CYBERARK UNIVERSITY

The Enterprise Password Vault

CyberArk Training

OBJECTIVES

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

- Describe the main components of the CyberArk Digital Vault
- Understand the Digital Vault Security Standard
- Describe the Vault server environment
- Describe the different Layers of Security that protect the Vault Data
- Preview the Digital Vault installation

MULTIPLE LAYERS OF SECURITY

ENTERPRISE PASSWORD VAULT OVERVIEW

The Enterprise Password Vault (EPV)

- The core of CyberArk's PAS (Privileged Access Manager) solution
- The secure storage location for all privileged account information
- Secured using CyberArk's patented Vaulting technology

END TO END SECURITY

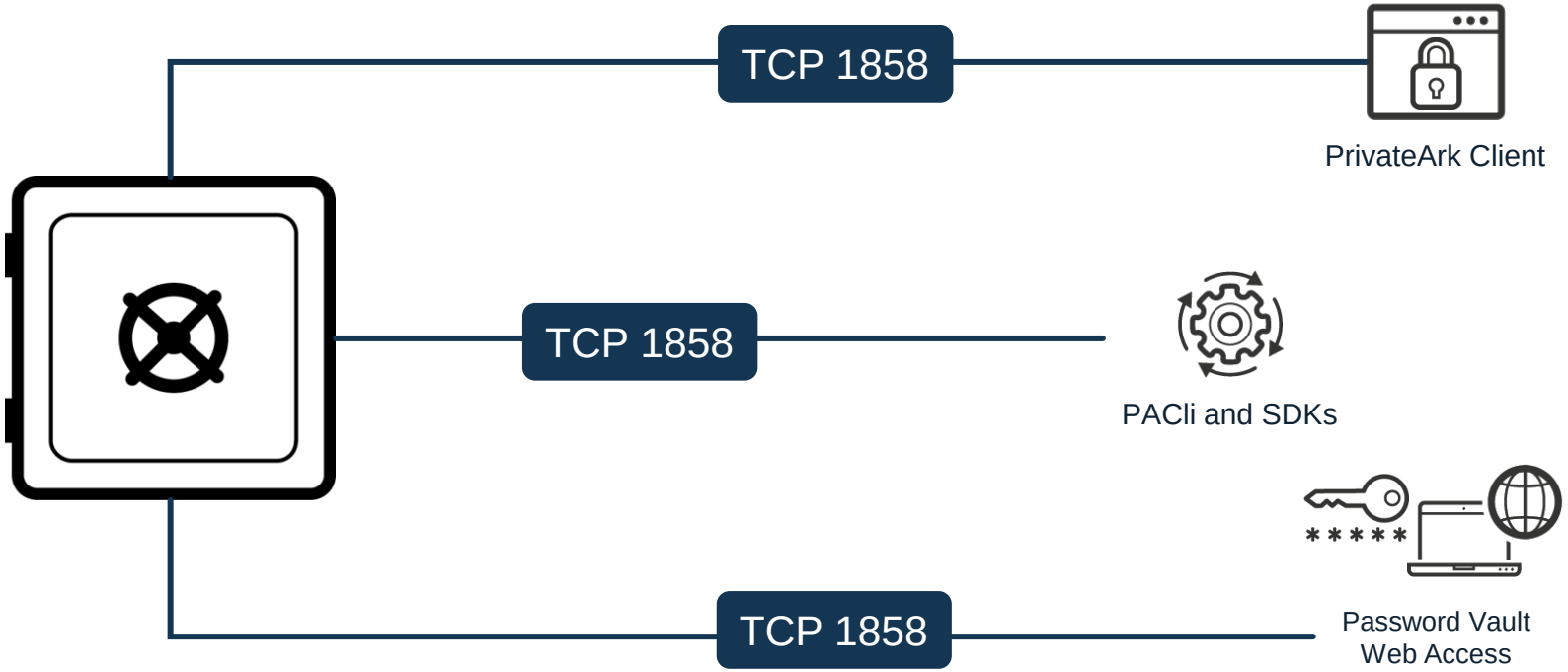
VAULT USER

Session Encryption	• Proprietary Protocol • OpenSSL Encryption
Firewall	• Hardened built-in Windows Firewall
Authentication	• Single or **2 Factor Authentication (recommended)**
Role Based Access Control	• Granular Entitlements • Discretionary Access Control Support
Mandatory Access Control	• Subnet-Based Access Control • Time Limits and Delays
Auditing	• Tamper-proof Audit Trail • Event Based Alerts
File Encryption	• Hierarchical Encryption Model • Every object has a unique key

STORED CREDENTIAL

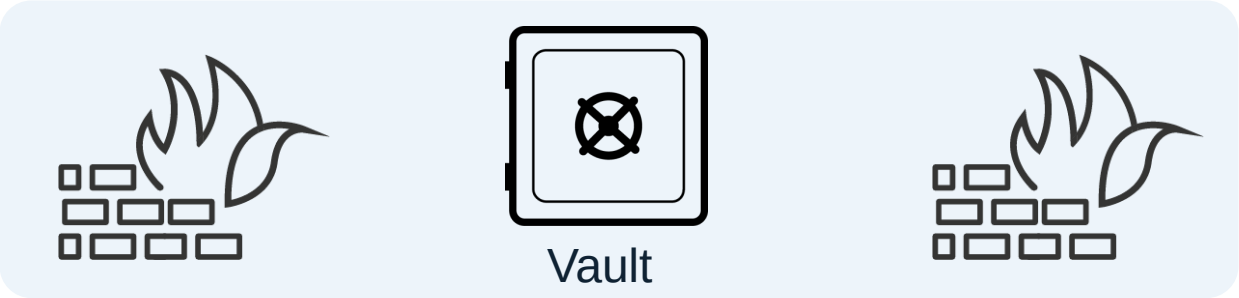
SESSION ENCRYPTION

- The CyberArk Proprietary Protocol or VPN uses TCP1858
- The VPN forces users to use CyberArk interfaces to access the **Vault**
- User accounts can be restricted to specific interfaces such as the PVWA
- 95% of the encryption processes occur on the client side, thus offloading the Vault and allowing higher throughput



FIREWALL

- During installation, the Vault takes control of the Windows firewall and re-brands it the “CyberArk Hardened Windows Firewall”
- By default, only the CyberArk Proprietary Protocol is allowed, via port (TCP 1858)
- Additional firewall rules can be added and managed through CyberArk configuration files, not through the Windows Advanced Firewall utility
- If the PrivateArk Server Service on the Vault is stopped the firewall is closed. No external communication is allowed



AUTHENTICATION METHODS

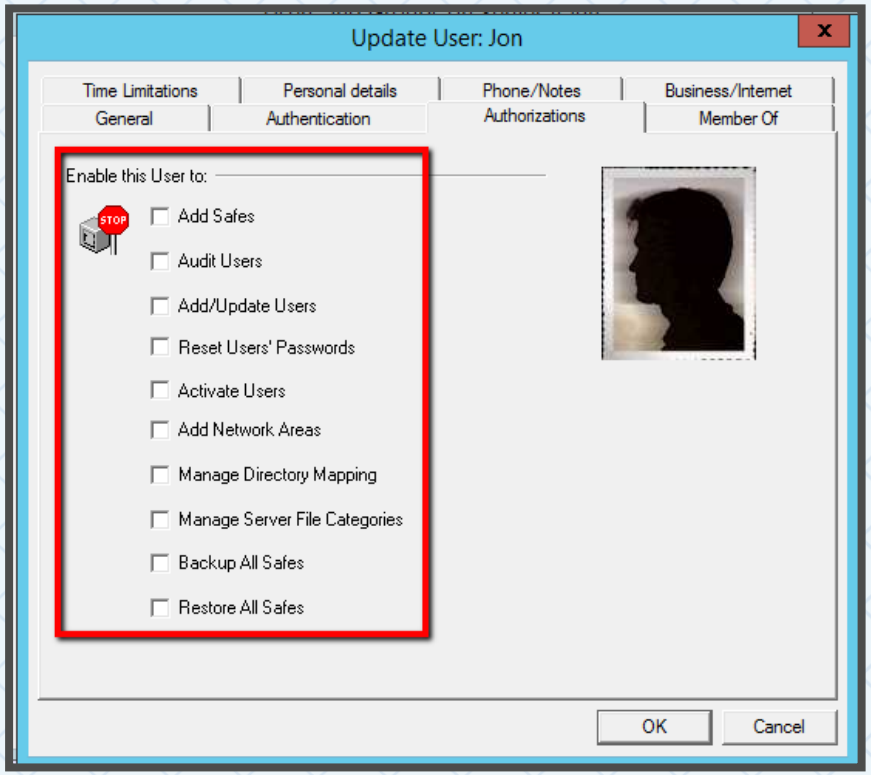
- Every access to the Vault must be authenticated!
- The Privileged Access Manager solution also supports third-party authentication and can be integrated with an organization's existing authentication server

CyberArk (Vault Authentication)	LDAP Authentication
Radius including Challenge-Response	Windows Authentication
PKI Auth (Personal Certificate)	RSA SecurID
Amazon Cognito	SAML
Google Authentication	Oracle SSO

ROLE BASED ACCESS CONTROLS

VAULT LEVEL ROLES

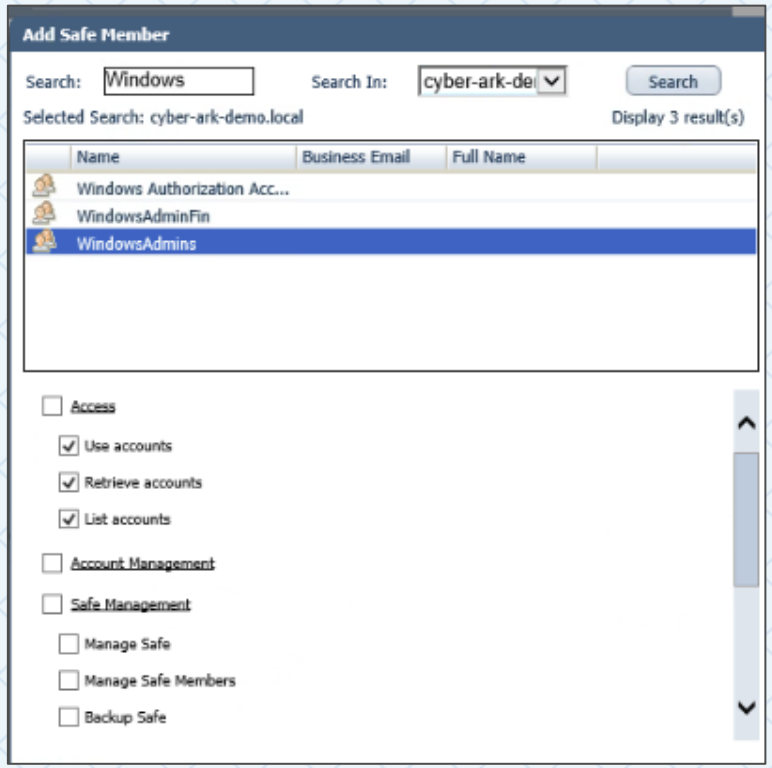
- Vault Admins
- Safe Managers
- Auditors
- Users
- Custom?



Screenshot from PAClient

SAFE LEVEL ROLES

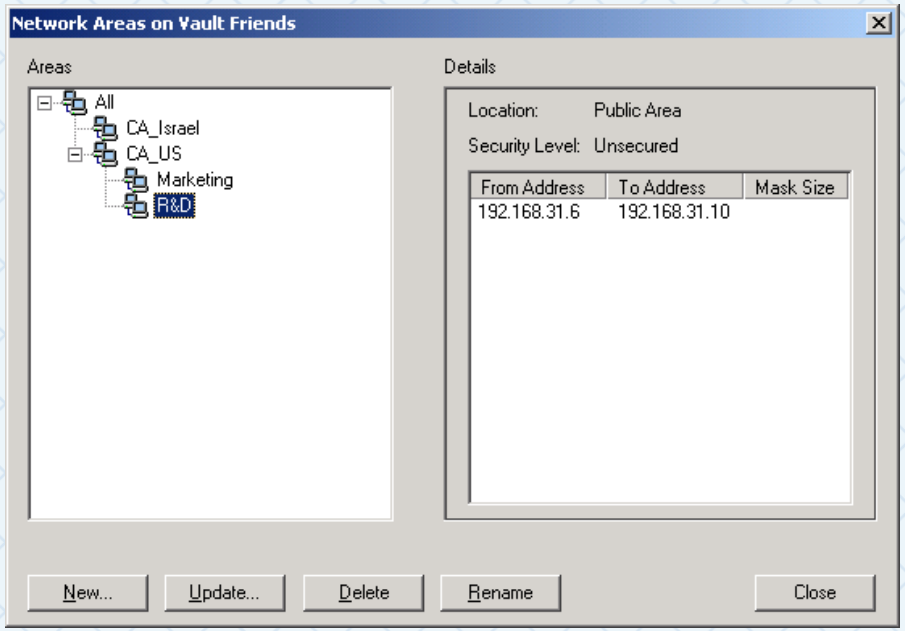
- User Access
- Account Management
- Safe Management
- Custom?

