CYBERARK®

CYBERARK UNIVERSITY

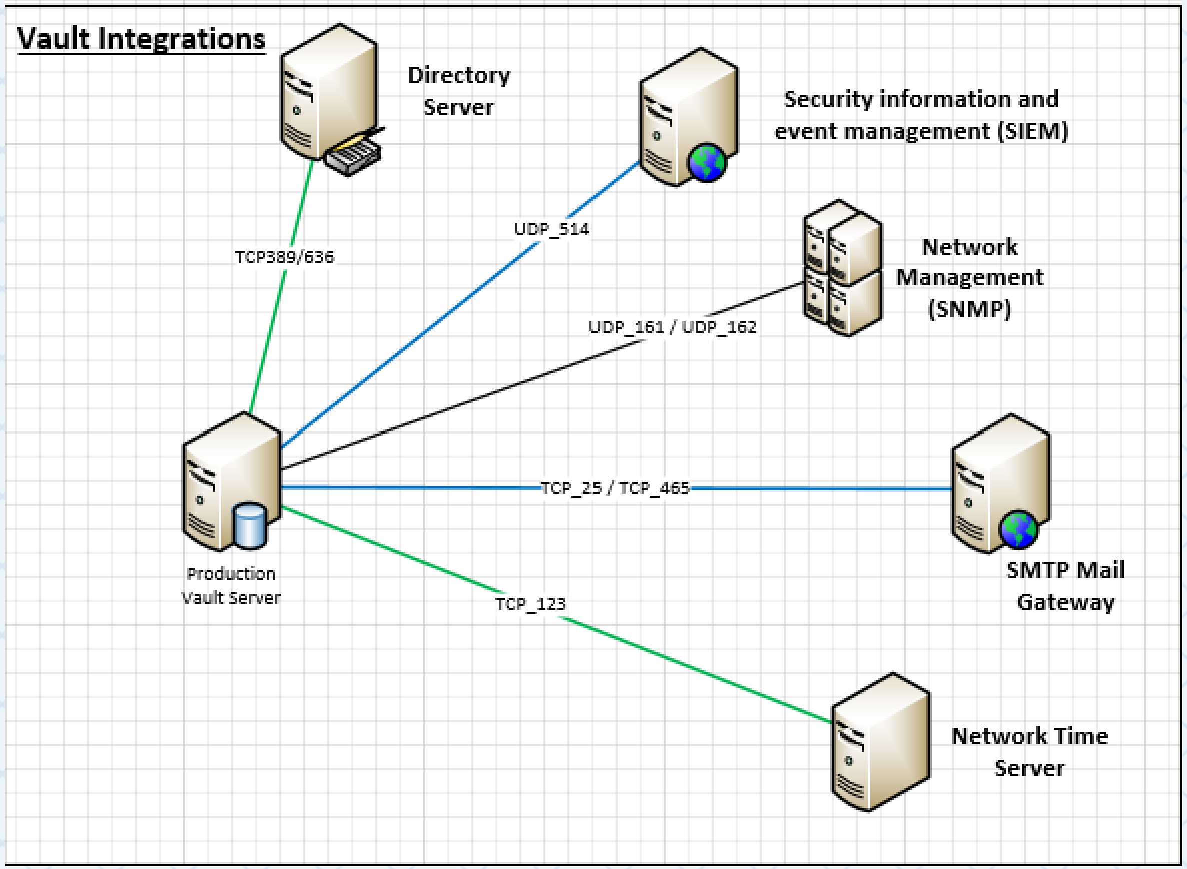
Vault Integrations

CyberArk Training

OBJECTIVES

By the end of this session you will be able to:

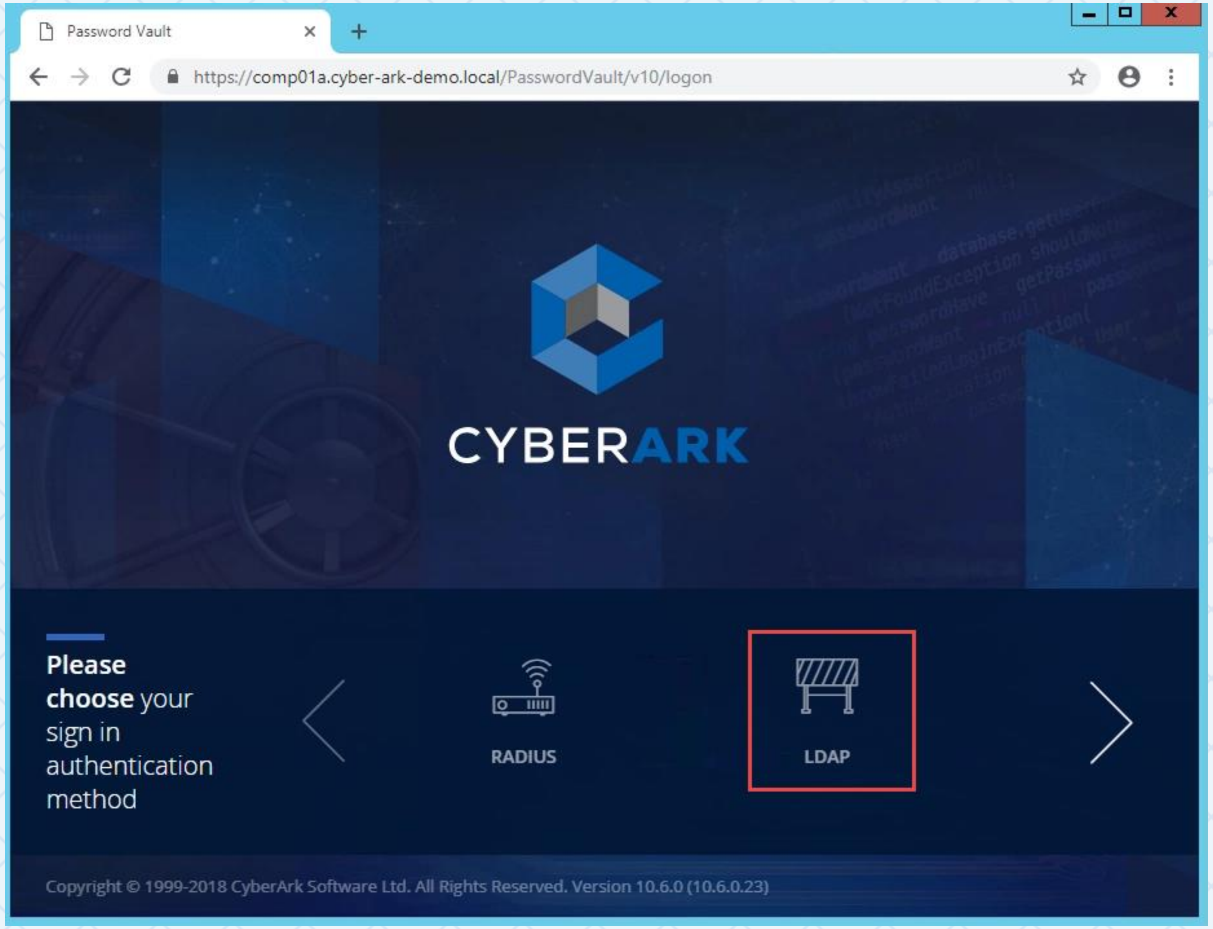
- Describe the main purpose for integrating CyberArk with other enterprise software, namely:
  - LDAP
  - SMTP
  - SNMP
  - SIEM
  - NTP
- Integrate CyberArk with other enterprise software



LDAP INTEGRATION

LDAP INTEGRATION - PURPOSE

- The Privileged Account Security solution can be configured to manage users transparently through a centralized User database, such as LDAP
- The Enterprise Password Vault is a full LDAP (Lightweight Directory Access Protocol) client, and is capable of communicating with LDAP-compliant or compatible directory servers to obtain User identification and security information
- LDAP Integration enables the automatic provisioning of users and allows for the use of LDAP groups providing Access Control to safes



https://comp01a.cyber-ark-demo.local/PasswordVault/v10/logon

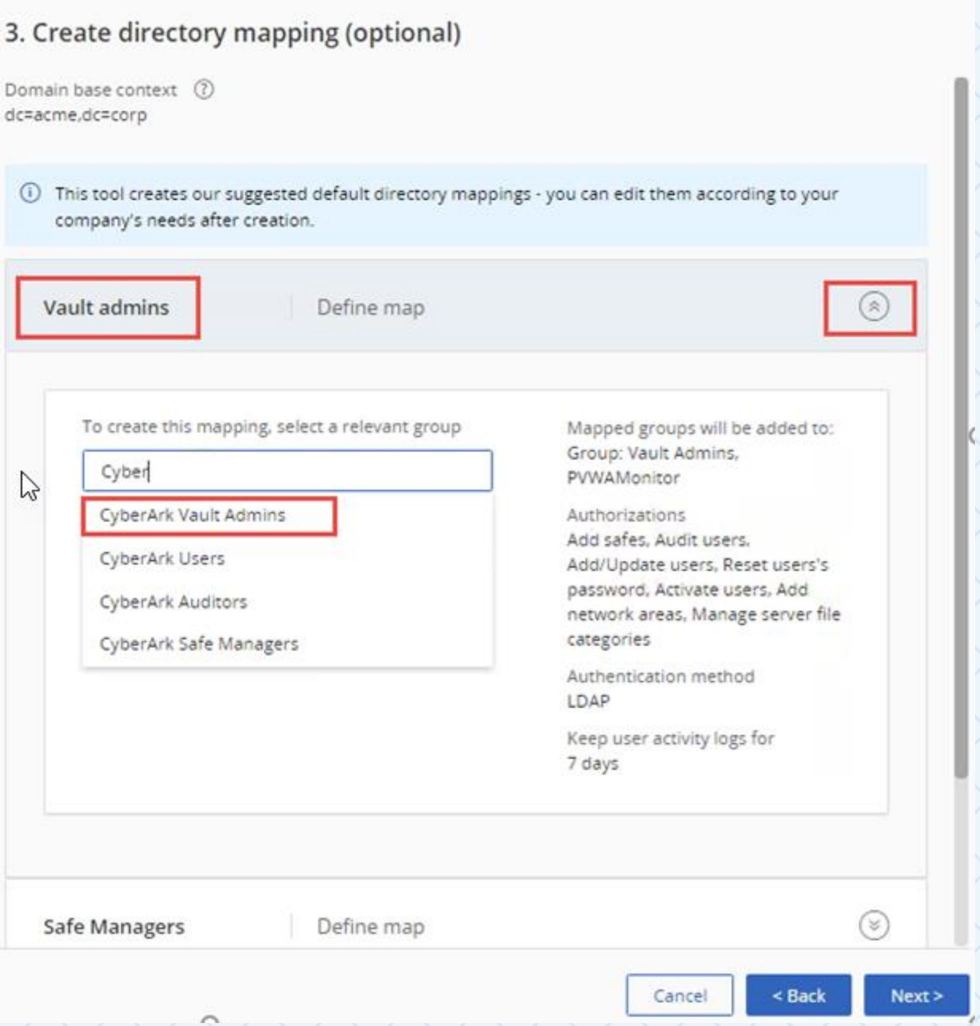
Please choose your sign in authentication method

Copyright © 1999-2018 CyberArk Software Ltd. All Rights Reserved. Version 10.6.0 (10.6.0.23)

LDAP INTEGRATION - PREREQUISITES

The customer must provide

- An LDAP Bind account with READ ONLY access to the directory.
  - Have the User Name, Password, and DN available
- Four LDAP groups representing roles in the Digital Vault
  - CyberArk Administrators
  - CyberArk Safe Managers
  - CyberArk Auditors
  - CyberArk Users



3. Create directory mapping (optional)

Domain base context
dc=acme,dc=corp

This tool creates our suggested default directory mappings - you can edit them according to your company's needs after creation.

Mapped groups will be added to:
Group: Vault Admins, PVWAMonitor

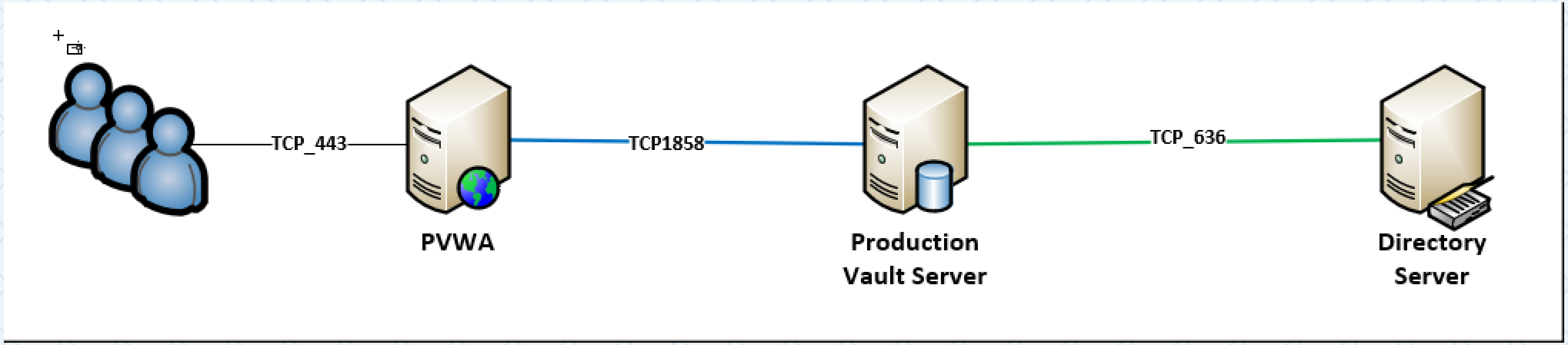
Authorizations
Add safes, Audit users, Add/Update users, Reset users's password, Activate users, Add network areas, Manage server file categories

Authentication method
LDAP

Keep user activity logs for
7 days

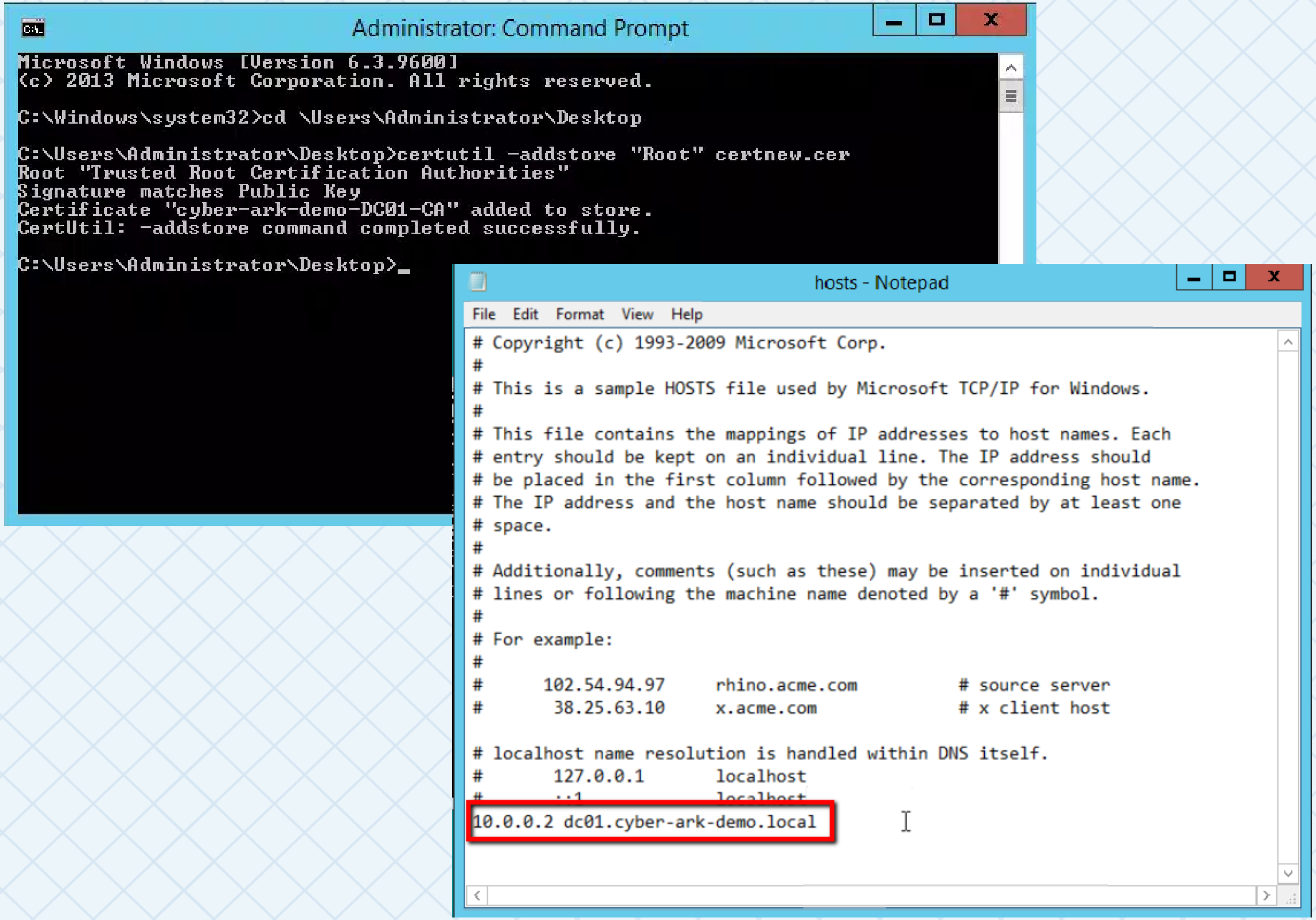
LDAP INTEGRATION - PREREQUISITES

- LDAP/S is required to secure the communications channel between the Digital Vault and the Directory Server.
  - This ensures that all the traffic between the Domain Controller or LDAP authenticating Server and the Vault is encrypted
  - Install all relevant Root and Intermediate Certificates for the CA that issued the certificate on the directory servers to the Vault Servers.
  - Create a hosts file on the vault servers for host name resolution



LDAP OVER SSL

- Import the CA Certificate that signed the certificate used by the External Directory into the Vault server certificate store.
- Configure the DNS of the LDAP host in the hosts file
- **A Vault Firewall rule is not required** and will expose the vault to unnecessary risk!
- The implementation and use of secure protocols is an emphasized area of study for all CyberArk certifications!

