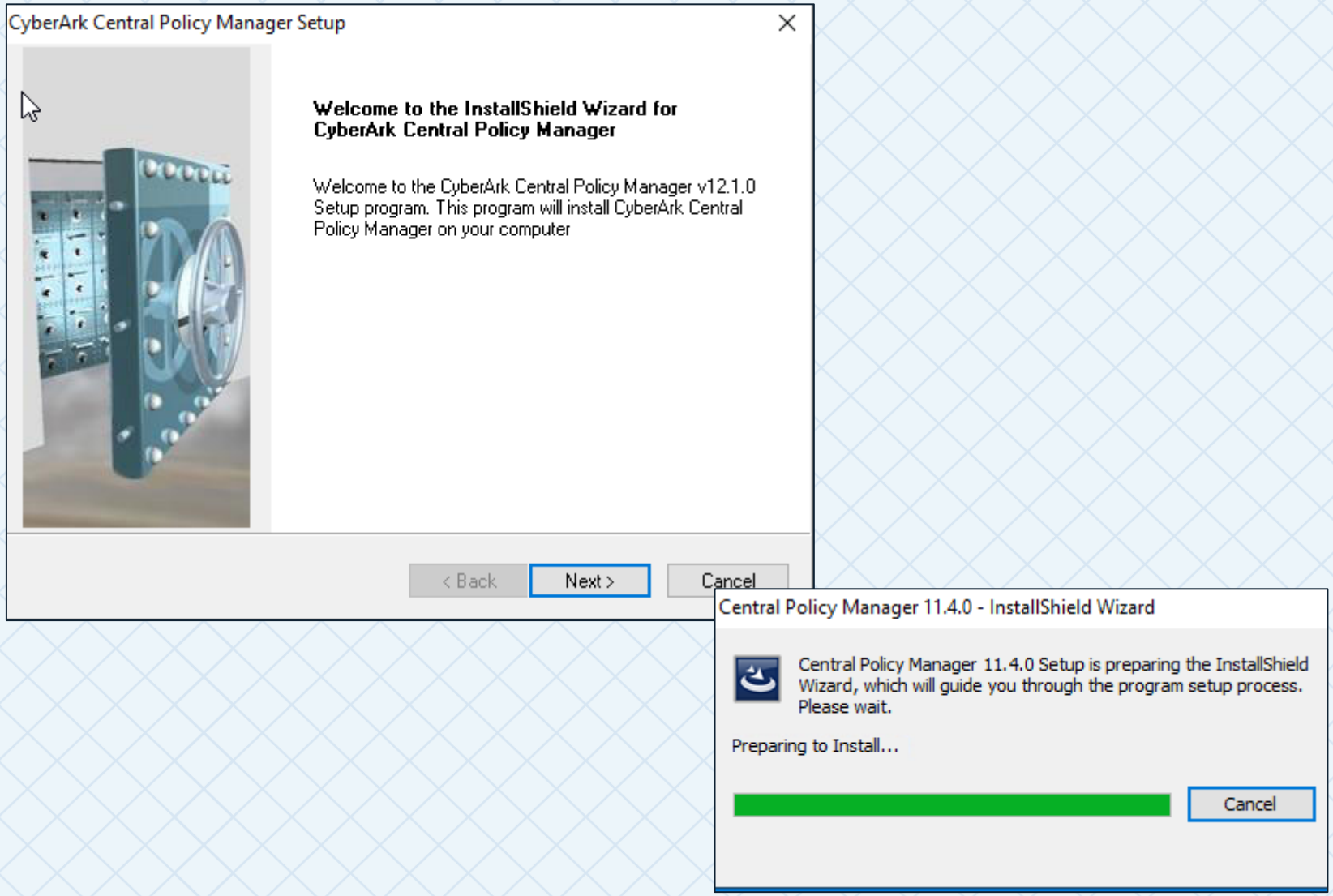


CPM INSTALLATION



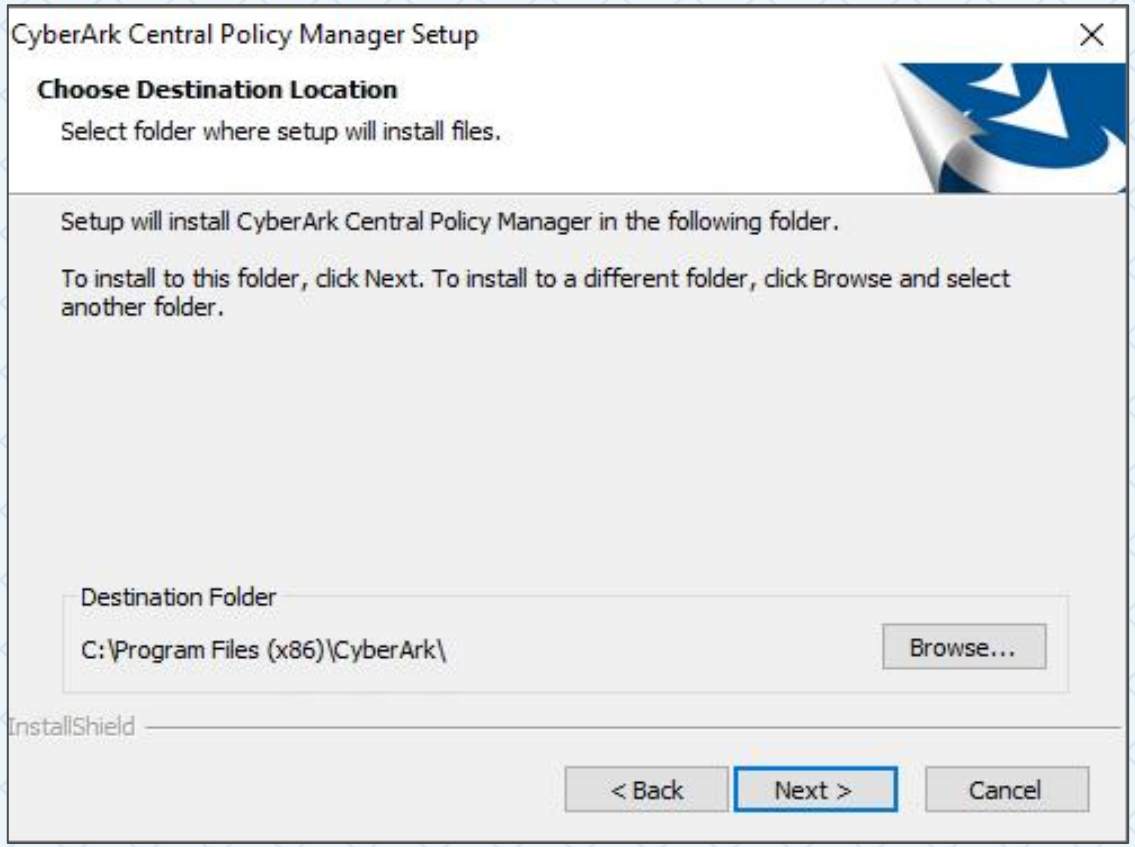
LAUNCH CPM SETUP

- Run setup.exe as administrator
- Press **Install** to install the required Microsoft Redistributable Package(s), if applicable
- Optionally install the CPM using Installation Automation script



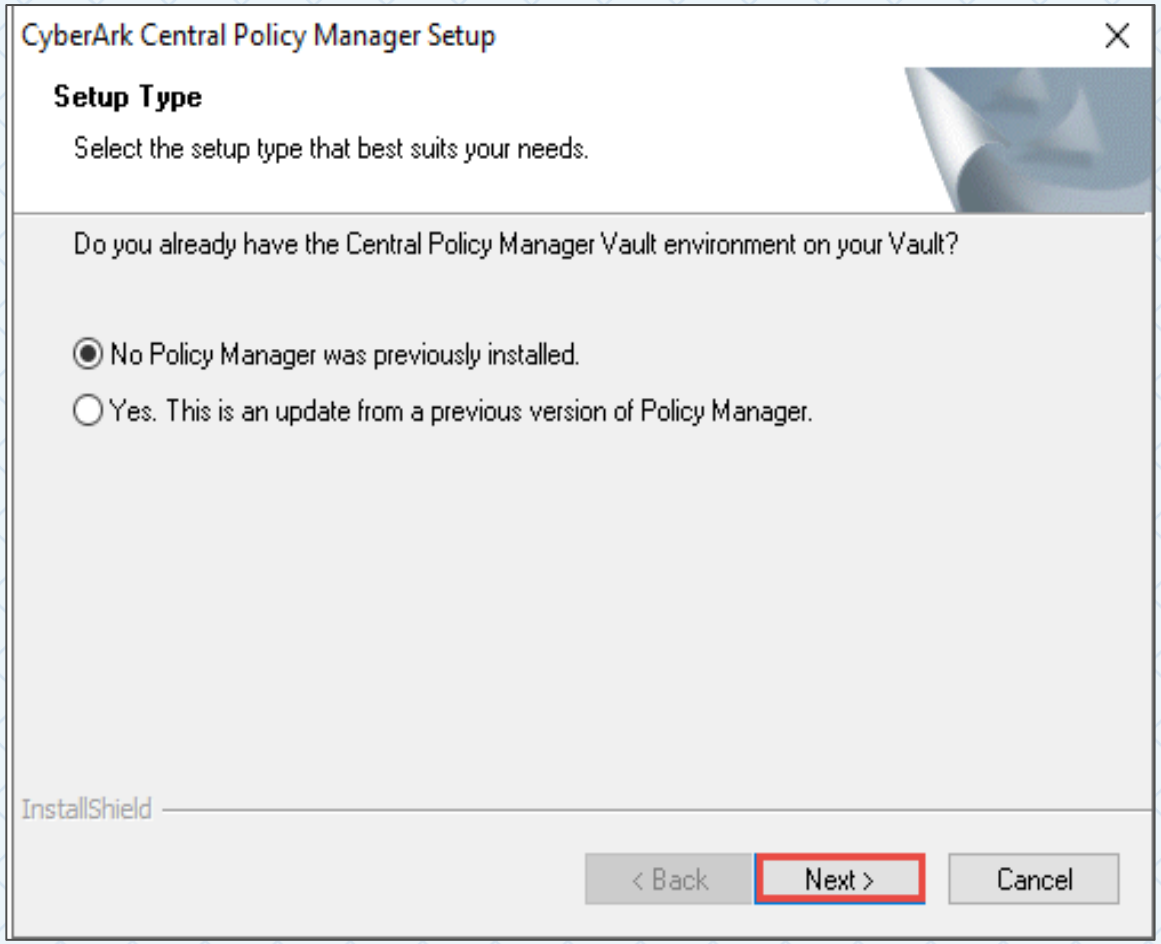
CHOOSE DESTINATION FOLDER

- Select the destination folder for the CPM files



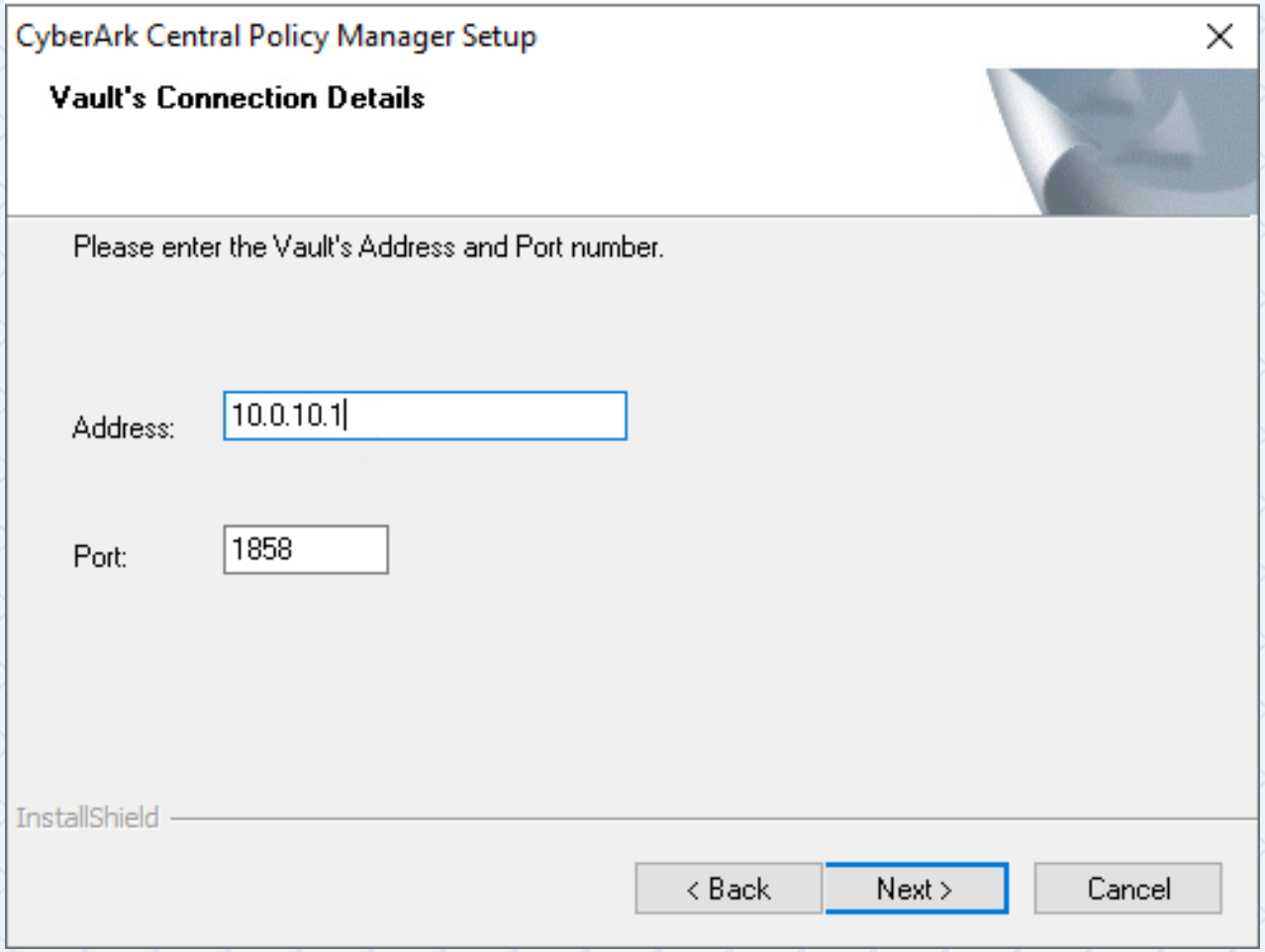
SETUP TYPE

- When installing a new CPM select *No Policy Manager was previously installed* and press **Next**
- Select **Yes** only in case of re-installing CPM software, that will use the license of a previously installed CPM.