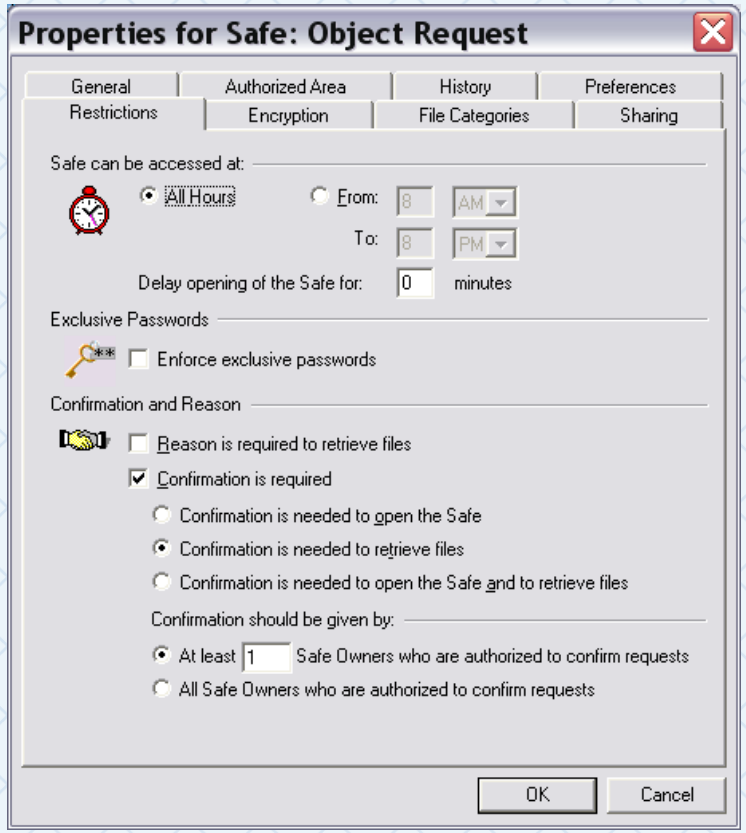


Screenshot from PVWA

MANDATORY ACCESS CONTROL

- Geographical Control (Network Area)
- Time Limitations





Screenshots from PAClient

AUDITING

- Each time files are accessed for any purpose, the activity is written in the Vault activity log
- Event-based notifications allow for alerting on specific Vault actions
- The Audit database is protected and is not accessible to users or administrators, providing a tamper-proof audit trail

	A	B	C	D		F	G	H	I
1	Time	User	Action	Safe	Target	Target Platform	Target System	Target Account	New Target
2	18/06/2014 10:15:59	Administrator	Logon		10.0.1.13				
3	18/06/2014 10:16:02	Administrator	Clear User History		Administrator				
4	18/06/2014 10:16:43	Administrator	Update User Detailed Infor		Auditor				
5	18/06/2014 10:16:43	Administrator	Reset User Password Detai		Auditor				
6	18/06/2014 10:16:43	Administrator	Update User Detailed Infor		Auditor				
7	18/06/2014 10:16:43	Administrator	Update User		Auditor				
8	18/06/2014 10:16:43	Administrator	Reset User Password		Auditor				
9	18/06/2014 10:17:07	Administrator	Logoff		10.0.1.13				
10	18/06/2014 10:18:06	Administrator	Logon		10.0.1.13				
11	18/06/2014 10:18:31	Administrator	Add Group Member		PVWAMonitor				Auditor
12	18/06/2014 10:16:43	Administrator	Update User Detailed Infor		Auditor				
13	18/06/2014 10:16:43	Administrator	Reset User Password Detai		Auditor				
14	18/06/2014 10:16:43	Administrator	Update User Detailed Infor		Auditor				
15	18/06/2014 10:16:43	Administrator	Update User		Auditor				
16	18/06/2014 10:16:43	Administrator	Reset User Password		Auditor				
17	18/06/2014 10:17:35	Auditor	Full Gateway Connection		PVWAGWUser				
18	18/06/2014 10:17:35	Auditor	Logon		10.0.1.12				10.0.1.13
19	18/06/2014 10:17:49	Auditor	Logoff		10.0.1.12				
20	18/06/2014 10:18:31	Administrator	Add Group Member		PVWAMonitor				Auditor
21	18/06/2014 10:18:48	Auditor	Full Gateway Connection		PVWAGWUser				

from the PVWA

FILE ENCRYPTION

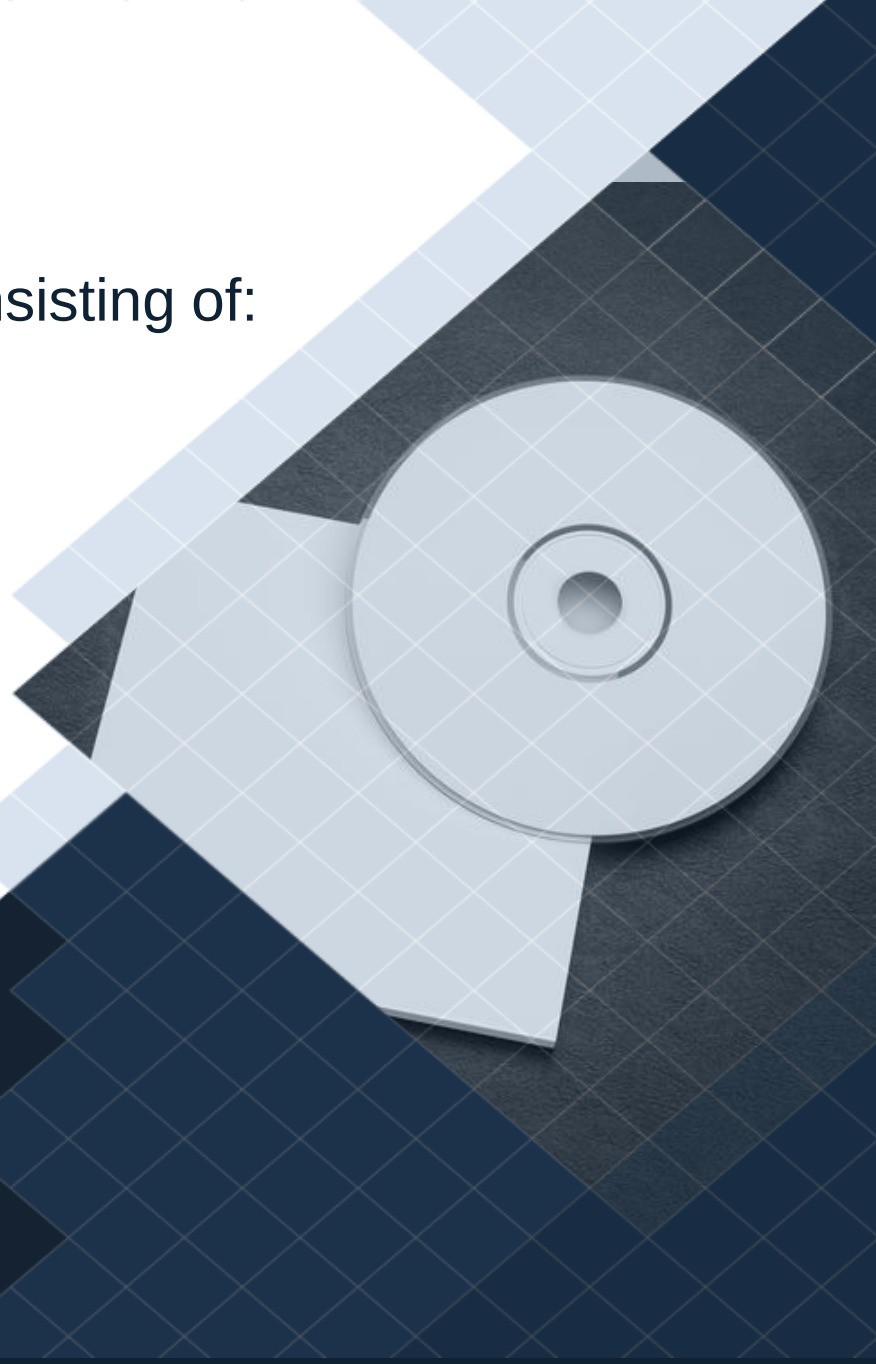
- Modular structure – Encryption, Hashing, and Authentication modules can be replaced by the customer
- Supported Encryption and Hash Algorithms –
  - AES-256 / AES-128
  - RSA-2048 / RSA-1024
  - 3DES
  - SHA-256
- Every object has a unique encryption key
- When a user is removed from the system, they hold no encryption key
- Secure recovery mechanism for encryption keys
- Backups are always encrypted and always recoverable

STANDALONE VAULT INSTALLATION

HOW ENCRYPTION KEYS ARE DISTRIBUTED

Every New Customer will receive an Installation package consisting of:

- **Two copies of the Operator CD**
  - Operator CD contains:
    - Server Key
    - Recovery Public Key
  - Operator CD keys are required to install and start the Vault server
- **Two copies of the Master CD**
  - The Master CD contains the contents of the Operator CD plus;
    - ***Recovery Private Key***
  - Master CD should only be used in emergency situations
- **CyberArk License Agreement**



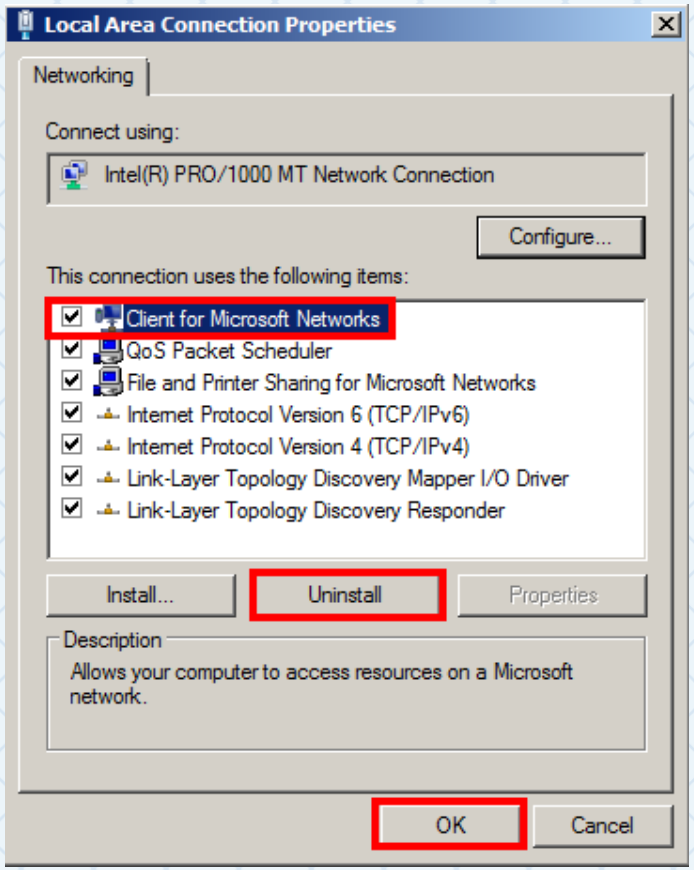
INSTALLATION PACKAGE

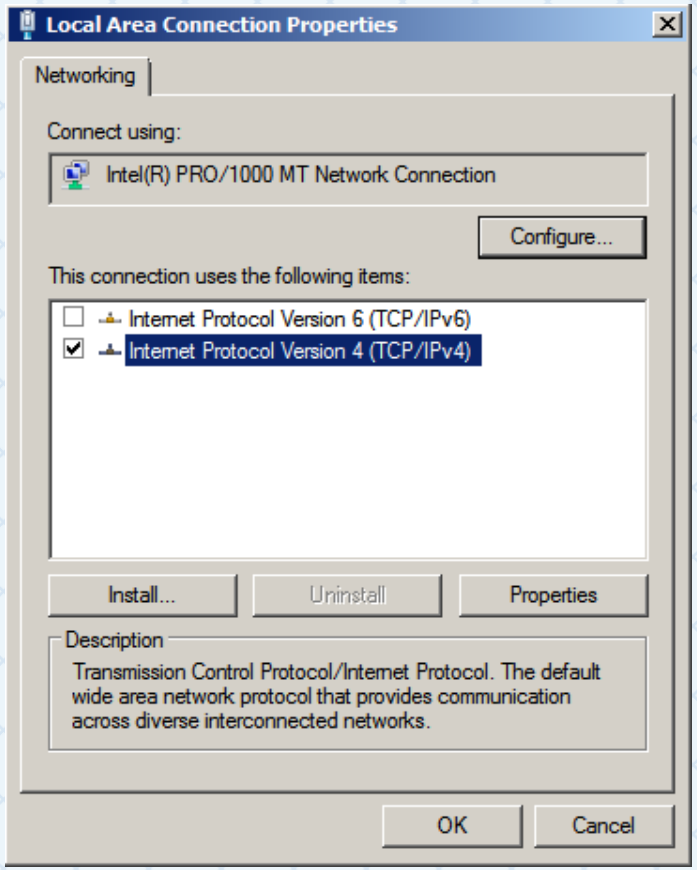
- Vault Installation Package:
  - Ensure that the following items are copied locally to the Vault Server before hardening.
    - CyberArk Server and Client Installation software
    - Operator CD, can be copied locally in preparation for HSM integration (recommended) or inserted into CD drive
    - CyberArk License file downloaded from the Secure File Exchange
    - Digital Certificates installed in support of LDAP Integration

INSTALLATION PREREQUISITE – PREPARE NIC

Prepare the Network Interface, and uninstall unnecessary network components

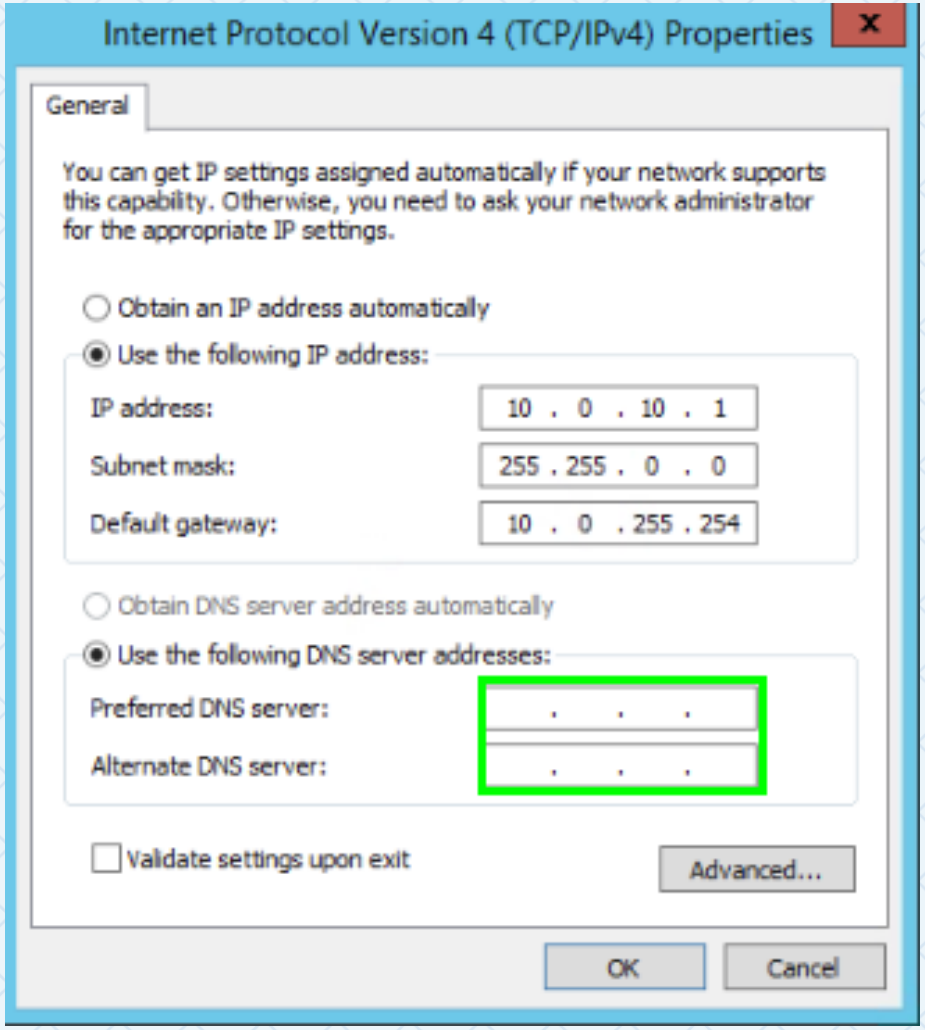
Note: Windows Server 2019 no longer allows the uninstall of components and services. They can only be disabled.