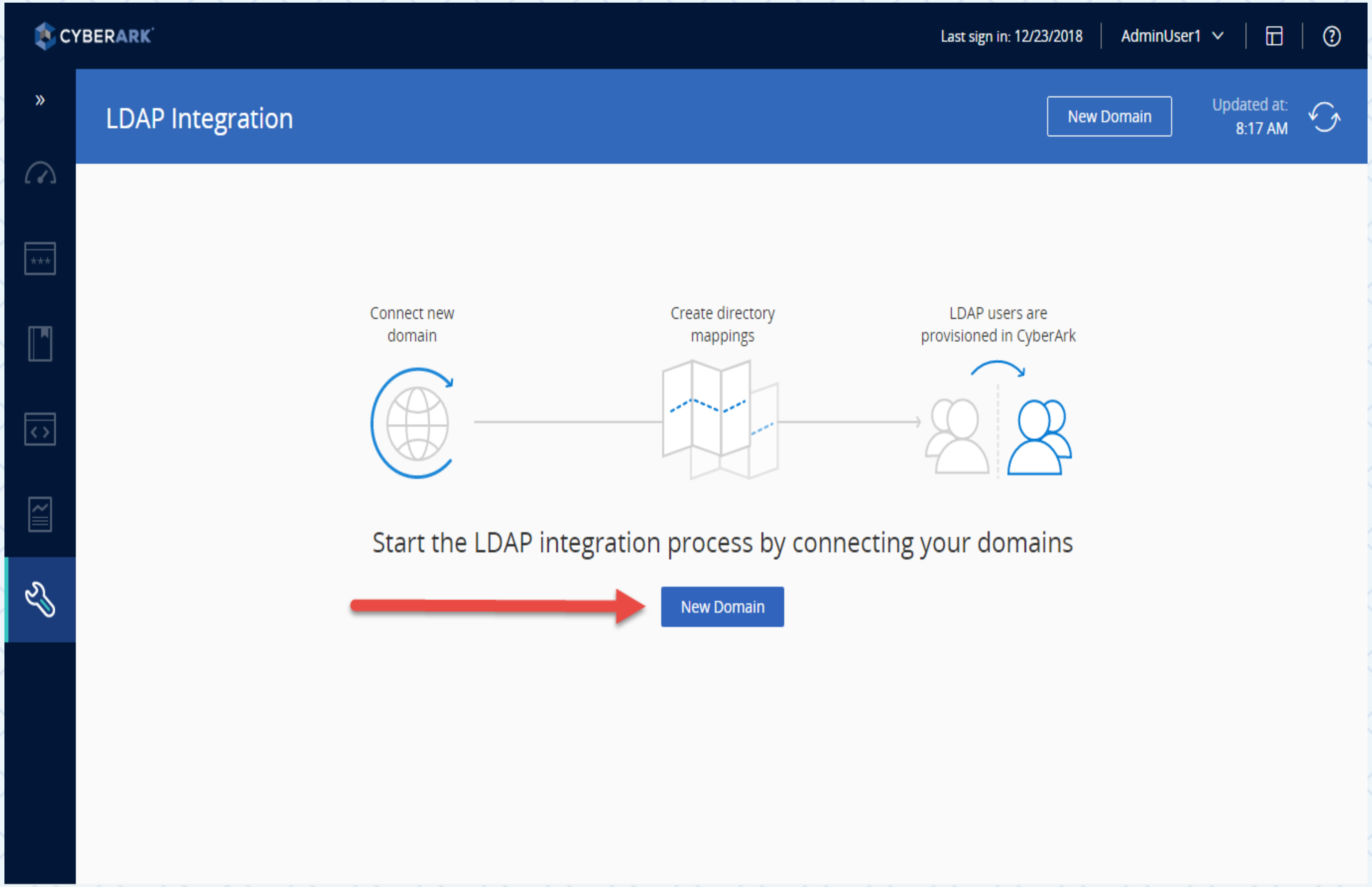


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd \Users\Administrator\Desktop

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

C:\Users\Administrator\Desktop>_
```

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
10.0.0.2 dc01.cyber-ark-demo.local
```

LDAP SETUP WIZARD

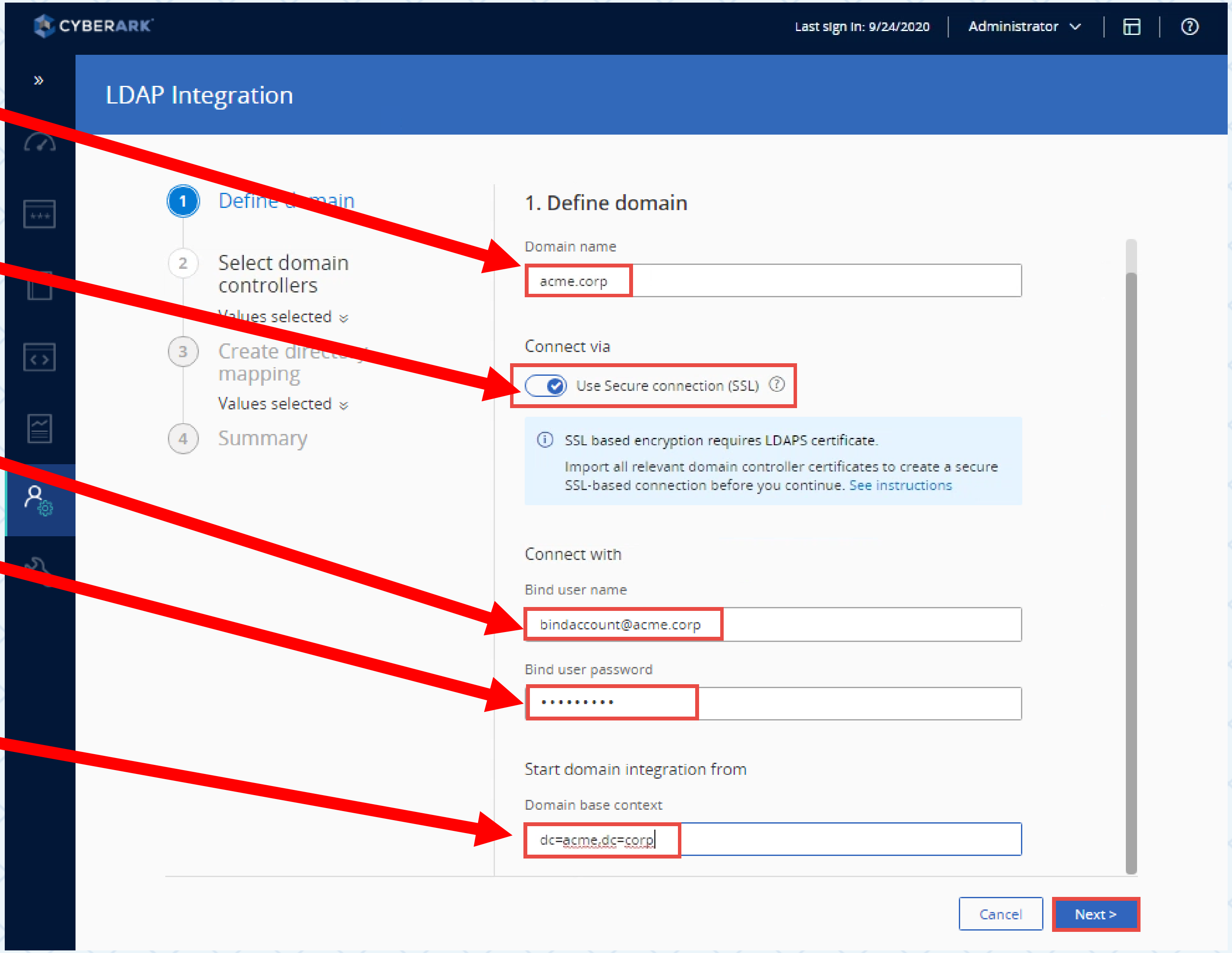
- LDAP Integration is configured easily in the PVWA
- The Vault can be configured to integrate with multiple directories easily by selecting the “New Domain” link in the LDAP Integration page of PVWA
- Only the Vault’s built-in Administrator can configure LDAP Integration.



Start the LDAP integration process by connecting your domains

LDAP SETUP WIZARD – DEFINE DOMAIN

- Enter the domain name
- Select “Use Secure connection (SSL)” to encrypt authentication traffic on the network
- Enter the Bind user name and password
- Enter the Domain base context using LDAP Notation



1. Define domain

Domain name: acme.corp

Connect via

☑ Use Secure connection (SSL)

SSL based encryption requires LDAPS certificate.
Import all relevant domain controller certificates to create a secure SSL-based connection before you continue. See instructions

Connect with

Bind user name: bindaccount@acme.corp

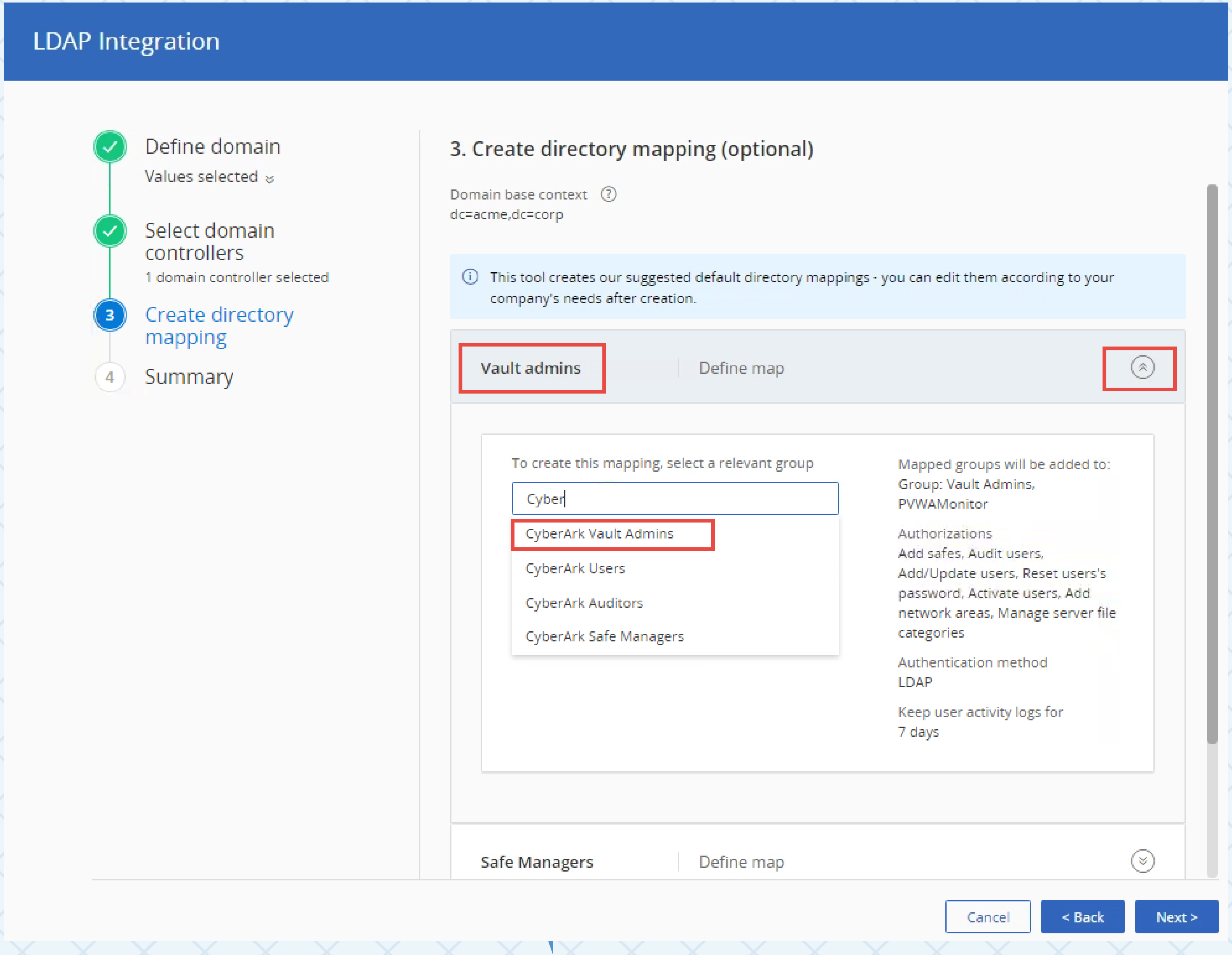
Bind user password: •••••••••

Start domain integration from

Domain base context: dc=acme,dc=corp

LDAP SETUP WIZARD – CREATE DIRECTORY MAPPING

- Select and assign external directory groups to CyberArk internal roles
- All 4 default directory mappings must be defined before proceeding



LDAP Integration

✓ Define domain
Values selected
✓ Select domain controllers
1 domain controller selected
3 Create directory mapping
4 Summary

3. Create directory mapping (optional)

Domain base context
dc=acme,dc=corp

This tool creates our suggested default directory mappings - you can edit them according to your company's needs after creation.

Vault admins | Define map

To create this mapping, select a relevant group

Cyber

- CyberArk Vault Admins
- CyberArk Users
- CyberArk Auditors
- CyberArk Safe Managers

Mapped groups will be added to:
Group: Vault Admins, PVWAMonitor

Authorizations
Add safes, Audit users, Add/Update users, Reset users's password, Activate users, Add network areas, Manage server file categories

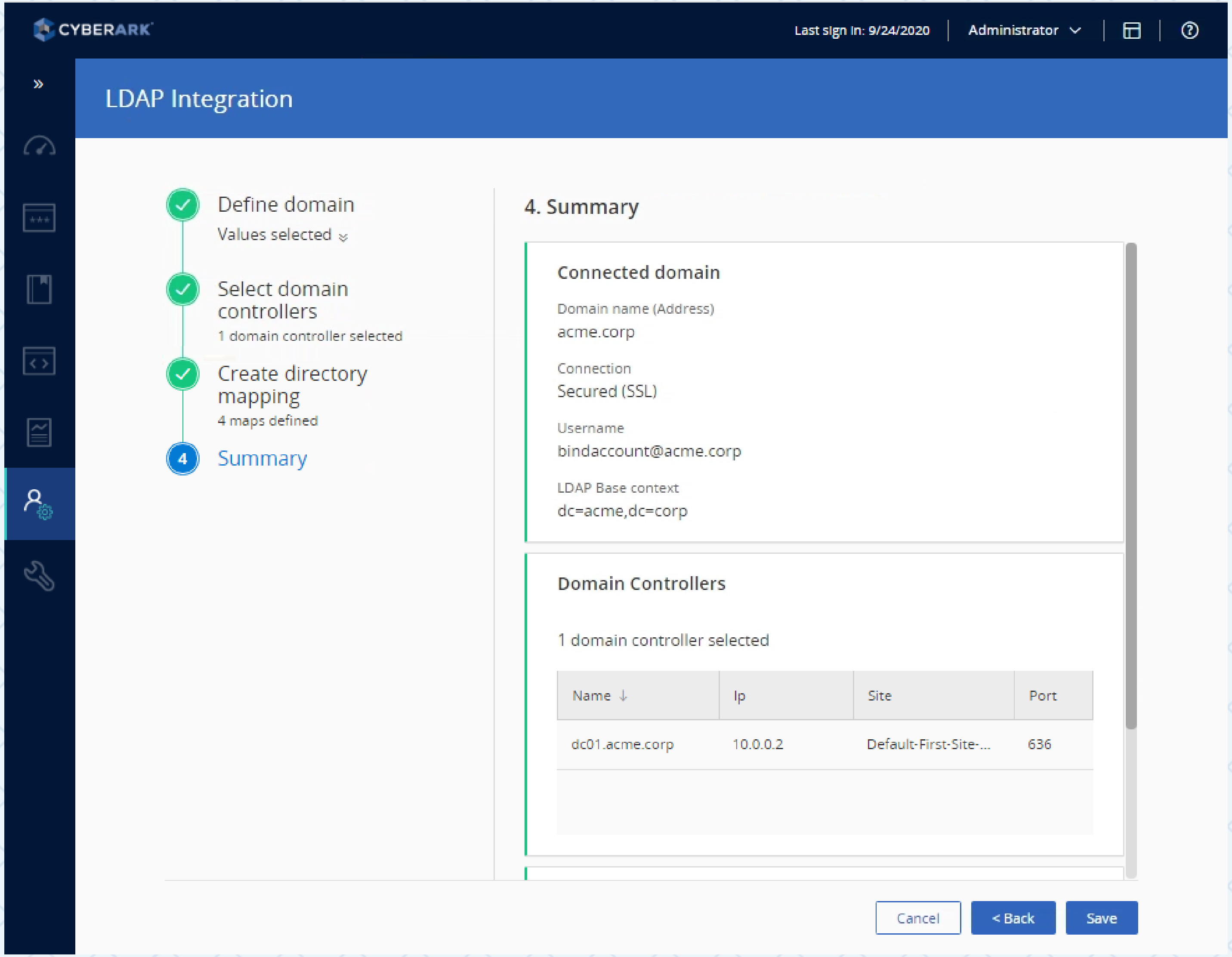
Authentication method
LDAP

Keep user activity logs for
7 days

Safe Managers | Define map

LDAP SETUP WIZARD - SUMMARY

- Review the summary of the LDAP Integration details
- Save the LDAP configuration and sign in to the PVWA as an LDAP user to confirm the integration



Define domain
Values selected

Select domain controllers
1 domain controller selected

Create directory mapping
4 maps defined

4 Summary

4. Summary

Connected domain

Domain name (Address)
acme.corp

Connection
Secured (SSL)

