CYBERARK UNIVERSITY

AUTHENTICATION METHODS

CyberArk Training

OBJECTIVES

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

- Describe the various authentication methods supported by CyberArk
- Describe how to configure and combine two different authentication methods to achieve 2 factor authentication

SUPPORTED AUTHENTICATION METHODS

SUPPORTED AUTHENTICATION METHODS

- CyberArk supports the following authentication methods:
  - CyberArk Password
  - LDAP Authentication
  - RADIUS including Challenge-Response
  - Windows Authentication
  - PKI
  - RSA SecurID
  - OracleSSO
  - SAML
  - Google Authentication
  - Amazon Cognito
- Not all authentication methods are supported on all user interfaces.
- Some authentication methods may require installing a 3rd party agent on the PVWA or the Vault server.

.

SUPPORTED AUTHENTICATION METHODS

	PVWA	PrivateArk Client	PSM Windows PSM SSH
CyberArk	X	X	X
LDAP	X	X	X
RADIUS	X	X	X
Windows	X	X	
RSA	X	X	
PKI	X	X	
OracleSSO	X		
SAML	X		
Google Authentication	X		
Amazon Cognito	X		

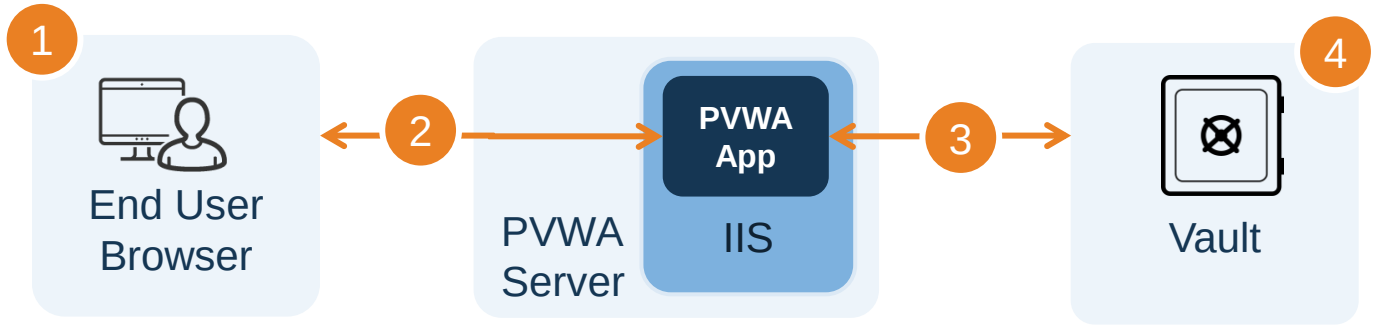
PVWA AUTHENTICATION

AUTHENTICATION CATEGORIES

Authentication via PVWA can be divided into 3 categories:

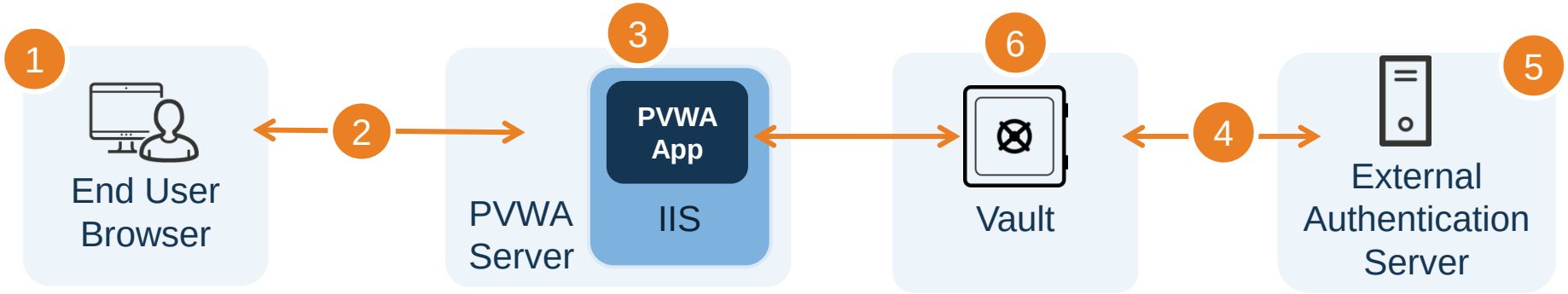
CyberArk Authentication	• The PVWA sends details to the Vault, which performs the authentication.
Vault Integrated External Authentication	• The PVWA sends the credentials to the Vault, which in turn which in turn forwards the request to the external authentication servers.
IIS Integrated External Authentication	• The PVWA sends the credentials to the server's IIS service. IIS forwards the request to the external authenticating server, and confirms authentication to the PVWA web application, which confirms authentication to the vault.