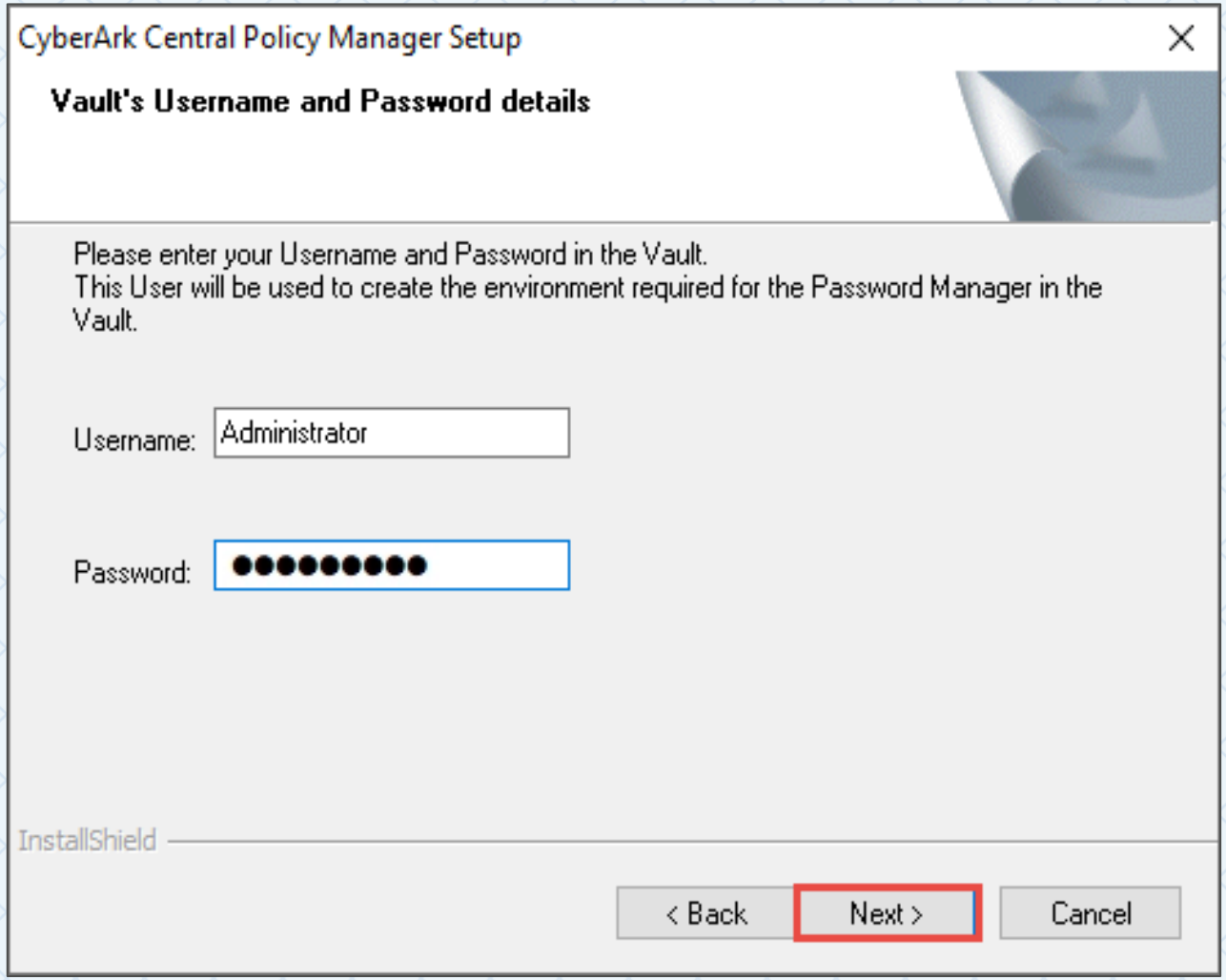
VAULT CONNECTION DETAILS

- Enter the IP **Address** of your Vault server
- By default the **Port** number is*1858*



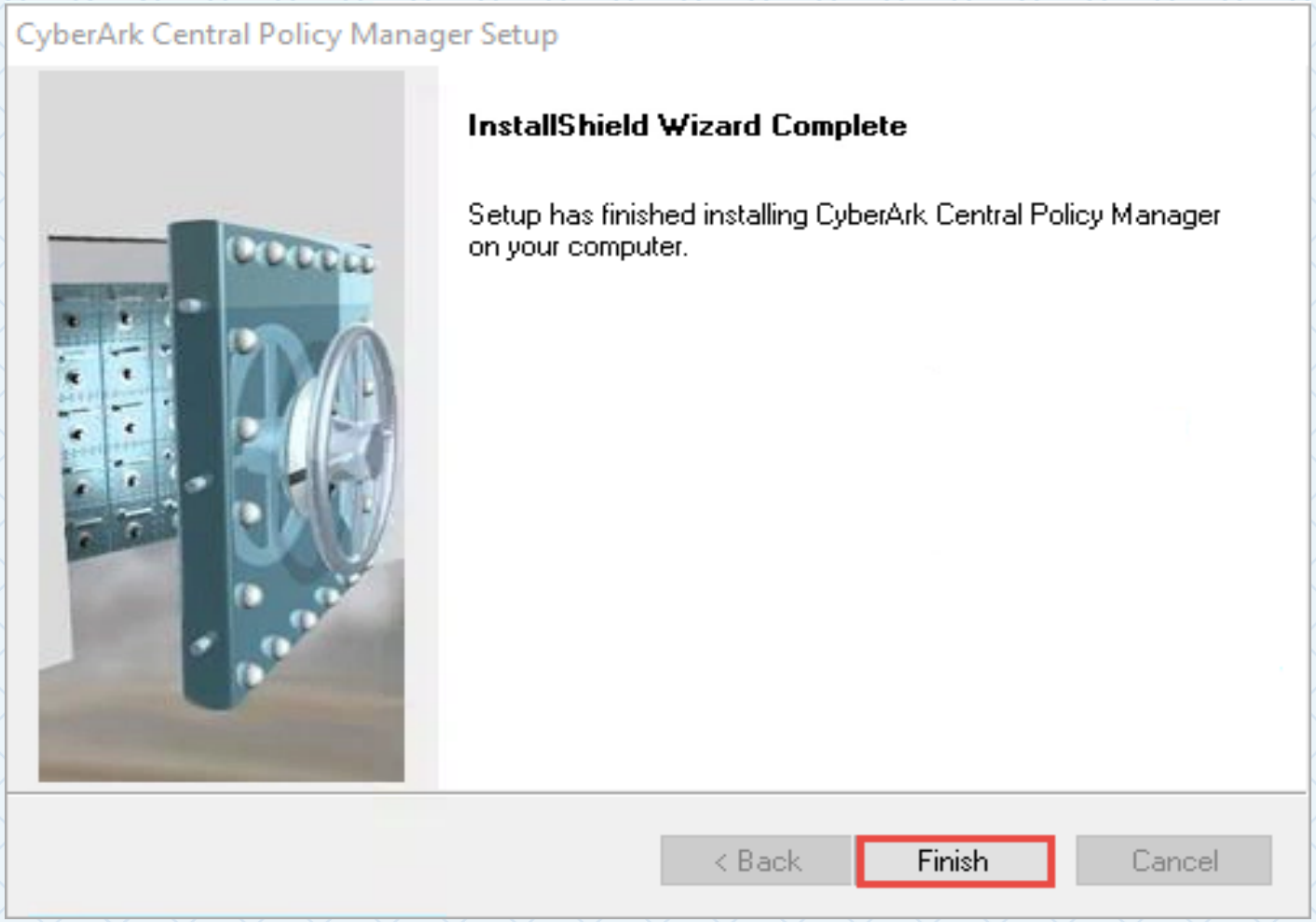
VAULT USERNAME AND PASSWORD DETAILS

- Enter the username and password of the Vault user that will be used to create the CPM environment on the Vault
- Typically, the built-in Administrator is used for installing the components

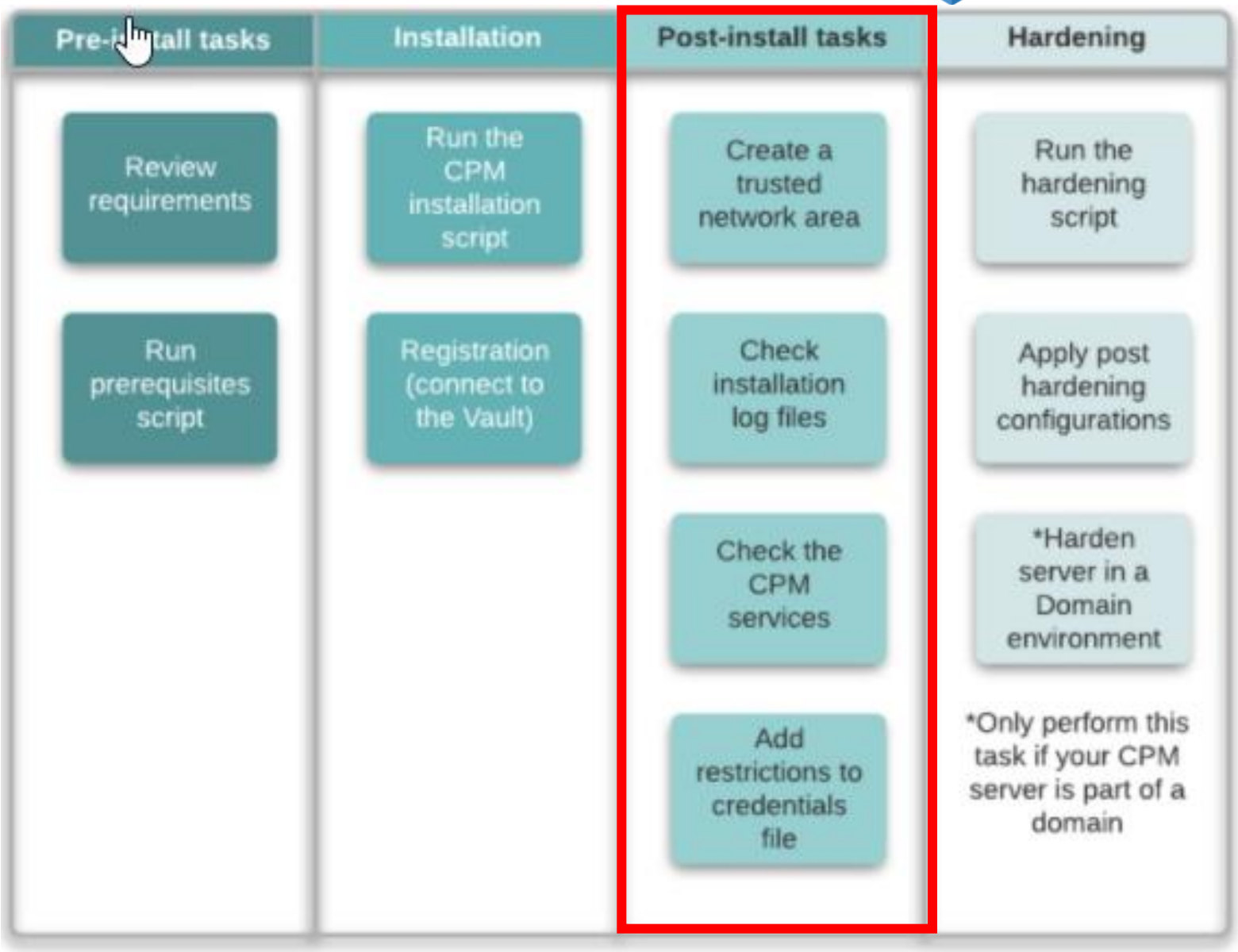


FINISH

- Press the **Finish** button to complete the installation
- There is no need for a reboot