Username
bindaccount@acme.corp

LDAP Base context
dc=acme,dc=corp

Domain Controllers

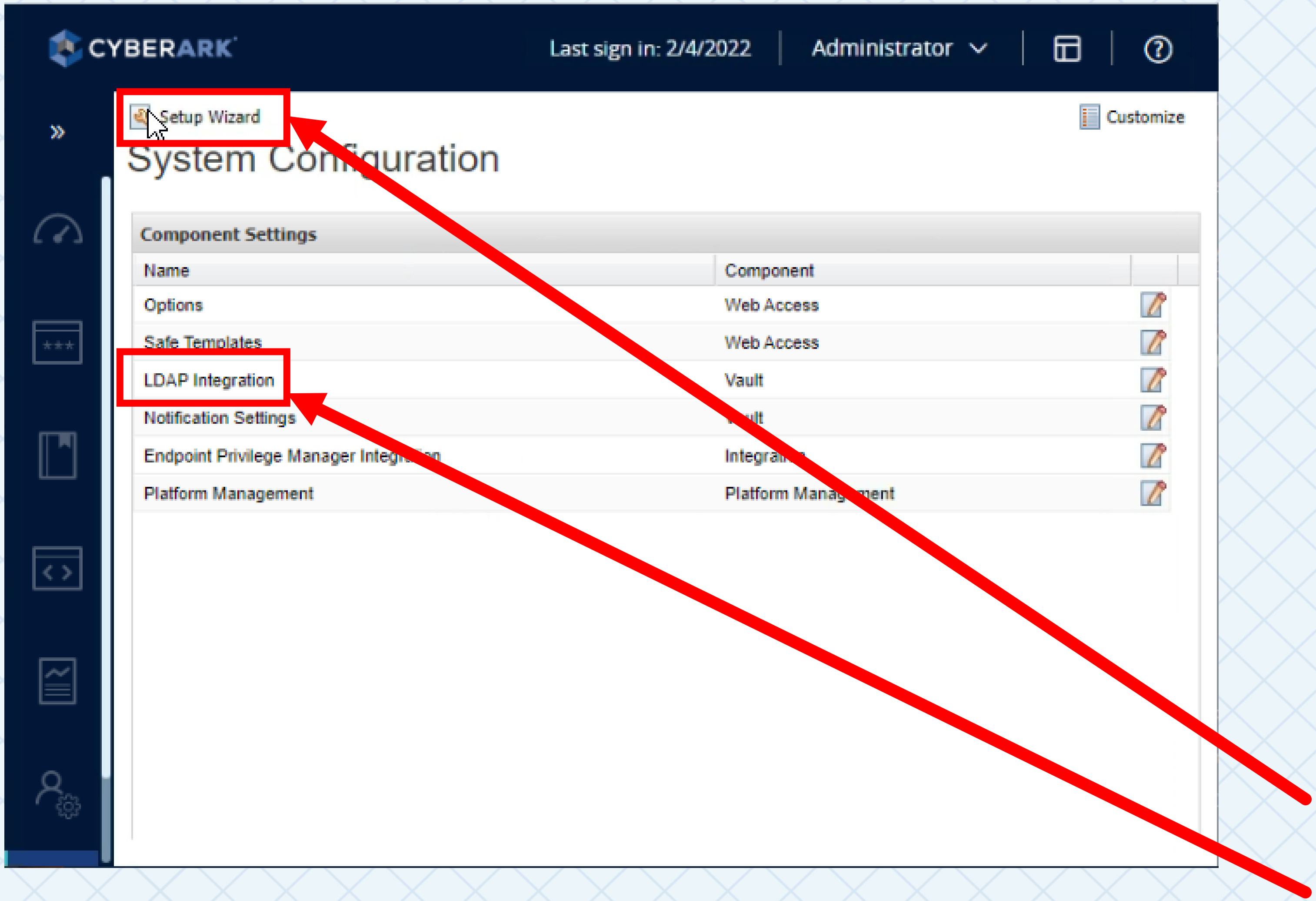
1 domain controller selected

Name ↓	Ip	Site	Port
dc01.acme.corp	10.0.0.2	Default-First-Site-...	636

LDAP SETUP WIZARD - CLASSIC

- The Classic LDAP Wizard can be used to configure the Global Catalog port (3268 and 3269) or any other custom ports required

- Customization can also be achieved via the LDAP Integration link



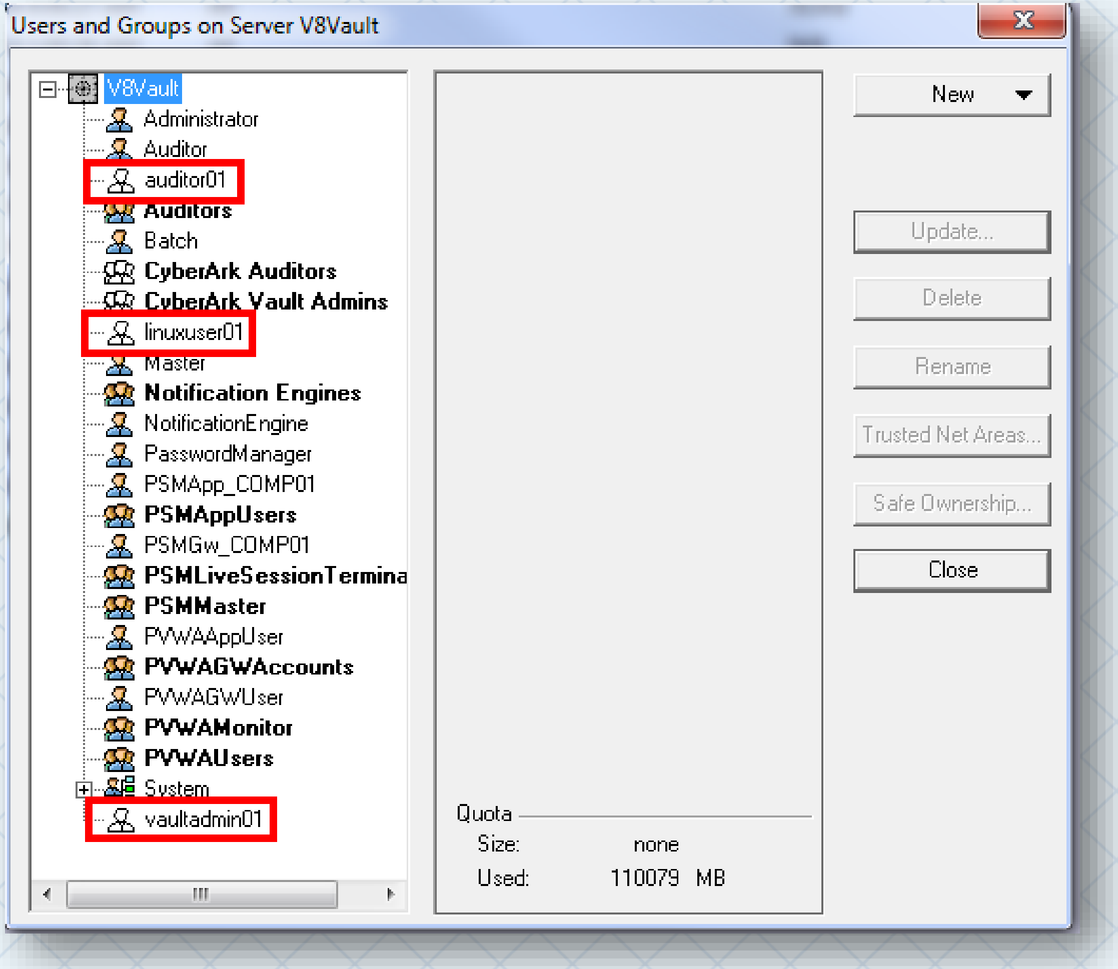
System Configuration

Component Settings

Name	Component
Options	Web Access
Safe Templates	Web Access
LDAP Integration	Vault
Notification Settings	Vault
Endpoint Privilege Manager Integration	Integration
Platform Management	Platform Management

TRANSPARENT PROVISIONING

- Using the PrivateArk Client, under **Users and Groups**. you will see the white icons are used to indicate which users are externally authenticated
- If you delete a user within CyberArk, it will be automatically re-created upon login if it still exists within AD and is still a member of one of the groups defined in a Directory Mapping
    - As long as permissions are assigned via groups, there is no real affect to the user
    - Assigning safe permissions to a specific individual, if deleted that user will lose their permissions to the safes where they were specifically assigned
- To permanently delete a user, it would have to be removed from all groups that have a directory mapping or deleted from the external directory



Size: none

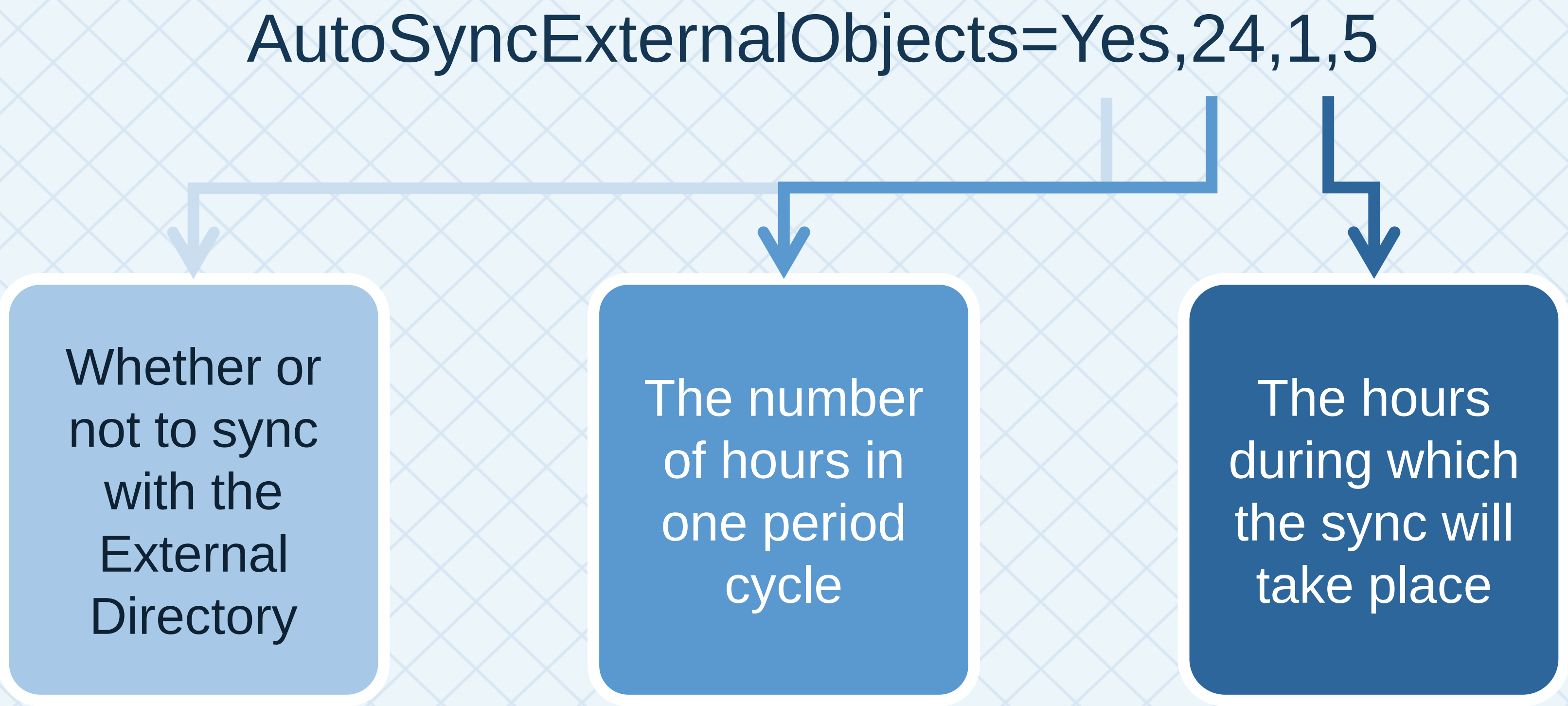
Used: 110079 MB

LDAP SYNCHRONIZATION

A process runs daily to synchronize transparent user attributes with the external directory

A user must be deleted from the external directory, or the user will not be removed from the Vault

In the DBParm.ini this parameter determines synchronization with the external directory.



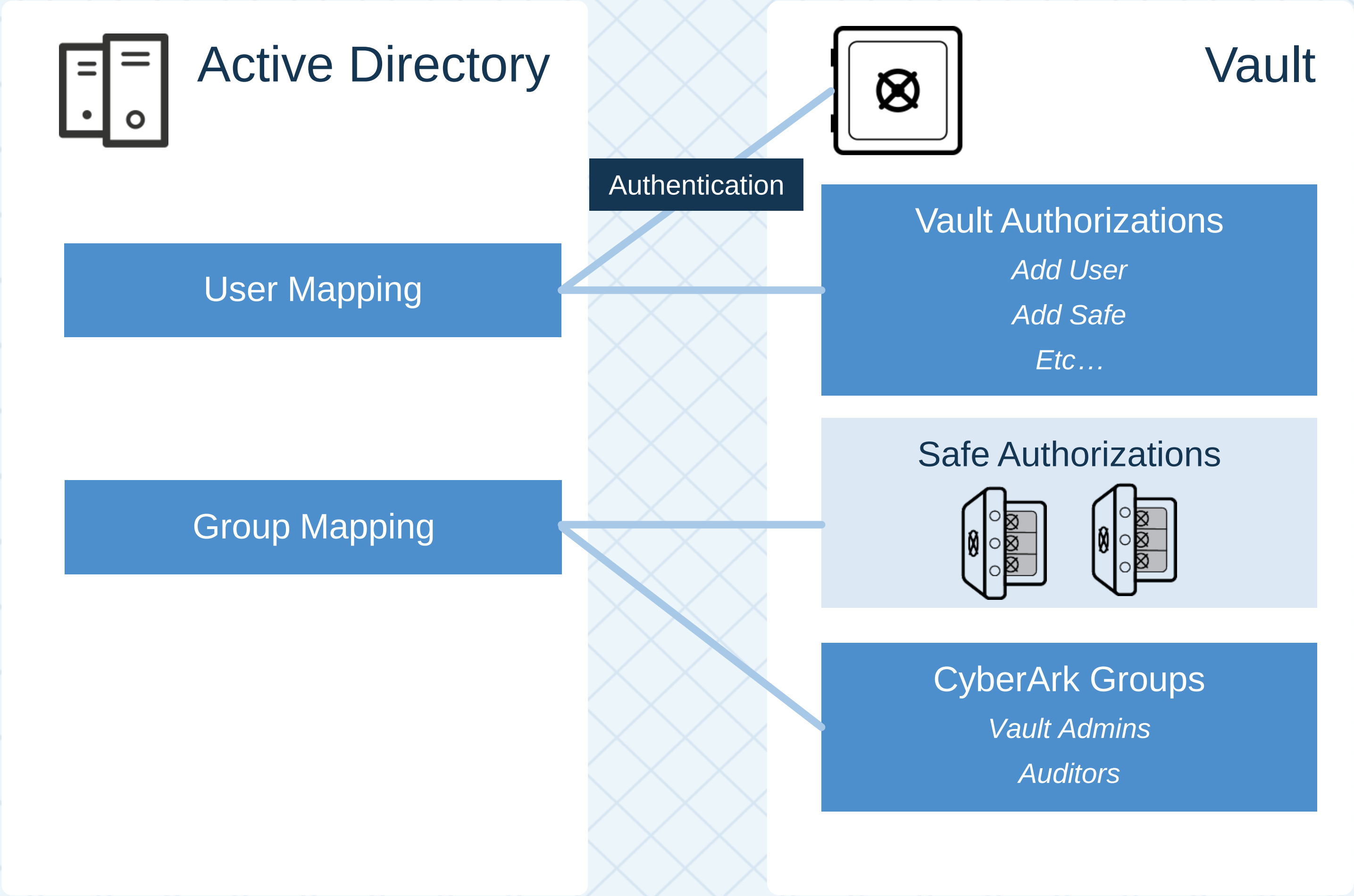
AutoSyncExternalObjects=Yes,24,1,5

Whether or not to sync with the External Directory
The number of hours in one period cycle
The hours during which the sync will take place

LDAP INTEGRATION
(DIRECTORY MAPPING)

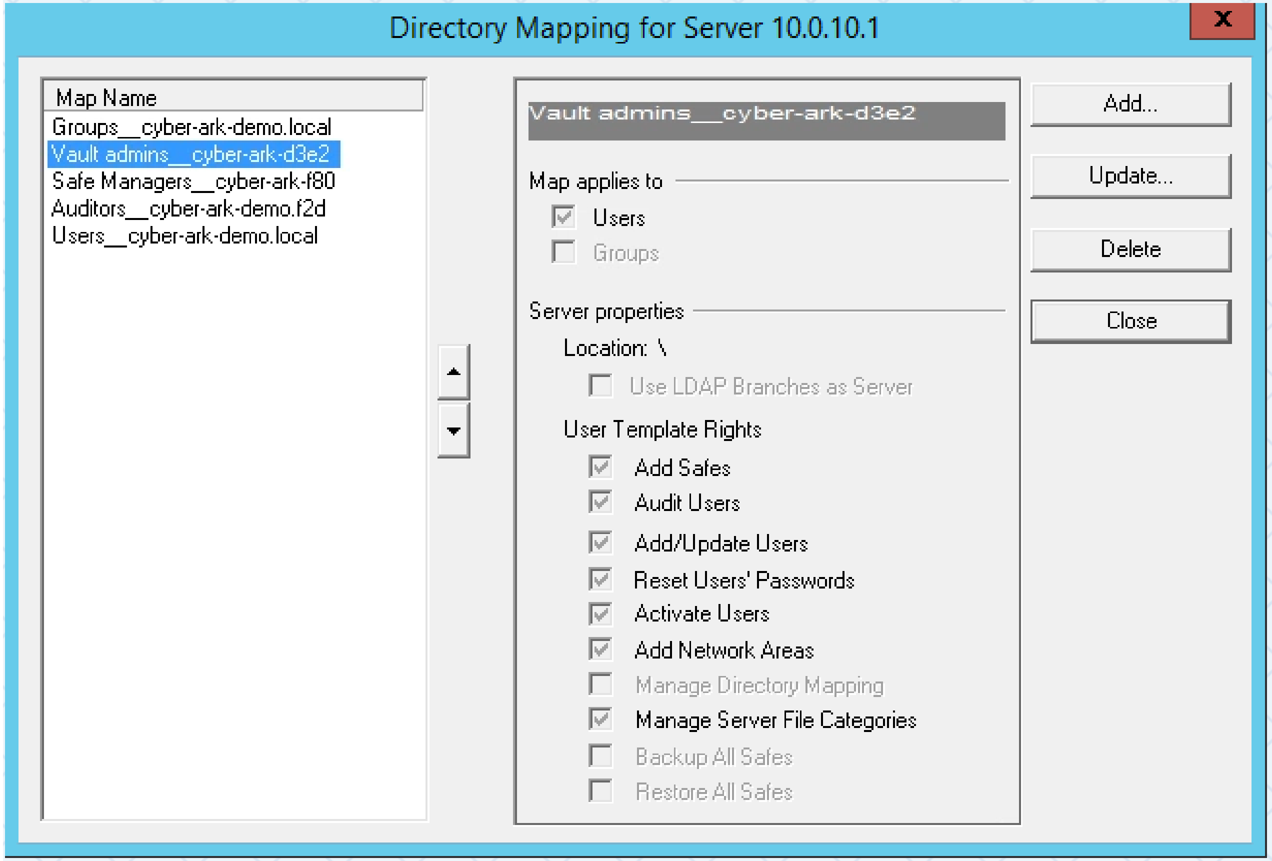
DIRECTORY MAPPING OVERVIEW

- **User Mapping** – allows for authentication and defines user's attributes, such as Vault Authorizations and Location
- **Group Mapping** – makes LDAP groups searchable from within CyberArk and allows mapped LDAP groups to be granted Safe authorizations based upon group membership.