CYBERARK AUTHENTICATION FLOW



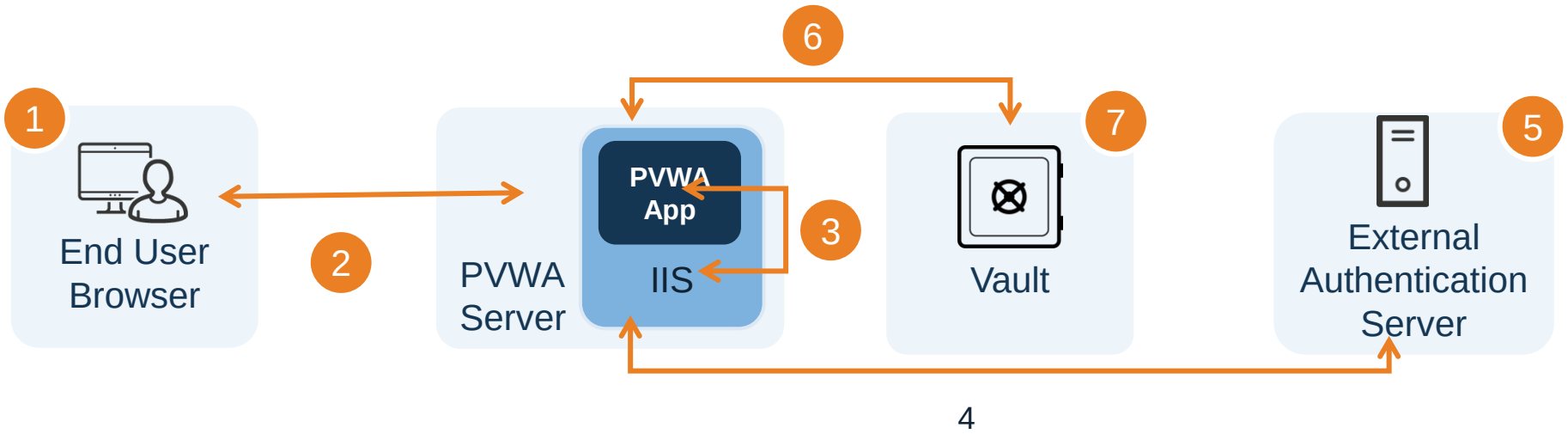
1. User chooses the CyberArk authentication type in the PVWA
2. User sends authentication details: Username and Password
3. The PVWA forwards the authentication request to the Vault
4. The Vault performs the actual authentication by validating the credentials and grants the user access to the system

VAULT INTEGRATED AUTHENTICATION FLOW



1. User chooses the relevant authentication method in the PVWA
2. User sends authentication details: Username and Password/Token
3. The PVWA forwards the authentication request to the Vault
4. The Vault forwards the authentication request to the external trusted authority, such as a Domain Controller for LDAP, or a RADIUS server
5. The external authenticating server validates the request and authenticates the user
6. The Vault grants the user access to the system