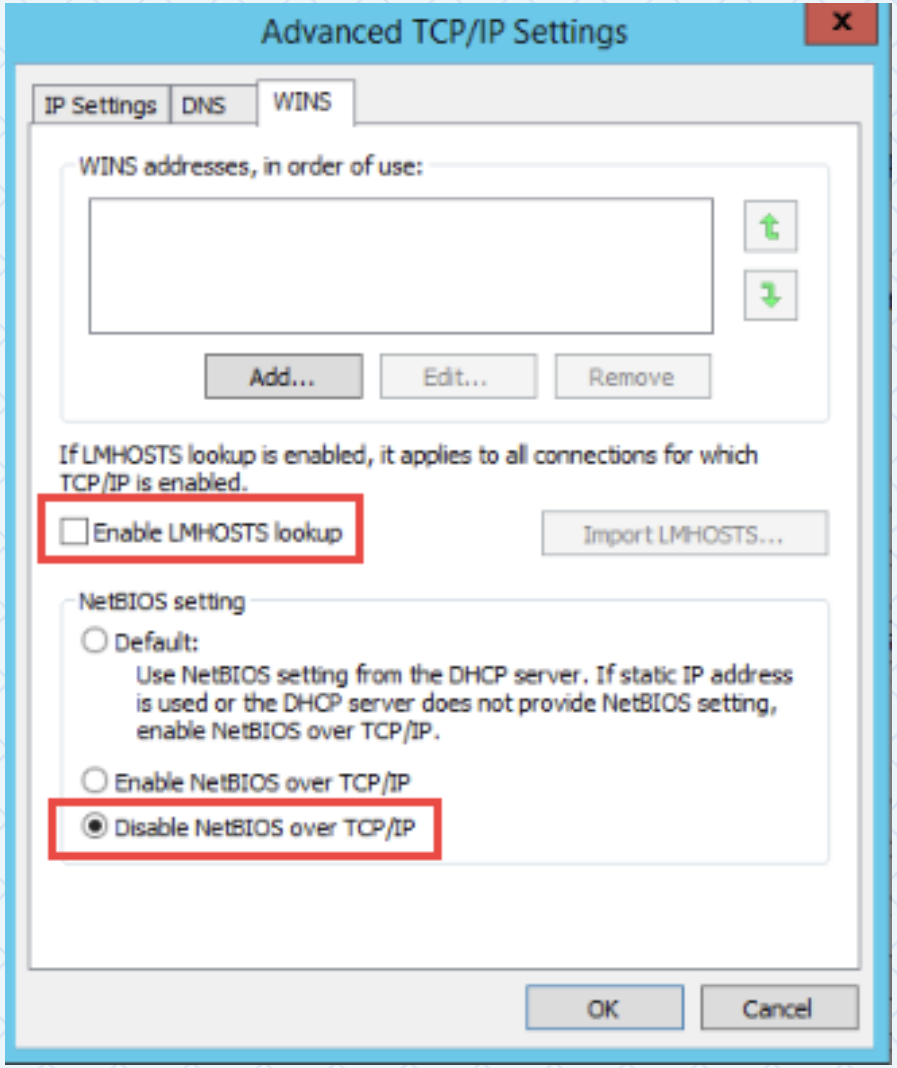
INSTALLATION PREREQUISITE - NO DNS ENTRIES

- The Vault's DNS sever settings should remain empty to eliminate the risk of attack initiated through compromised DNS servers



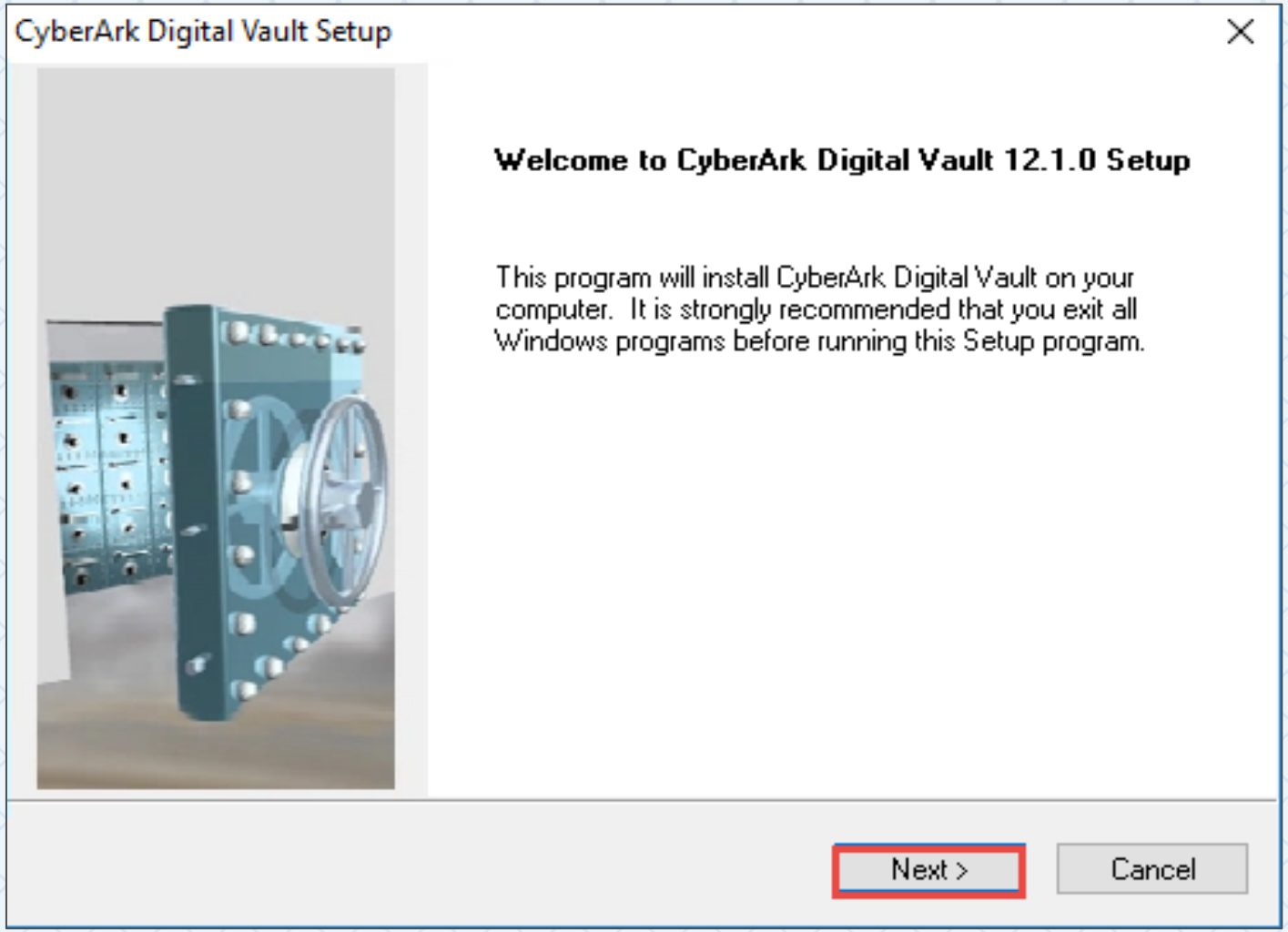
INSTALLATION PREREQUISITE - DISABLE WINS

- Ensure that Enable LMHOSTS lookup is deselected.
- And Disable NetBIOS over TCP/IP is selected.



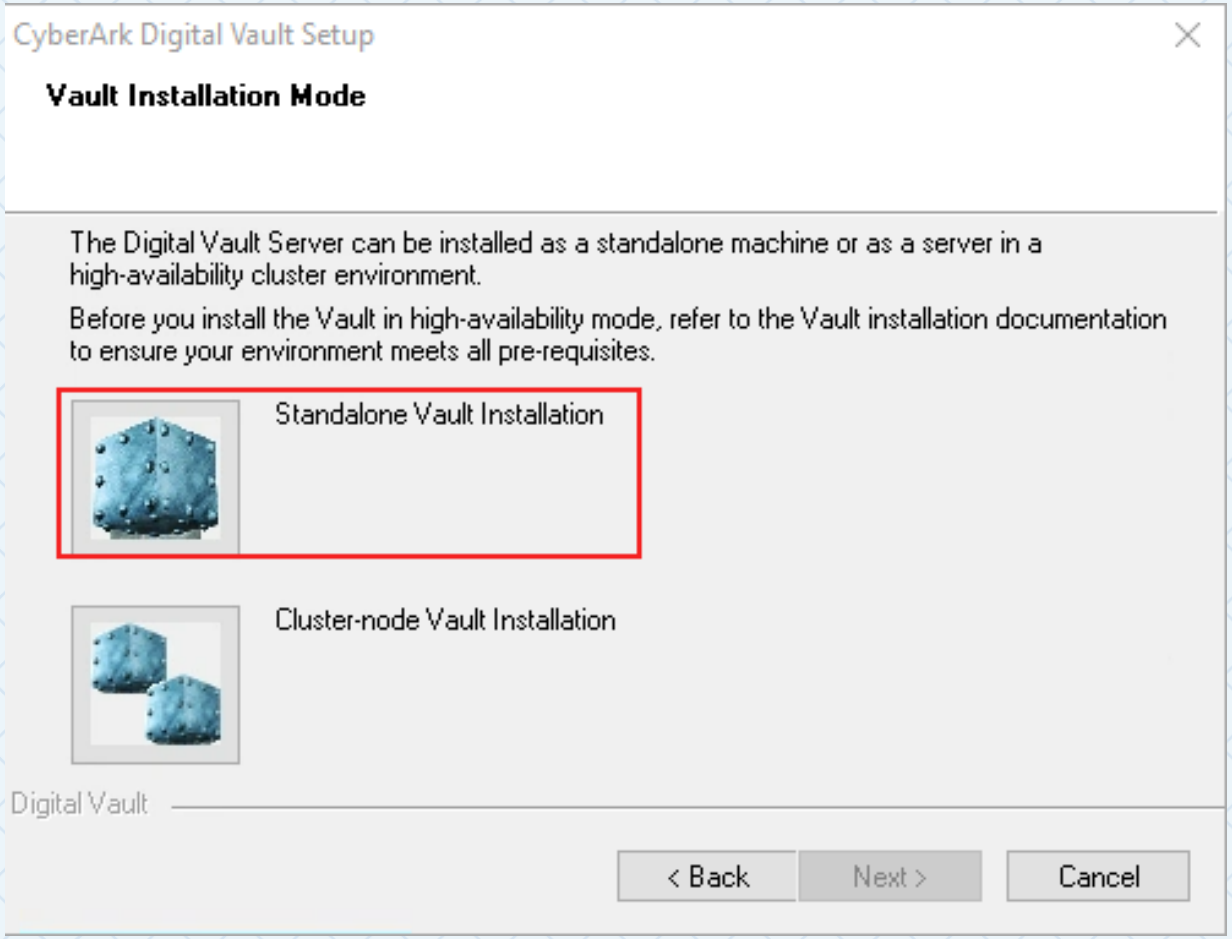
INSTALL PREREQUISITES

- Ensure the Windows Server has .Net 4.8 installed prior to launching setup
- Launch v12.1 setup.exe
- Accept the installation of any required "Microsoft Visual C++ Redistributable packages”
- Then click Next > at “Welcome to CyberArk Digital Vault Setup”