DEFAULT DIRECTORY MAPPINGS

- Directory mappings are created by the LDAP Integration Wizard automatically assigning default Vault Authorizations with nested group settings for:
  - **Vault Users**
  - **Safe Managers**
  - **Vault Admins**
  - **Auditors**
- Custom roles can be defined by modifying existing Directory Maps or by creating new directory maps
- Only the built-in Administrator can edit the Directory Mappings.



Directory Mapping for Server 10.0.10.1

Map Name
Groups__cyber-ark-demo.local
Vault admins__cyber-ark-d3e2
Safe Managers__cyber-ark-f80
Auditors__cyber-ark-demo.f2d
Users__cyber-ark-demo.local

Vault admins__cyber-ark-d3e2

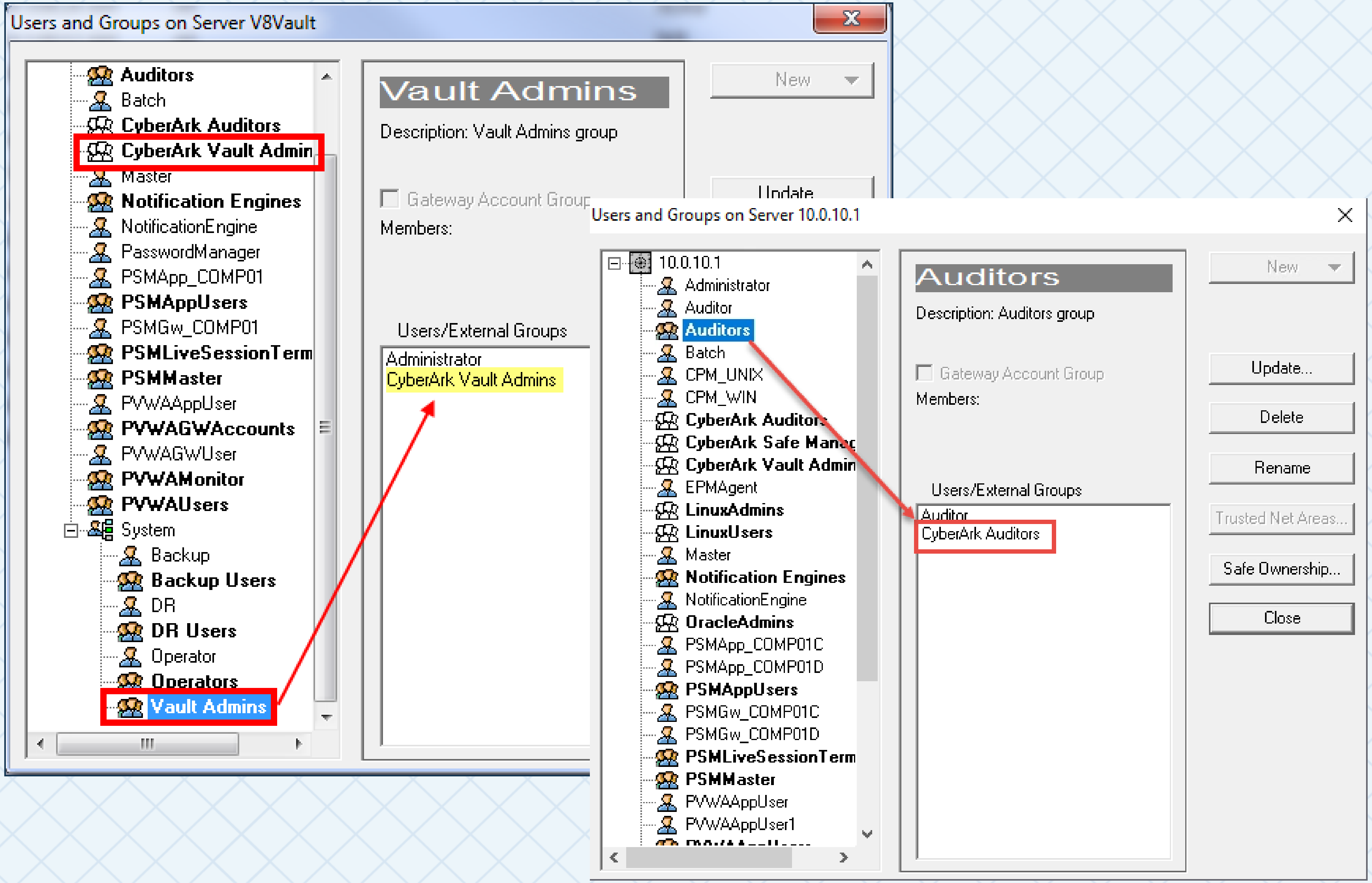
Map applies to
☑ Users
□ Groups

Server properties
Location: \
□ Use LDAP Branches as Server

User Template Rights
☑ Add Safes
☑ Audit Users
☑ Add/Update Users
☑ Reset Users' Passwords
☑ Activate Users
☑ Add Network Areas
□ Manage Directory Mapping
☑ Manage Server File Categories
□ Backup All Safes
□ Restore All Safes

USER MAPPING: NESTED GROUPS

- External groups are nested in internal groups to enable the display of necessary options in the PVWA
  - the external group ***CyberArk Vault Admins*** is added to the internal Vault Admins group
  - the external group ***CyberArk Auditors*** is added to the internal Vault Admins group



Users and Groups on Server V8Vault

Vault Admins

Description: Vault Admins group

□ Gateway Account Group

Members:

Users/External Groups

Administrator
CyberArk Vault Admins

Users and Groups on Server 10.0.10.1

Auditors

Description: Auditors group

□ Gateway Account Group

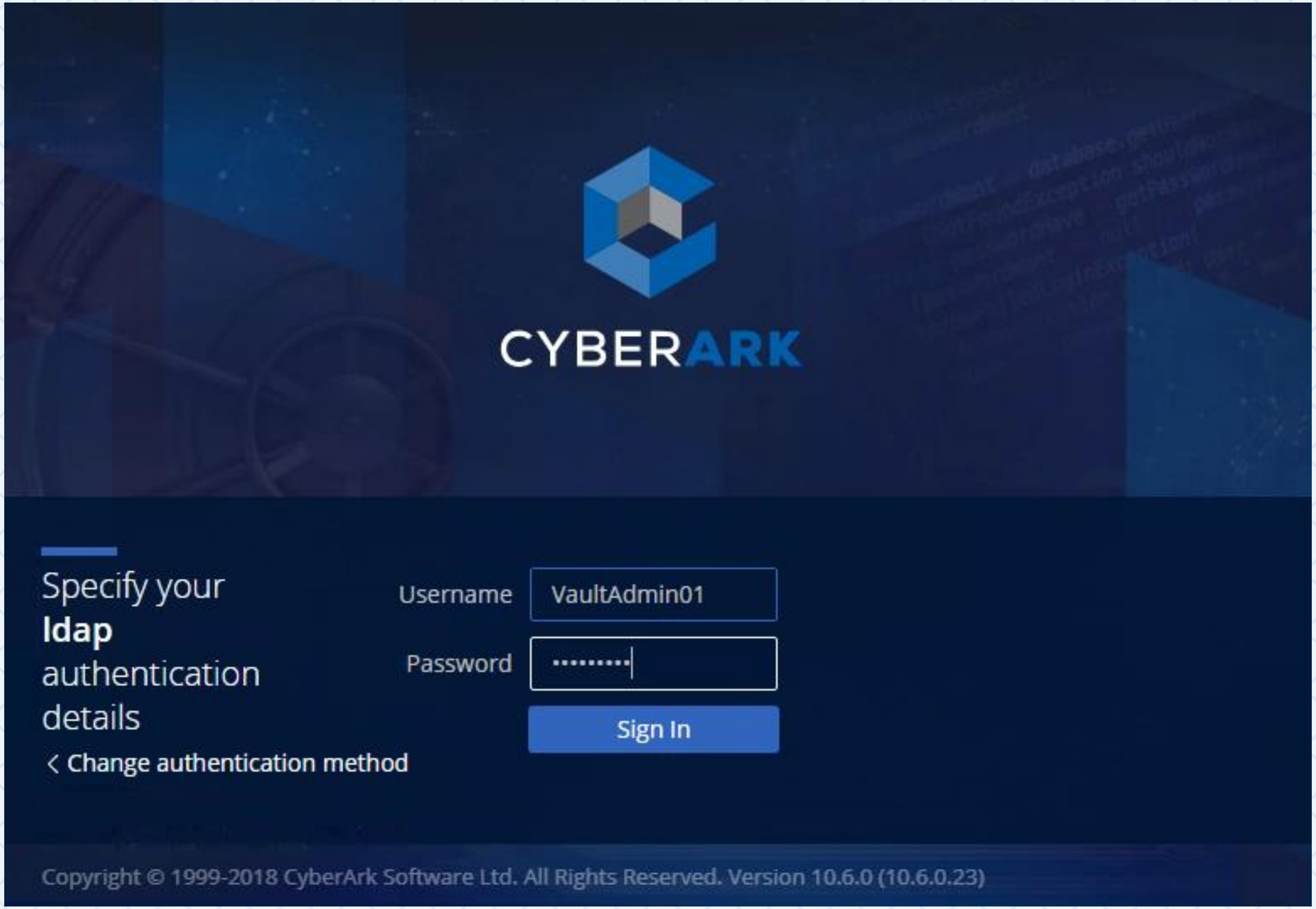
Members:

Users/External Groups

Auditor
CyberArk Auditors

USER MAPPING: VAULT ADMINS

- After completing the configuration using the Wizard:
  - the AD group *CyberArk Vault Admins* will be created in the Vault and nested under the internal Vault Admins group.
  - LDAP users who are members of *CyberArk Vault Admins* will be able to authenticate to CyberArk using LDAP authentication.



Specify your **ldap** authentication details

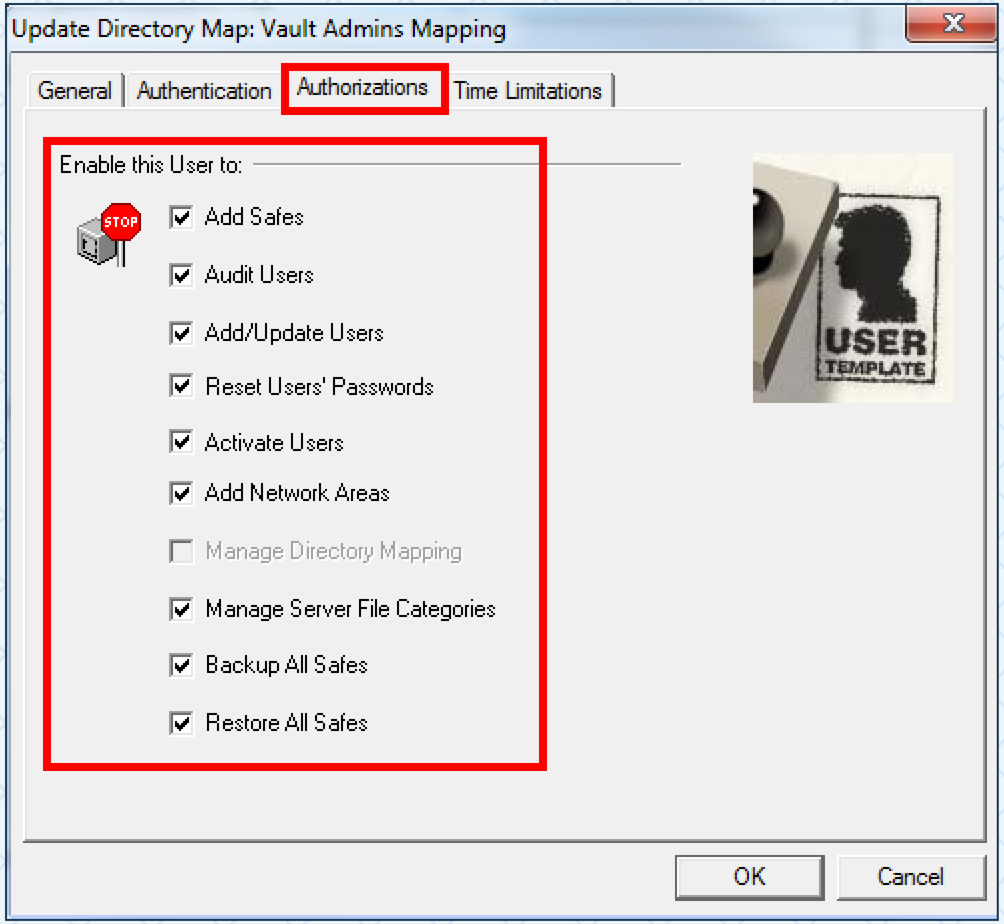
Username: VaultAdmin01

Password: •••••••••

Copyright © 1999-2018 CyberArk Software Ltd. All Rights Reserved. Version 10.6.0 (10.6.0.23)

USER MAPPING: VAULT ADMINS

- After completing the configuration using the Wizard:
  - the AD group *CyberArk Vault Admins* will be created in the Vault and nested under the internal Vault Admins group.
  - LDAP users who are members of *CyberArk Vault Admins* will be able to authenticate to CyberArk using LDAP authentication.
  - LDAP users who are members of *CyberArk Vault Admins* will receive all Vault authorizations based on the User Template in the directory mapping.



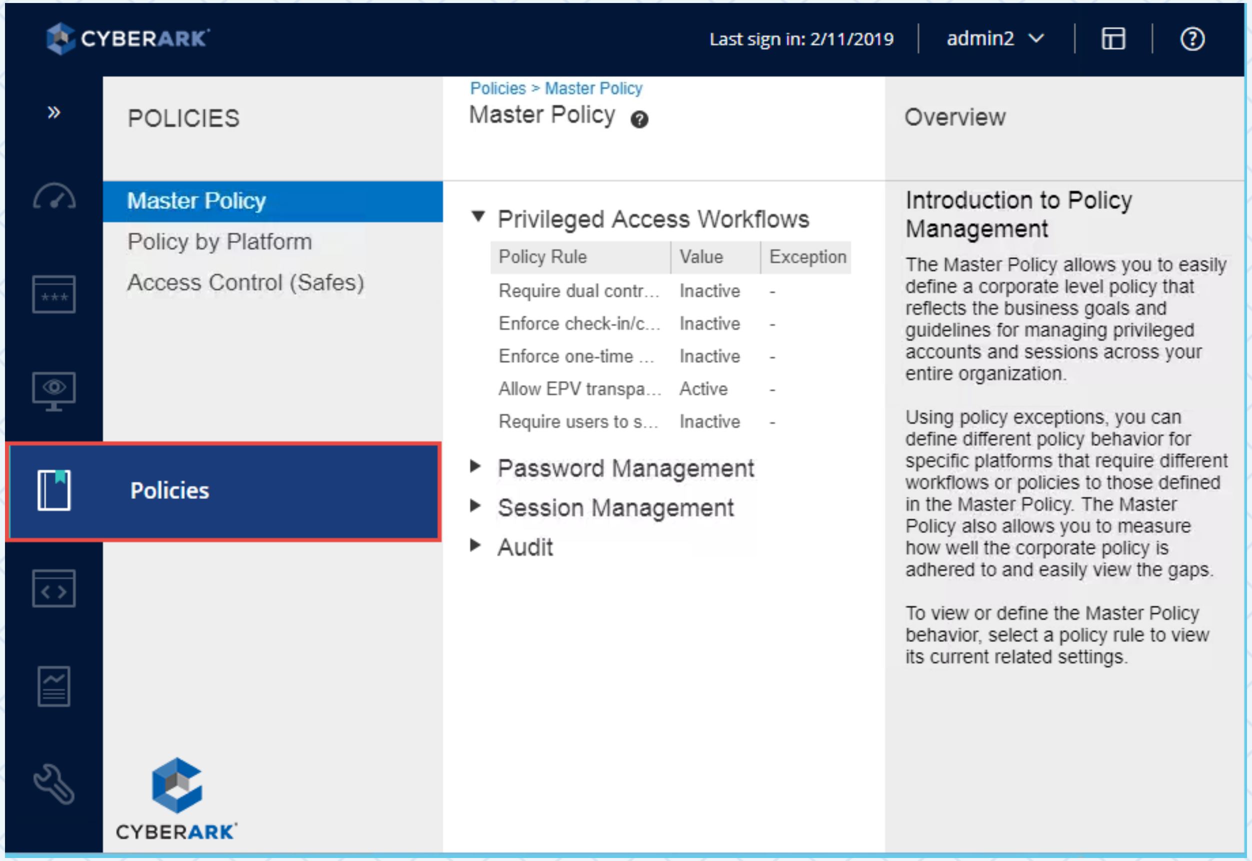
Update Directory Map: Vault Admins Mapping

Enable this User to:

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

USER MAPPING: VAULT ADMINS (4)

- After completing the configuration using the Wizard LDAP users who are members of *CyberArk Vault Admins* will be able to:
  - authenticate to CyberArk using LDAP authentication
  - receive all Vault authorizations based on the User Template in the directory mapping
  - View Policies, Administration, System Configuration, Platform Management and other options



▼ Privileged Access Workflows

Policy Rule	Value	Exception
Require dual contr...	Inactive	-
Enforce check-in/c...	Inactive	-
Enforce one-time ...	Inactive	-
Allow EPV transpa...	Active	-
Require users to s...	Inactive	-