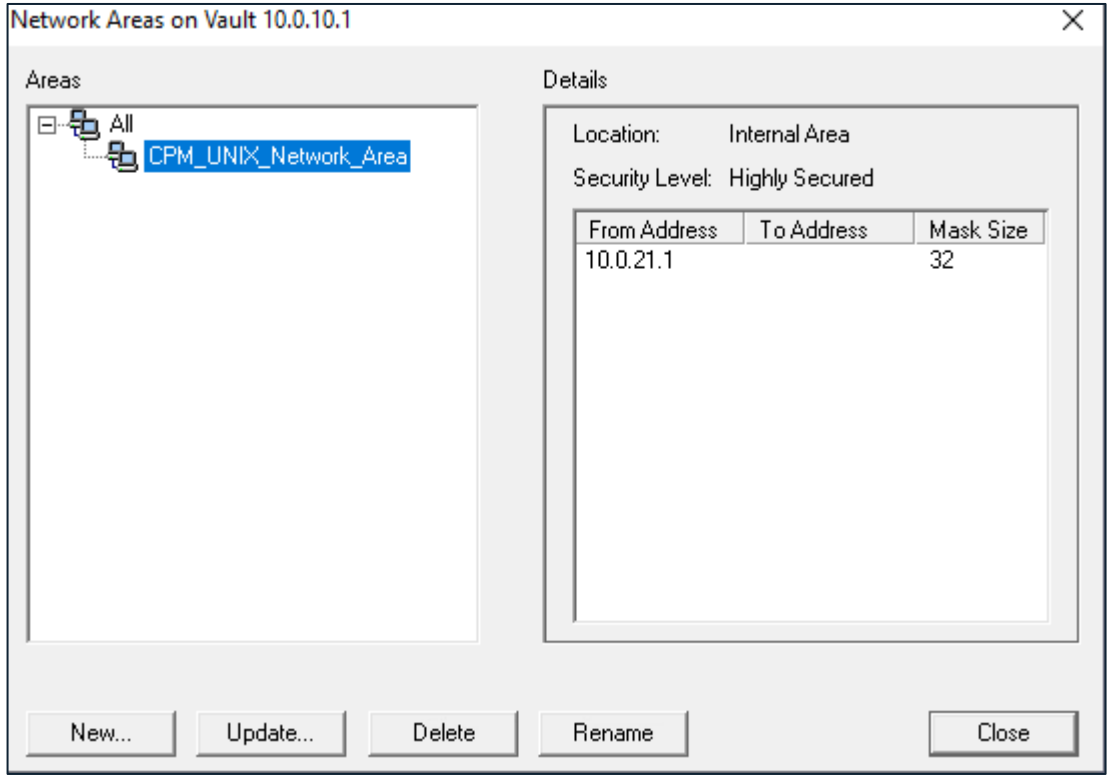


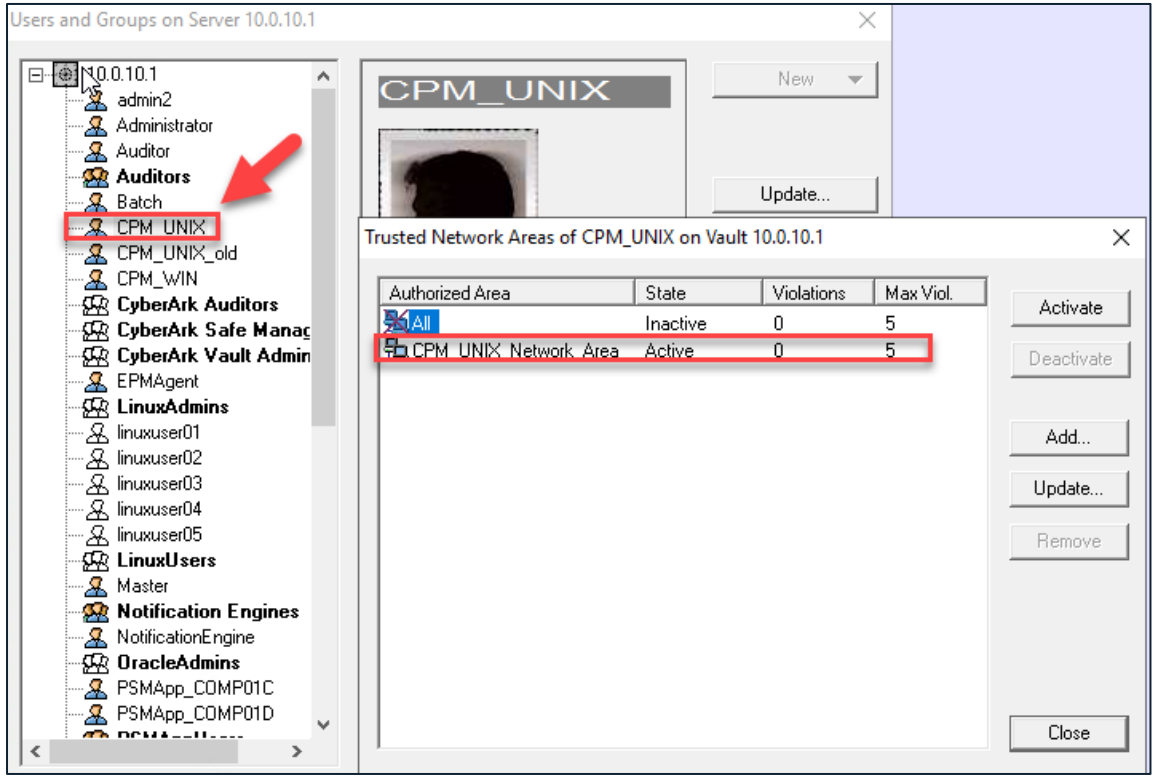
CPM POST-INSTALLATION



CREATE A TRUSTED NETWORK AREA

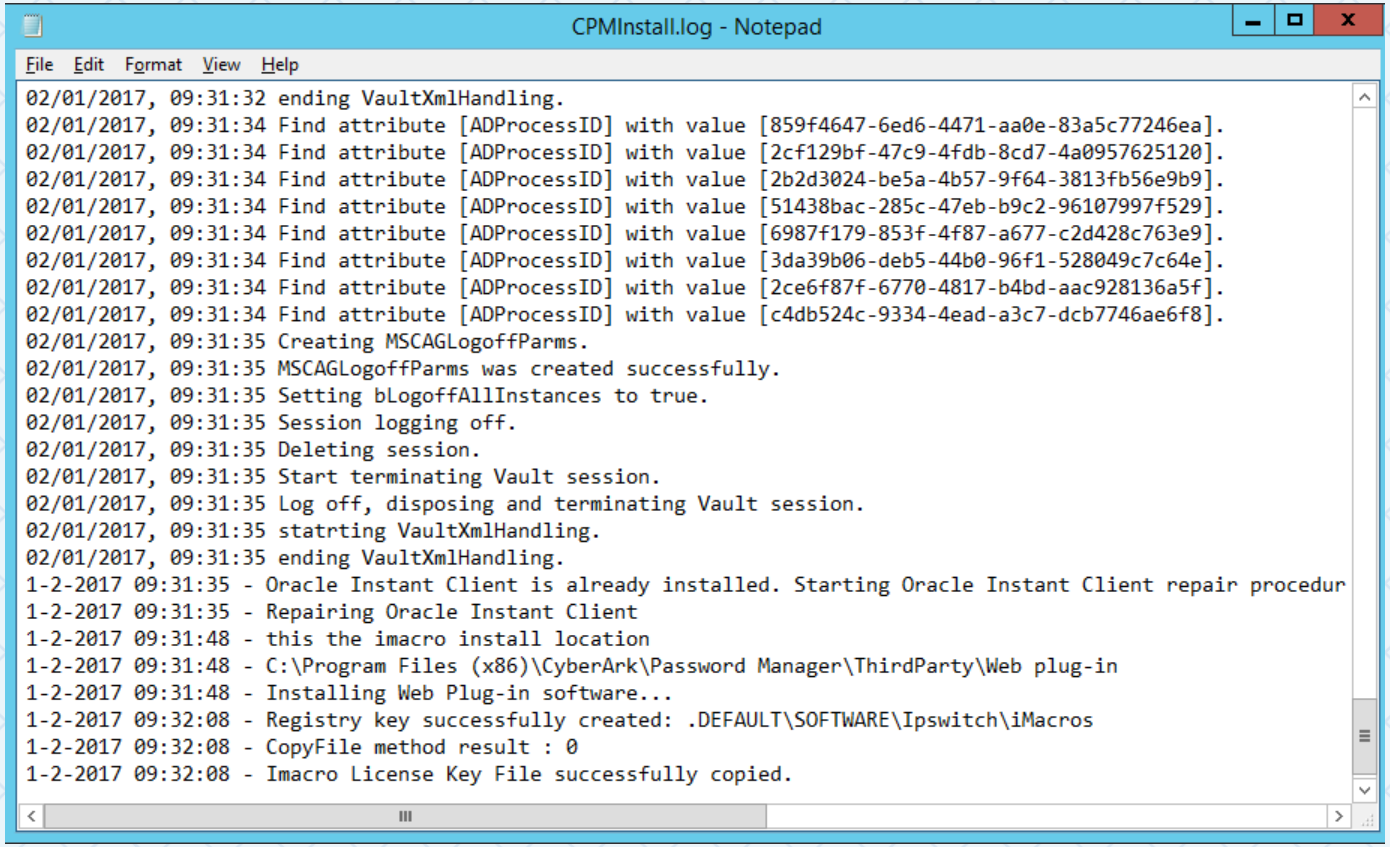
- CyberArk recommends creating a Trusted Network Area for the CPM, to ensure the CPM user can only log on to the Vault from the CPM machine
- Create a Network Area that includes only the IP address of the CPM machine, and from where the CPM user will log on to the Vault





CHECK THE INSTALLATION LOG FILES

- Review the CPMInstall.log to make sure the installation completed successfully.
- Errors during the installation process will show in this file
- The file is located in C:\Users\Administrator\AppData\Local\Temp
- Capture the log and move it to a different folder if an auditor intends to review it.




```
02/01/2017, 09:31:32 ending VaultXmlHandling.
02/01/2017, 09:31:34 Find attribute [ADProcessID] with value [859f4647-6ed6-4471-aa0e-83a5c77246ea].
02/01/2017, 09:31:34 Find attribute [ADProcessID] with value [2cf129bf-47c9-4fdb-8cd7-4a0957625120].
02/01/2017, 09:31:34 Find attribute [ADProcessID] with value [2b2d3024-be5a-4b57-9f64-3813fb56e9b9].
02/01/2017, 09:31:34 Find attribute [ADProcessID] with value [51438bac-285c-47eb-b9c2-96107997f529].
02/01/2017, 09:31:34 Find attribute [ADProcessID] with value [6987f179-853f-4f87-a677-c2d428c763e9].
02/01/2017, 09:31:34 Find attribute [ADProcessID] with value [3da39b06-deb5-44b0-96f1-528049c7c64e].
02/01/2017, 09:31:34 Find attribute [ADProcessID] with value [2ce6f87f-6770-4817-b4bd-aac928136a5f].
02/01/2017, 09:31:34 Find attribute [ADProcessID] with value [c4db524c-9334-4ead-a3c7-dcb7746ae6f8].
02/01/2017, 09:31:35 Creating MSCAGLogoffParms.
02/01/2017, 09:31:35 MSCAGLogoffParms was created successfully.
02/01/2017, 09:31:35 Setting bLogoffAllInstances to true.
02/01/2017, 09:31:35 Session logging off.
02/01/2017, 09:31:35 Deleting session.
02/01/2017, 09:31:35 Start terminating Vault session.
02/01/2017, 09:31:35 Log off, disposing and terminating Vault session.
02/01/2017, 09:31:35 statrting VaultXmlHandling.
02/01/2017, 09:31:35 ending VaultXmlHandling.
1-2-2017 09:31:35 - Oracle Instant Client is already installed. Starting Oracle Instant Client repair procedur
1-2-2017 09:31:35 - Repairing Oracle Instant Client
1-2-2017 09:31:48 - this the imacro install location
1-2-2017 09:31:48 - C:\Program Files (x86)\CyberArk\Password Manager\ThirdParty\Web plug-in
1-2-2017 09:31:48 - Installing Web Plug-in software...
1-2-2017 09:32:08 - Registry key successfully created: .DEFAULT\SOFTWARE\Ipswitch\iMacros
1-2-2017 09:32:08 - CopyFile method result : 0
1-2-2017 09:32:08 - Imacro License Key File successfully copied.
```

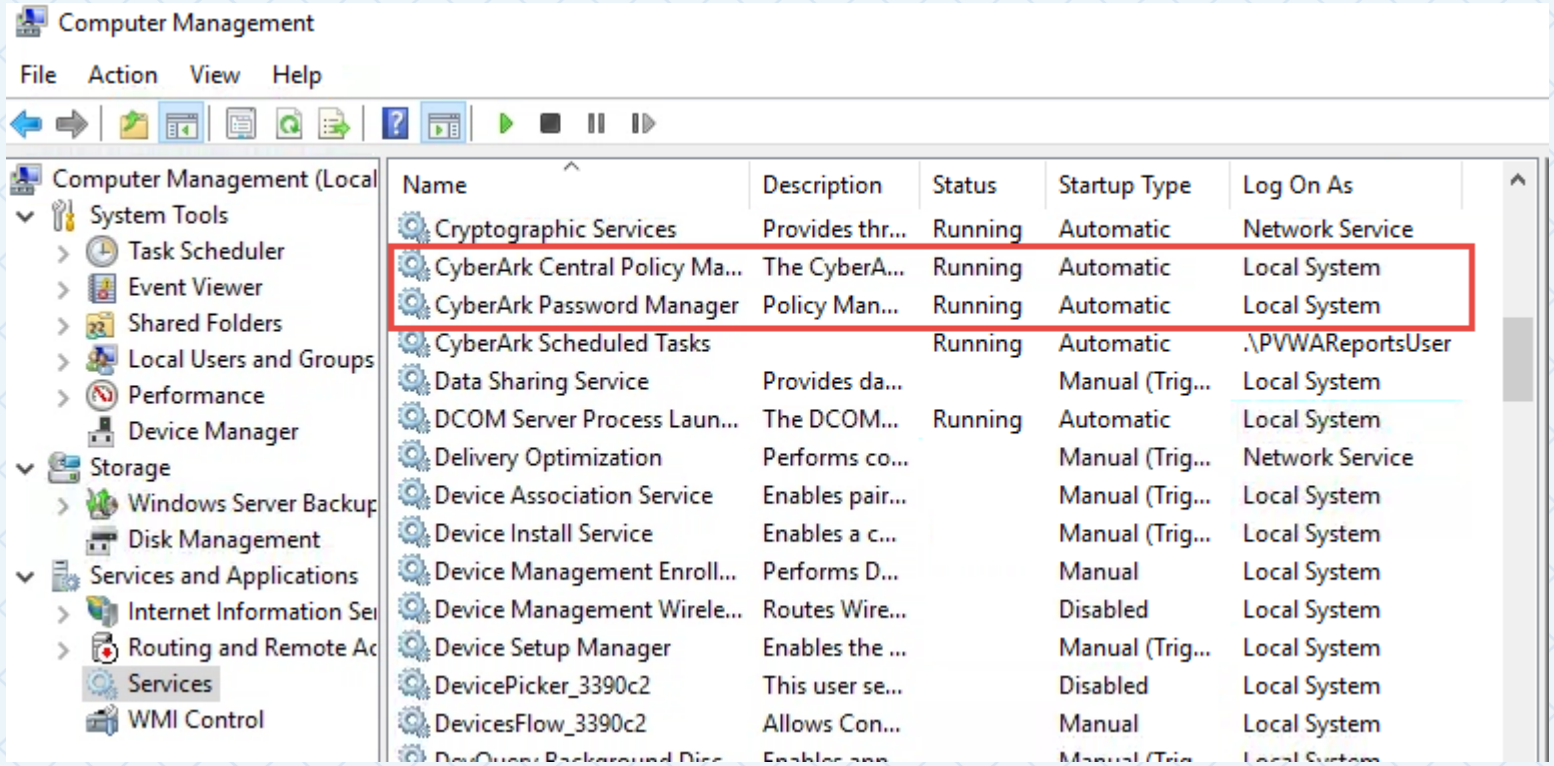
CPM LOGS

Activity Logs (Logs folder)	• pm.log – contains all the log messages, including general and informative messages, errors, and warnings. • pm_error.log – contains only warning and error messages.
Third party log files (Logs\ThirdParty folder)	• Generated by the Central Password Manager built-in password generation plug-ins when an error occurs • Name of the log file: <type of password>-<Safe>-<folder>-<name of password object>.log Operating System-UnixSSH-1.1.1.250-Root.log:
History log files (Logs\History folder)	• After a log file has been uploaded into the Safe, it is renamed and moved into the History subfolder. • The file is marked with a time stamp and renamed as follows: <filename> (<date>-<time>).log

Search on “Configure Debug Levels” online at docs.cyberark.com for reference for detailed information

CHECK THE CPM SERVICES

- CyberArk Password Manager executes all password management operations.
- CyberArk Central Policy Manager Scanner is associated with the Accounts Discovery utility
- Note that the CPM Services <u>before hardening</u> are running under “Local System”



CREDENTIAL FILE SECURITY

Add restrictions to the protected credentials file

- During installation, a credentials file is created to enable the CPM user to log on to the Vault
- To enhance the security of the credentials file, use the CreateCredFile utility in the Env folder to create a protected credentials file
- For more information, see "*User credential files*" on docs.cyberark.com

Administrator: Windows PowerShell

```
PS C:\Program Files (x86)\CyberArk\Password Manager\Vault> .\CreateCredFile.exe user.ini
Vault Username [mandatory] ==> CPM_UNIX
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] ==> CPM
Restrict to Executable Path [optional] ==>
Restrict to current machine IP (yes/no) [No] ==> yes
Restrict to current machine hostname (yes/no) [No] ==> yes
Restrict to OS User name [optional] ==>
Display Restrictions in output file (yes/no) [No] ==> yes
Use Operating System Protected Storage for credentials file secret (Machine/User/No) [No] ==>
Command ended successfully
PS C:\Program Files (x86)\CyberArk\Password Manager\Vault>
```

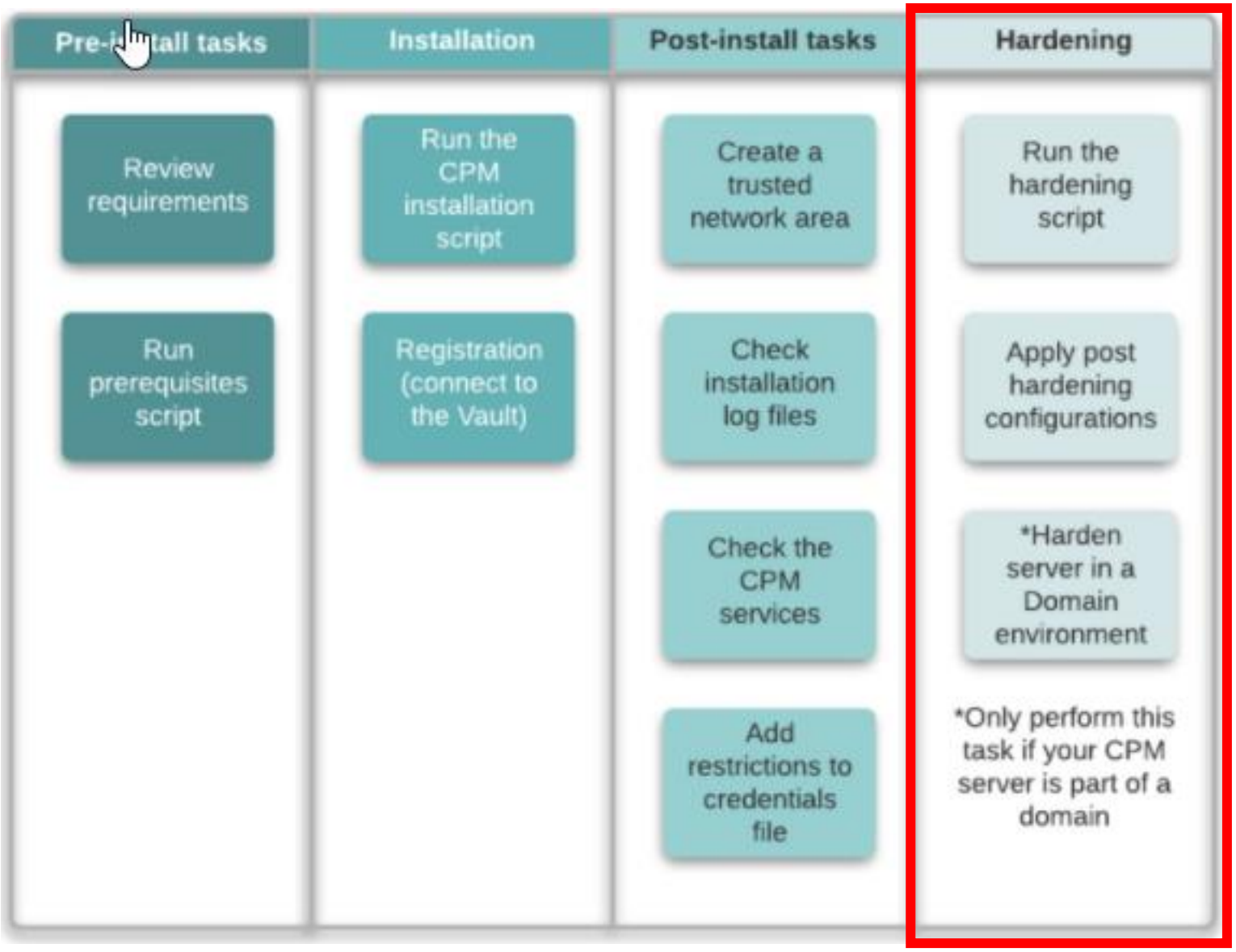
user.ini - Notepad

File Edit Format View Help

```
CredFileType=Password
CredFileVersion=2
Username=CPM_UNIX
VerificationsFlag=53
Password=4208064856CF2AA59F7ACFA039C451A874C6A043A4B10F565279D8F0B4B8
ExternalAuthentication=No
AdditionalInformation=18865AC801485BF14BC1E8A7FF1EB59A0380C255
ClientApp=CPM
ClientIP=10.0.21.1
ClientHostname=comp01b
```

HARDENING THE CPM

Security hardening operations on CyberArk PAS component servers is an emphasized area of study for all CyberArk certifications!