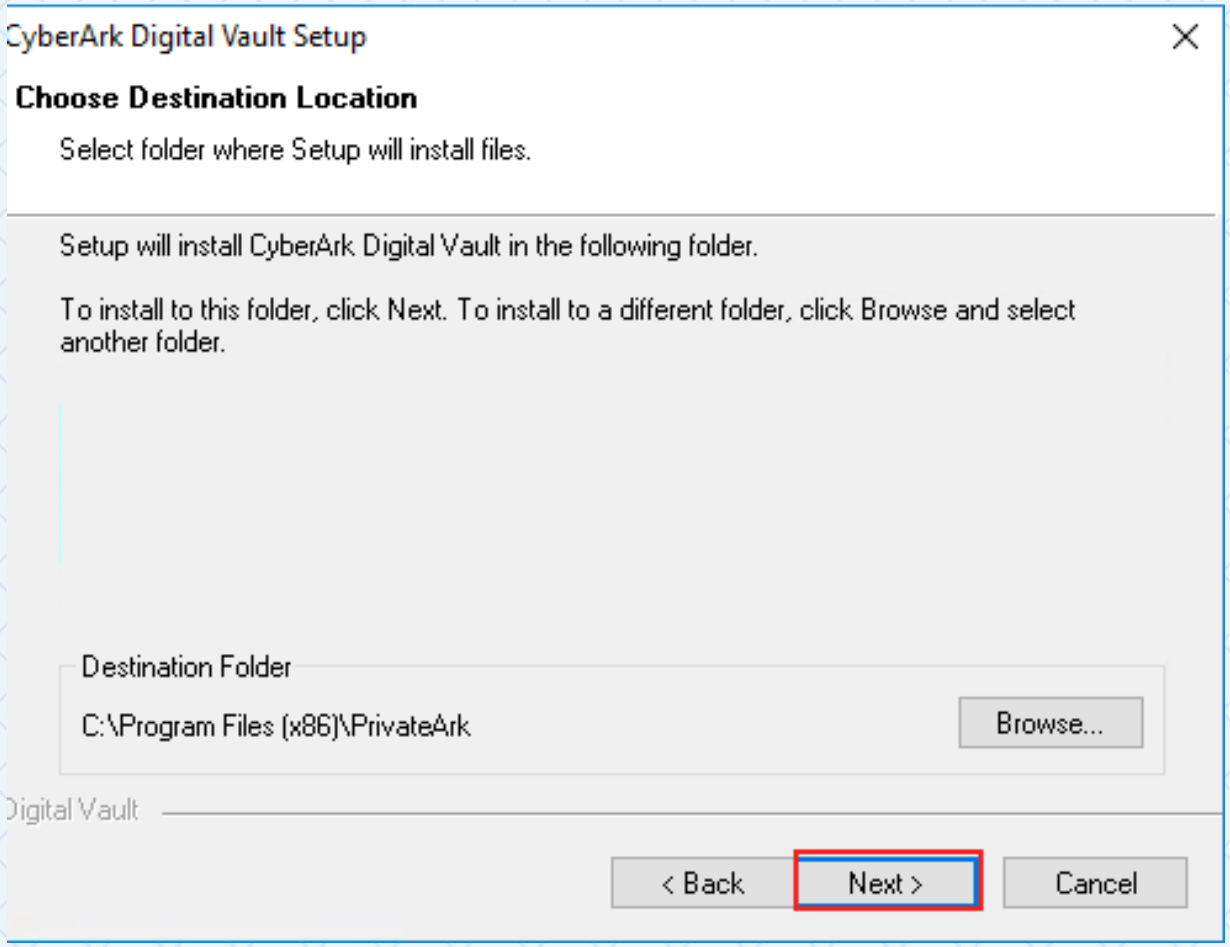
STANDALONE VAULT INSTALLATION

- Select Standalone Vault Installation
- Note that The Cluster-node Vault Installation requires a separate license



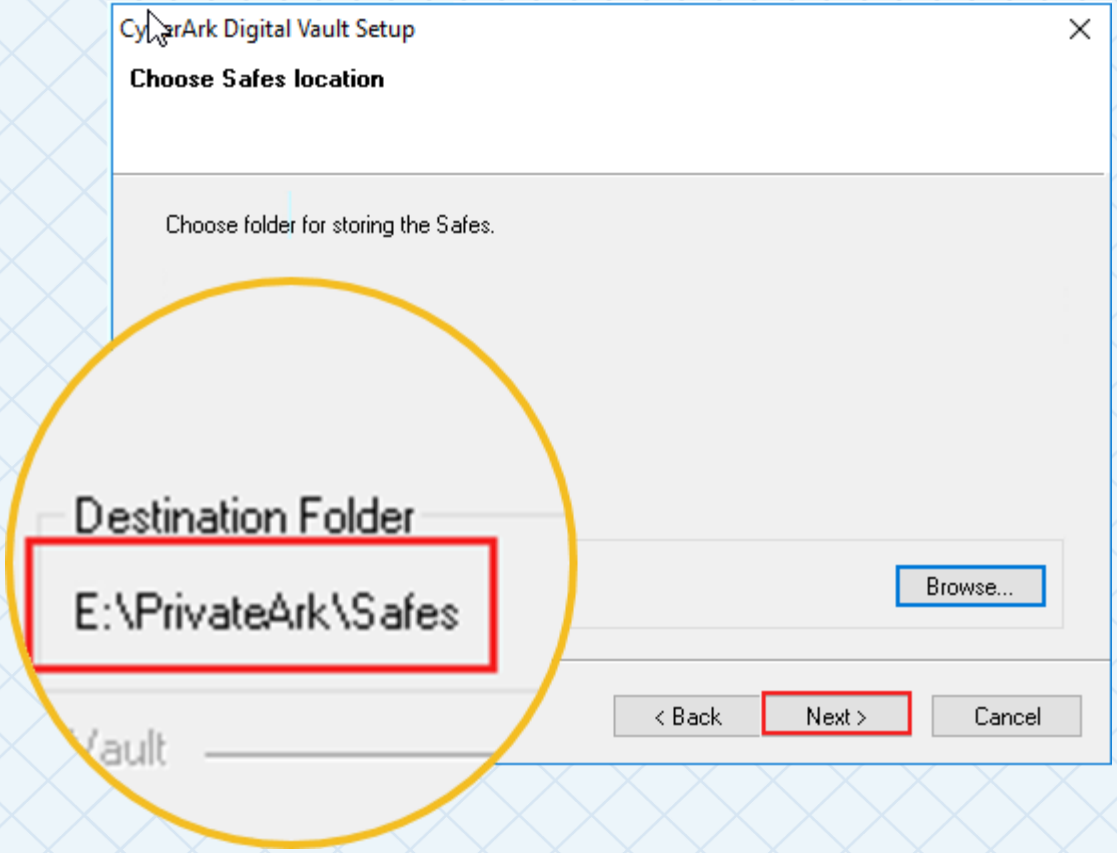
DESTINATION LOCATION

- Select destination for Vault Files.
- Although this can be changed to any local drive it is recommend to maintain the directory path and only change the drive letter if necessary.



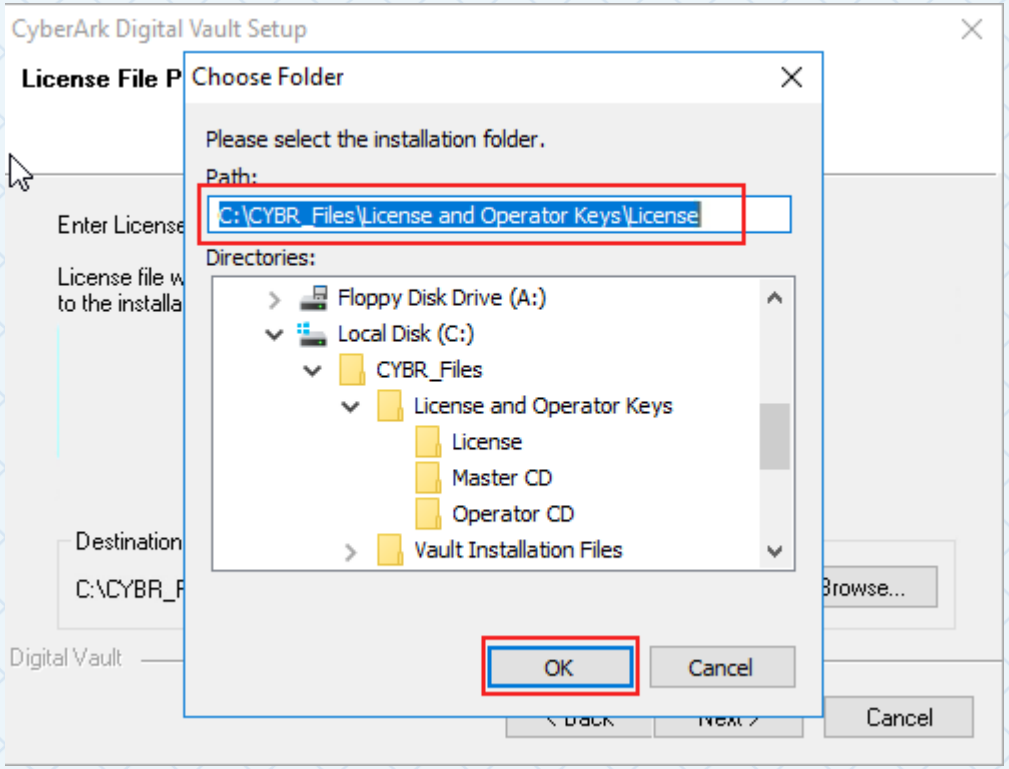
SAFES LOCATION

- A separate volume should be created specifically to store the vault's data
- The Safes directory will be the data store for all CyberArk objects (passwords, files, etc)
- Consider future size requirements. PSM recordings may require up to terabytes of data



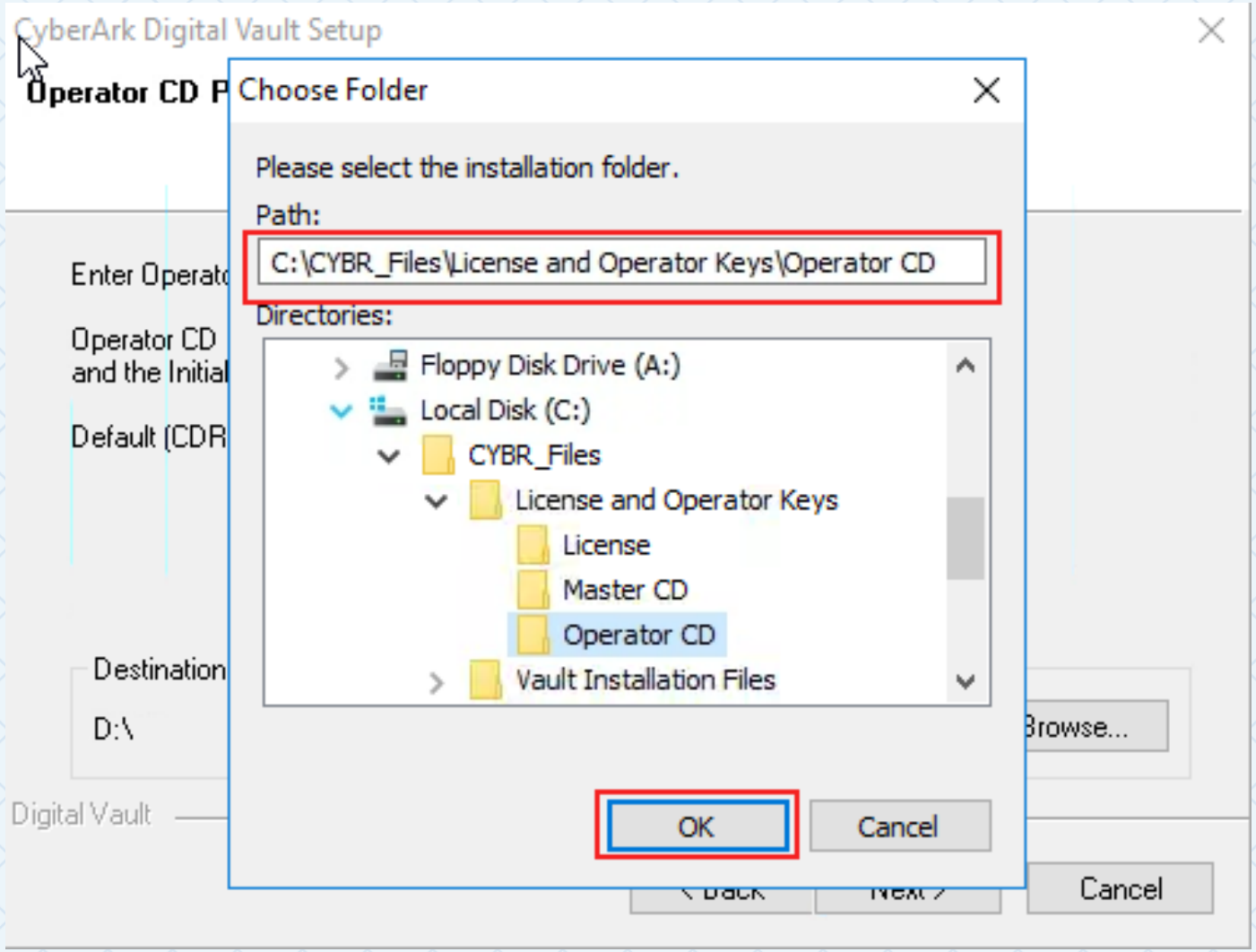
LICENSE FILE PATH

- Select the License file location.
- The license file will be provided by your Account Executive for download from the Secure File Exchange
- Ensure the license file is copied locally prior to configuring the network interface