▶ Password Management

▶ Session Management

▶ Audit

Introduction to Policy Management

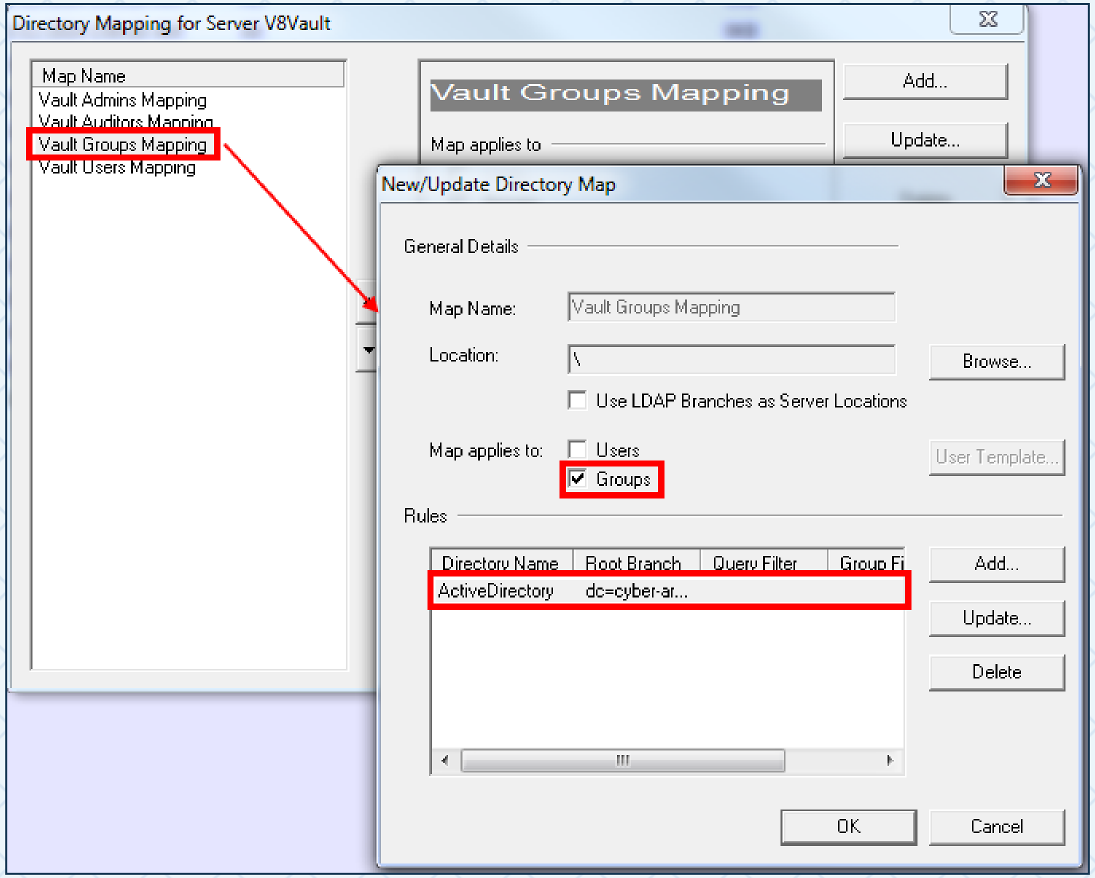
The Master Policy allows you to easily define a corporate level policy that reflects the business goals and guidelines for managing privileged accounts and sessions across your entire organization.

Using policy exceptions, you can define different policy behavior for specific platforms that require different workflows or policies to those defined in the Master Policy. The Master Policy also allows you to measure how well the corporate policy is adhered to and easily view the gaps.

To view or define the Master Policy behavior, select a policy rule to view its current related settings.

ADDING A FILTER TO A GROUP MAPPING

- Update the rule to add a filter to the Groups Mapping Allows you to restrict which LDAP groups can be listed when adding groups to Safe permissions
- It is recommended to restrict the search to groups that should be used for CyberArk Safe permissions
- Exclude the groups used for Vault Authorizations, i.e., CyberArk Vault Admins, CyberArk Vault Auditors, CyberArk Vault Users



Directory Mapping for Server V8Vault

Map Name
Vault Admins Mapping
Vault Auditors Mapping
Vault Groups Mapping
Vault Users Mapping

Vault Groups Mapping

Map applies to

New/Update Directory Map

General Details

Map Name: Vault Groups Mapping

Location: \

☐ Use LDAP Branches as Server Locations

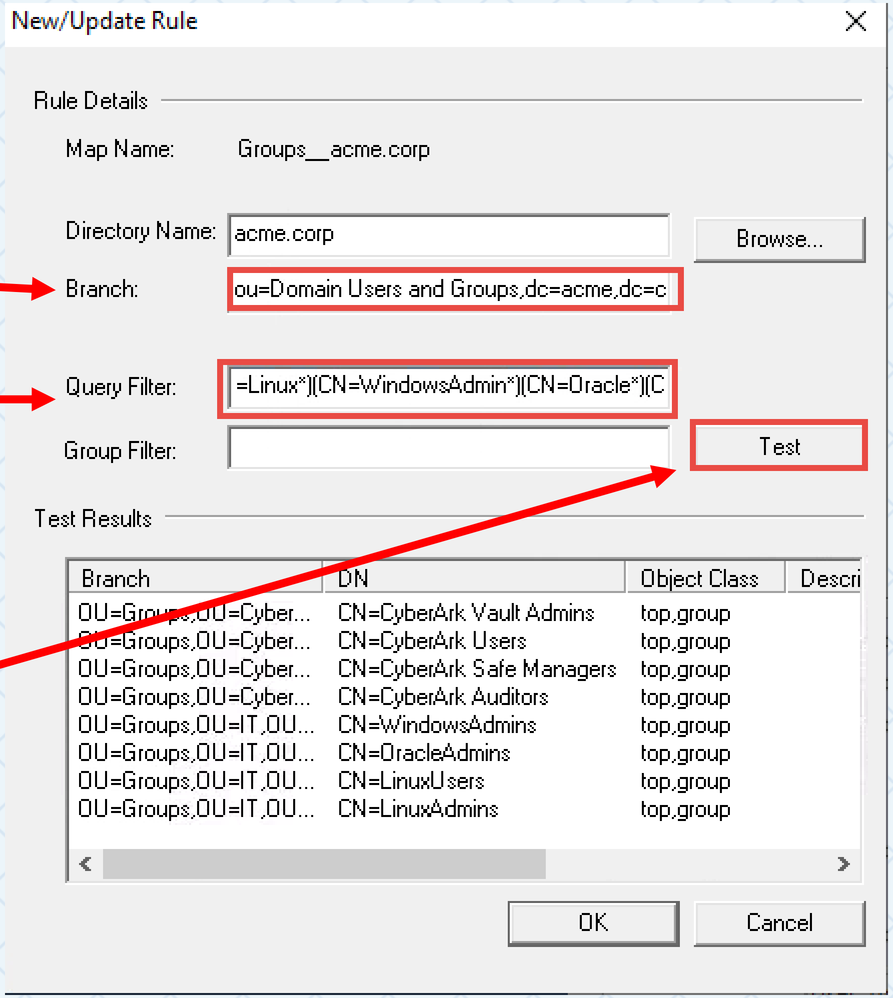
Map applies to: ☐ Users ☑ Groups

Rules

Directory Name	Root Branch	Query Filter	Group Fi
ActiveDirectory	dc=cyber-ar...		

CONFIGURING GROUP MAPPING FILTERS

- The Branch parameter restricts where in the LDAP directory the query will be executed
- The Query Filter shown will restrict the search of the external directory when adding members to a safe, to only the groups listed
- Selecting the “Test” button will execute the query and display the results



Rule Details

Map Name: Groups__acme.corp

Directory Name: acme.corp

Branch: ou=Domain Users and Groups,dc=acme,dc=c

Query Filter: =Linux*)(CN=WindowsAdmin*)(CN=Oracle*)(C

Group Filter:

Test Results

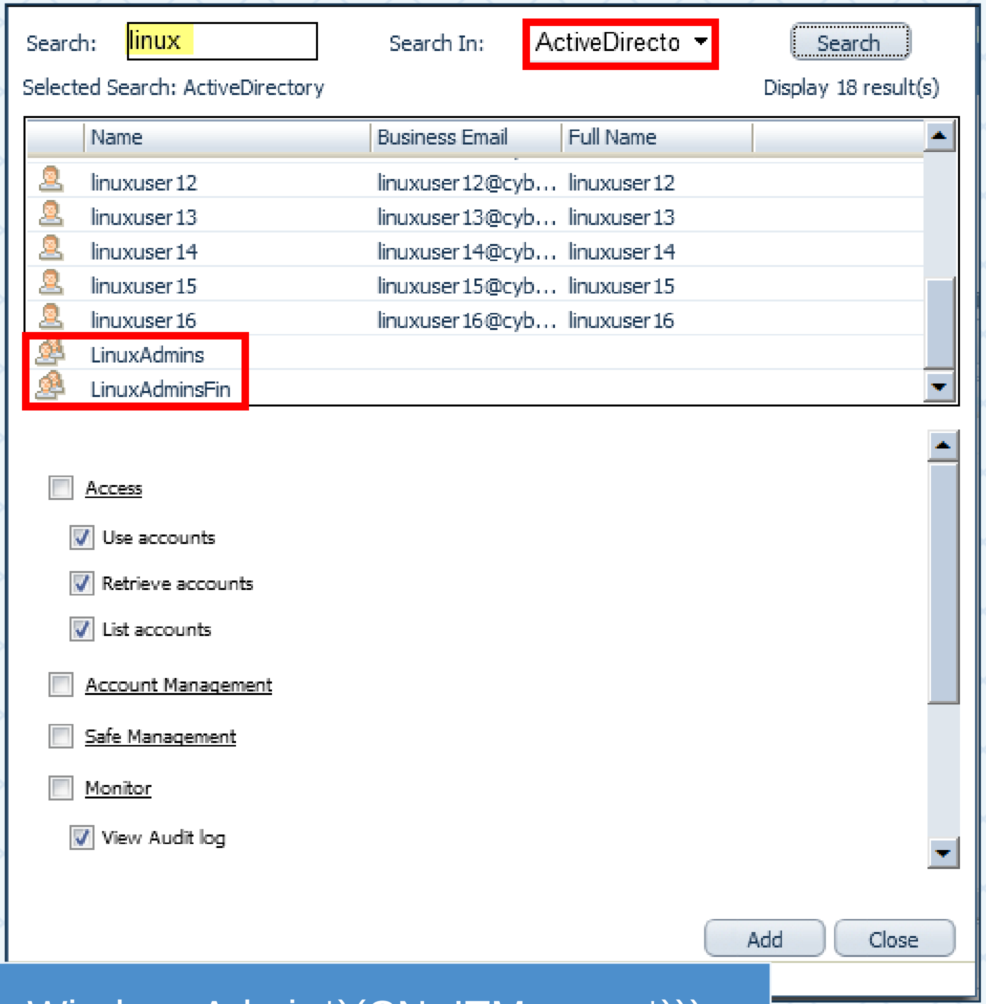
Branch	DN	Object Class	Descri
OU=Groups,OU=Cyber...	CN=CyberArk Vault Admins	top,group	
OU=Groups,OU=Cyber...	CN=CyberArk Users	top,group	
OU=Groups,OU=Cyber...	CN=CyberArk Safe Managers	top,group	
OU=Groups,OU=Cyber...	CN=CyberArk Auditors	top,group	
OU=Groups,OU=IT,OU...	CN=WindowsAdmins	top,group	
OU=Groups,OU=IT,OU...	CN=OracleAdmins	top,group	
OU=Groups,OU=IT,OU...	CN=LinuxUsers	top,group	
OU=Groups,OU=IT,OU...	CN=LinuxAdmins	top,group	

(&(objectClass=group)(|(CN=Cyber*)(CN=Linux*)(CN=Oracle*)(CN=WindowsAdmin*)(CN=ITManage*)))

CONFIGURING GROUP MAPPING FILTERS

- The Query Filter shown will restrict the search in the external directory when adding members to a safe

- When searching for external LDAP groups, only groups that are allowed by the query can be listed and added as members



Search: linux   Search In: ActiveDirecto

Selected Search: ActiveDirectory   Display 18 result(s)

Name	Business Email	Full Name
linuxuser12	linuxuser12@cyb…	linuxuser12
linuxuser13	linuxuser13@cyb…	linuxuser13
linuxuser14	linuxuser14@cyb…	linuxuser14
linuxuser15	linuxuser15@cyb…	linuxuser15
linuxuser16	linuxuser16@cyb…	linuxuser16
LinuxAdmins		
LinuxAdminsFin		

□ Access

- ☑ Use accounts
- ☑ Retrieve accounts
- ☑ List accounts

□ Account Management

□ Safe Management

□ Monitor

- ☑ View Audit log

(&(objectClass=group)(|(CN=Cyber*)(CN=Linux*)(CN=Oracle*)(CN=WindowsAdmin*)(CN=ITManage*)))

SMTP INTEGRATION

SMTP INTEGRATION

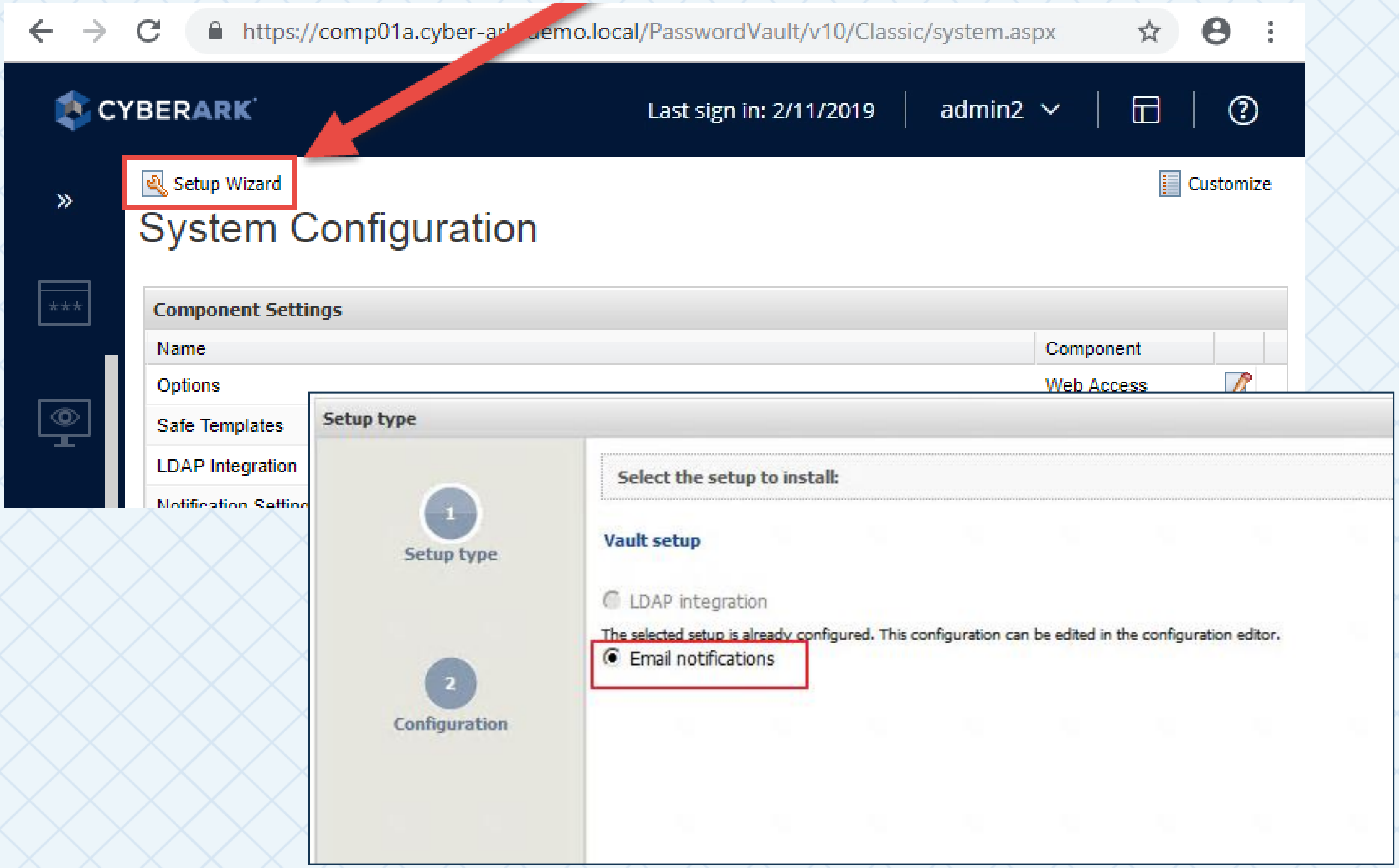
Email integration is critical for vault activity alerts and notifications and to facilitate workflow processes.

Prerequisites:

- Have the IP address of the SMTP Gateway Available.
- Ensure that any necessary firewall rules or ACLs allow communications from the Vault Servers to the SMTP Gateway.

SETUP WIZARD

- SMTP setup is configured via the Setup Wizard



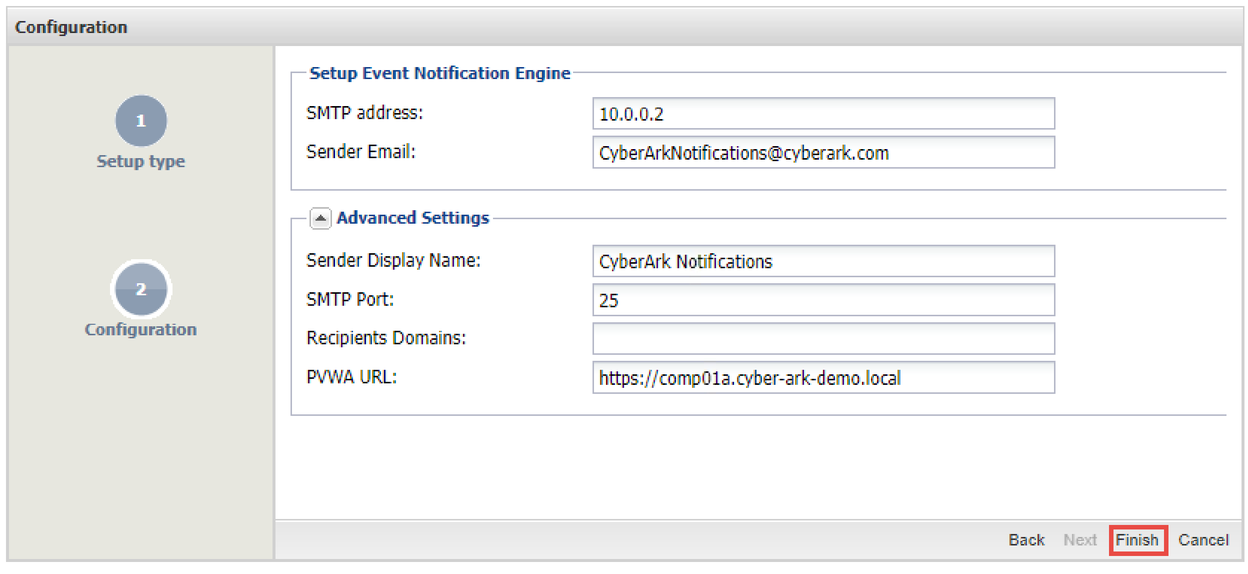
○ LDAP integration

The selected setup is already configured. This configuration can be edited in the configuration editor.