INSTALLATION AUTOMATION HARDENING SCRIPT

- In v12.x there are separate hardening scripts for In-domain and workgroup installations
  - CPM_In_Domain_Hardening.ps1
  - CPM_Hardening.ps1

CPM_In_Domain_Hardening_Config.xml

```xml
<Stage Name="Hardening" Version="1.0">
  <Step Name="ImportingINFConfiguration" DisplayName="Importing INF Configuration" ScriptName="ImportingINFConfiguration.psm1" Enable="No" Version="10.1">
    <Parameters>
      <Parameter Name="IsPSMInstalled" Value="False"/>
    </Parameters>
  </Step>

  <Step Name="ValidateServerRoles" DisplayName="Validate Server Roles" ScriptName="ValidateServerRoles.psm1"  Enable="Yes" Version="10.1">
    <Parameters>
      <Parameter Name="IsPSMInstalled" Value="False"/>
    </Parameters>
  </Step>

  <Step Name="DisableScreenSaver" DisplayName="Disable ScreenSaver" ScriptName="DisableScreenSaver.psm1" Enable="No" Version="10.1"/>

  <Step Name="AdvancedAuditPolicyConfiguration" DisplayName="Advanced Audit Policy Configuration" ScriptName="AdvancedAuditPolicyConfiguration.psm1"  Enable="No" Version="10.1"/>

  <Step Name="RemoteDesktopServices" DisplayName="Remote Desktop Services" ScriptName="RemoteDesktopServices.psm1" Enable="No" Version="10.1">
    <Parameters>
      <Parameter Name="IsPSMInstalled" Value="False"/>
    </Parameters>
  </Step>

  <Step Name="EventLogSizeAndRetention" DisplayName="EventLog Size And Retention" ScriptName="EventLogSizeAndRetention.psm1" Enable="No" Version="10.1"/>

  <Step Name="RegistryAudits" DisplayName="Registry Audits" ScriptName="RegistryAudits.psm1"  Enable="No" Version="10.1"/>

  <Step Name="RegistryPermissions" DisplayName="Registry Permissions" ScriptName="RegistryPermissions.psm1" Enable="No" Version="10.1"/>

  <Step Name="FileSystemPermissions" DisplayName="FileSystem Permissions" ScriptName="FileSystemPermissions.psm1" Enable="No" Version="10.1"/>

  <Step Name="FileSystemAudit" DisplayName="FileSystem Audit" ScriptName="FileSystemAudit.psm1"  Enable="No" Version="10.1"/>

  <Step Name="PasswordManagerServicesLocalUser" DisplayName="CPM Password Manager Services LocalUser" ScriptName="CPM_Password_Manager_Services_LocalUser.psm1" Enable="Yes" Version="10.1"/>

  <Step Name="DisableServices" DisplayName="Disable Services" ScriptName="DisableServices.psm1" Enable="Yes" Version="10.1"/>

  <Step Name="EnableFIPSCryptography" DisplayName="CPM Enable FIPS Cryptography" ScriptName="CPMEnableFIPSCryptography.psm1" Enable="No" Version="10.1"/>

  <Step Name="DisableDEPForExecutables" DisplayName="CPM Disable DEP For Executables" ScriptName="CPM_DisableDEPForExecutables.psm1" Enable="Yes" Version="10.1"/>

</Stage>
```

INSTALLATION AUTOMATION HARDENING SCRIPT

- Both hardening scripts have a corresponding configuration file
- CPM_In_Domain_Hardening_Config.xml
- CPM_Hardening_Config.xml

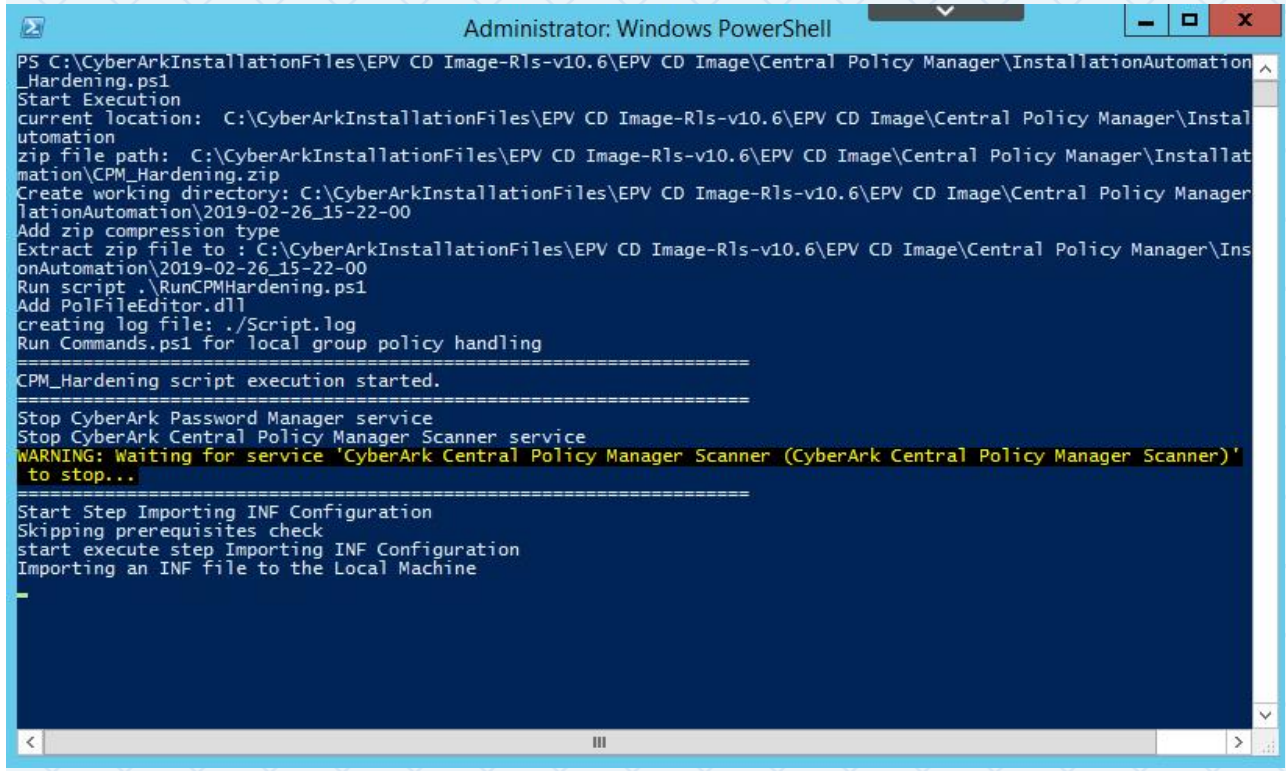
- The options provided in the configuration files are intended for CPM upgrades to prevent a reset of intentional changes

CPM_In_Domain_Hardening_Config.xml

```xml
<Stage Name="Hardening" Version="1.0">
  <Step Name="ImportingINFConfiguration" DisplayName="Importing INF Configuration" ScriptName="ImportingINFConfiguration.psm1" Enable="No" Version="10.1">
    <Parameters>
      <Parameter Name="IsPSMInstalled" Value="False"/>
    </Parameters>
  </Step>

  <Step Name="ValidateServerRoles" DisplayName="Validate Server Roles" ScriptName="ValidateServerRoles.psm1"  Enable="Yes" Version="10.1">
    <Parameters>
      <Parameter Name="IsPSMInstalled" Value="False"/>
    </Parameters>
  </Step>

  <Step Name="DisableScreenSaver" DisplayName="Disable ScreenSaver" ScriptName="DisableScreenSaver.psm1" Enable="No" Version="10.1"/>

  <Step Name="AdvancedAuditPolicyConfiguration" DisplayName="Advanced Audit Policy Configuration" ScriptName="AdvancedAuditPolicyConfiguration.psm1"  Enable="No" Version="10.1"/>

  <Step Name="RemoteDesktopServices" DisplayName="Remote Desktop Services" ScriptName="RemoteDesktopServices.psm1" Enable="No" Version="10.1">
    <Parameters>
      <Parameter Name="IsPSMInstalled" Value="False"/>
    </Parameters>
  </Step>

  <Step Name="EventLogSizeAndRetention" DisplayName="EventLog Size And Retention" ScriptName="EventLogSizeAndRetention.psm1" Enable="No" Version="10.1"/>

  <Step Name="RegistryAudits" DisplayName="Registry Audits" ScriptName="RegistryAudits.psm1"  Enable="No" Version="10.1"/>

  <Step Name="RegistryPermissions" DisplayName="Registry Permissions" ScriptName="RegistryPermissions.psm1" Enable="No" Version="10.1"/>

  <Step Name="FileSystemPermissions" DisplayName="FileSystem Permissions" ScriptName="FileSystemPermissions.psm1" Enable="No" Version="10.1"/>

  <Step Name="FileSystemAudit" DisplayName="FileSystem Audit" ScriptName="FileSystemAudit.psm1"  Enable="No" Version="10.1"/>

  <Step Name="PasswordManagerServicesLocalUser" DisplayName="CPM Password Manager Services LocalUser" ScriptName="CPM_Password_Manager_Services_LocalUser.psm1" Enable="Yes" Version="10.1"/>

  <Step Name="DisableServices" DisplayName="Disable Services" ScriptName="DisableServices.psm1" Enable="Yes" Version="10.1"/>

  <Step Name="EnableFIPSCryptography" DisplayName="CPM Enable FIPS Cryptography" ScriptName="CPMEnableFIPSCryptography.psm1" Enable="No" Version="10.1"/>

  <Step Name="DisableDEPForExecutables" DisplayName="CPM Disable DEP For Executables" ScriptName="CPM_DisableDEPForExecutables.psm1" Enable="Yes" Version="10.1"/>

</Stage>
```

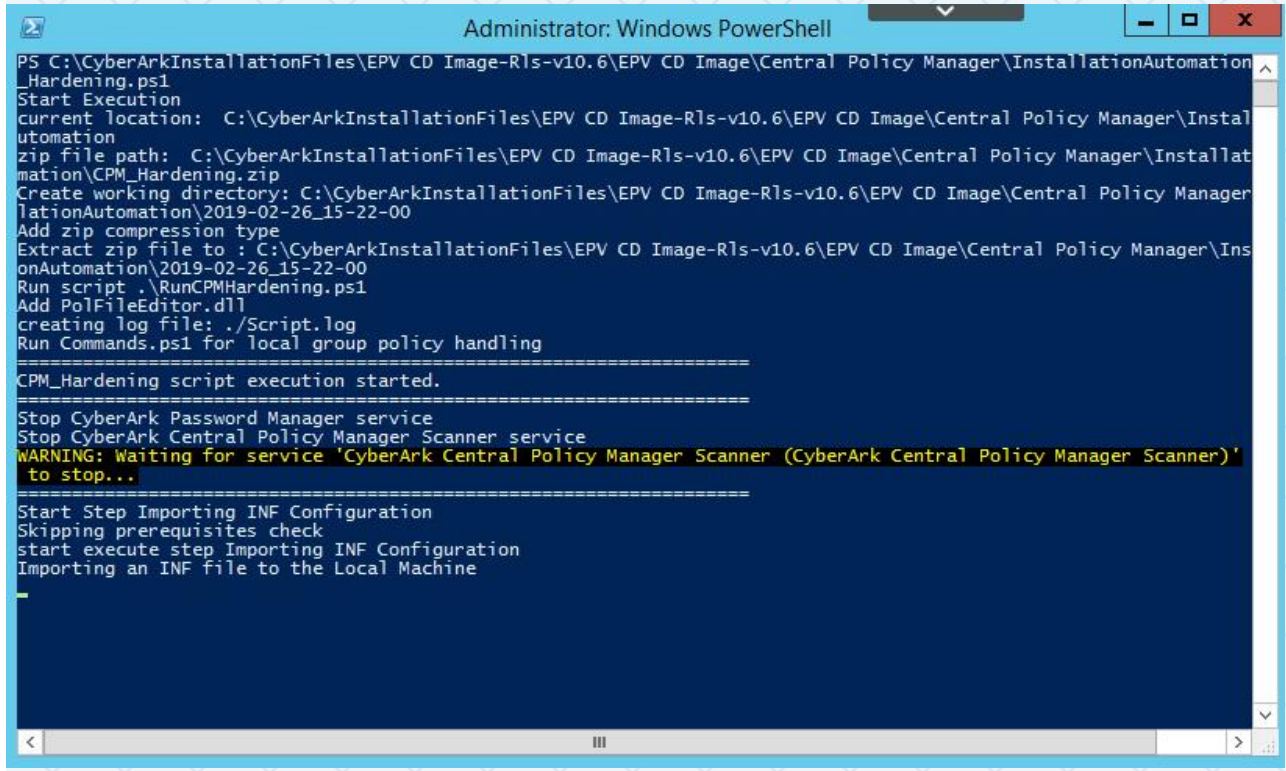
RUN THE HARDENING SCRIPT

- CPM Installation Automation hardening PowerShell script accomplishes the following
  - Validates roles and services, and sets file system permissions
  - Policy configuration
  - Sets EventLog size and retention

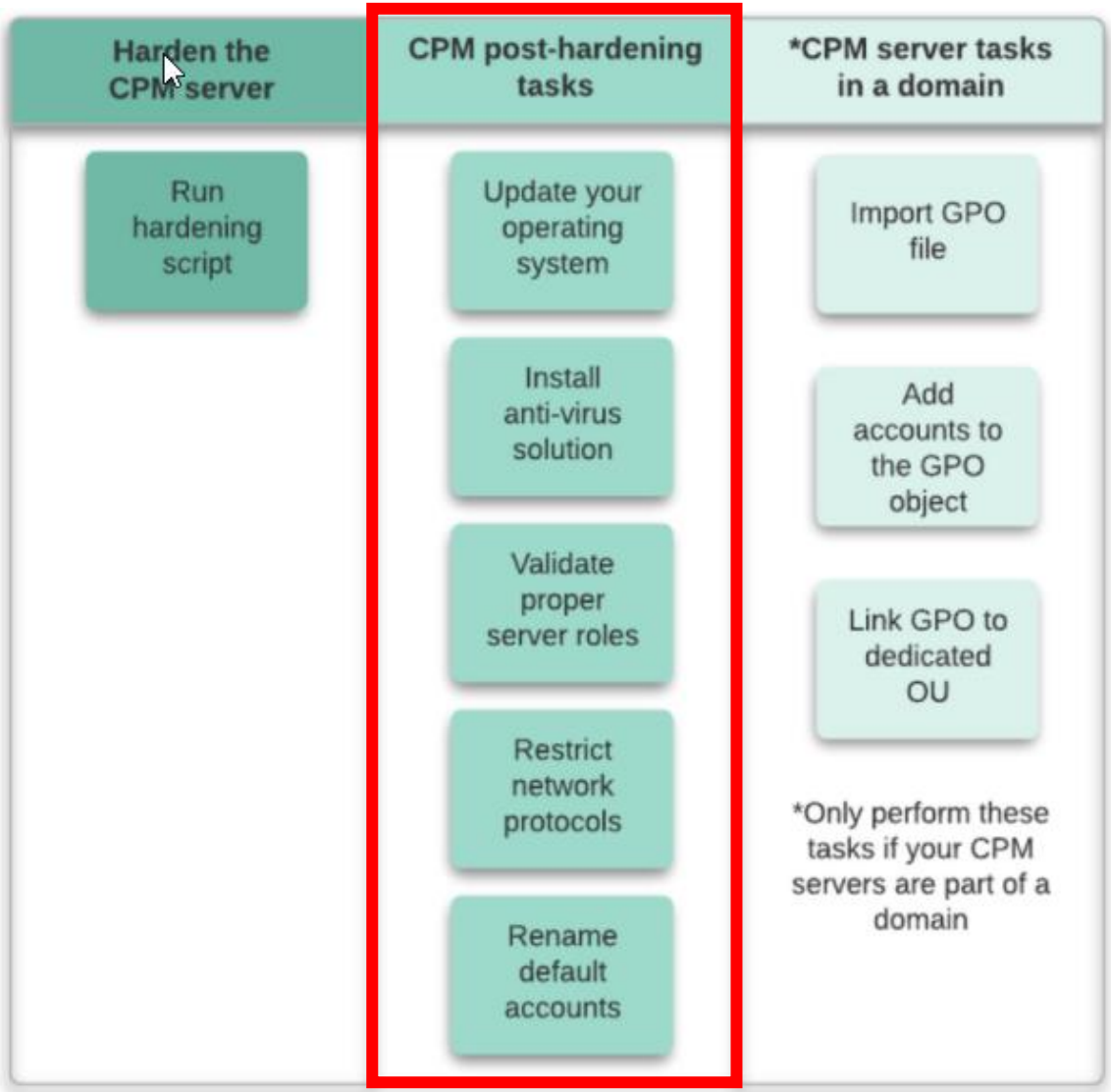


RUN THE HARDENING SCRIPT

- CPM Installation Automation hardening PowerShell script accomplishes the following
  - General auditing, registry, and file system configuration
  - Creates the CPM Password Manager Services local user "*PasswordManagerUser*"
    - Account property "Password never expires" should be set
  - Disables unnecessary services
  - Configures an exception in Data Execution Prevention(DEP) on files used by the CPM



APPLY POST HARDENING CONFIGURATIONS



POST HARDENING CONFIGURATIONS

Update your operating system

- Component servers should participate in an organizations Vulnerability Management Program
- Microsoft releases periodic updates (security updates and service packs) to address security issues that have been discovered in their software
- Make sure your operating system is updated to the latest version

Install an Anti-Virus Solution

- Servers without anti-virus protection are exposed to two risks:
  - Servers infected with viruses that might damage the server and the entire network
  - Trojan horses that are planted to allow remote control of the server and to all the information on it
- Keep your Anti-Virus solution updated!