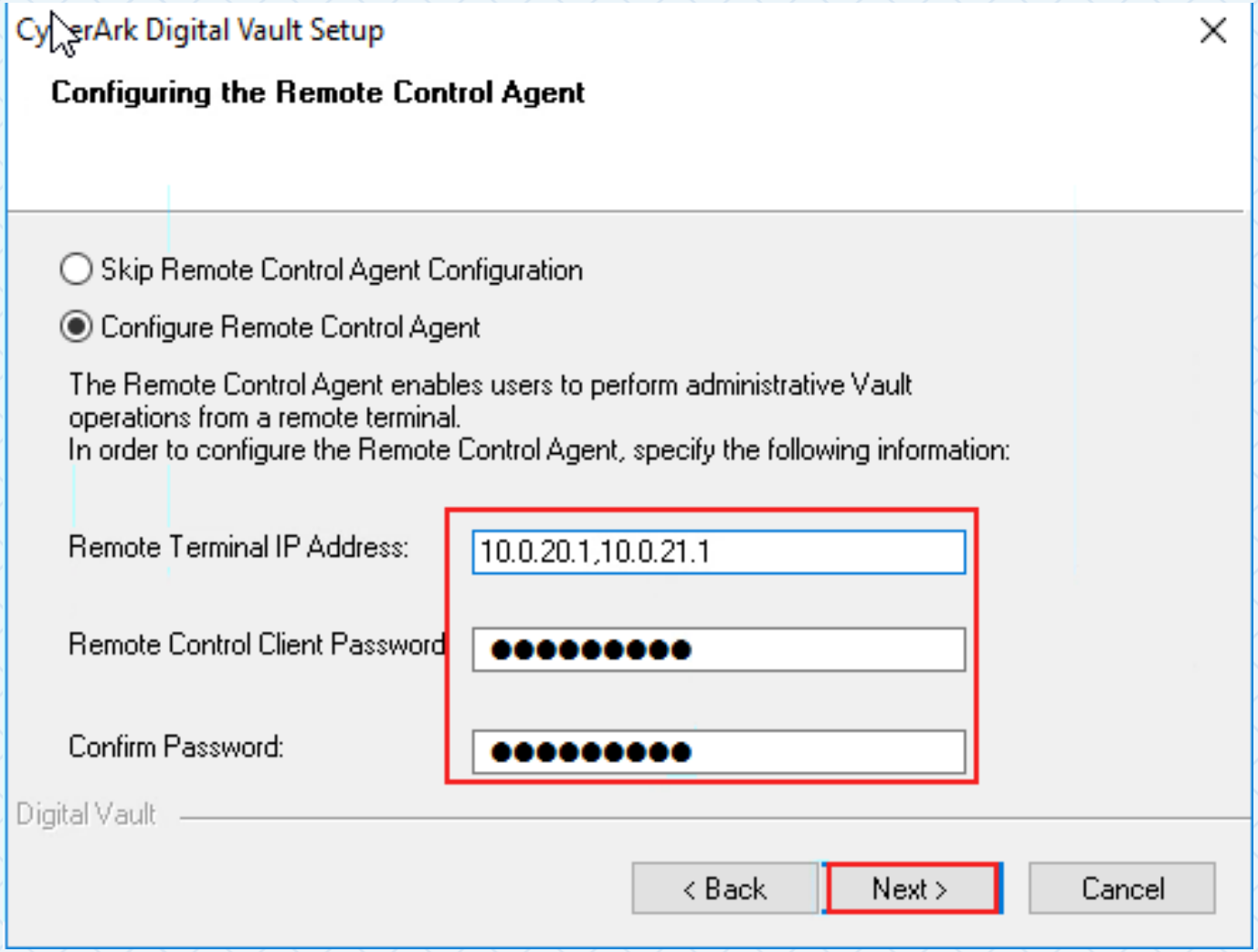
OPERATOR CD PATH

- Select location of the Operator CD keys
- The contents of the Operator CD must be accessible when starting the service
- These keys can be stored on the CD, copied to a secure location on the vault server, or stored on an HSM (recommended)



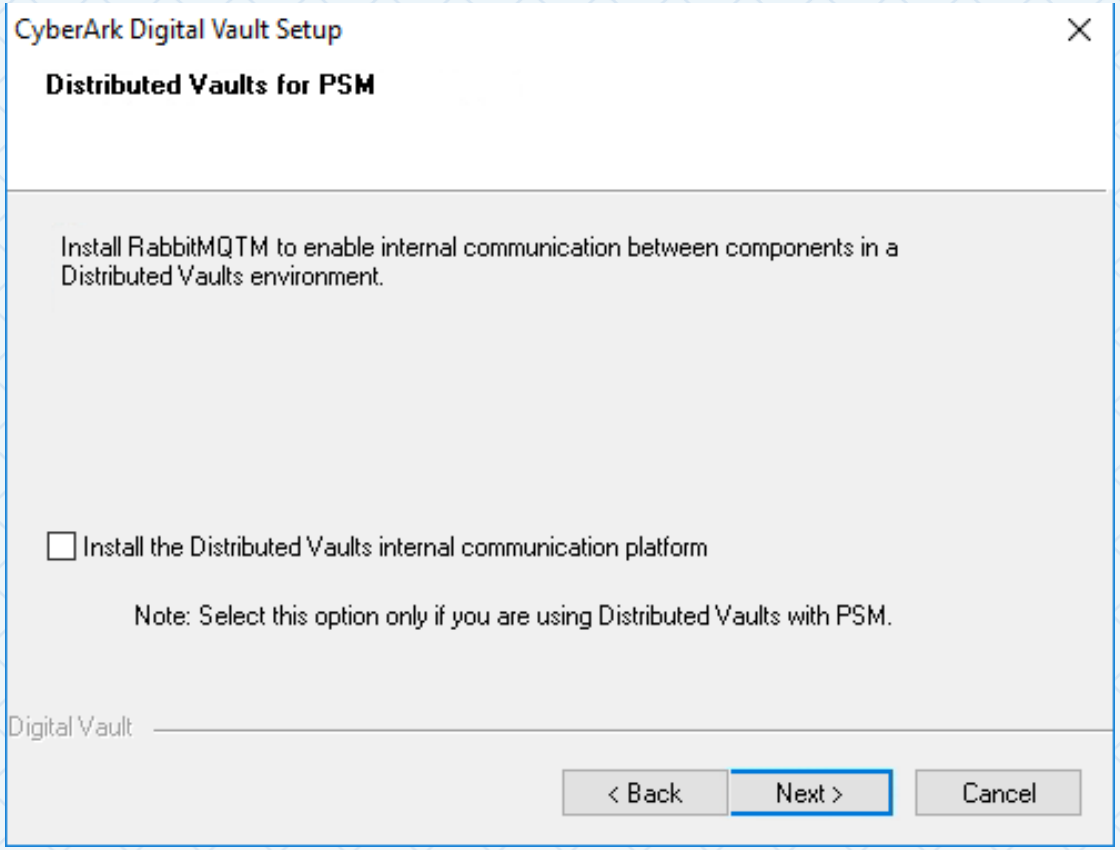
REMOTE CONTROL AGENT

- Select the IP of the station where the Remote Control Client will be used and the password that will be used by the Client to access the Remote Control Agent
- Recommended to only use CyberArk Component Servers for Remote Terminals
- The RCA can be enabled later if not enabled during Vault Installation



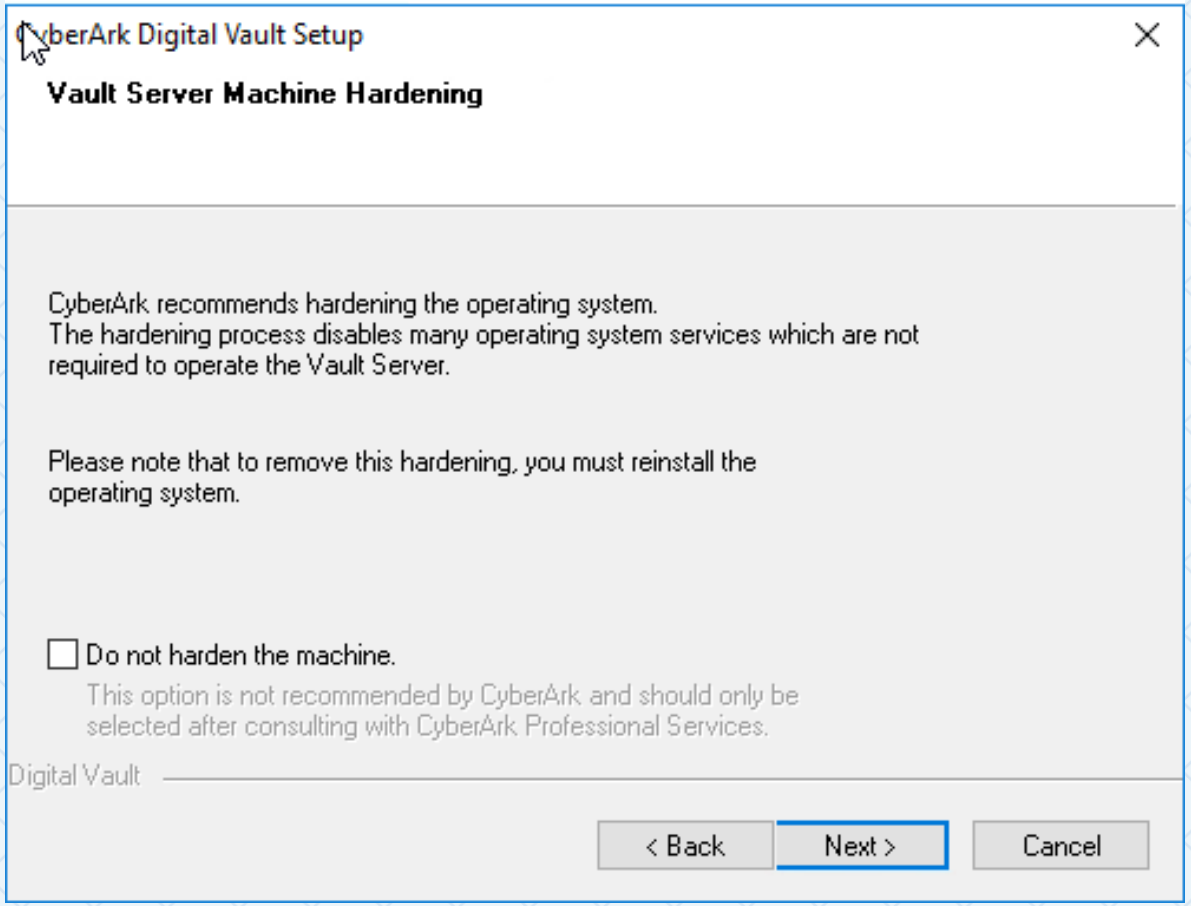
DISTRIBUTED VAULTS FOR PSM

- This step of the installation installs the Distributed Vaults internal communication platform, RabbitMQ.
- RabbitMQ must be installed in the default installation path (C:\Program Files (X86) and cannot be changed.
- Installing this feature is recommended if you think there may be a possibility of converting your environment to a DV environment.
- If you do not install RabbitMQ at this step, you will either need to reinstall the vault completely to install RabbitMQ on your current version or upgrade the Vault and install the RabbitMQ application during the upgrade process.



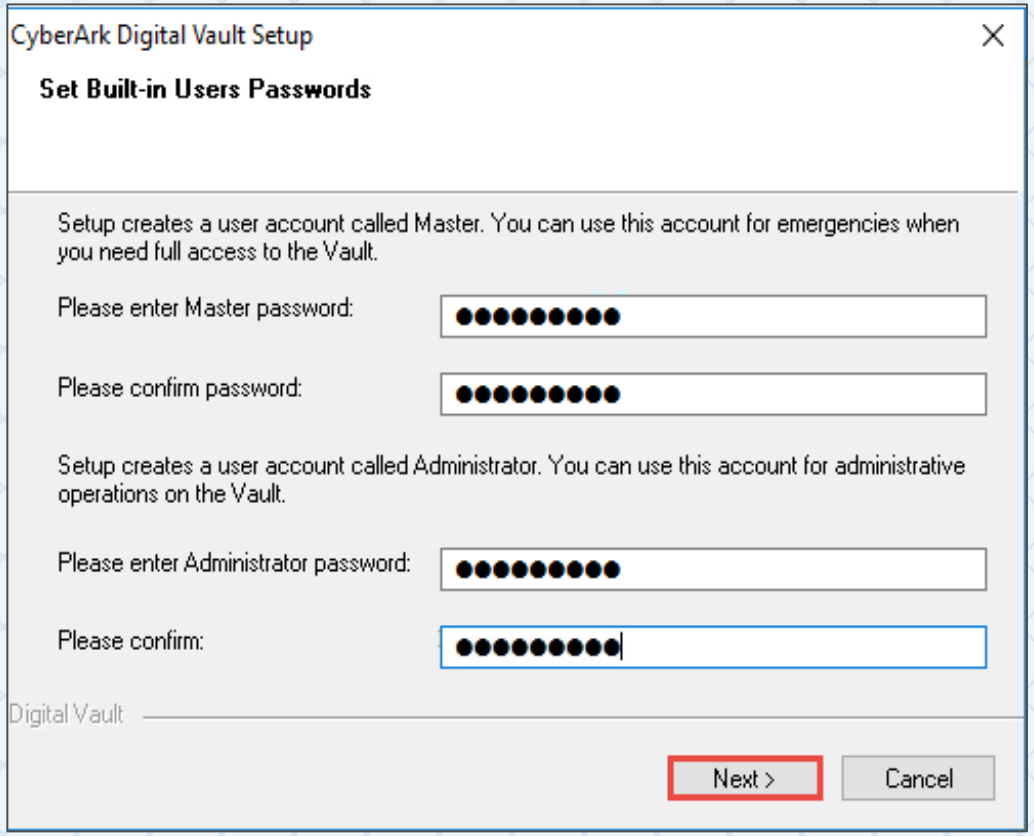
VAULT SERVER MACHINE HARDENING

- CyberArk installs the Vault Server on a hardened operating system, based on Microsoft Security Compliance Manager (SCM) server hardening recommendations
- Select “Next” to harden the Vault server