● Email notifications

SMTP SETTINGS

- **SMTP address** – The IP address of the SMTP server. You can specify multiple IP addresses for high availability implementations. Separate multiple IP addresses with commas.
- **Sender Email** – The mail address that will appear as the notification sender.
- **Sender Display Name** – The name that will appear as the sender’s name.
- **SMTP Port** – The port through which the ENE will send notifications.
- **Recipients Domain** – The name of the domain where the recipient’s email account exists.
- **PVWA URL** – The URL of the machine where the PVWA is installed (e.g. https://www.myserver.com)



Configuration

Setup Event Notification Engine

SMTP address: 10.0.0.2

Sender Email: CyberArkNotifications@cyberark.com

Advanced Settings

Sender Display Name: CyberArk Notifications

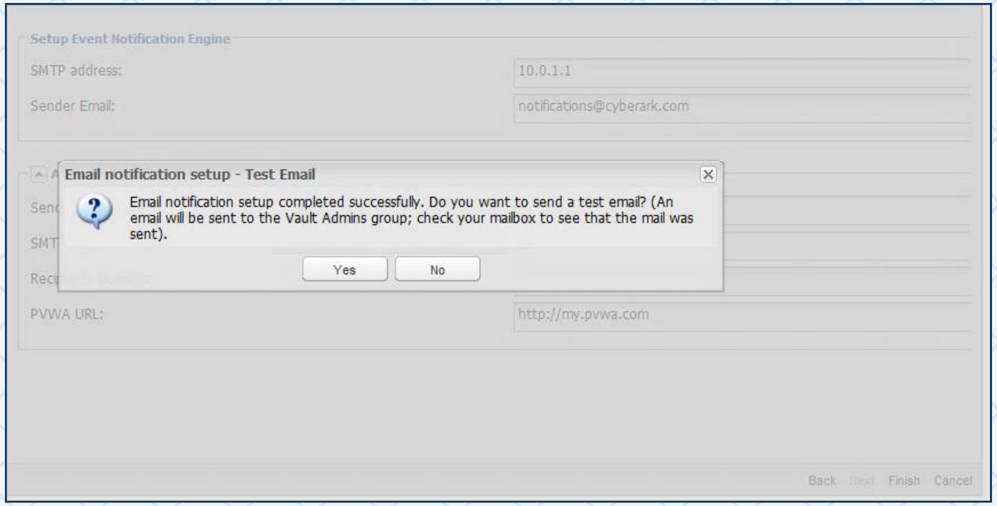
SMTP Port: 25

Recipients Domains:

PVWA URL: https://comp01a.cyber-ark-demo.local

CONFIRMATION EMAIL

- Once you click on Finish the initial ENE configuration is saved and the Email notification setup message appears.
- Click Yes to send a test email to the members of the Vault Admins group.



Setup Event Notification Engine

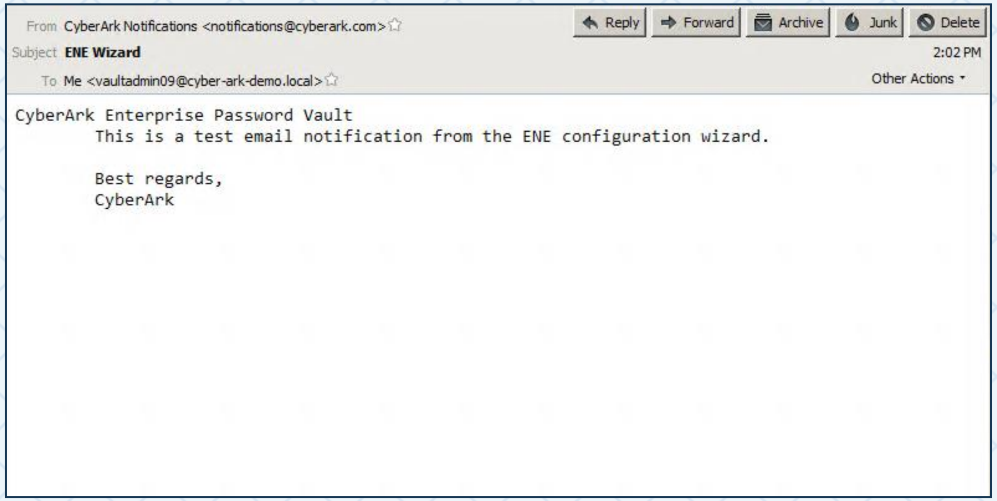
SMTP address: 10.0.1.1

Sender Email: notifications@cyberark.com

Email notification setup - Test Email

Email notification setup completed successfully. Do you want to send a test email? (An email will be sent to the Vault Admins group; check your mailbox to see that the mail was sent).

PVWA URL: http://my.pvwa.com



From CyberArk Notifications <notifications@cyberark.com>

Subject **ENE Wizard**

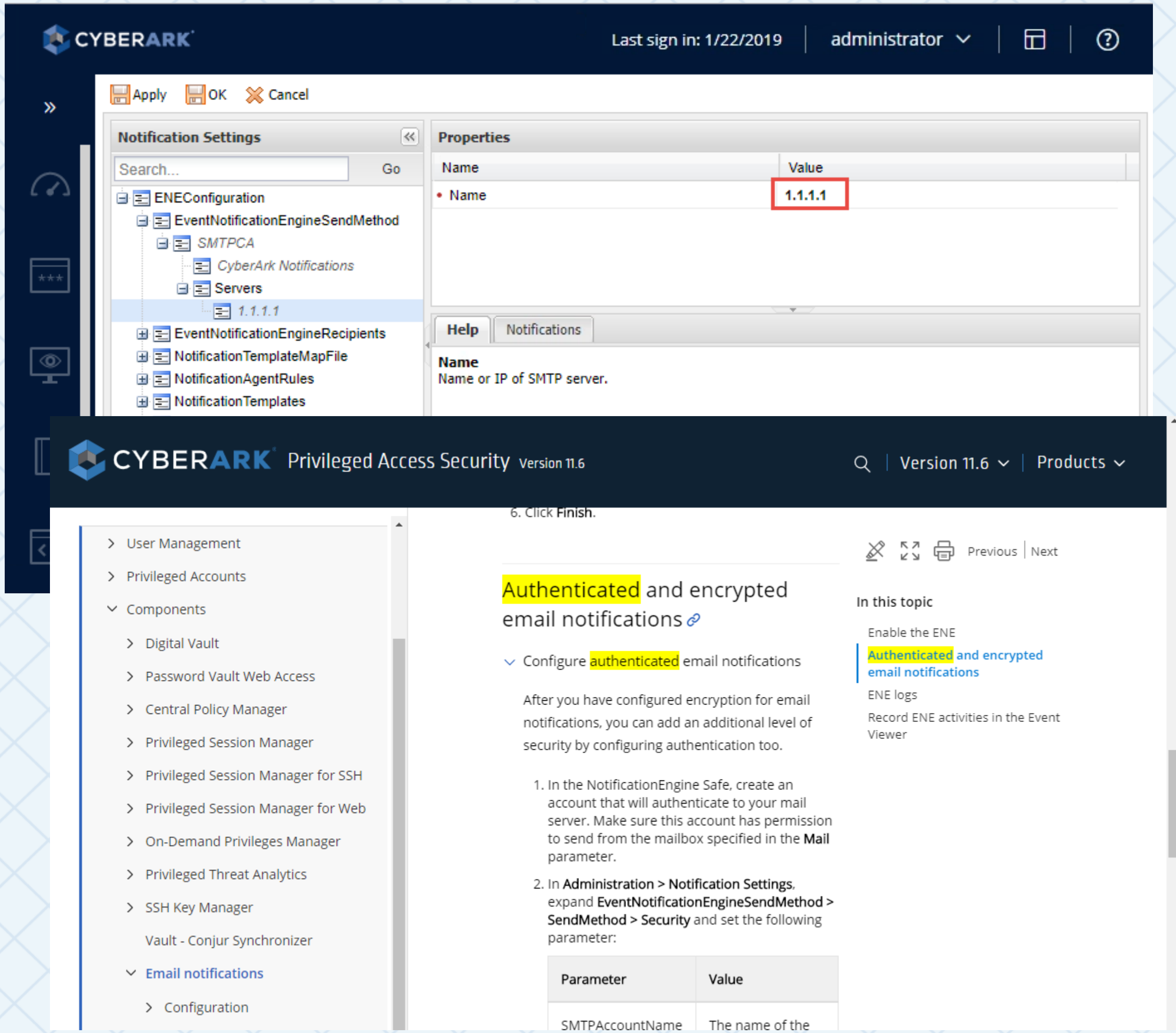
To Me <vaultadmin09@cyber-ark-demo.local>

2:02 PM

```
CyberArk Enterprise Password Vault
        This is a test email notification from the ENE configuration wizard.

        Best regards,
        CyberArk
```

RUN WIZARD AGAIN

- After the ENE has been configured using the wizard, the ENE setup wizard will be disabled
- To enable the ENE setup wizard set the SMTP address to 1.1.1.1 in System Configuration > Notification Settings
- CyberArk's Digital Vault supports authenticated and encrypted email notifications
  - For more information, search CyberArk online documentation for "Authenticated and encrypted email notifications"



CYBERARK
Last sign in: 1/22/2019
administrator
Apply
OK
Cancel
Notification Settings
Search...
Go
ENEConfiguration
EventNotificationEngineSendMethod
SMTPCA
CyberArk Notifications
Servers
1.1.1.1
EventNotificationEngineRecipients
NotificationTemplateMapFile
NotificationAgentRules
NotificationTemplates
Properties
Help
Notifications
CYBERARK Privileged Access Security Version 11.6
Version 11.6
Products
User Management
Privileged Accounts
Components
Digital Vault
Password Vault Web Access
Central Policy Manager
Privileged Session Manager
Privileged Session Manager for SSH
Privileged Session Manager for Web
On-Demand Privileges Manager
Privileged Threat Analytics
SSH Key Manager
Vault - Conjur Synchronizer
Email notifications
Configuration
Previous
Next
In this topic
Enable the ENE
Authenticated and encrypted email notifications
ENE logs
Record ENE activities in the Event Viewer

Name	Value
Name	1.1.1.1

Name
Name or IP of SMTP server.

6. Click **Finish**.

Authenticated and encrypted email notifications

Configure authenticated email notifications

After you have configured encryption for email notifications, you can add an additional level of security by configuring authentication too.

1. In the NotificationEngine Safe, create an account that will authenticate to your mail server. Make sure this account has permission to send from the mailbox specified in the **Mail** parameter.
2. In **Administration > Notification Settings**, expand **EventNotificationEngineSendMethod > SendMethod > Security** and set the following parameter:

Parameter	Value
SMTPAccountName	The name of the

SNMP INTEGRATION

(OR, HOW TO CONFIGURE REMOTE MONITORING)

PURPOSE

- Remote Monitoring relies upon SNMP to send Vault traps to a remote terminal. This enables users to receive both Operating System and Vault Server information.

Operating System information:	• CPU, memory, and disk usage • Event log notifications • Service status
Component-specific information:	• Password Vault and DR Vault status • Password Vault and DR Vault logs

CONFIGURE SNMP INTEGRATION

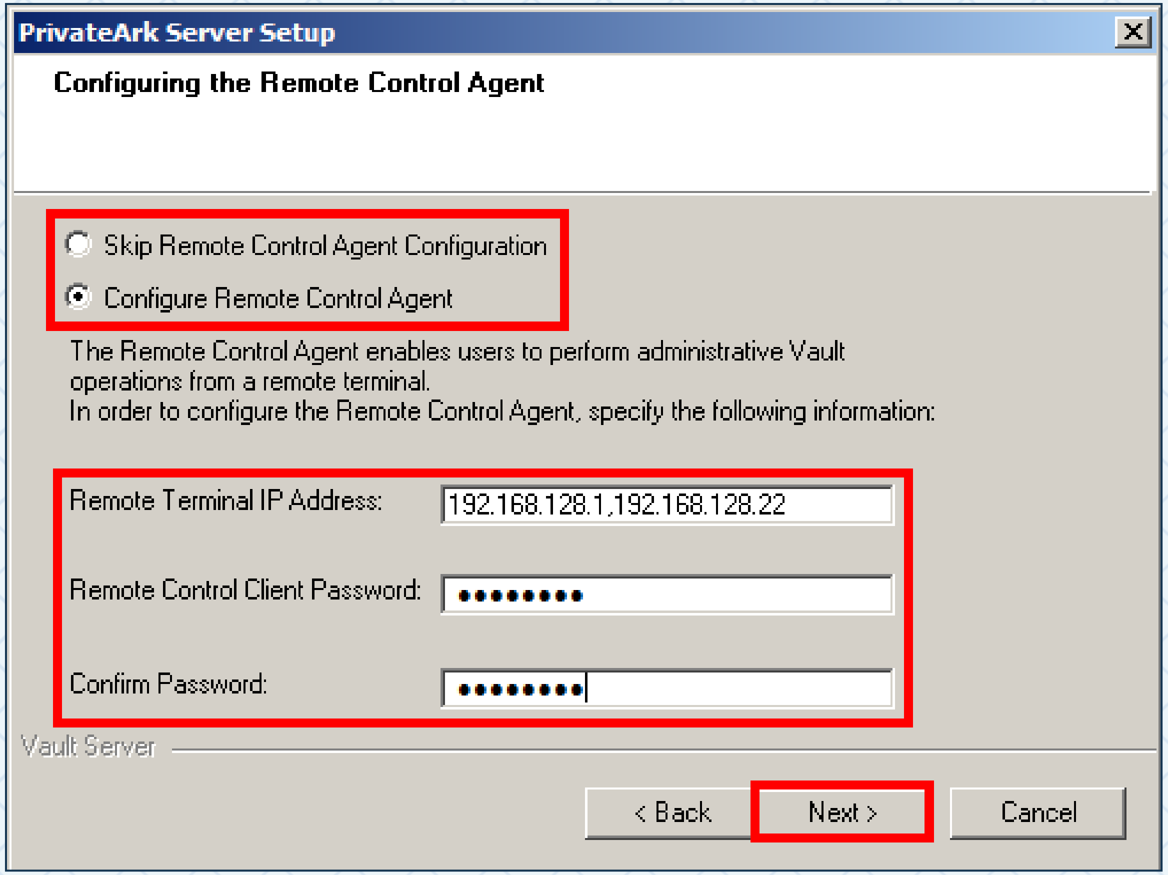
CyberArk discourages installing any third-party monitoring agents. The Digital Vault can send status information to your monitoring solution using SNMP.

Prerequisites:

- Have IP Addresses of all servers that can accept SNMP traps available
- Have Community String available
- Provide the Management Information Base (MIB) files to the SNMP administrator for loading into the management console. MIB files are included with the Digital Vault software
- Have a resource from the team responsible for SNMP monitoring

CONFIGURE REMOTE CONTROL AGENT

- SNMP is enabled by configuring the Remote-Control Agent during the initial vault server installation
- If the Remote-Control Agent is not configured during initial vault installation, it can be configured post installation
- See “To Configure Remote Monitoring” docs.cyberark.com for step by step instructions.