IIS INTEGRATED AUTHENTICATION FLOW

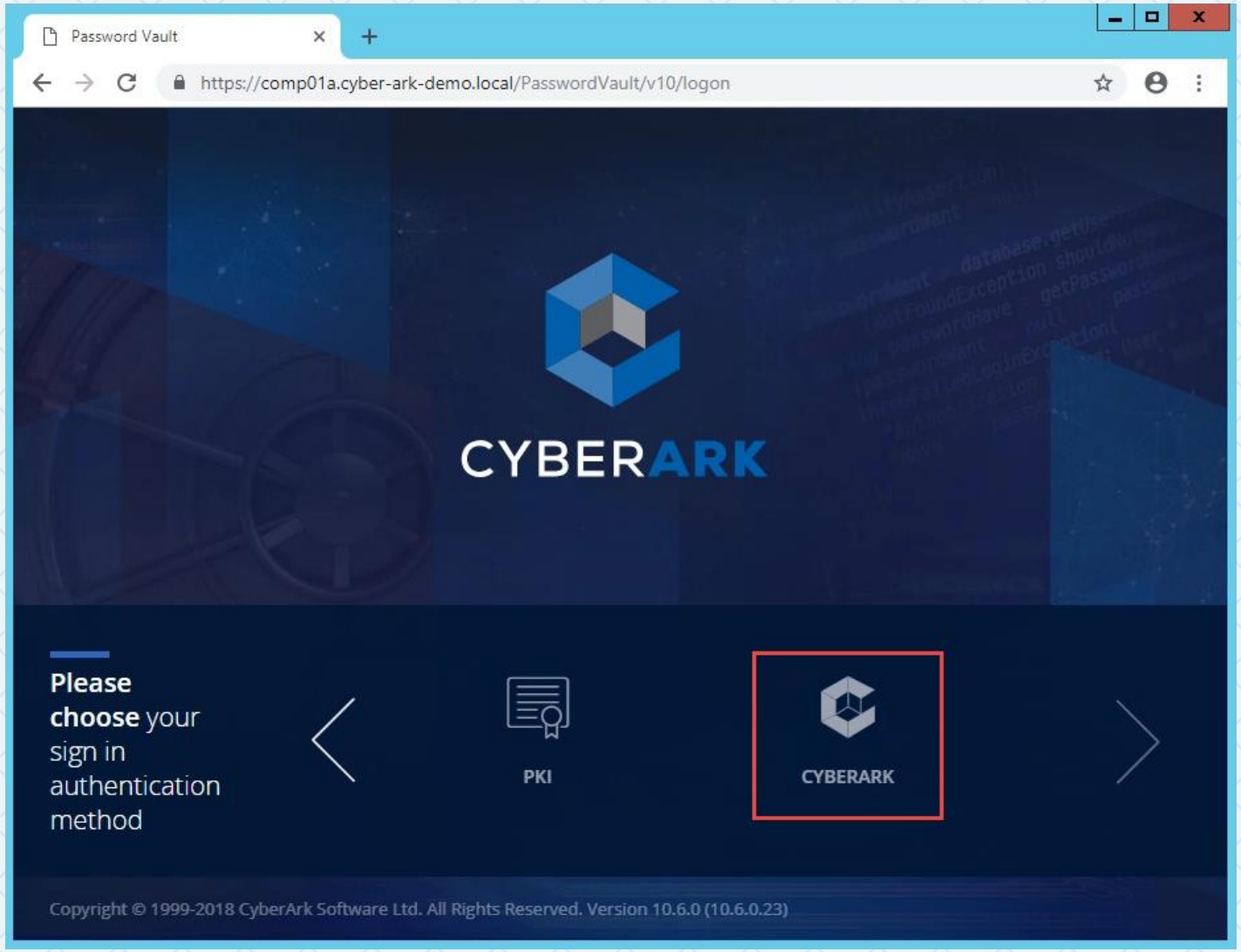


1. User chooses the relevant authentication method in the PVWA
2. User sends authentication details: Username and Password/Token/Certificate
3. The PVWA Application sends the authentication type and credentials to the IIS service
4. IIS sends then forwards the authentication request to the external trusted authority
5. The external authenticating server validates the request and authenticates the user
6. The PVWA confirms the user’s identity to the Vault
7. The Vault grants the user access to the system

CYBERARK AUTHENTICATION

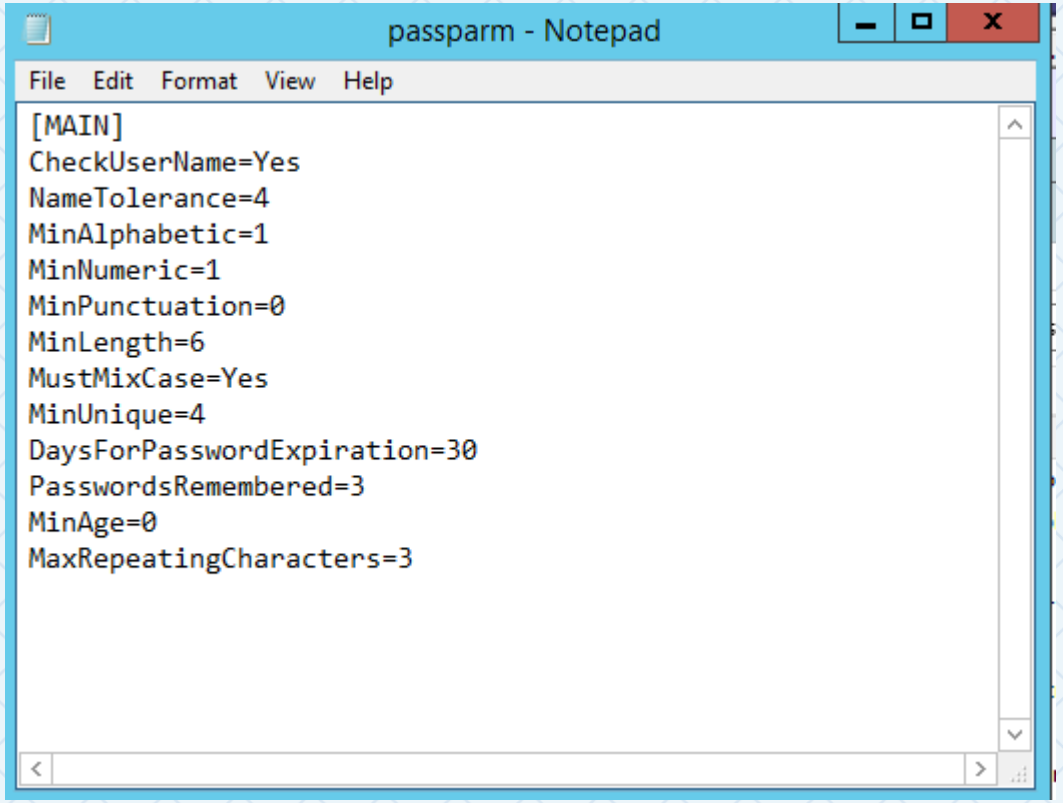
CYBERARK AUTHENTICATION

- The Vault uses a shared secret (password)
- When a user logs on to the Vault the client sends a logon request
- The vault and the client use two-way challenge-response protocol