POST HARDENING CONFIGURATIONS

Validate proper server roles

- Server roles can be set using the Server Manager.
- Ensure that unnecessary roles are not installed on the server

Restrict network protocols

- Install only the required protocols, clients and services.
- Remove anything unnecessary to the operation of the CPM
- Only the following network protocols, services or clients are required for a CPM and/or a PVWA Component Server:
  - Client for Microsoft Network
  - File and Printer Sharing for Microsoft Network
  - Internet Protocol Version 4 (TCP/IPv4)

POST HARDENING CONFIGURATIONS

Validate proper server roles

- Server roles can be set using the Server Manager.
- Ensure that unnecessary roles are not installed on the server

Rename default accounts

- CyberArk recommends to change the names of both the Administrator and the guest account to names that don't provide information about their permissions

Restrict network protocols

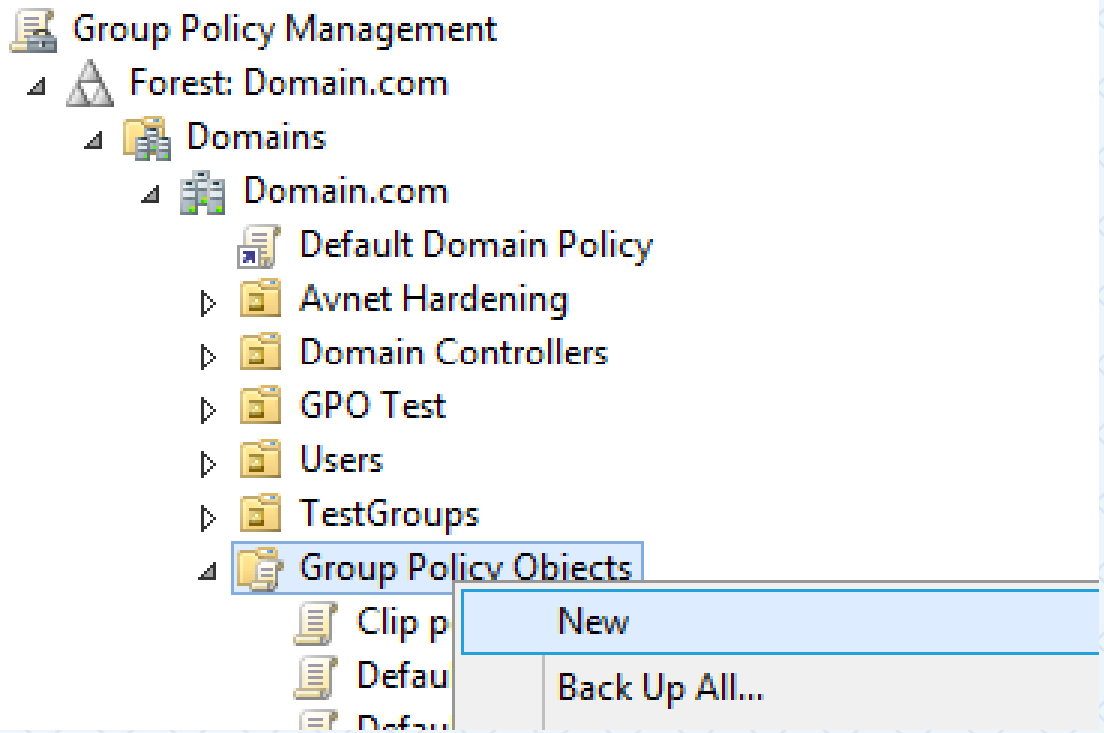
- Install only the required protocols, clients and services.
- Remove anything unnecessary to the operation of the CPM
- Only the following network protocols, services or clients are required for a CPM and/or a PVWA Component Server:
  - Client for Microsoft Network
  - File and Printer Sharing for Microsoft Network
  - Internet Protocol Version 4 (TCP/IPv4)

APPLY POST HARDENING CONFIGURATIONS

Harden the CPM server	CPM post-hardening tasks	*CPM server tasks in a domain
Run hardening script	Update your operating system	Import GPO file
	Install anti-virus solution	Add accounts to the GPO object
	Validate proper server roles	Link GPO to dedicated OU
	Restrict network protocols	*Only perform these tasks if your CPM servers are part of a domain
	Rename default accounts	

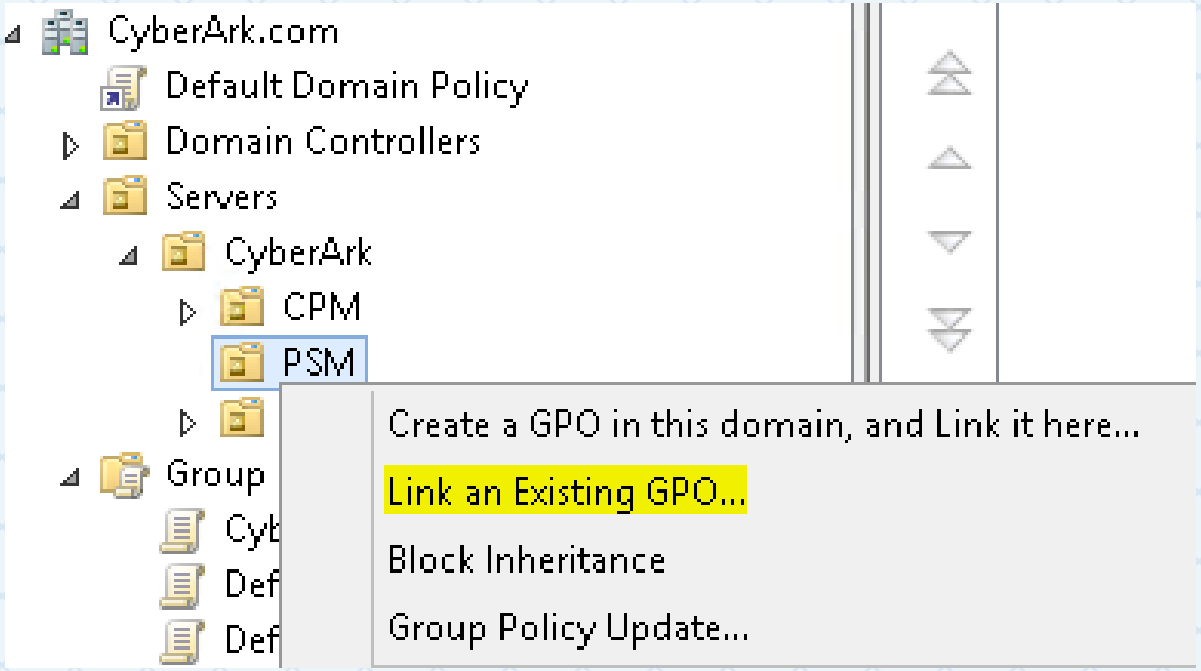
IMPORT A GPO FILE TO AN ACTIVE DIRECTORY DOMAIN

- Online documentation provides instructions are provided for GPO deployment for in-Domain environments
- The Domain Administrator should create a dedicated OU for each component server type and configure “Block Inheritance” of existing Group Policy Objects
- Add applicable accounts to the GPO object
  - The CPM hardening script created a local user to run CPM services. This user requires the “Logon as a service” right that is enforced by the hardening GPO
  - Update other settings as required by the organization



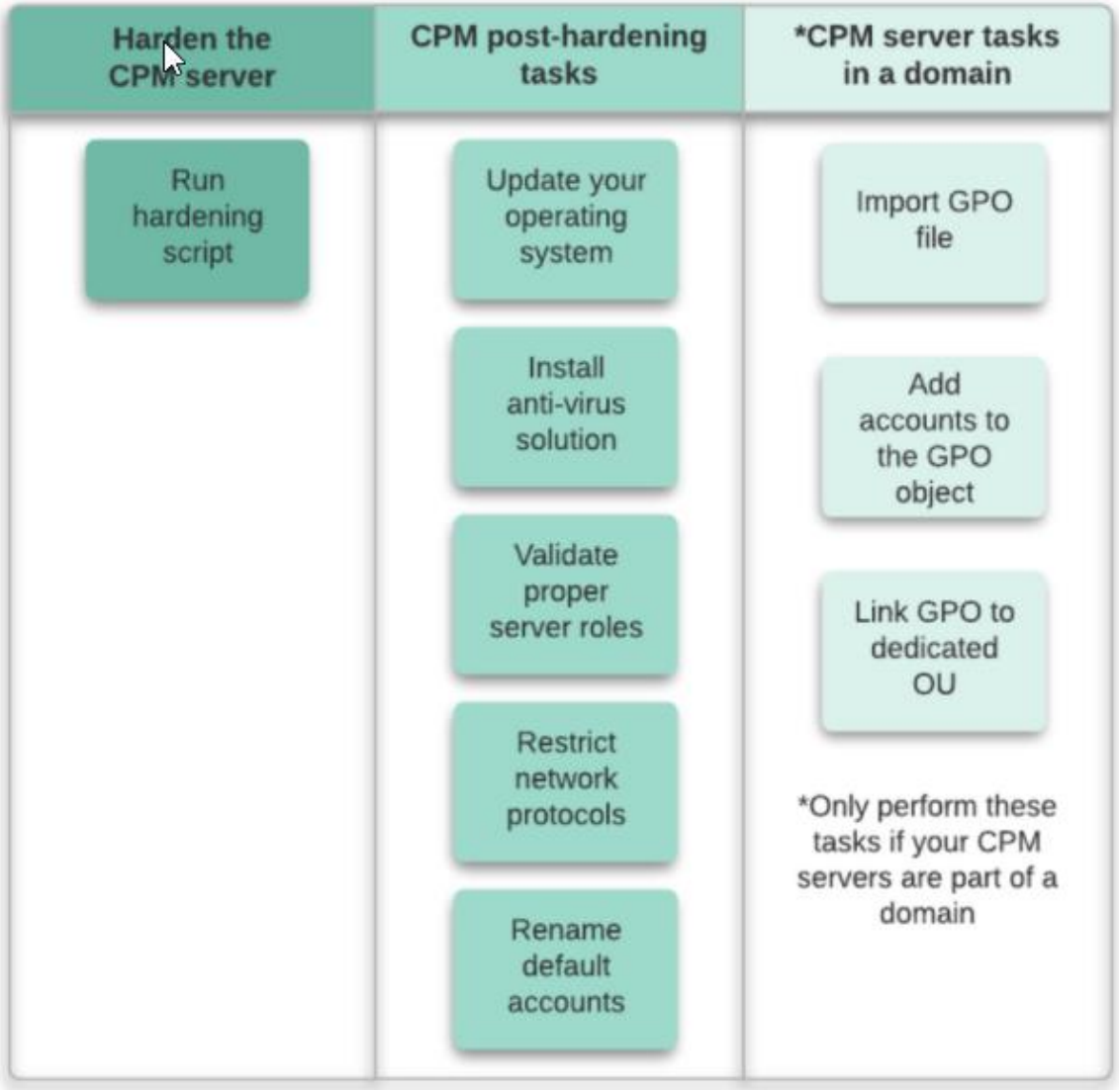
LINK THE CYBERARK CPM GPO TO A DEDICATED OU

- Link the GPO to a dedicated OU containing CyberArk servers
- Make sure all CPM servers are located under a dedicated OU, so the GPO will not affect any other server
- Update the GPO as required to comply with the customers security policies



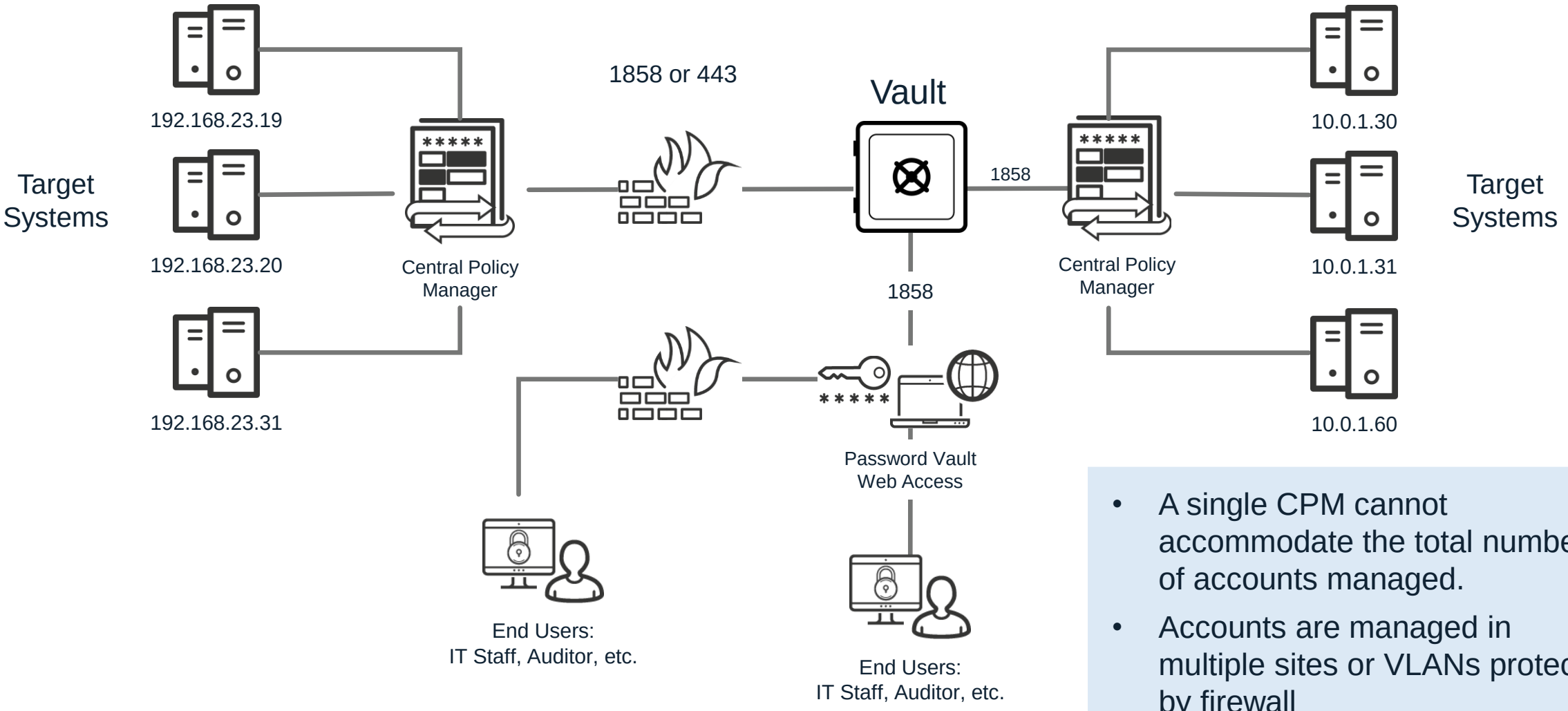
HARDENING OVERVIEW – GPO/INF

- Out of Domain (Workgroup) Hardening via INF Import
  - When the CPM and PVWA server environments are not a member of an Active Directory domain ('Out of Domain'), the hardening procedure is applied via an INF file
- A complete list of all CyberArk GPO settings is available online at docs.cyberark.com
- Search CyberArk Docs for "*CPM Hardening*" for automatic and manual procedures for hardening CyberArk's CPM and PVWA servers