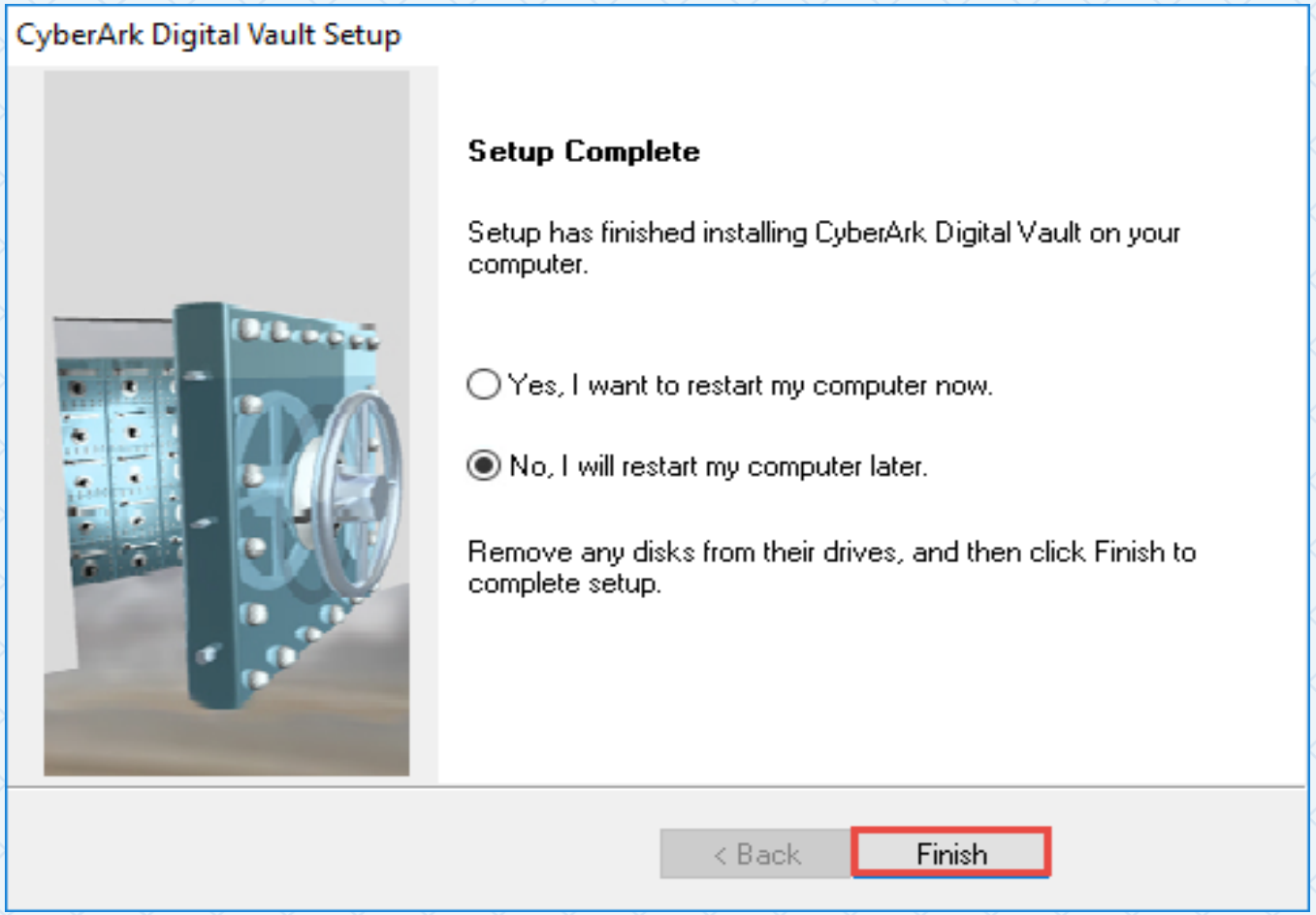
BUILT-IN USERS PASSWORDS

- Assign passwords for the built-in users Master and Administrator
- The passwords should be at least be 12 characters long and use a combination of upper- and lower-case characters and at least 1 special character.
- The Master password must be recorded accurately and stored in a secured physical location.



COMPLETE SETUP

- A restart is required after the Vault has been installed but first install the PrivateArk Client



VERIFY INSTALLATION SERVER AND VAULT ENVIRONMENT

VERIFY ALL SERVICES STARTED

- The installation process adds six new services:
  - Cyber-Ark Event Notification Engine
  - Cyber-Ark Hardened Windows Firewall
  - CyberArk Logic Container
  - PrivateArk Database
  - PrivateArk Remote Control Agent
  - PrivateArk Server

Name	Description	Status
Cyber-Ark Event Notification Engine		Started
Cyber-Ark Hardened Windows Firewall	Windows Firewall helps prot...	Started
CyberArk Logic Container		Started
DCOM Server Process Launcher	The DCOMLAUNCH service l...	Started
DHCP Client	Registers and updates IP a...	Started
DNS Client	The DNS Client service (dns...	Started
Group Policy Client	The service is responsible f...	Started
Net.Pipe Listener Adapter	Receives activation request...	Started
Net.Tcp Listener Adapter	Receives activation request...	Started
Net.Tcp Port Sharing Service	Provides ability to share TC...	Started
Network Connections	Manages objects in the Net...	Started
Network List Service	Identifies the networks to ...	Started
Network Location Awareness	Collects and stores configur...	Started
Network Store Interface Service	This service delivers networ...	Started
Plug and Play	Enables a computer to reco...	Started
Power	Manages power policy and ...	Started
PrivateArk Database		Started
PrivateArk Remote Control Agent		Started
PrivateArk Server		Started
Remote Desktop Services	Allows users to connect inte...	Started
Remote Procedure Call (RPC)	The RPCSS service is the Se...	Started
RPC Endpoint Mapper	Resolves RPC interfaces ide...	Started

- Total number of previously running services has been reduced to 31 as part of the hardening process
- Vault installation has added 6 new services

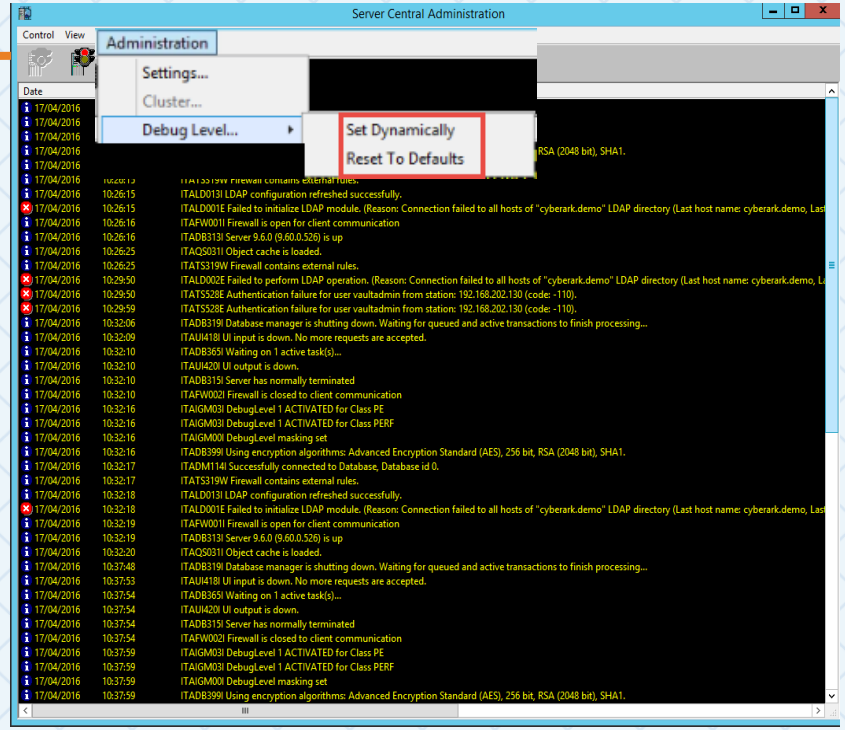
VERIFY THE SERVER STARTED

- It is not recommended to restart the PrivateArk Server Service using the Server Central Administration tool at this time.

- It is recommended to use the Windows Services applet to properly handle Windows Service dependencies.

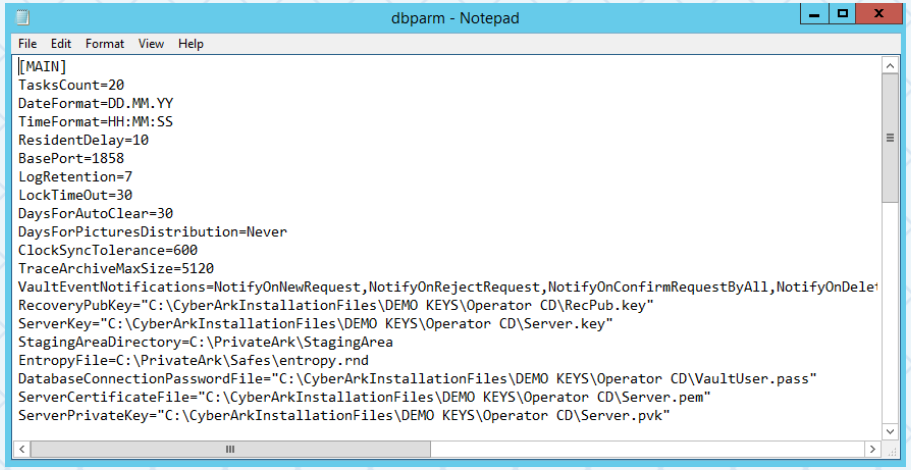
~~stop/start~~

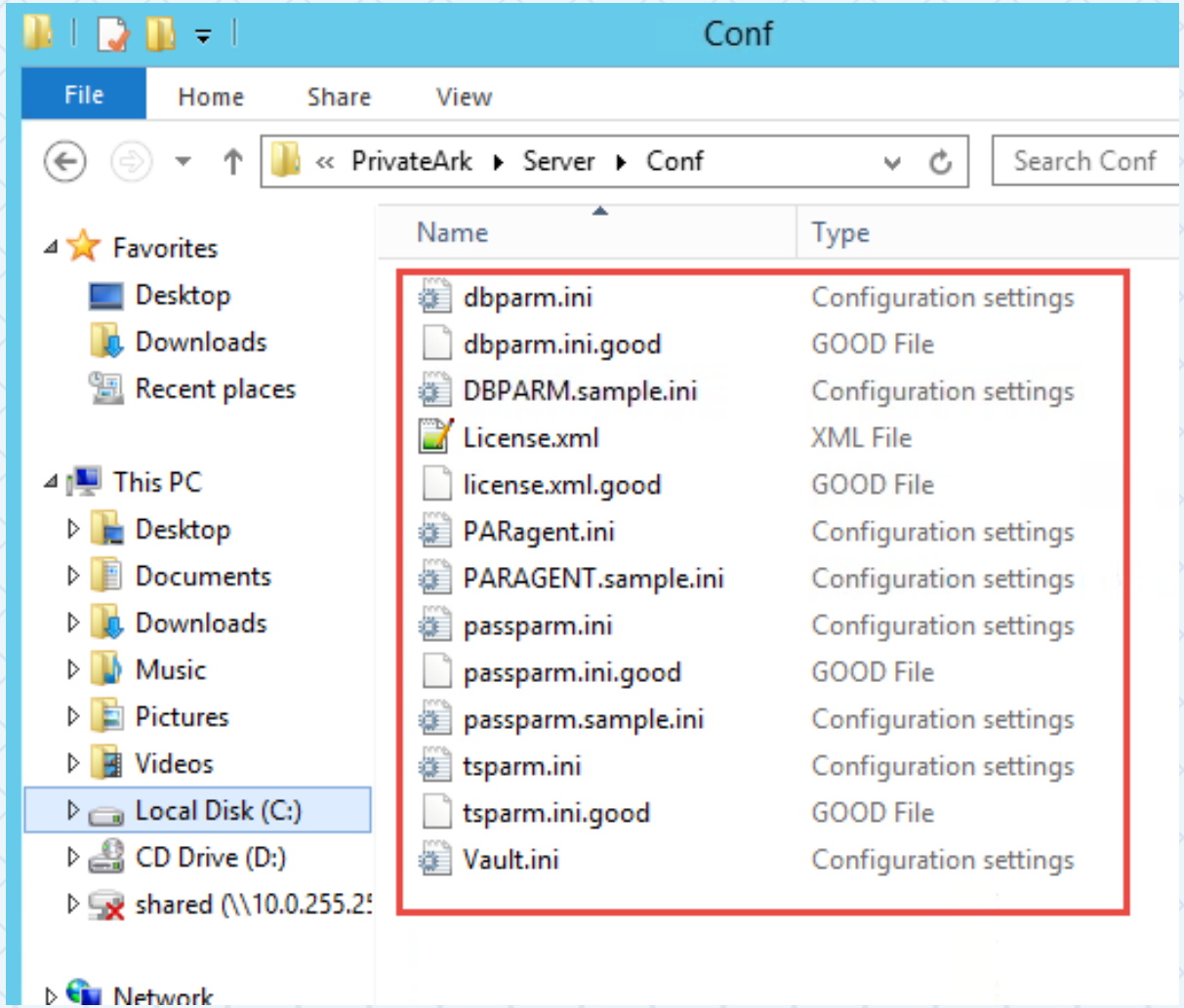
ITALOG.LOG



LOCATE VAULT CONFIGURATION AND LOG FILES (FILE SYSTEM)