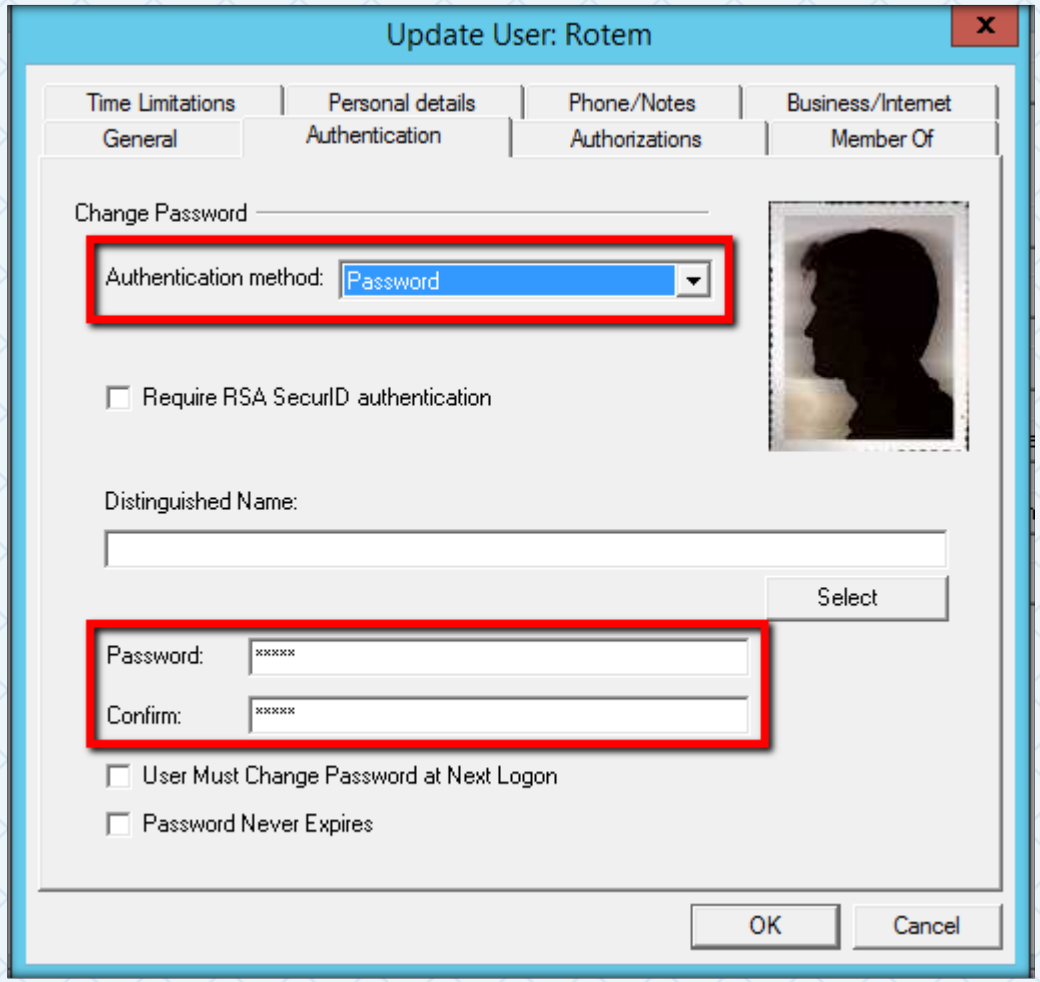
CYBERARK AUTHENTICATION

- The CyberArk internal Password Policy is configured in the passparm.ini file
- Passparm.ini is stored locally on the Vault server and uploaded to the System safe automatically