MULTIPLE CPMS

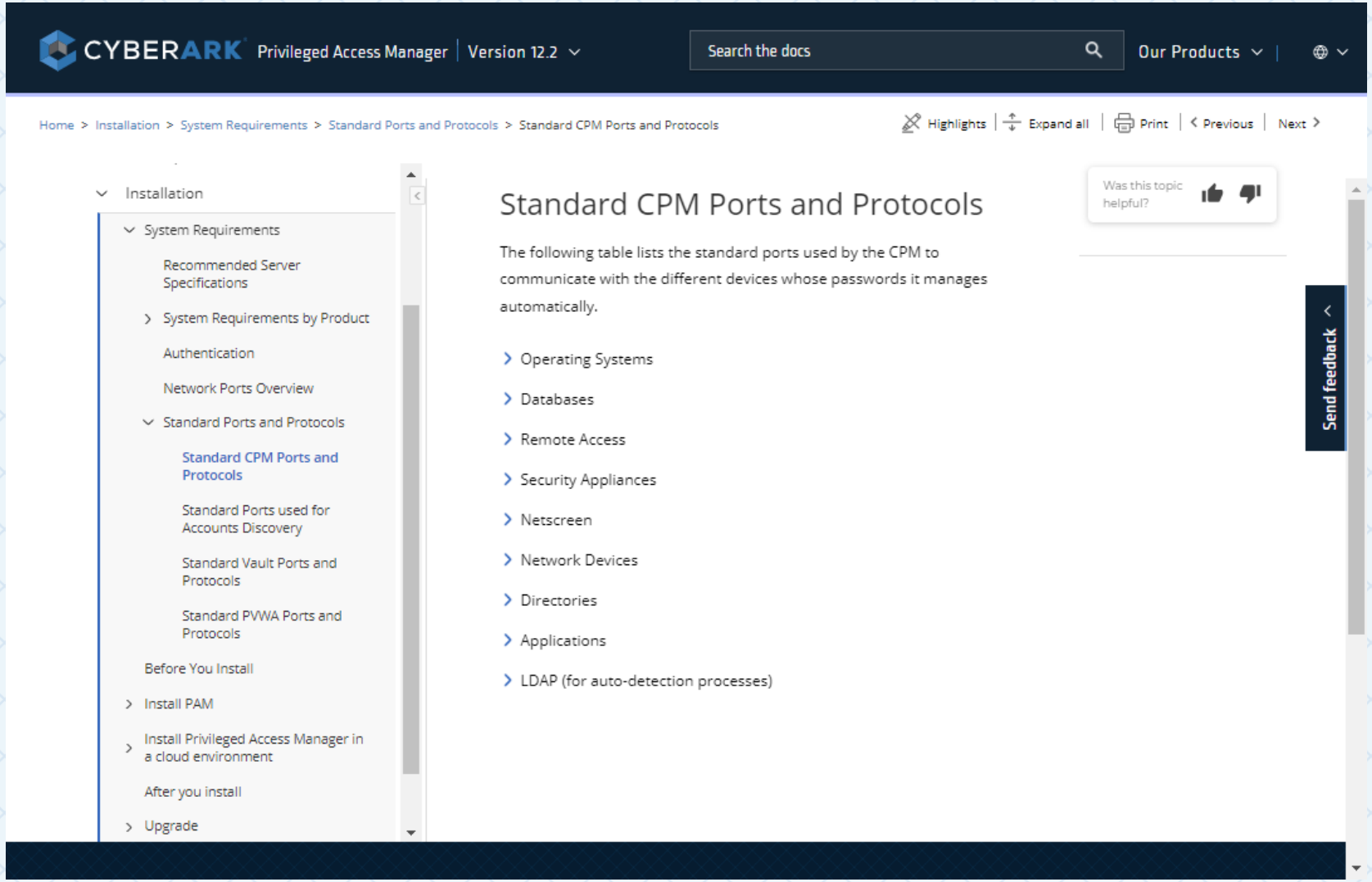
USE CASES



- A single CPM cannot accommodate the total number of accounts managed.
- Accounts are managed in multiple sites or VLANs protected by firewall

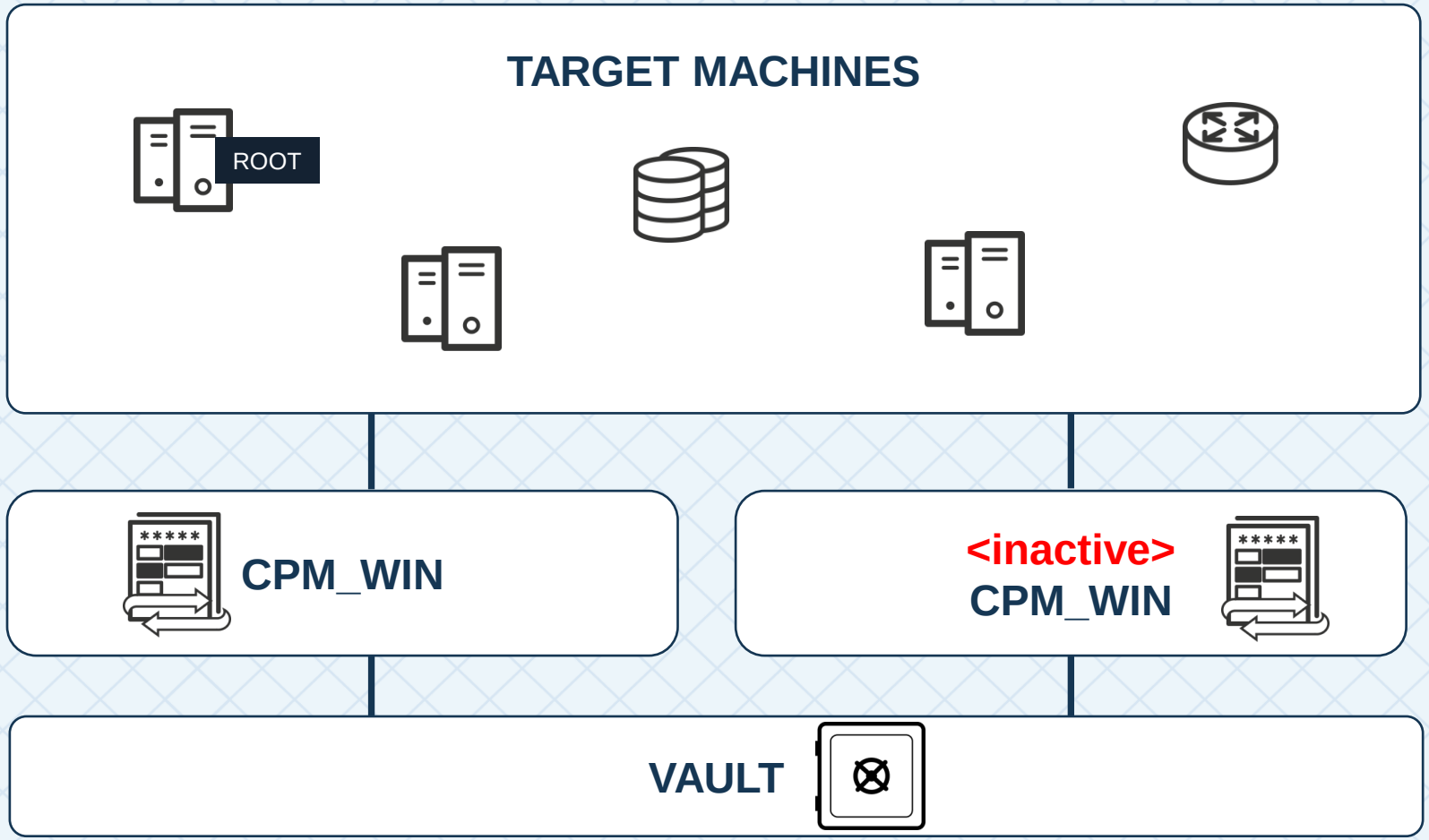
PORT REQUIREMENTS

- Reference “Standard CPM Ports and Protocols” on docs.cyberark.com for more information.
- The link to this information should be provided to the customer early in the planning stages of the CyberArk deployment project.



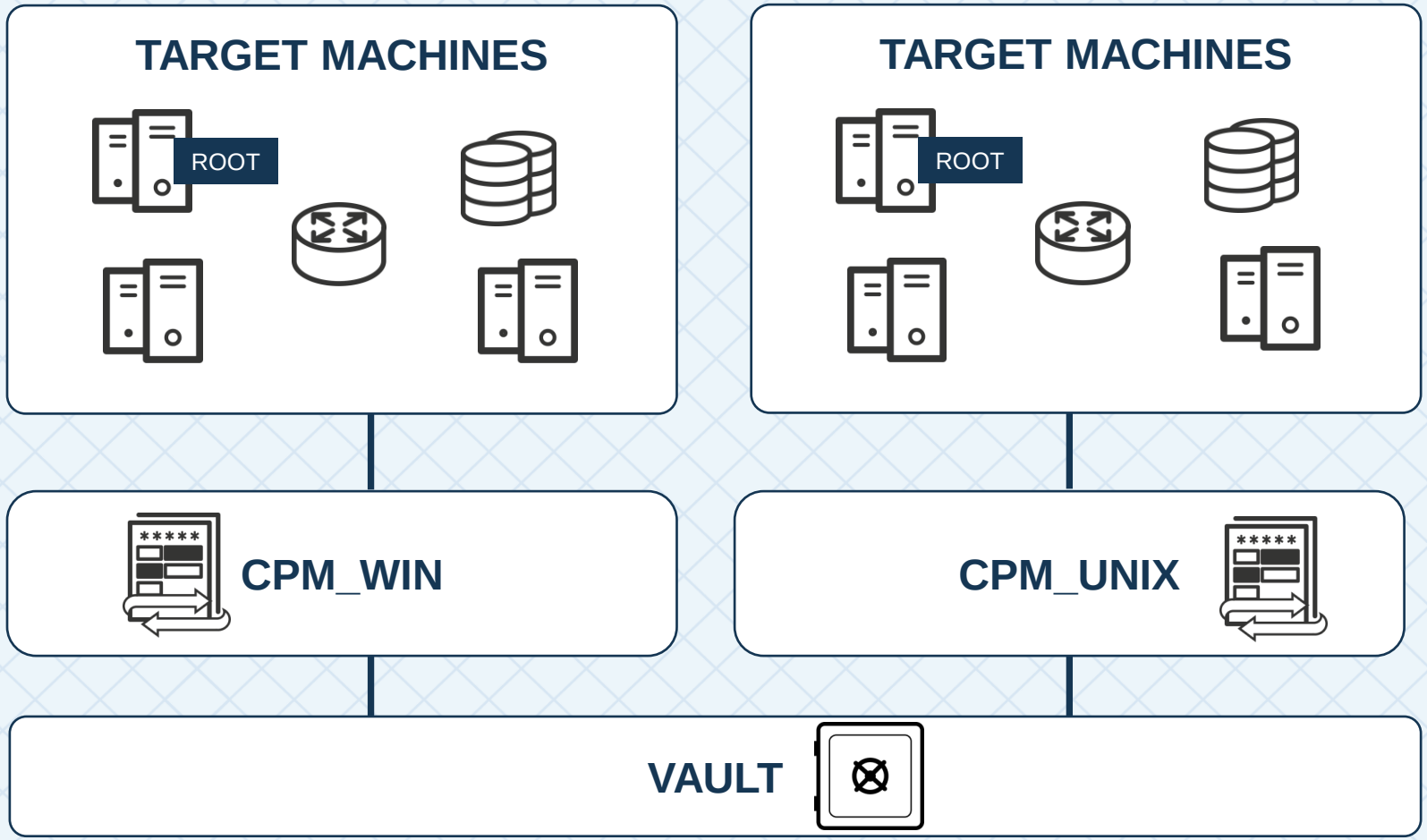
MULTIPLE CPM SERVERS – ACTIVE-PASSIVE

- CPM is installed at multiple locations, but only enabled at one
- Activating and deactivating CPMs is a manual process
- Inactive CPMs will need to assume a license from the active CPM. This is commonly seen in DR implementations
- Detailed information to "Set up a Disaster Recovery CPM" can be found on docs.cyberark.com



MULTIPLE CPM SERVERS

- Multiple CPMs are active simultaneously
- Individual safes are assigned to individual CPMs
- Provides distributed architecture
- Each CPM must be licensed separately



NAMING CONVENTION

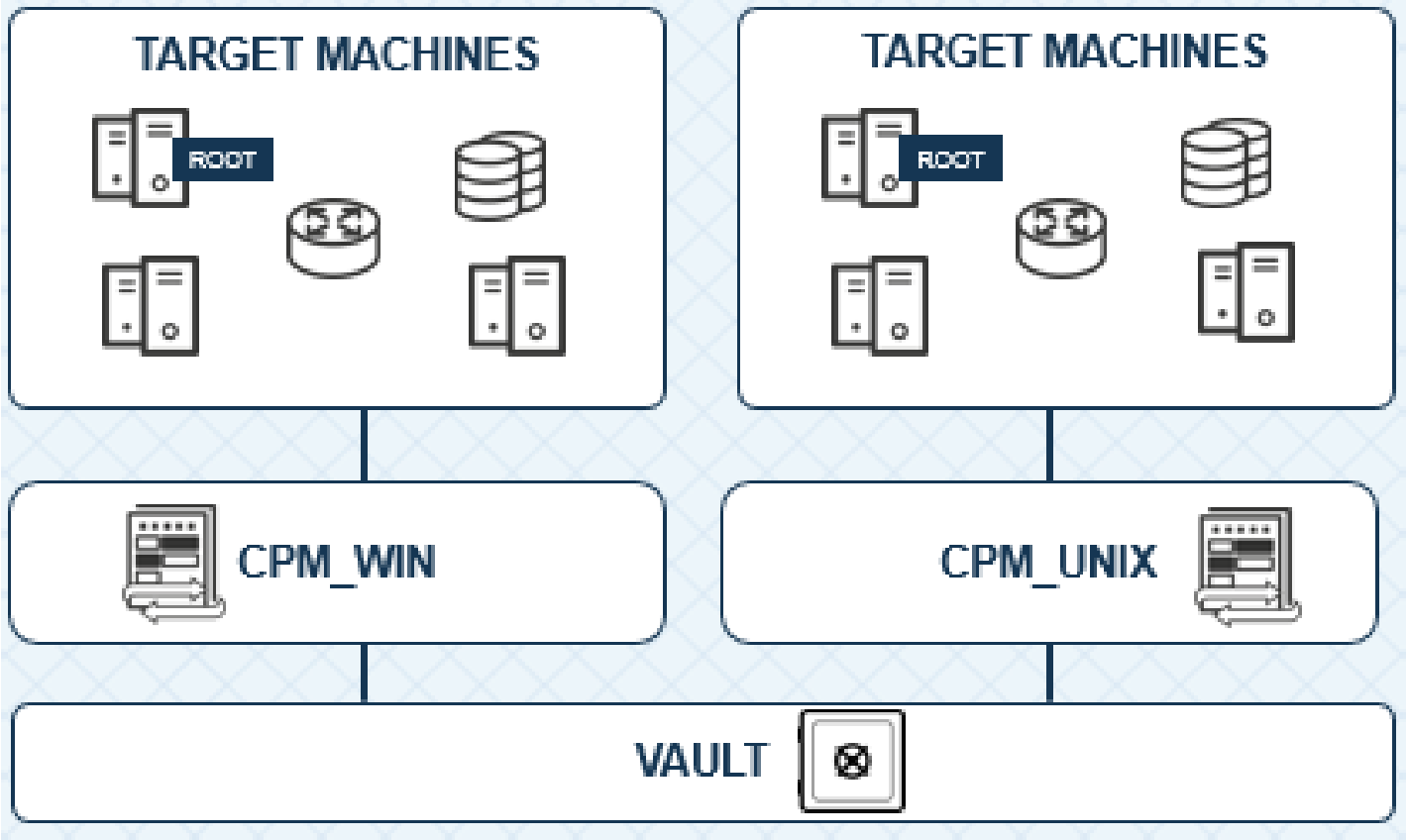
Create a naming convention to name each CPM according to the safes it will manage.