Configuring the Remote Control Agent

○ Skip Remote Control Agent Configuration

● Configure Remote Control Agent

The Remote Control Agent enables users to perform administrative Vault operations from a remote terminal.
In order to configure the Remote Control Agent, specify the following information:

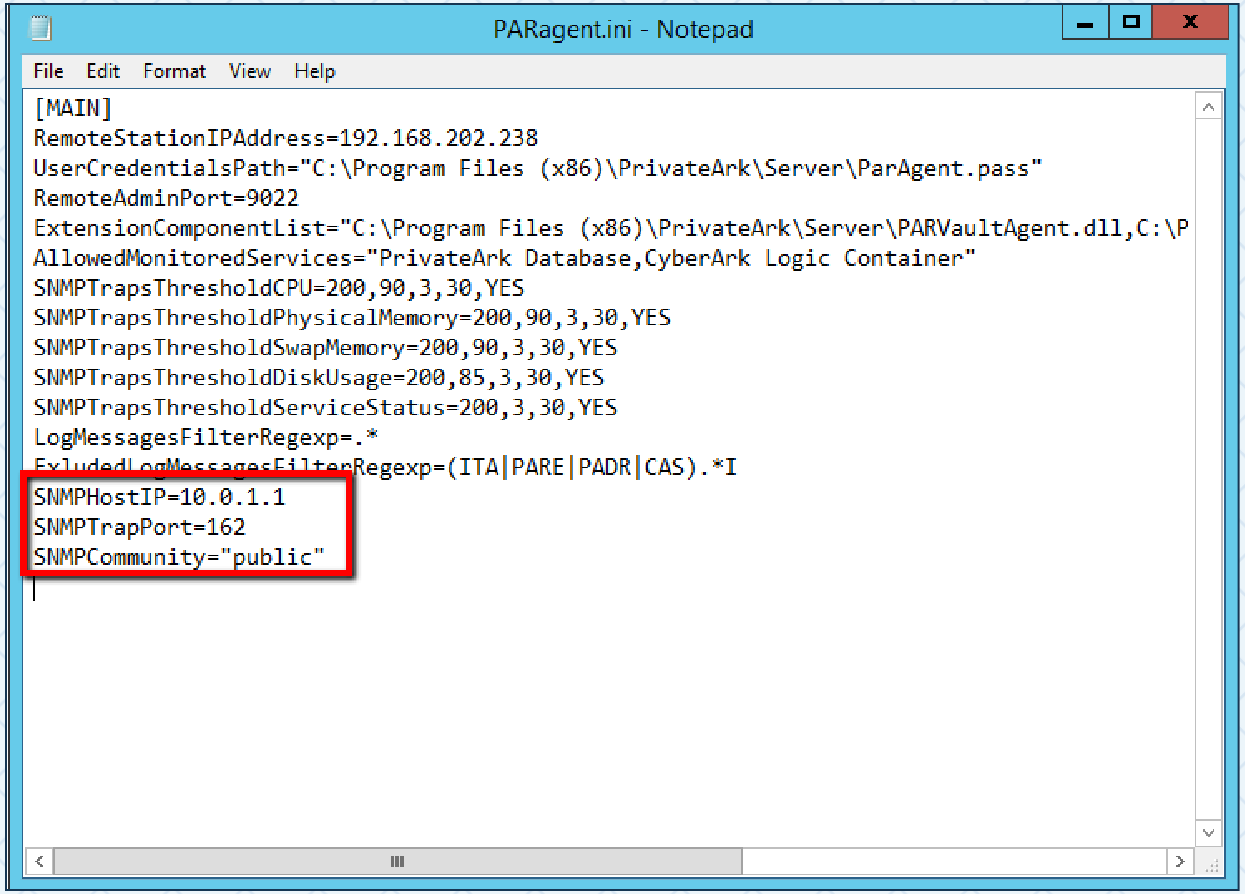
Remote Terminal IP Address: 192.168.128.1,192.168.128.22

Remote Control Client Password: ••••••••••

Confirm Password: ••••••••••

SNMP CONFIGURATION

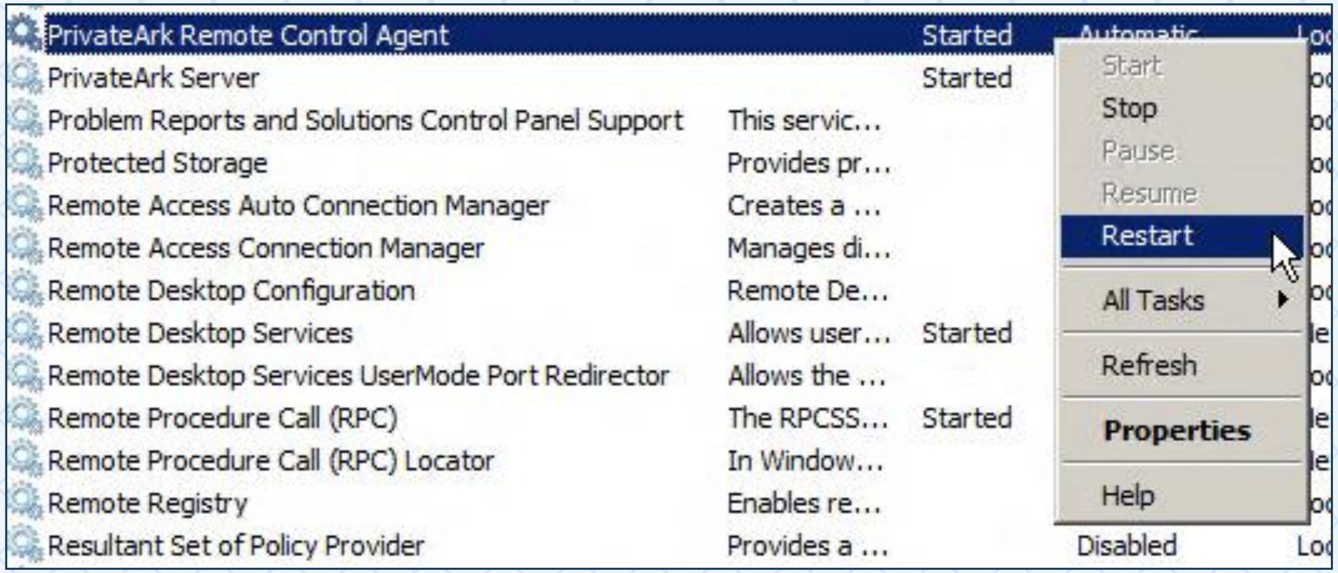
- Configure paragent.ini with the following information:
  - **SNMPHostIP** – The IP address of the remote computer where SNMP traps will be sent.
  - **SNMPTrapPort** – The port through which SNMP traps will be sent to the remote computer.
  - **SNMPCommunity** – The name of location where the SNMP traps originated.



```
[MAIN]
RemoteStationIPAddress=192.168.202.238
UserCredentialsPath="C:\Program Files (x86)\PrivateArk\Server\ParAgent.pass"
RemoteAdminPort=9022
ExtensionComponentList="C:\Program Files (x86)\PrivateArk\Server\PARVaultAgent.dll,C:\P
AllowedMonitoredServices="PrivateArk Database,CyberArk Logic Container"
SNMPTrapsThresholdCPU=200,90,3,30,YES
SNMPTrapsThresholdPhysicalMemory=200,90,3,30,YES
SNMPTrapsThresholdSwapMemory=200,90,3,30,YES
SNMPTrapsThresholdDiskUsage=200,85,3,30,YES
SNMPTrapsThresholdServiceStatus=200,3,30,YES
LogMessagesFilterRegexp=.*
ExludedLogMessagesFilterRegexp=(ITA|PARE|PADR|CAS).*I
SNMPHostIP=10.0.1.1
SNMPTrapPort=162
SNMPCommunity="public"
```

SNMP CONFIGURATION

- Restart the PrivateArk Remote Control Agent service to read the changes made into memory.
- Check with the administrator of the SNMP console to ensure that the SNMP messages sent are being received and are readable.



PrivateArk Remote Control Agent		Started	Automatic	Loc
PrivateArk Server		Started		
Problem Reports and Solutions Control Panel Support	This servic…			
Protected Storage	Provides pr…			
Remote Access Auto Connection Manager	Creates a …			
Remote Access Connection Manager	Manages di…			
Remote Desktop Configuration	Remote De…			
Remote Desktop Services	Allows user…	Started		
Remote Desktop Services UserMode Port Redirector	Allows the …			
Remote Procedure Call (RPC)	The RPCSS…	Started		
Remote Procedure Call (RPC) Locator	In Window…			
Remote Registry	Enables re…			
Resultant Set of Policy Provider	Provides a …		Disabled	Loc

SIEM INTEGRATION

SIEM INTEGRATION

SIEM Integration is a powerful way to correlate Privileged Account Usage with Privileged Account Activity.

- IP addresses of all servers that can accept SYSLOG messages
- The Vault uses any of the following protocols to send messages:
  - TLS, TCP or UDP
  - Configuring the Vault to use TLS requires a signed Certificate for the syslog server.

McAfee®

splunk®>

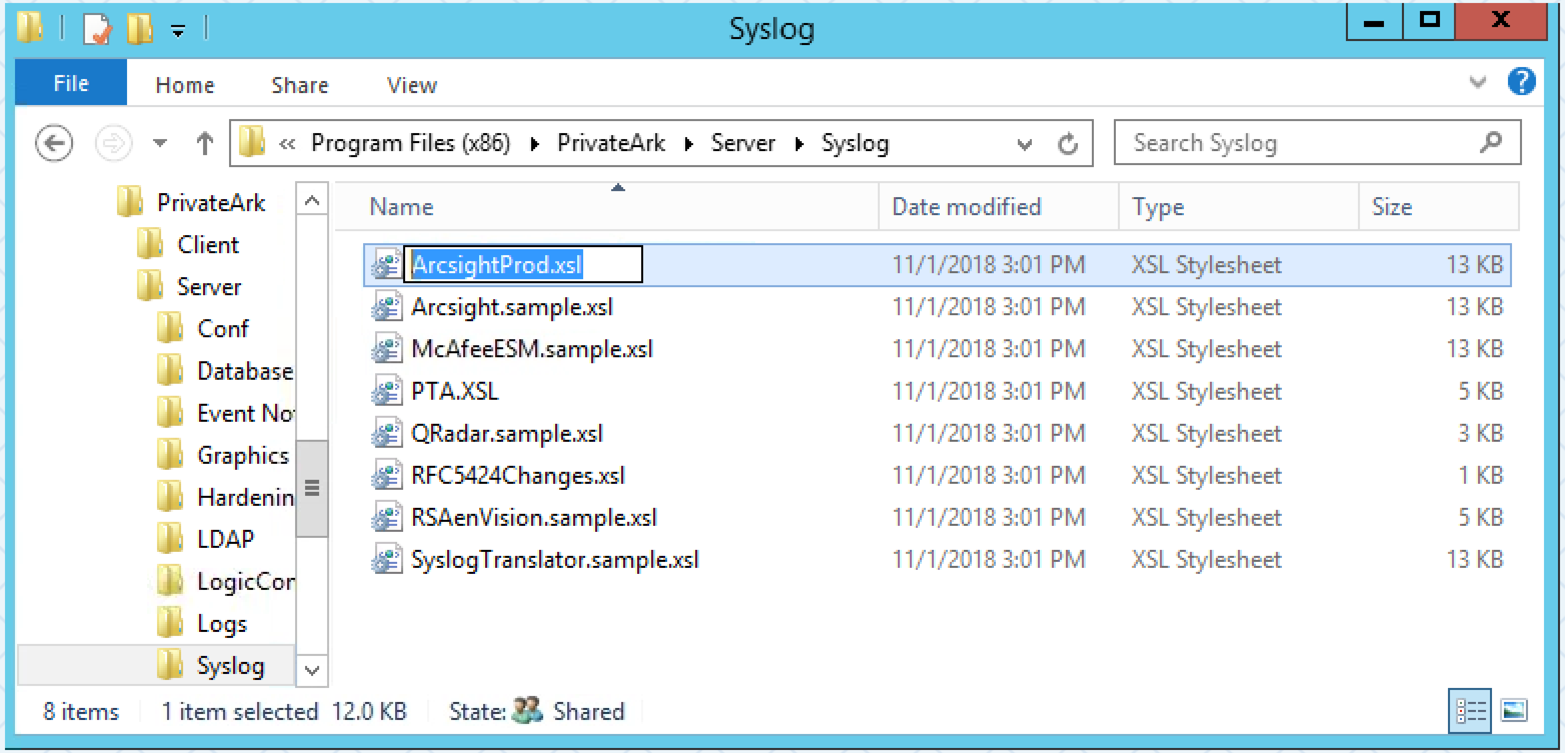
ArcSight™

LogRhythm™

RSA SECURITY ENVISION

SIEM SETUP

- Integration with a SIEM means that Audit log information will be sent to the SIEM console for aggregation, reporting and alerting.
- Rename one of the sample translator files
  - Translator files translate CyberArk logging format into the SIEM logging format
  - These five files will cover the most commonly deployed SIEM systems
  - For Splunk integration, download the Splunk add-on for CyberArk from the Splunk website.

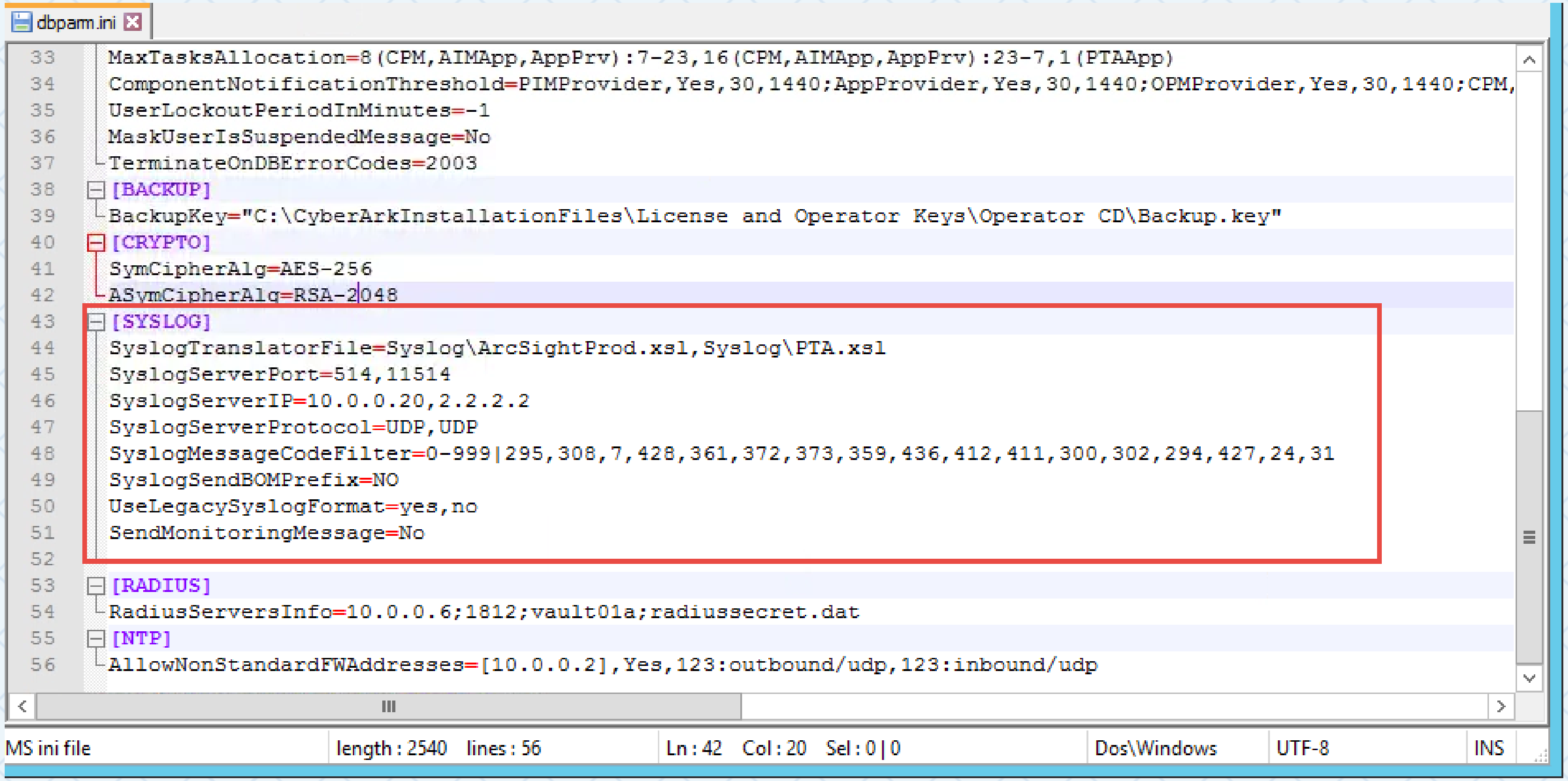


Name	Date modified	Type	Size
ArcsightProd.xsl	11/1/2018 3:01 PM	XSL Stylesheet	13 KB
Arcsight.sample.xsl	11/1/2018 3:01 PM	XSL Stylesheet	13 KB
McAfeeESM.sample.xsl	11/1/2018 3:01 PM	XSL Stylesheet	13 KB
PTA.XSL	11/1/2018 3:01 PM	XSL Stylesheet	5 KB
QRadar.sample.xsl	11/1/2018 3:01 PM	XSL Stylesheet	3 KB
RFC5424Changes.xsl	11/1/2018 3:01 PM	XSL Stylesheet	1 KB
RSAenVision.sample.xsl	11/1/2018 3:01 PM	XSL Stylesheet	5 KB
SyslogTranslator.sample.xsl	11/1/2018 3:01 PM	XSL Stylesheet	13 KB

8 items 1 item selected 12.0 KB State: Shared

SIEM INTEGRATION

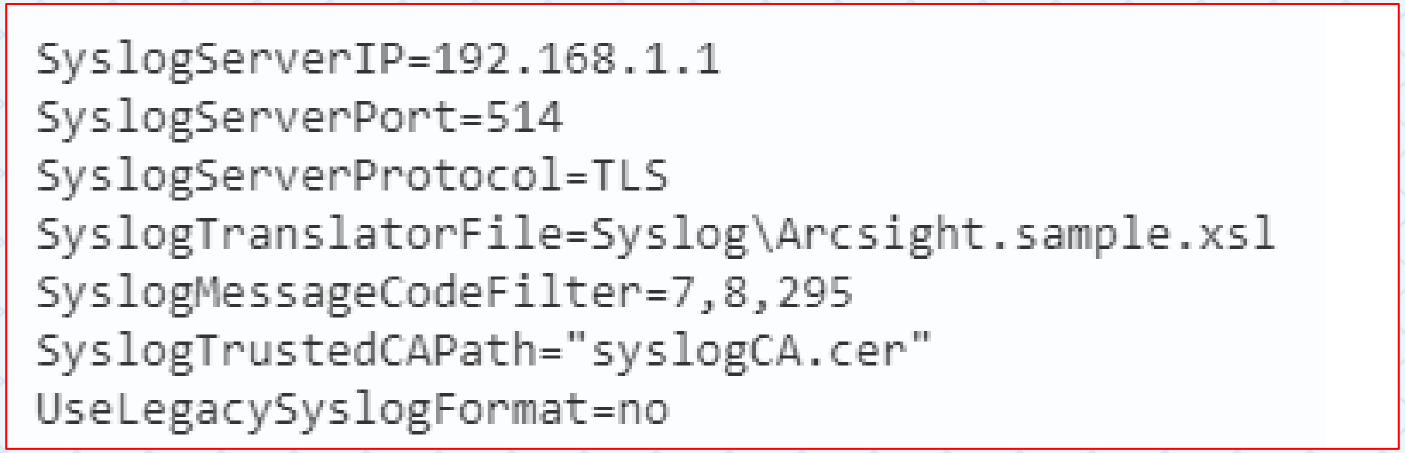
- Add SYSLOG configuration to dbparm.ini
- The Syslog configuration allows for multiple IP addresses and Message Code filters



```
MaxTasksAllocation=8(CPM,AIMApp,AppPrv):7-23,16(CPM,AIMApp,AppPrv):23-7,1(PTAApp)
ComponentNotificationThreshold=PIMProvider,Yes,30,1440;AppProvider,Yes,30,1440;OPMProvider,Yes,30,1440;CPM,
UserLockoutPeriodInMinutes=-1
MaskUserIsSuspendedMessage=No
TerminateOnDBErrorCodes=2003
[BACKUP]
BackupKey="C:\CyberArkInstallationFiles\License and Operator Keys\Operator CD\Backup.key"
[CRYPTO]
SymCipherAlg=AES-256
ASymCipherAlg=RSA-2048
[SYSLOG]
SyslogTranslatorFile=Syslog\ArcSightProd.xsl,Syslog\PTA.xsl
SyslogServerPort=514,11514
SyslogServerIP=10.0.0.20,2.2.2.2
SyslogServerProtocol=UDP,UDP
SyslogMessageCodeFilter=0-999|295,308,7,428,361,372,373,359,436,412,411,300,302,294,427,24,31
SyslogSendBOMPrefix=NO
UseLegacySyslogFormat=yes,no
SendMonitoringMessage=No

[RADIUS]
RadiusServersInfo=10.0.0.6;1812;vault01a;radiussecret.dat
[NTP]
AllowNonStandardFWAddresses=[10.0.0.2],Yes,123:outbound/udp,123:inbound/udp
```