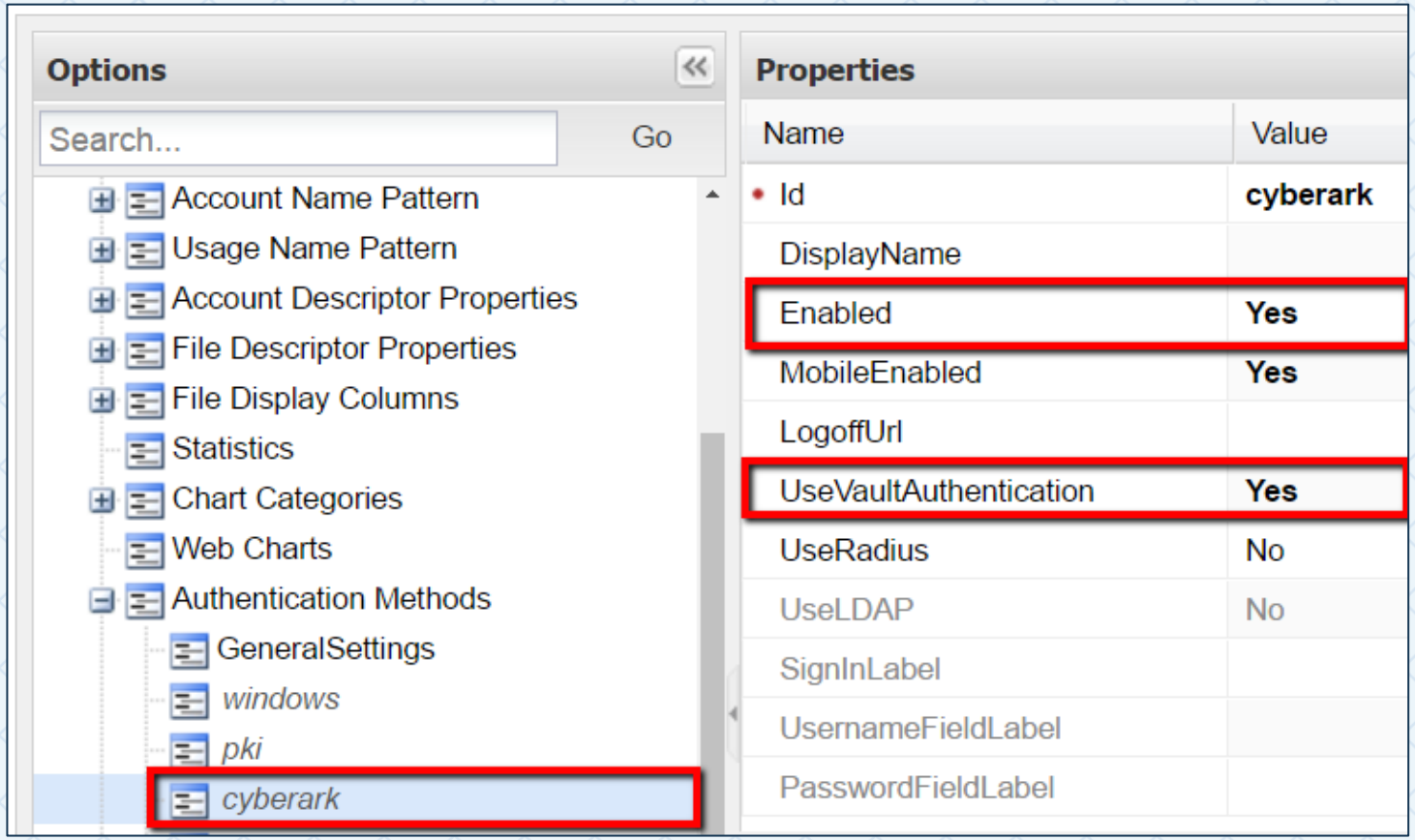
CYBERARK AUTHENTICATION

- Select the authentication method for the internal user and set the password
- Authentication method: *Password* means CyberArk authentication



CYBERARK AUTHENTICATION

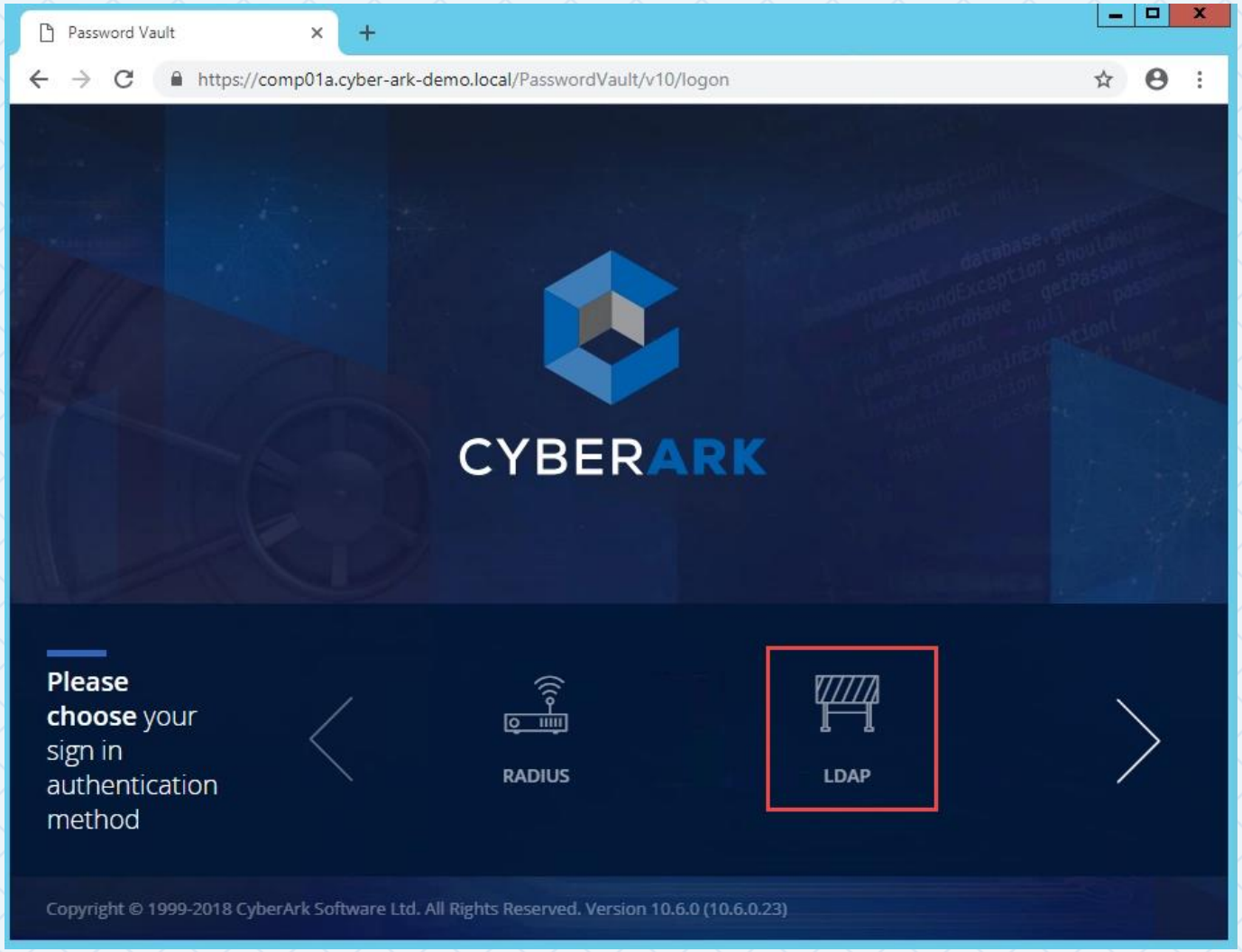
- Enable “CyberArk” authentication in the PVWA as shown
- If this option is not enabled, a user can still authenticate to the Vault via the PrivateArk Client using CyberArk Authentication