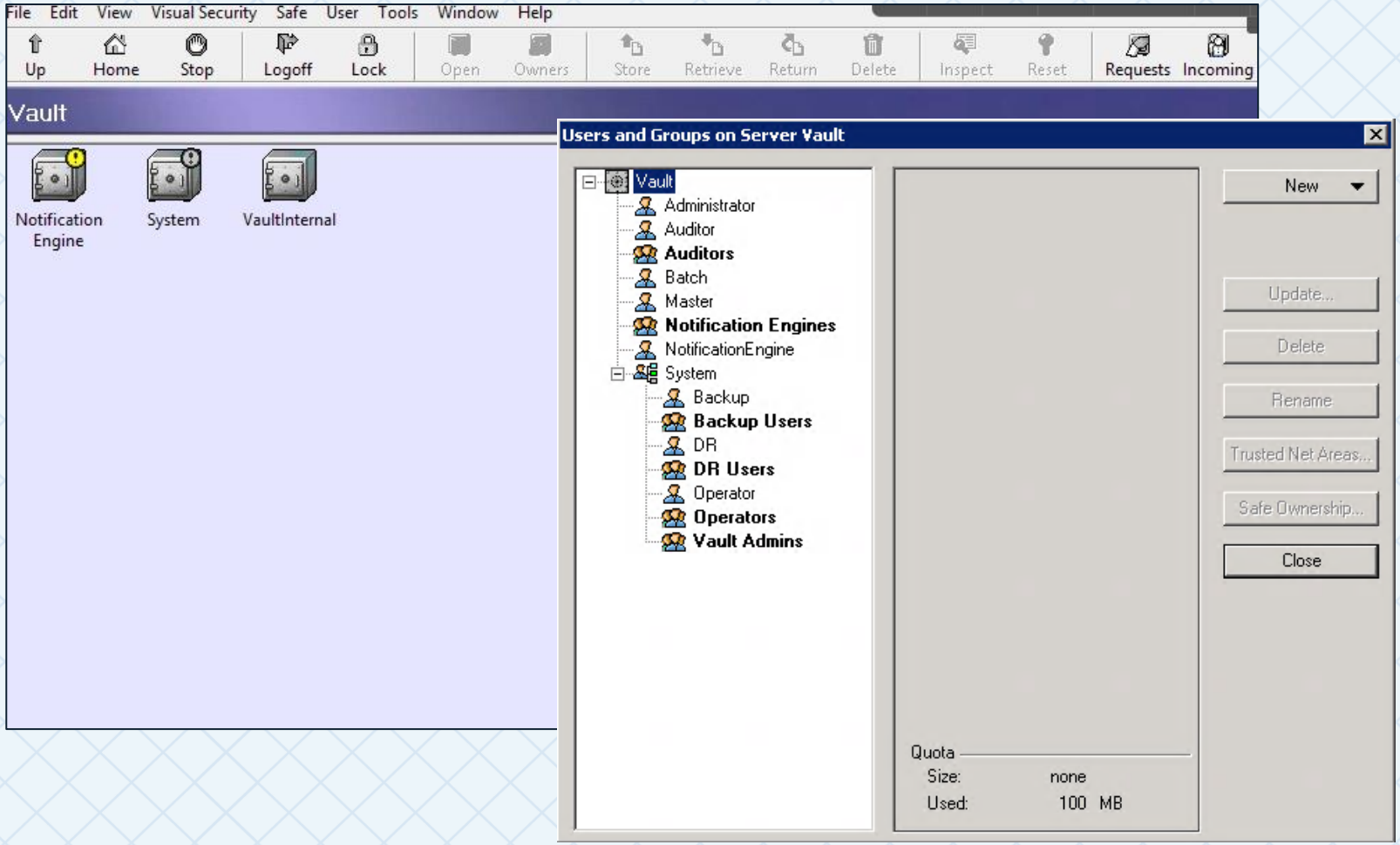
- The **Vault** main configuration files can be found in the Server\Conf folder:
  - dbparm.ini
  - license.xml
  - paragent.ini
  - passparm.ini
  - tsparm.ini
- Vault log files are found in Server\Logs





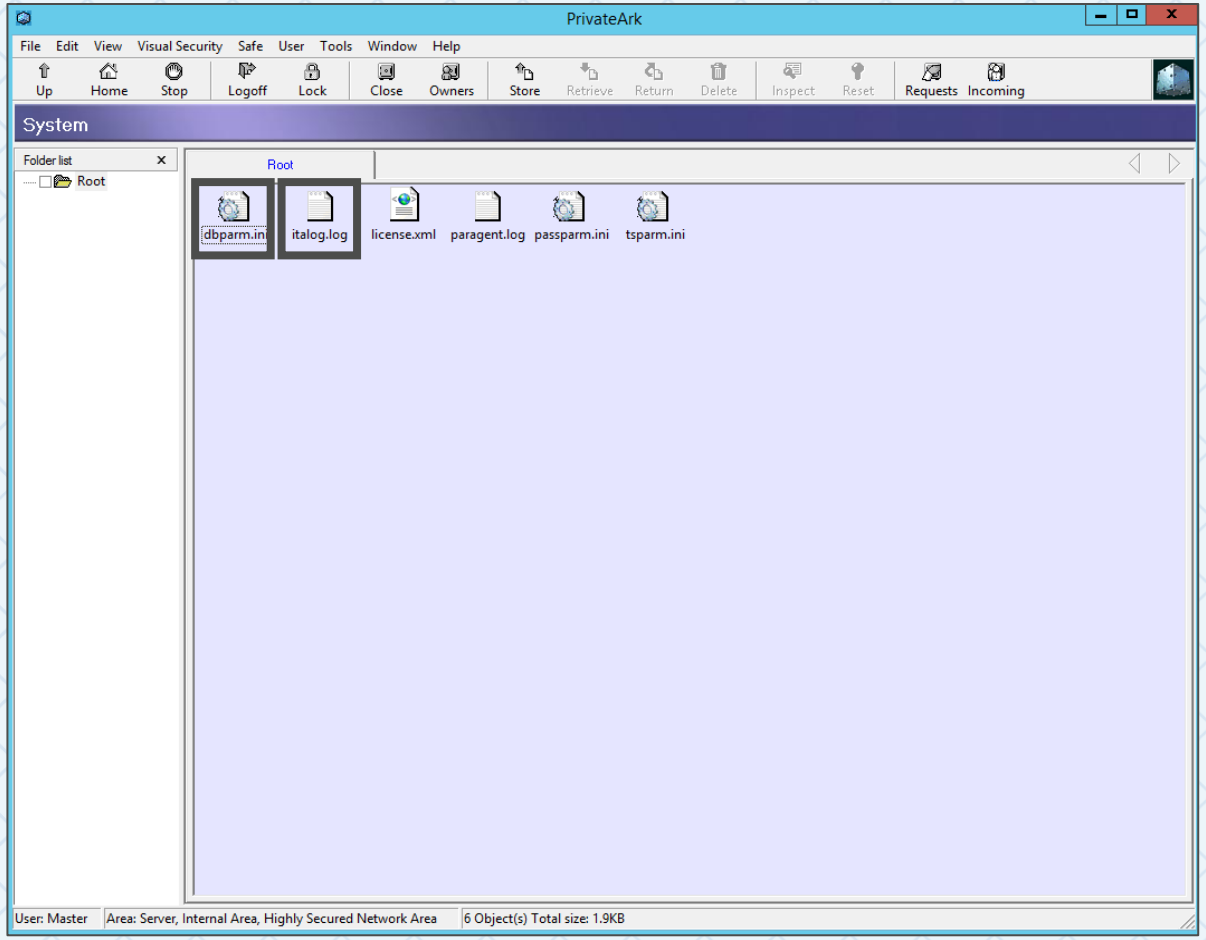
VERIFY BUILT-IN SAFES AND USERS

- The PrivateArk Client is the primary administrative interface to the Vault and can be installed on any station with access to the Vault
- Verify you can login to the Vault using the PrivateArk Client and that the Built-in Safes and Users were created properly



LOCATE VAULT CONFIGURATION FILES AND LOGS (PRIVATEARK)

- The **Vault**'s main configuration files and logs can also be accessed from remote stations using the PrivateArk Client (located in the ***system*** safe)
  - dbparm.ini
  - Italog.log
  - license.xml
  - paragent.log
  - passparm.ini
  - tsparm.ini



DIGITAL VAULT SECURITY STANDARD

DIGITAL VAULT SECURITY STANDARD

- Implementing the CyberArk Digital Vault in accordance with the Digital Vault Security Standard means applying the highest levels of protection
- The Digital Vault Security Standard documents the security controls and procedures designed to significantly reduce the system's attack surface

DIGITAL VAULT SECURITY STANDARD

- The high level of security required by the Digital Vault Server likely differs from commonly used server configurations
- An acute awareness and understanding of the “The Digital Vault Security Standard” is a requirement for the CyberArk Certified Delivery Engineer certification

DIGITAL VAULT SECURITY STANDARD KEY RECOMMENDATIONS

- The Digital Vault should be installed on a dedicated physical machine (recommended) from original Microsoft installation media
- The dedicated Digital Vault Server should be built from the original Microsoft installation media, and NO third-party software, such as anti-virus or remote management solutions, should be installed
- The Digital Vault Server shall **NOT be a member of any enterprise domain** (Installing the Digital Vault software on a domain member server requires enabling protocols and services and exposes the Digital Vault to a wider array of attacks)

DIGITAL VAULT SECURITY STANDARD – SERVER HARDENING

- Vault installation includes hardening of the operating system based on the Microsoft Security Compliance Manager (SCM) server hardening recommendations.

- The Hardening process deactivates many operating system services that are not required for the operation of the Digital Vault application and will not function as a regular domain member in a Windows network.

Name	Description	Status	Startup Type	Log On As
Base Filtering Engine	The Base Filtering Engine (BFE) is a service that m...	Started	Automatic	Local Service
Certificate Propagation	Copies user certificates and root certificates from ...	Started	Manual	Local System
COM+ Event System	Supports System Event Notification Service (SENS)...	Started	Automatic	Local Service
COM+ System Application	Manages the configuration and tracking of Compo...	Started	Manual	Local System
Cryptographic Services	Provides four management services: Catalog Data...	Started	Automatic	Network Service
DCOM Server Process Launcher	The DCOMLAUNCH service launches COM and DC...	Started	Automatic	Local System
Desktop Window Manager Session...	Provides Desktop Window Manager startup and m...	Started	Automatic	Local System
DHCP Client	Registers and updates IP addresses and DNS reco...	Started	Automatic	Local Service
Diagnostic Policy Service	The Diagnostic Policy Service enables problem dete...	Started	Automatic (Delayed Start)	Local Service
Diagnostic System Host	The Diagnostic System Host is used by the Diagnos...	Started	Manual	Local System
Distributed Link Tracking Client	Maintains links between NTFS files within a comput...	Started	Automatic	Local System
Distributed Transaction Coordinator	Coordinates transactions that span multiple resour...	Started	Automatic (Delayed Start)	Network Service
DNS Client	The DNS Client service (dnscache) caches Domain ...	Started	Automatic	Network Service
Group Policy Client	The service is responsible for applying settings con...	Started	Automatic	Local System
IP Helper	Provides tunnel connectivity using IPv6 transition t...	Started	Automatic	Local System
Network Connections	Manages objects in the Network and Dial-Up Conn...	Started	Manual	Local System
Network List Service	Identifies the networks to which the computer has ...	Started	Manual	Local Service
Network Location Awareness	Collects and stores configuration information for th...	Started	Automatic	Network Service
Network Store Interface Service	This service delivers network notifications (e.g. int...	Started	Automatic	Local Service
Plug and Play	Enables a computer to recognize and adapt to har...	Started	Automatic	Local System
Power	Manages power policy and power policy notificatio...	Started	Automatic	Local System
Print Spooler	Loads files to memory for later printing	Started	Automatic	Local System
Remote Desktop Configuration	Remote Desktop Configuration service (RDCS) is r...	Started	Manual	Local System
Remote Desktop Services	Allows users to connect interactively to a remote c...	Started	Manual	Network Service
Remote Desktop Services UserMo...	Allows the redirection of Printers/Drives/Ports for ...	Started	Manual	Local System
Remote Procedure Call (RPC)	The RPCSS service is the Service Control Manager ...	Started	Automatic	Network Service
Remote Registry	Enables remote users to modify registry settings o...	Started	Automatic	Local Service
RPC Endpoint Mapper	Resolves RPC interfaces identifiers to transport en...	Started	Automatic	Network Service
Security Accounts Manager	The startup of this service signals other services t...	Started	Automatic	Local System

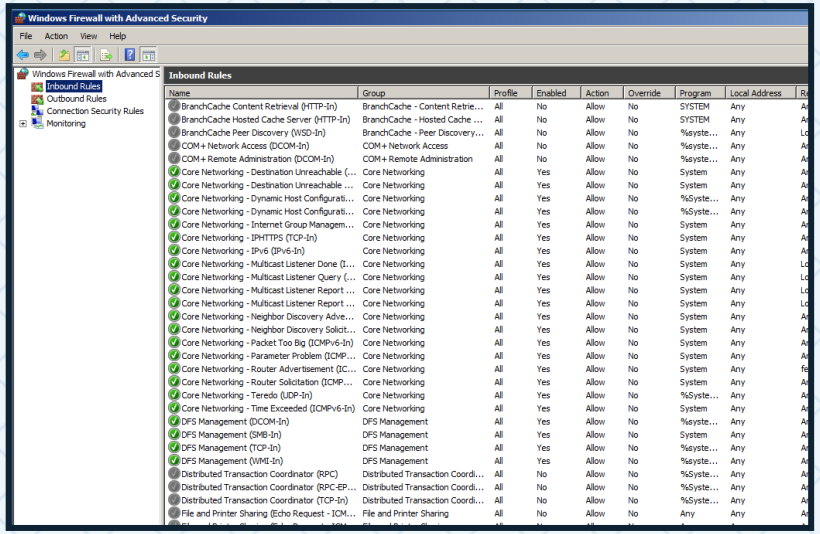
Name	Description	Status
Cyber-Ark Event Notification Engine		Started
Cyber-Ark Hardened Windows Firewall	Windows Firewall helps prot...	Started
CyberArk Logic Container		Started
DCOM Server Process Launcher	The DCOMLAUNCH service l...	Started
DHCP Client	Registers and updates IP a...	Started
DNS Client	The DNS Client service (dns...	Started
Group Policy Client	The service is responsible f...	Started
Net.Pipe Listener Adapter	Receives activation request...	Started
Net.Tcp Listener Adapter	Receives activation request...	Started
Net.Tcp Port Sharing Service	Provides ability to share TC...	Started
Network Connections	Manages objects in the Net...	Started
Network List Service	Identifies the networks to ...	Started
Network Location Awareness	Collects and stores configur...	Started
Network Store Interface Service	This service delivers networ...	Started
Plug and Play	Enables a computer to reco...	Started
Power	Manages power policy and ...	Started
PrivateArk Database		Started
PrivateArk Remote Control Agent		Started
PrivateArk Server		Started
Remote Desktop Services	Allows users to connect inte...	Started
Remote Procedure Call (RPC)	The RPCSS service is the Se...	Started
RPC Endpoint Mapper	Resolves RPC interfaces ide...	Started