SIEM INTEGRATION USING ENCRYPTED PROTOCOL

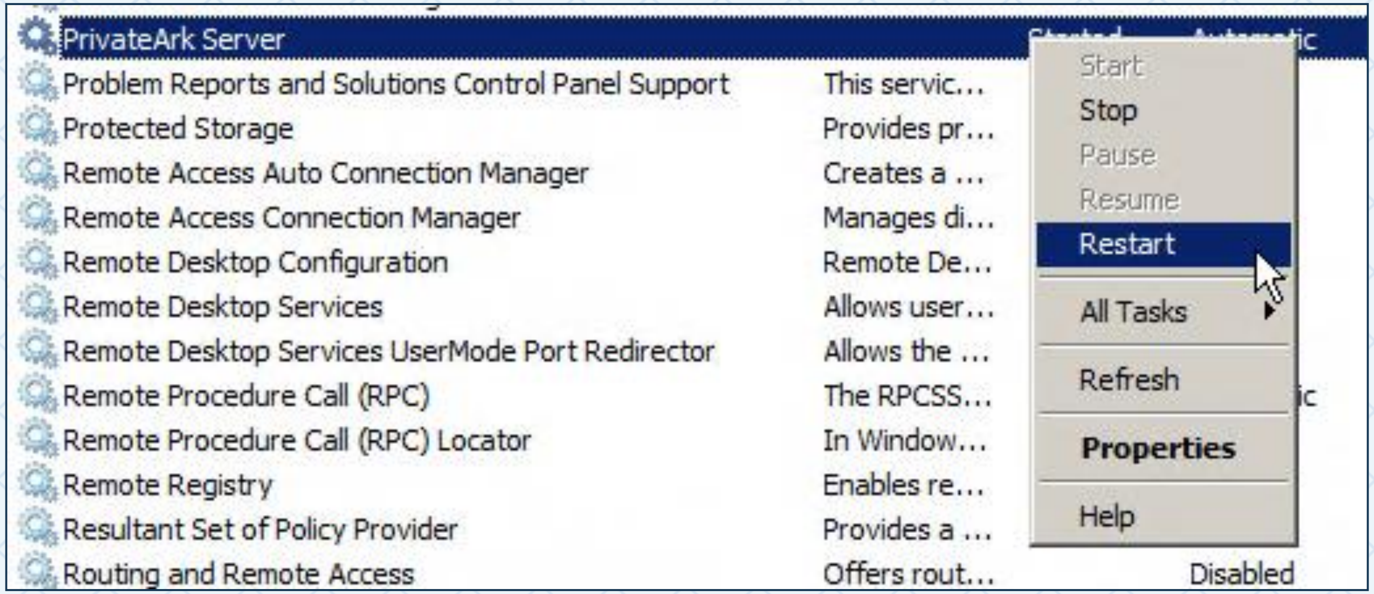
- The example shows a set of syslog properties that will send different syslog messages to one syslog server using encrypted syslog protocol
- The root CA certificate is stored in the root of the Vault installation directory
- More information can be found on docs.cyberark.com, *“Security Information and Event Management Applications”*



```
SyslogServerIP=192.168.1.1
SyslogServerPort=514
SyslogServerProtocol=TLS
SyslogTranslatorFile=Syslog\Arcsight.sample.xsl
SyslogMessageCodeFilter=7,8,295
SyslogTrustedCAPath="syslogCA.cer"
UseLegacySyslogFormat=no
```

SIEM INTEGRATION

- Restart the PrivateArk Server Service.
- Use the Windows Services applet to restart, to ensure that service dependencies restart successfully.
- Check with the administrator of the SIEM console to ensure that the SYSLOG messages sent are being received and are readable.
- Check logs for possible errors and validation.



PrivateArk Server		
Problem Reports and Solutions Control Panel Support	This servic...	
Protected Storage	Provides pr...	
Remote Access Auto Connection Manager	Creates a ...	
Remote Access Connection Manager	Manages di...	
Remote Desktop Configuration	Remote De...	
Remote Desktop Services	Allows user...	
Remote Desktop Services UserMode Port Redirector	Allows the ...	
Remote Procedure Call (RPC)	The RPCSS...	
Remote Procedure Call (RPC) Locator	In Window...	
Remote Registry	Enables re...	
Resultant Set of Policy Provider	Provides a ...	
Routing and Remote Access	Offers rout...	Disabled

TIME SYNCHRONIZATION

PURPOSE

- The vault server(s) are standalone and do not participate in
  a domain, time synchronization must be configured manually
- The vault servers must be configured to use NTP to synchronize system clocks to an external time source
- It is critically important to reduce or eliminate time drift between the Vault server and CyberArk system component.

NTP INTEGRATION

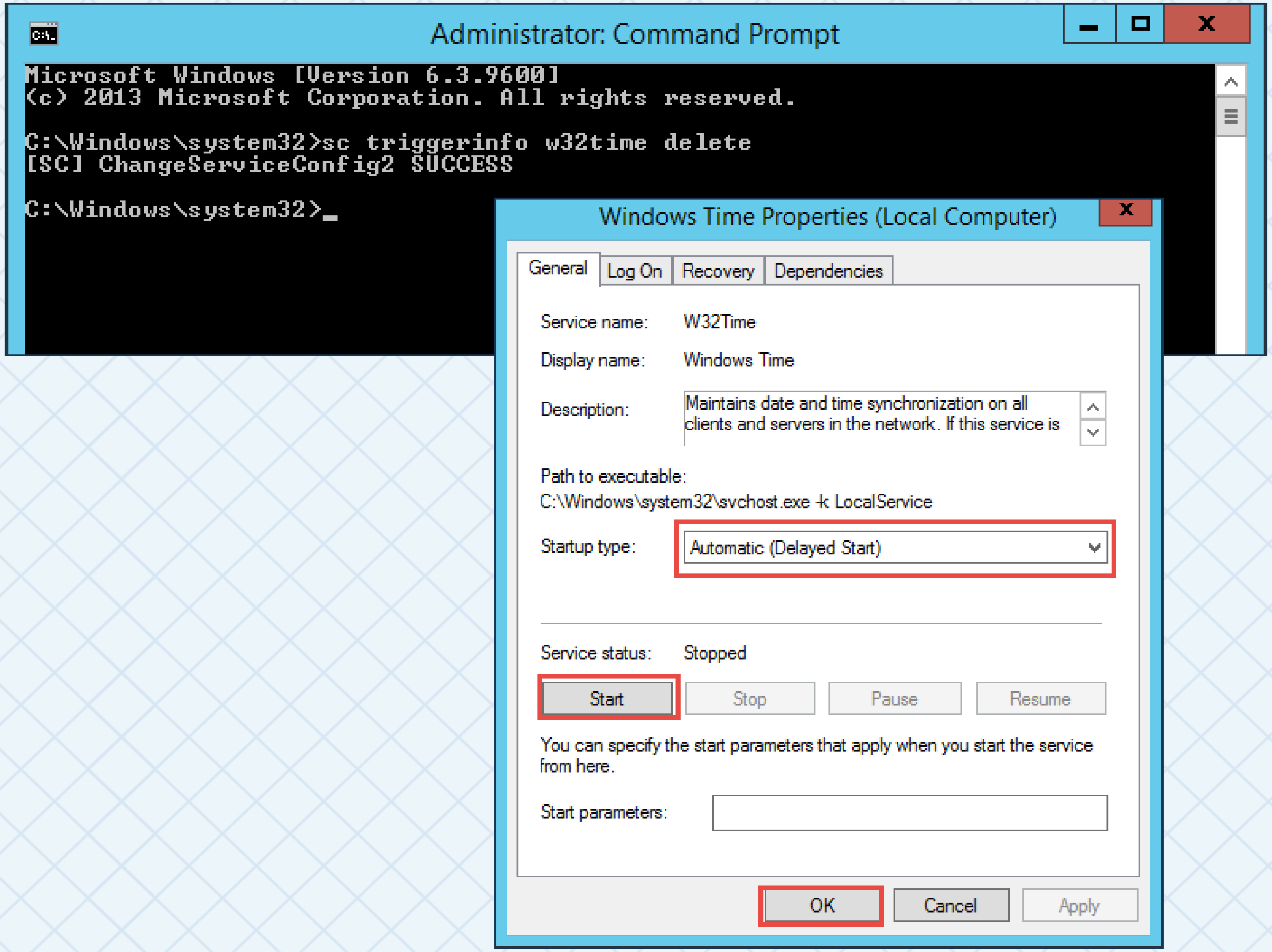
NTP integration is also important in environments where CyberArk is one of many systems producing security logs, so that times between all security devices can be correlated.

Prerequisites:

- IP Address of the Network Time Server.
- Open network path for NTP standard port tcp_123

NTP INTEGRATION

- Enable the Windows Time service, set to Automatic (Delayed Start)



Administrator: Command Prompt

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

C:\Windows\system32>sc triggerinfo w32time delete
[SC] ChangeServiceConfig2 SUCCESS

C:\Windows\system32>_
```

Windows Time Properties (Local Computer)
General
Log On
Recovery
Dependencies

Service name: W32Time

Display name: Windows Time

Description: Maintains date and time synchronization on all clients and servers in the network. If this service is

Path to executable:
C:\Windows\system32\svchost.exe -k LocalService

Startup type: Automatic (Delayed Start)

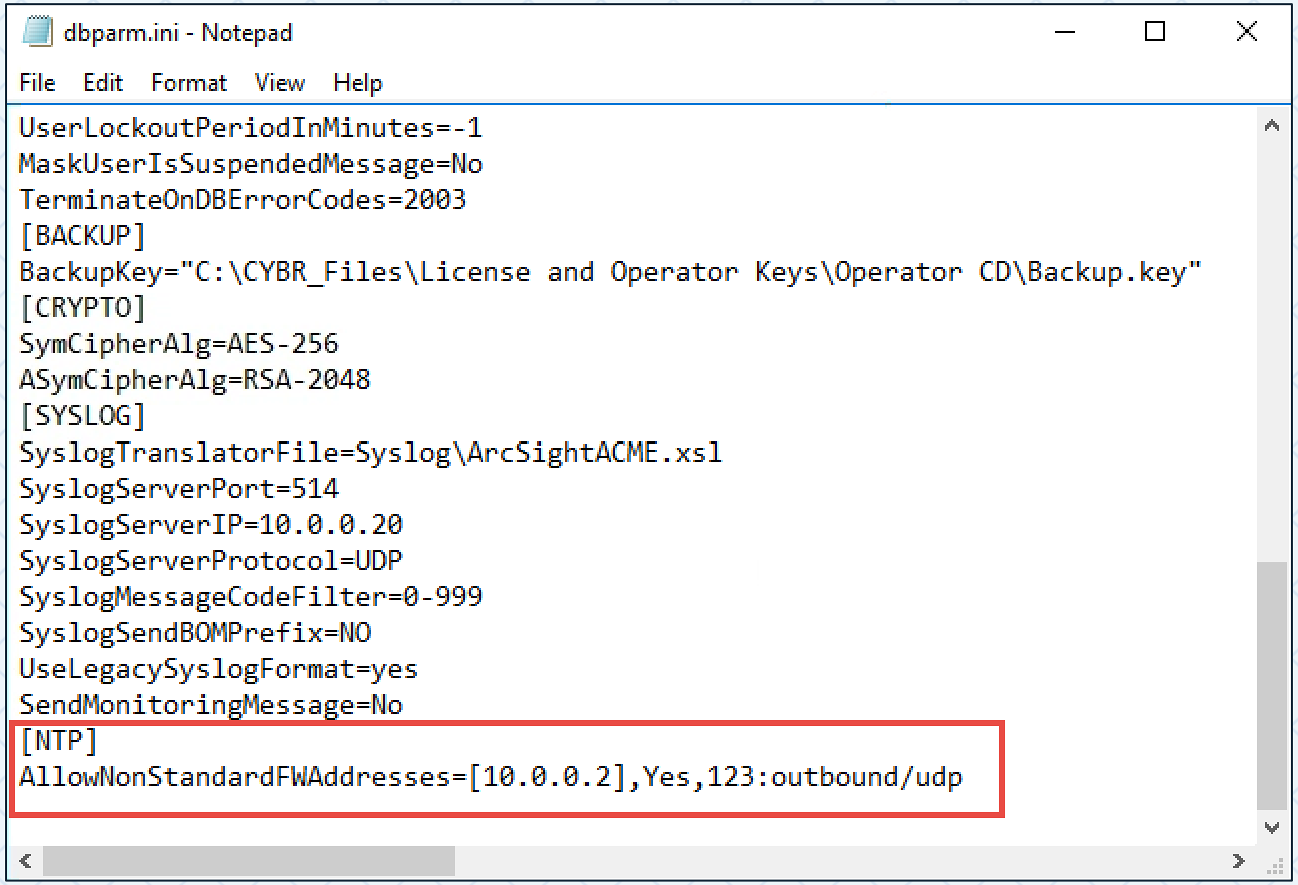
Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

NTP INTEGRATION

- Create a firewall exception in DBParm.ini to allow the vault to communicate on the NTP port tcp_123
- Restart the PrivateArk Server service to read the changes made into memory.



```
UserLockoutPeriodInMinutes=-1
MaskUserIsSuspendedMessage=No
TerminateOnDBErrorCodes=2003
[BACKUP]
BackupKey="C:\CYBR_Files\License and Operator Keys\Operator CD\Backup.key"
[CRYPTO]
SymCipherAlg=AES-256
ASymCipherAlg=RSA-2048
[SYSLOG]
SyslogTranslatorFile=Syslog\ArcSightACME.xsl
SyslogServerPort=514
SyslogServerIP=10.0.0.20
SyslogServerProtocol=UDP
SyslogMessageCodeFilter=0-999
SyslogSendBOMPrefix=NO
UseLegacySyslogFormat=yes
SendMonitoringMessage=No
[NTP]
AllowNonStandardFWAddresses=[10.0.0.2],Yes,123:outbound/udp
```

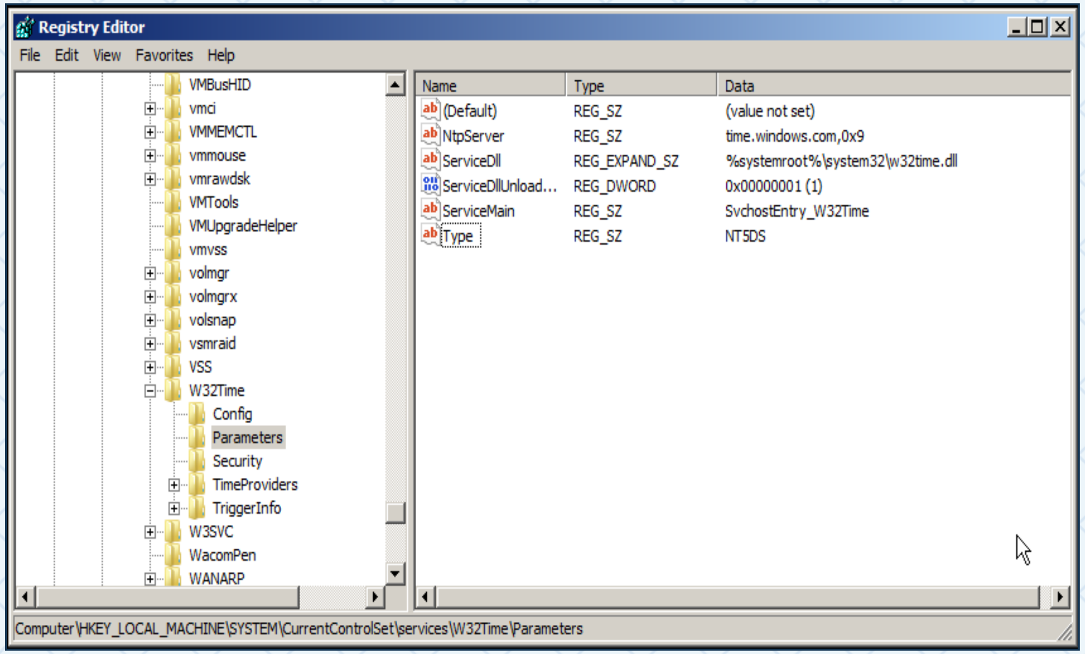
NTP INTEGRATION

Set a special time skew to prevent very large changes to the system clock.

- HKLM\System\CurrentControlSet\Services\W32Time\Parameters\Period=65532

Run the following command at an Administrators Command Prompt

- W32tm /config /manualpeerlist:1.1.1.1,2.2.2.2 /syncfromflags:manual /reliable:YES /update



Name	Type	Data
(Default)	REG_SZ	(value not set)
NtpServer	REG_SZ	time.windows.com,0x9
ServiceDll	REG_EXPAND_SZ	%systemroot%\system32\w32time.dll
ServiceDllUnload...	REG_DWORD	0x00000001 (1)
ServiceMain	REG_SZ	SvchostEntry_W32Time
Type	REG_SZ	NT5DS

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\W32Time\Parameters

SUMMARY

SUMMARY

In this session we covered:

- LDAP Integration
- SMTP Integration
- SNMP Integration
- SIEM Integration
- NTP Integration

THANK YOU