LDAP AUTHENTICATION

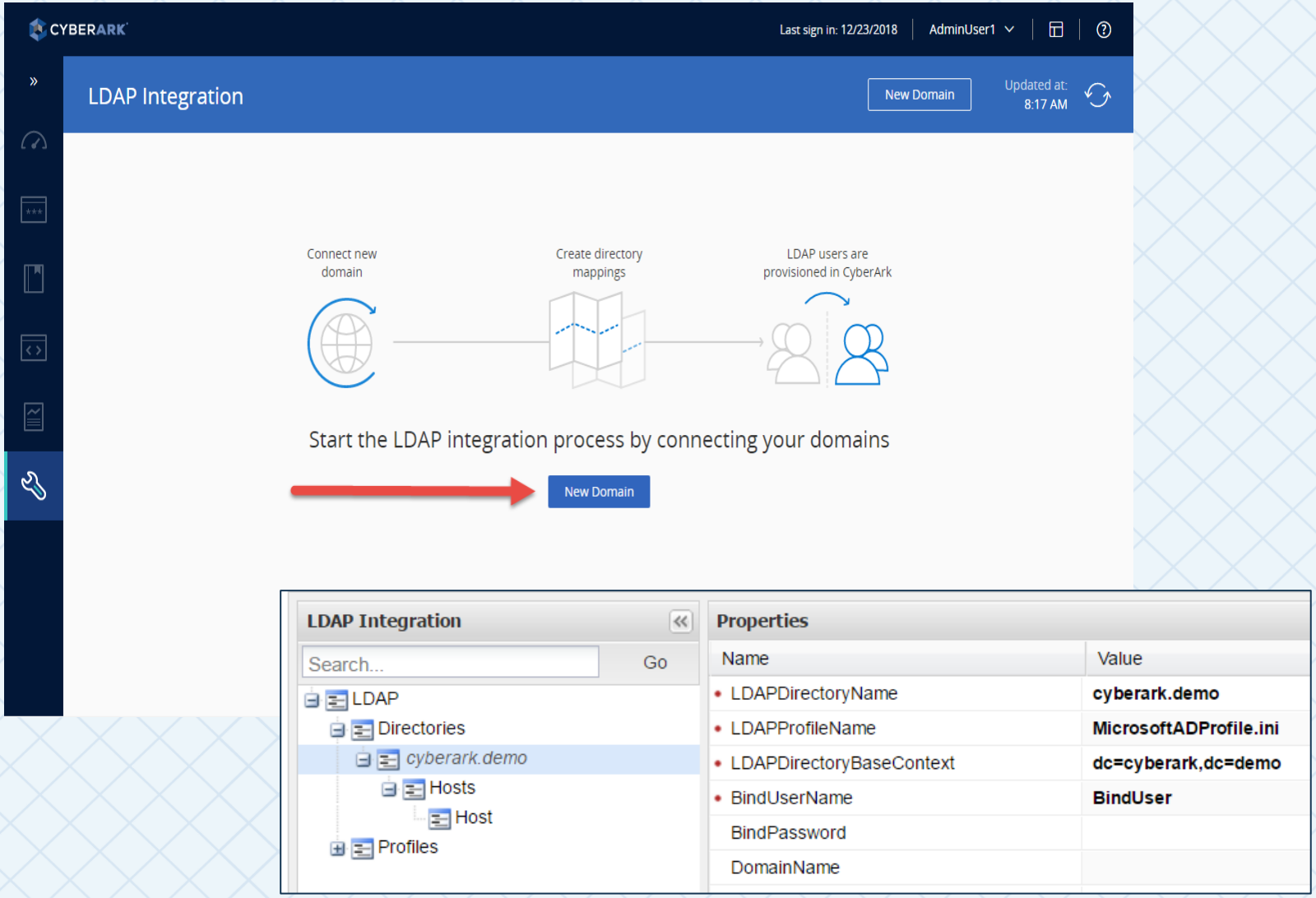
LDAP AUTHENTICATION

- The Vault transparently supports User Accounts and Groups of users whose details are stored externally in LDAP-compliant or LDAP-compatible directories.
- Users whose details are stored in an LDAP-compliant directory can authenticate to the Vault directly from the PrivateArk Client or the PVWA.