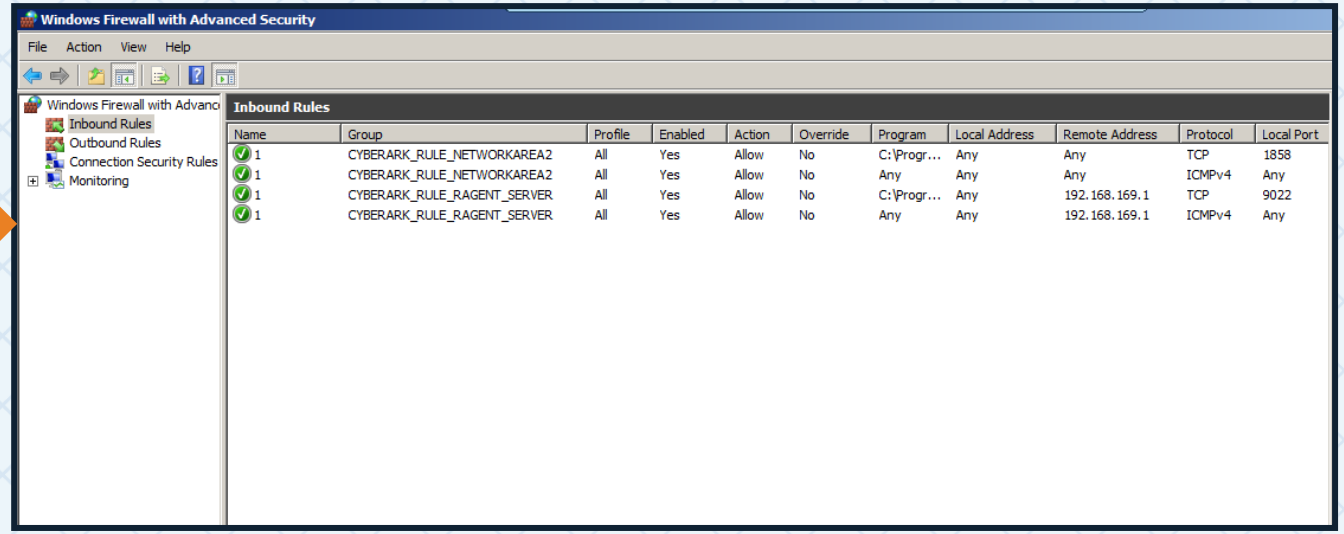
- Total number of previously running services has been reduced to 31 as part of the hardening process

- Vault installation has added 6 new services

DIGITAL VAULT SECURITY STANDARD – FIREWALL

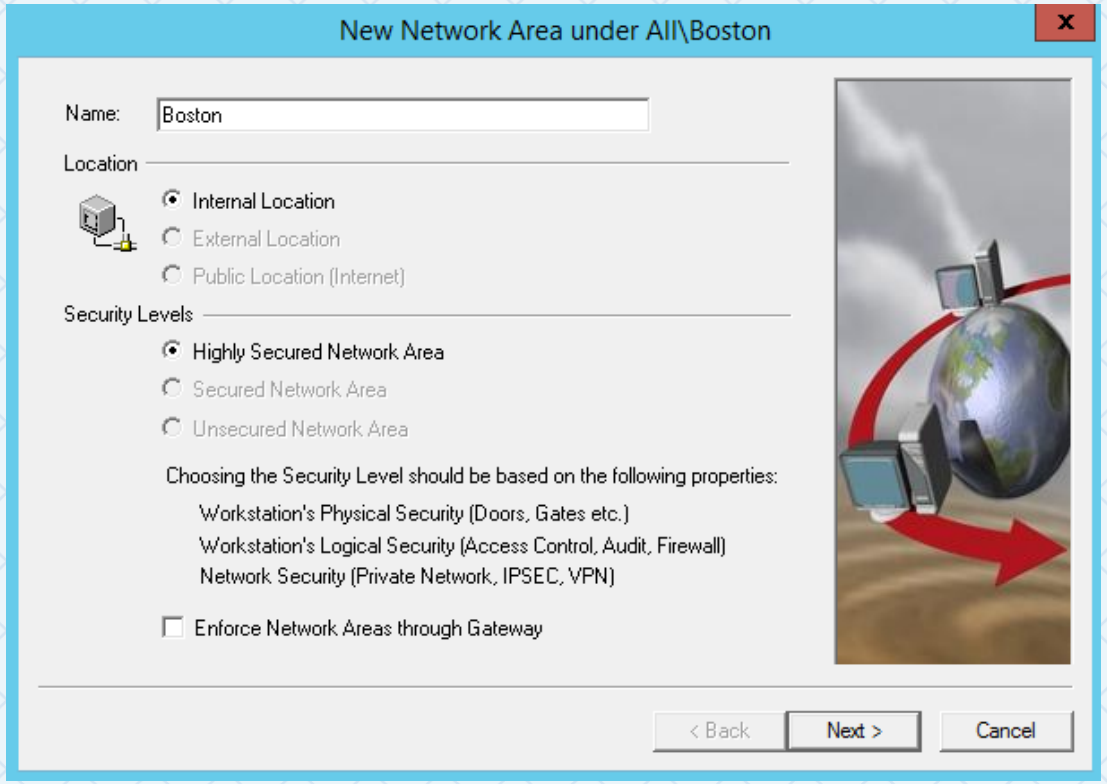
- The Microsoft Windows firewall shall be managed exclusively by the Digital Vault software, with only authorized inbound and outbound traffic permitted
- CyberArk utilizes and hardens the Microsoft firewall on the Digital Vault Server machine in such way that it verifies and permits only transmissions that are sent to the dedicated Vault port (by default – 1858), while blocking all other traffic. This restrictive firewall policy dramatically reduces the attack surface of the Digital Vault Server

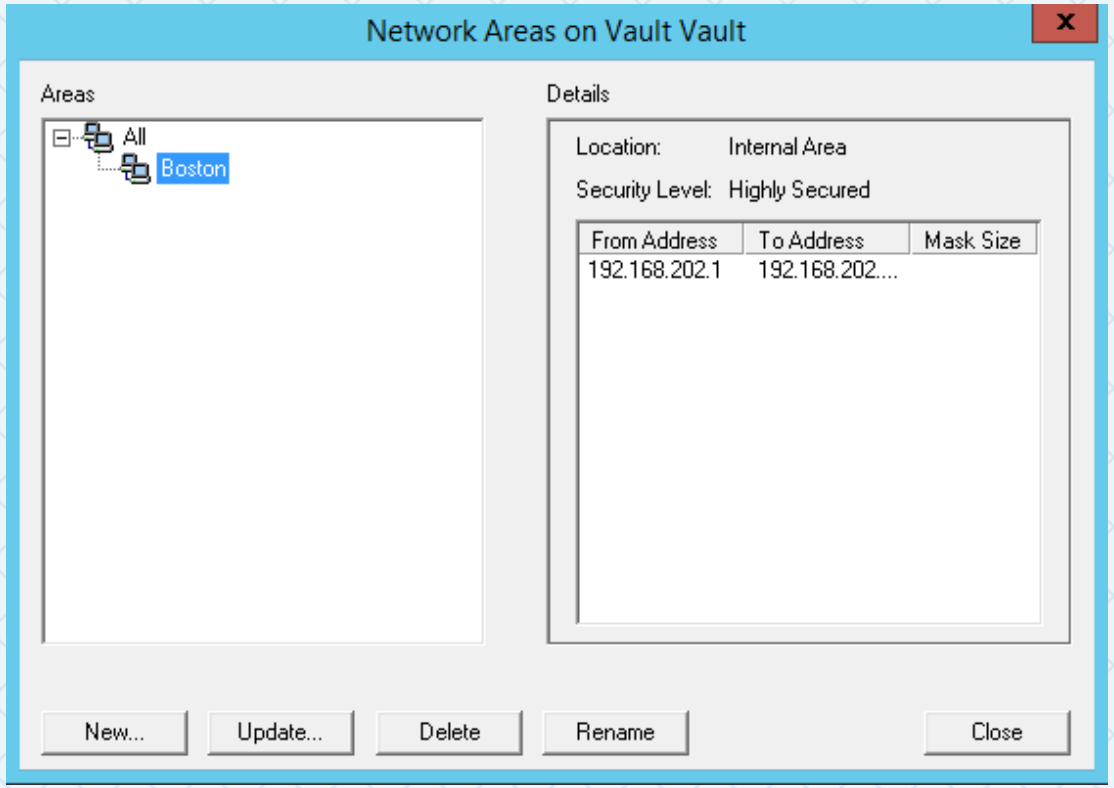




RESTRICT ACCESS USING NETWORK AREAS

Configuring Network Areas allows you to restrict access to the Vault to specific source IP addresses





VAULT HARDENING AND SECURITY SUMMARY

Isolate the Server

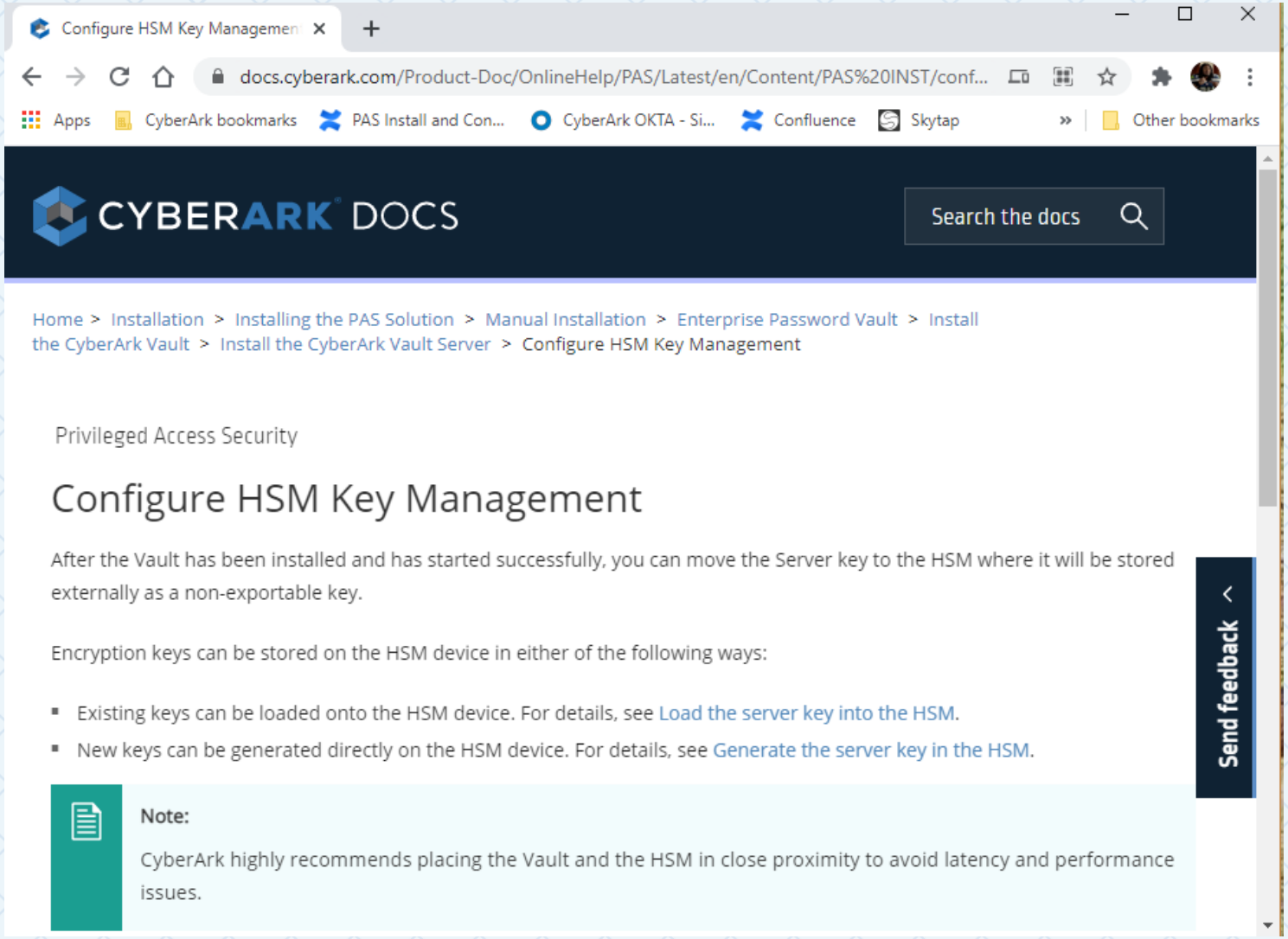
- Consider placing the Vault in a secure VLAN
- No domain membership or trusts
- Only TCP/IP v4
- No DNS or WINS
  - Uses a manually configured Host file when host name resolution is required

Harden the Server

- Remove unnecessary services
- Restrict network access to CyberArk protocol only
- Only Vault Server and PrivateArk Client should be installed
- No 3rd party applications or agents assuring a sterile environment

CYBERARK DOCS ONLINE – HSM KEY MANAGEMENT

- Detailed instructions for configuring HSM Key Management to store the Server.key, can be found online.
- Search docs.cyberark.com for “Configure HSM Key Management”



SUMMARY

- This session covered:
  - Hardened Vault Server
  - Multiple Layers of Security Controls
  - Installing a Standalone Vault Server
  - CyberArk Digital Vault Standard

THANK YOU