BY REGION	BY SITE	BY ENVIRONMENT
CPM_APAC	CPM_BOS	CPM_PROD
CPM_EMEA	CPM_SFO	CPM_DEV
CPM_NA	CPM_ORD	CPM_DMZ

INSTALLING ADDITIONAL CPMS

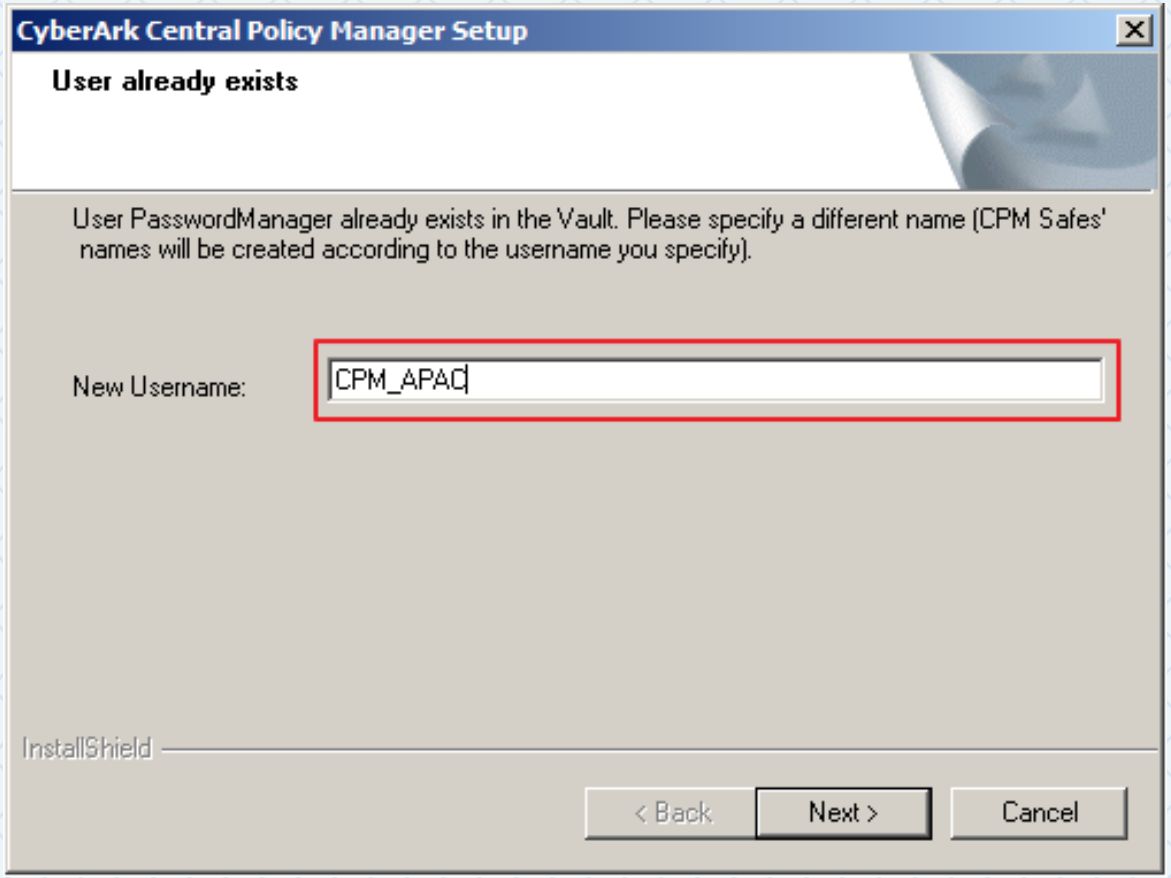
To install multiple CPMs:

- Install the first CPM according to the normal process
- Install additional CPMs
- Rename the first CPM to match your desired naming convention



INSTALLING ADDITIONAL CPMS

- The installer will automatically name the first CPM *PasswordManager*.
- Each subsequent installer will prompt you to provide a CPM name since *PasswordManager* is already in use.
- Name each new CPM according to your naming convention.

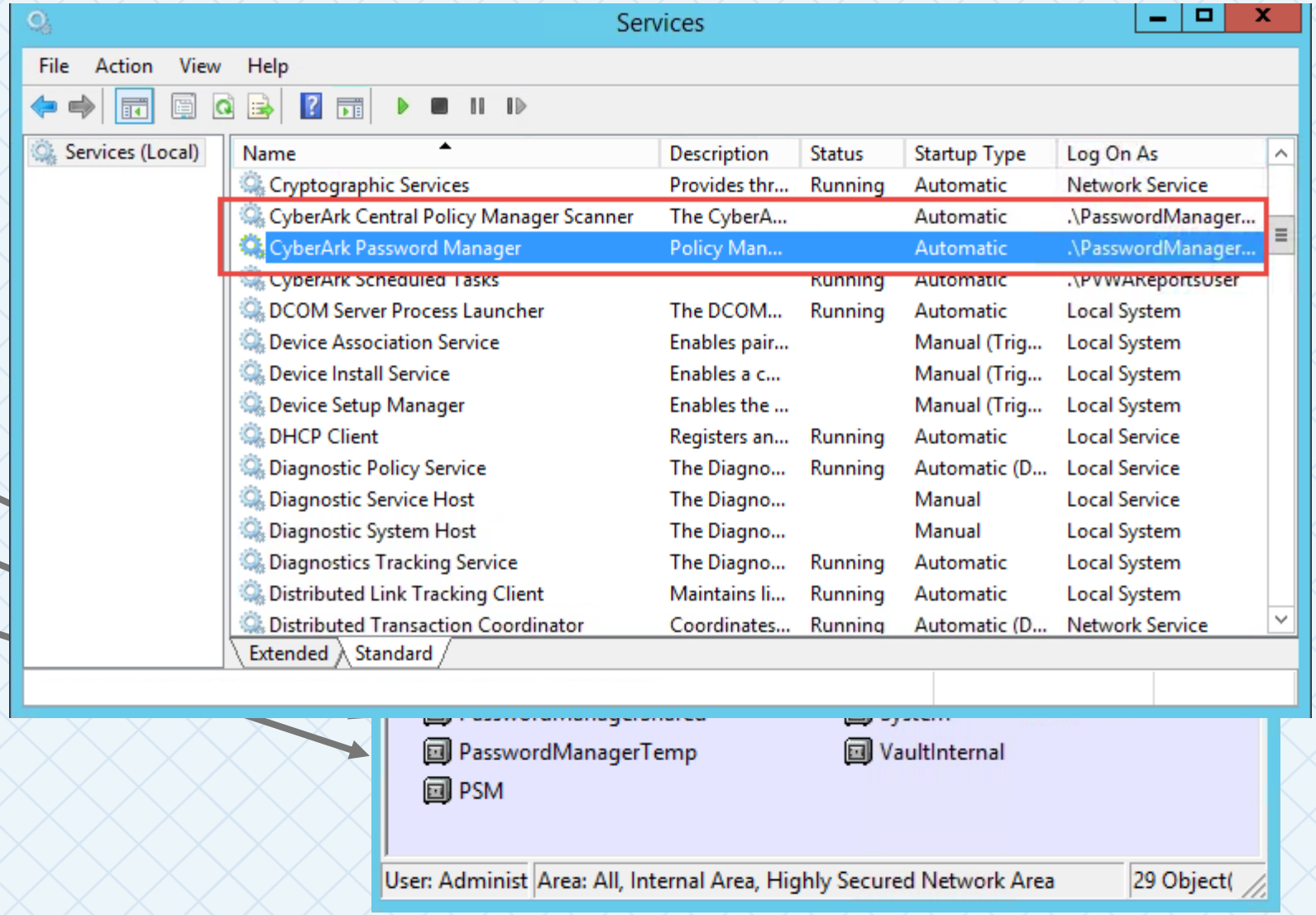


RENAME THE SAFES FOR THE FIRST CPM

- First step is to <u>STOP ALL CPM Services</u>
- Next rename the **PasswordManager_*** safes to the new name, however…

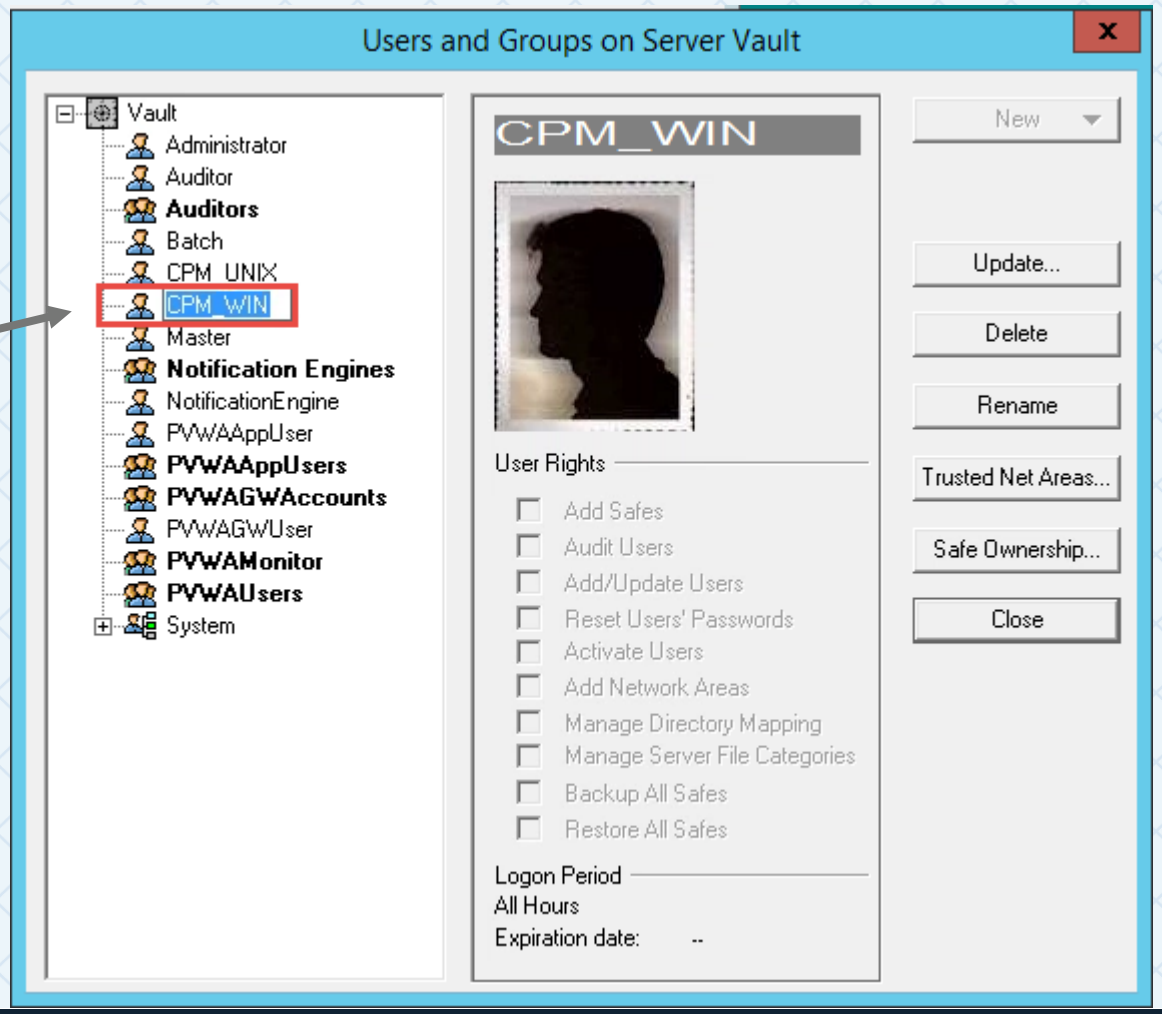
  Do NOT rename the following safes:

  - **PasswordManager_Pending**
  - **PasswordManagerShared**
  - **PasswordManagerTemp**



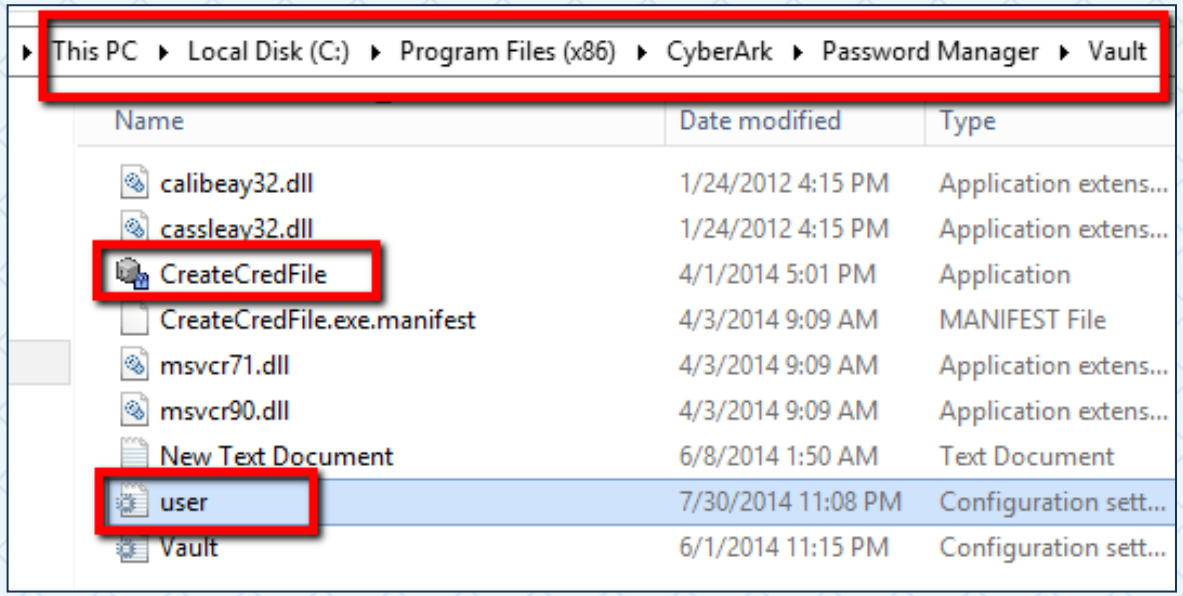
RENAME THE COMPONENT USER FOR THE FIRST CPM

- First step is to STOP BOTH CPM Services
- Rename the **PasswordManager_*** safes to the new name
- Rename the **PasswordManager** user and **reset its password**



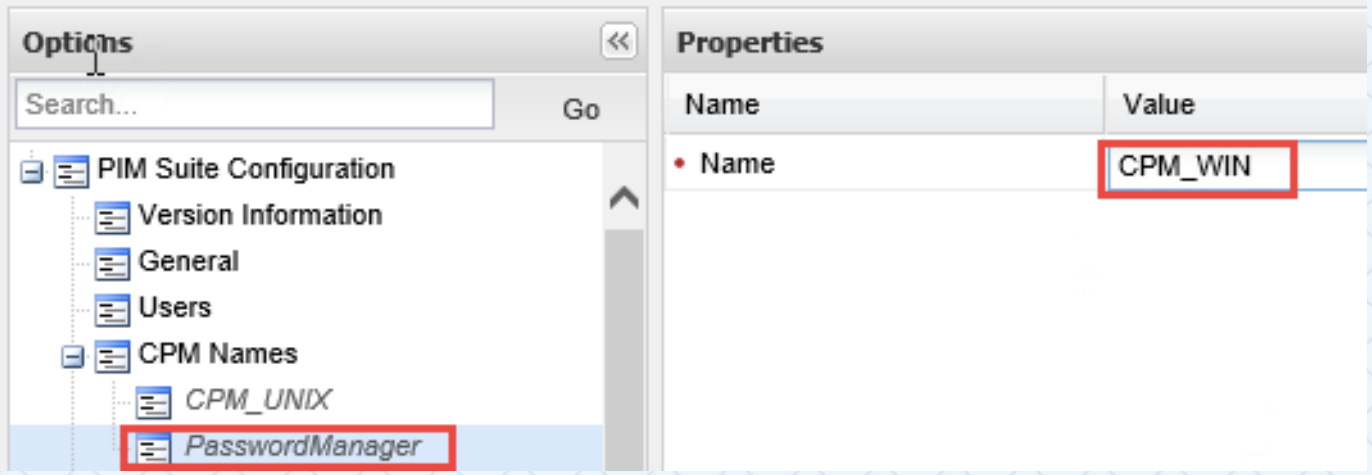
RESET THE CREDENTIAL FILE

- Rename the **PasswordManager_*** safes to the new name
- Rename the **PasswordManager** user and reset its password.
- Update the Credential File on the first CPM server so that the CPM can authenticate to the vault.



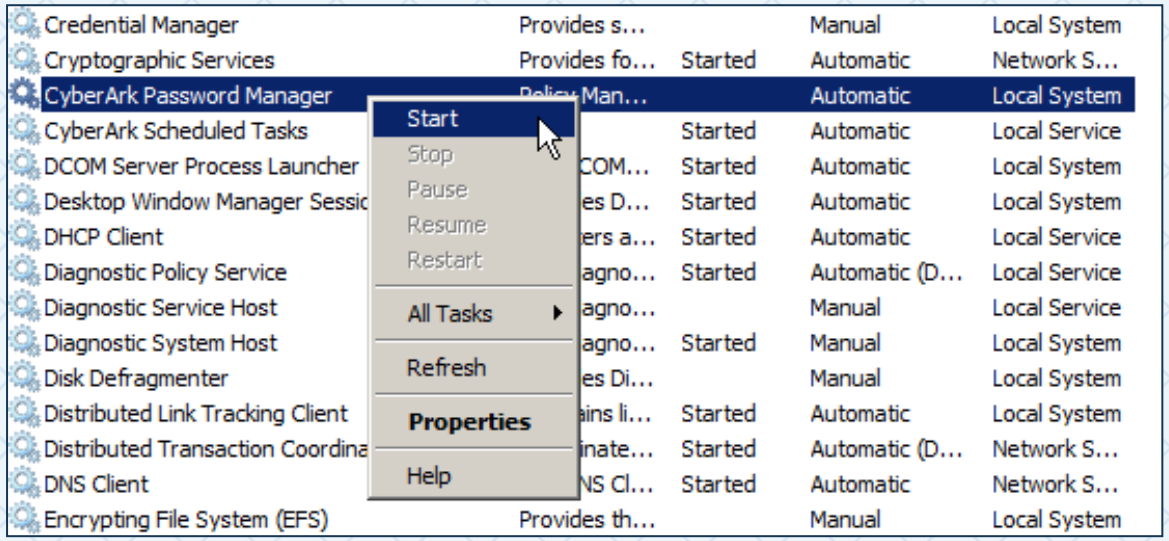
RENAME THE CPM IN THE PVWA

- Rename the **PasswordManager_*** safes to the new name
- Rename the **PasswordManager** user and reset its password.
- Update the Credential File on the first CPM server.
- Change the name of the CPM in the PVWA (under Options) so that it displays correctly in all PVWA options.