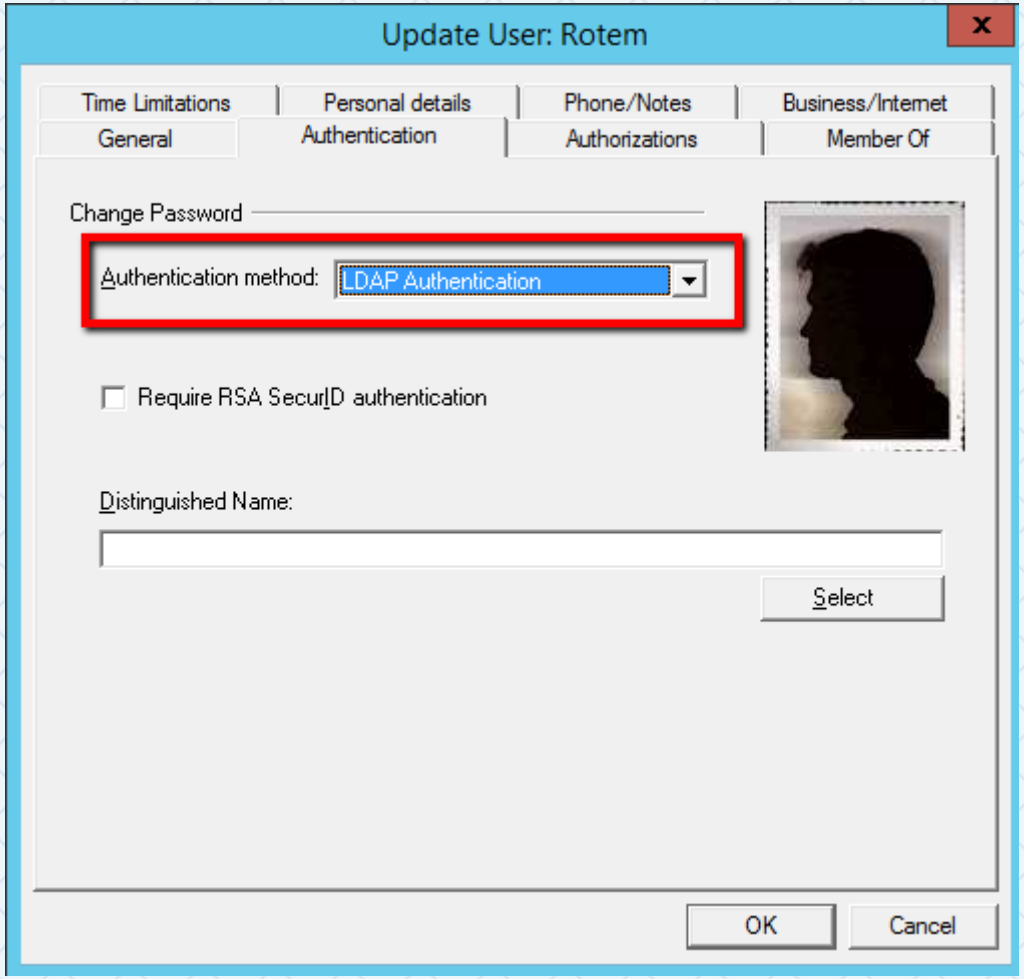
CONFIGURATION

1. Integrate the Vault with the LDAP server using PVWA
2. You must be logged in to the PVWA as Administrator to gain access to the Administration tab, and Setup Wizard
3. Multiple LDAP directories can be integrated if required