RESTART THE CPM SERVICES

- Rename the **PasswordManager_*** safes to the new name
- Rename the **PasswordManager** user and reset its password.
- Update the Credential File on the first CPM server.
- Change the name of the CPM in the PVWA (under Options).
- Restart the CPM services and check the PM.LOG.



CPM ASSIGNMENTS

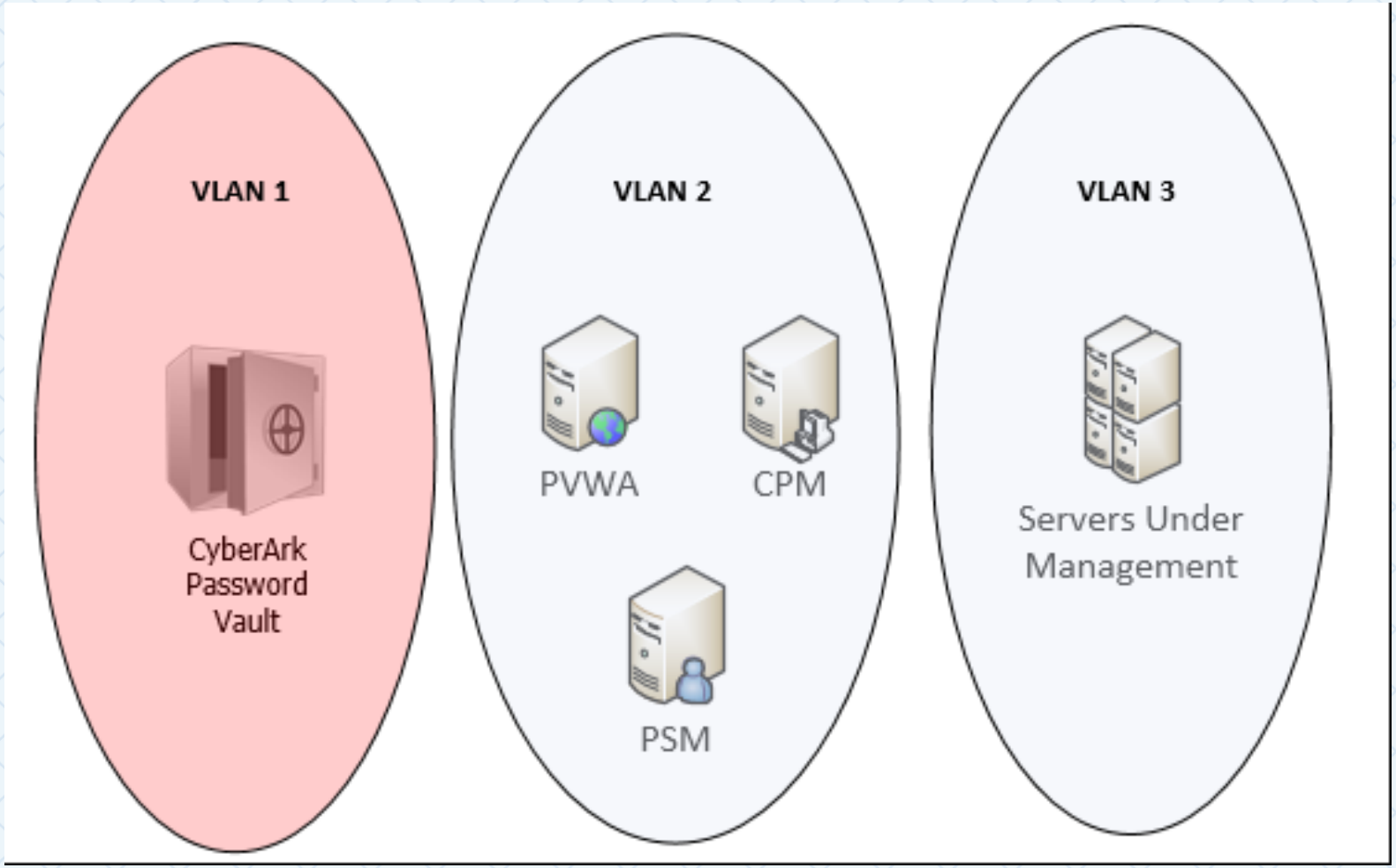
- Once the CPMs have been named correctly, assign CPMs to safes according to design.

SAFE	ASSIGNED CPM
MSSQL_NA	CPM_NA
MSSQL_APAC	CPM_APAC
SrvAcc_NA	CPM_NA
SrvAcc_APAC	CPM_APAC
Recon_NA	CPM_NA
Recon_APAC	CPM_APAC
Cybr_NA	CPM_APAC
Cybr_APAC	CPM_NA

GENERAL CONFIGURATION AND RECOMMENDATIONS

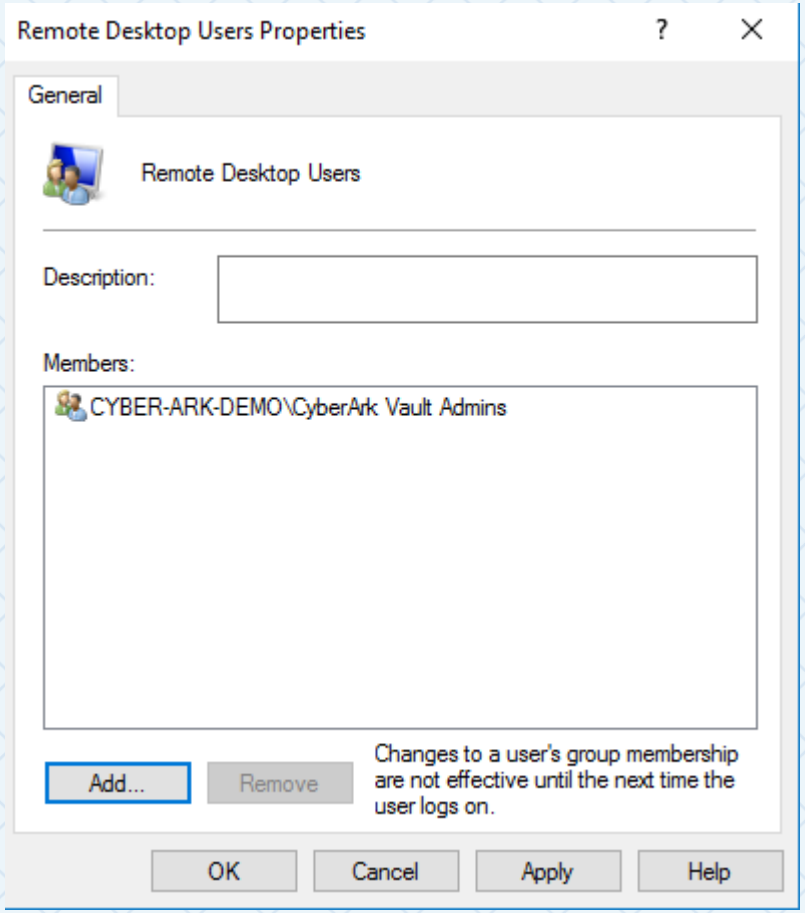
SECURE AND ISOLATE COMPONENT SERVERS

- Follow Best Practices to Mitigate Credential Theft on Servers
- Treat all CyberArk Components as Tier 0 applications and infrastructure
- Ensure any credentials that are authorized to log into CyberArk Component servers do not have Domain Administrator permissions.



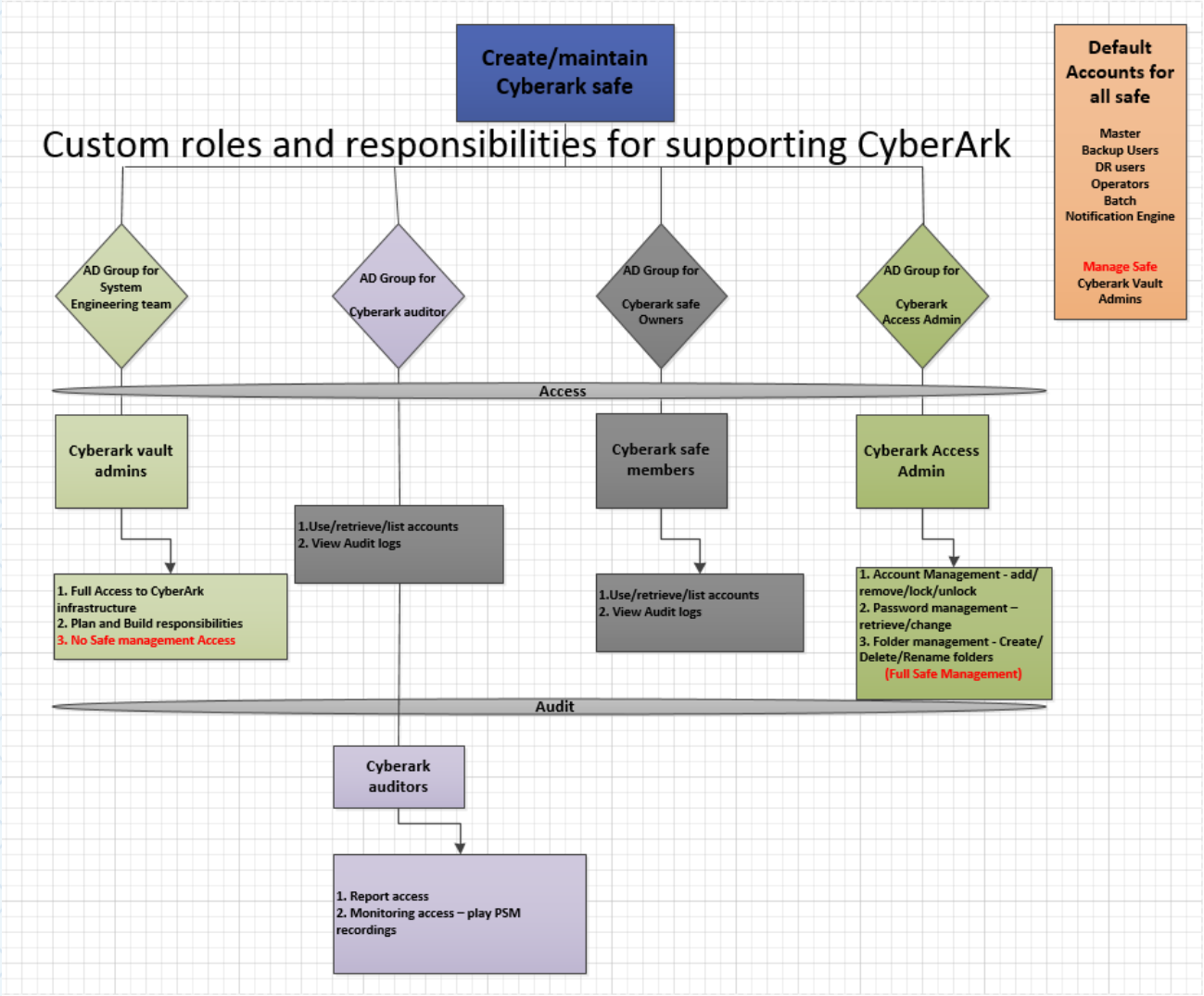
SECURE AND ISOLATE COMPONENT SERVERS

- Limit the number of domain credentials that are able to access the component servers
- Consider using host-based firewalls and IPsec to restrict, encrypt and authenticate inbound administrative traffic.
- Consider using CyberArk Privileged Session Manager and the local administrator account to access component servers providing Isolation, Control via Policy and Monitored access.
- Deploy application whitelisting and limit execution to authorized applications



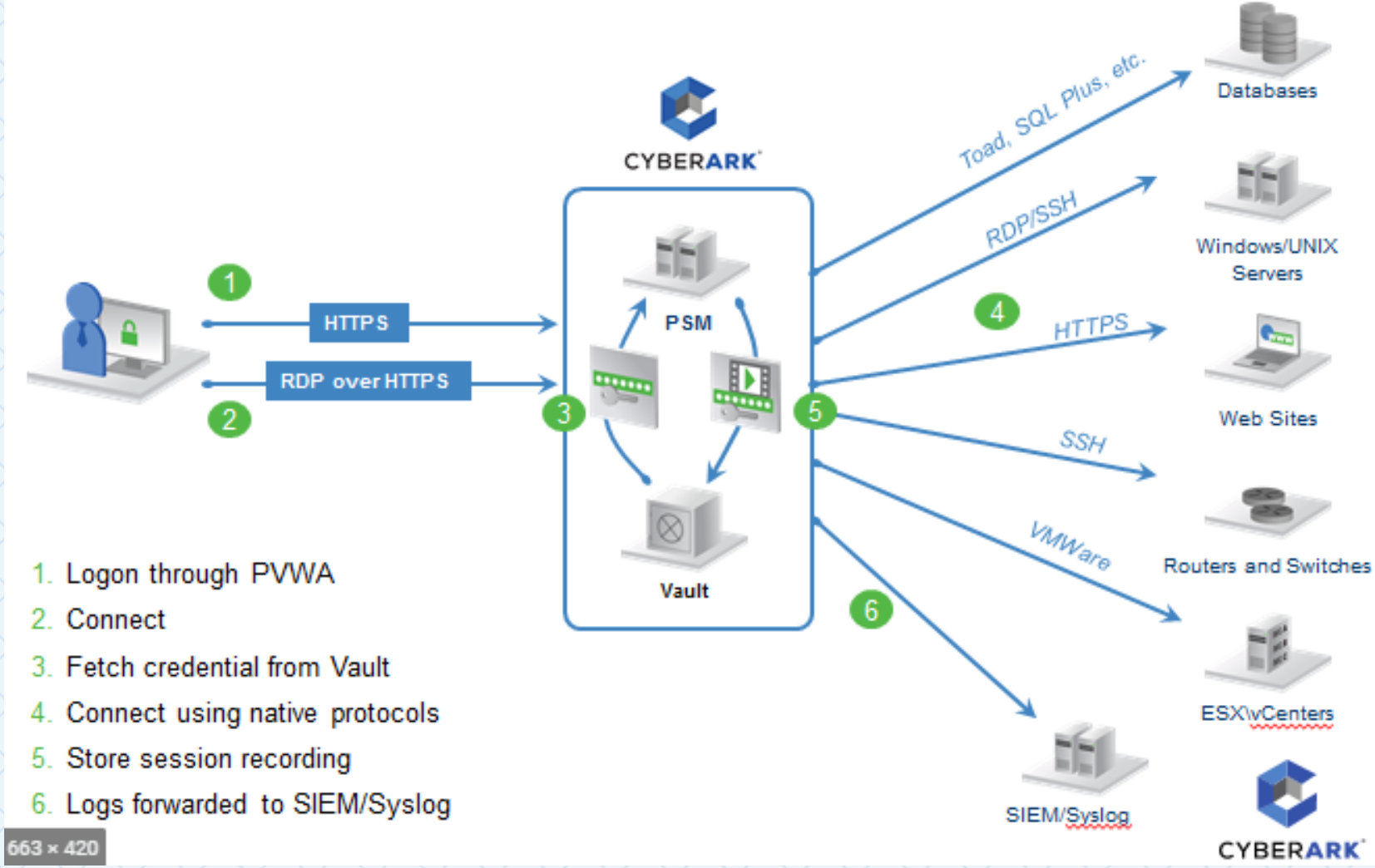
REDUCE APPLICATION ATTACK SURFACE

- Eliminate unnecessary CyberArk administrative accounts
- Reduce privileges of CyberArk administrative accounts
- Apply the concept of Least Permissions when accessing CyberArk component servers
- Restrict personal accounts to business-as-usual permissions justified for their role



REDUCE APPLICATION ATTACK SURFACE

- Consider requiring privilege elevation for system configuration changes.
- Use the CyberArk Privileged Session Manager to isolate and monitor CyberArk administration
- Require two-factor authentication for all avenues of administrative access



SUMMARY

SUMMARY

This session covered:

- Installing the CPM and PVWA
- Configuring the CPM and PVWA
- The CPM and PVWA Server Environment
- The CPM and PVWA Vault Environment
- Securing the CPM and PVWA

THANK YOU