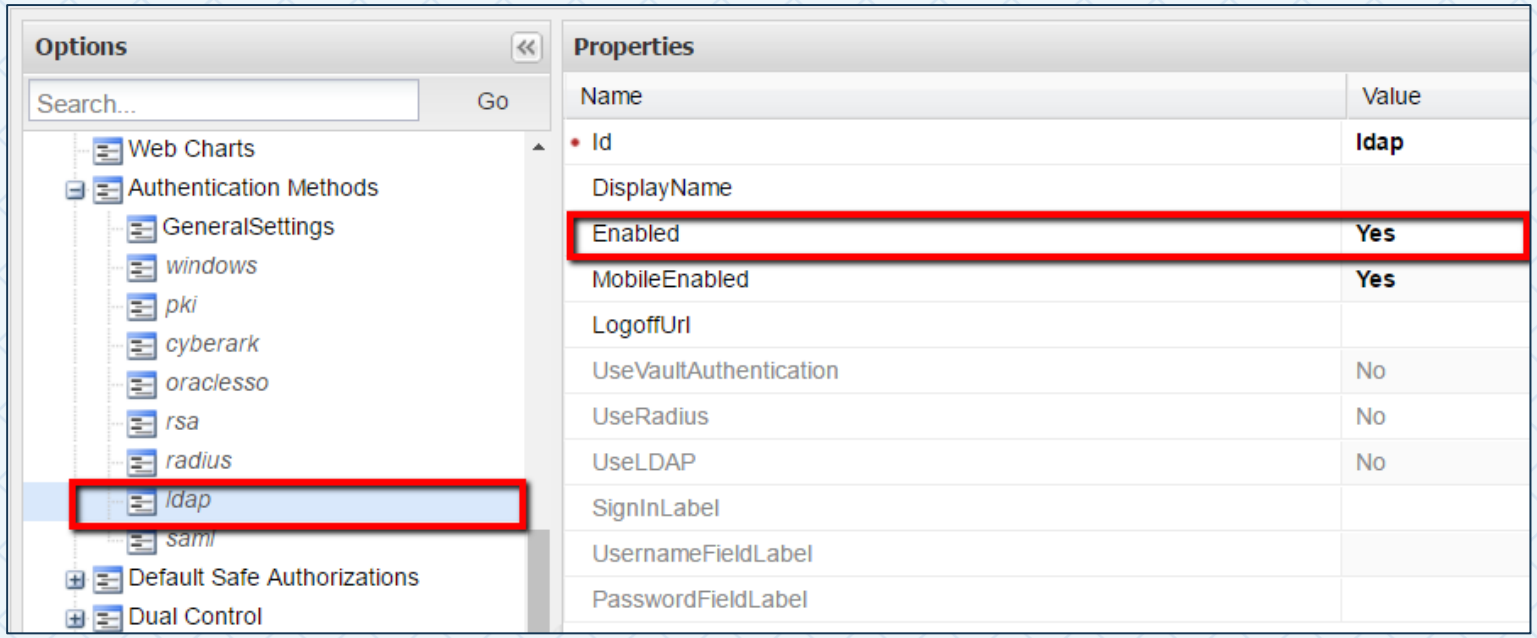
CONFIGURATION

1. Integrate the Vault with the LDAP server using PVWA
2. Set the user's Authentication Method as LDAP
3. Note: The Directory Map user template is only applied at the user's first authentication attempt and is not referenced during subsequent authentications!



CONFIGURATION

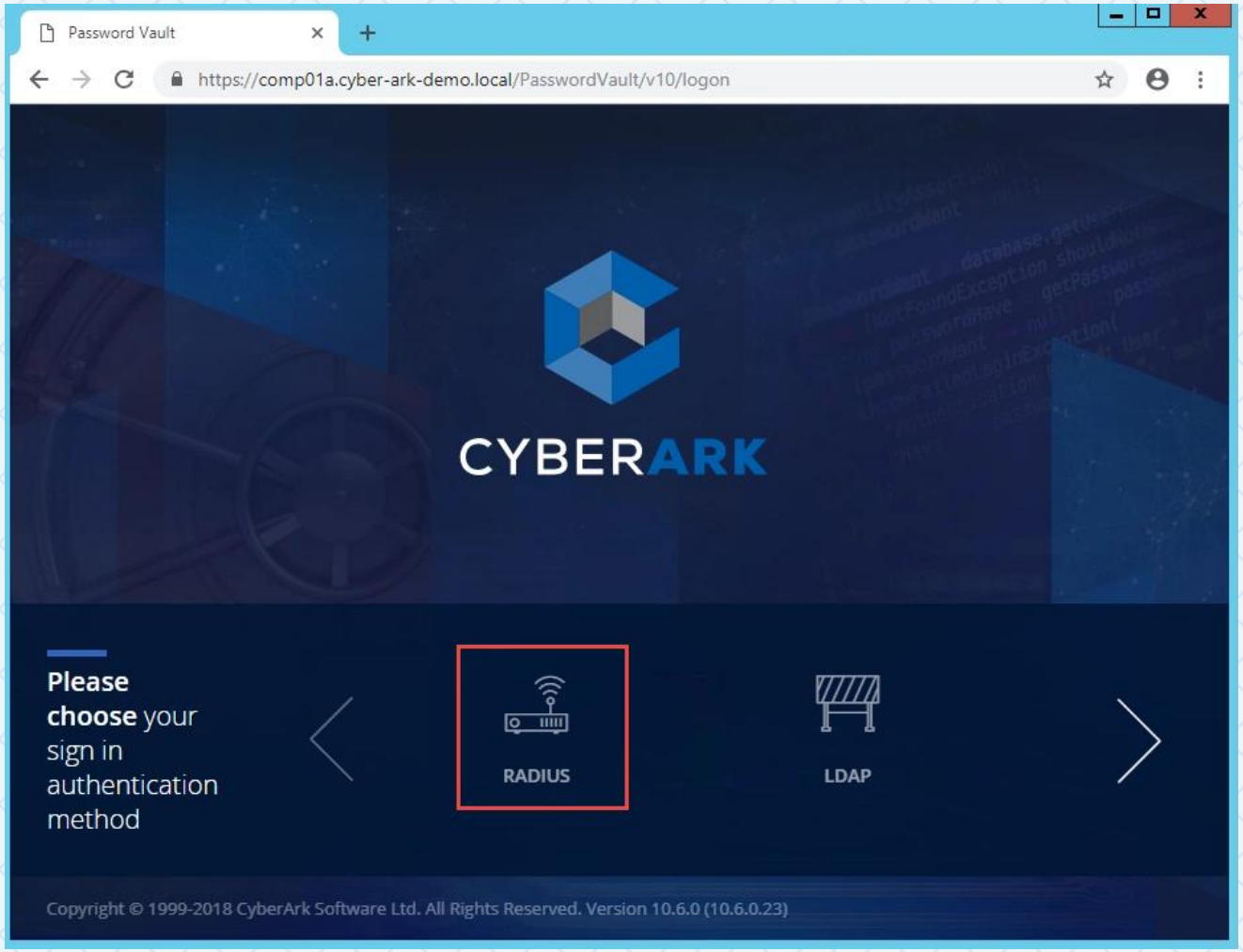
1. Integrate the Vault with the LDAP server using PVWA
2. Set the user's Authentication Method as LDAP
3. Enable "LDAP" Authentication in the PVWA



RADIUS AUTHENTICATION

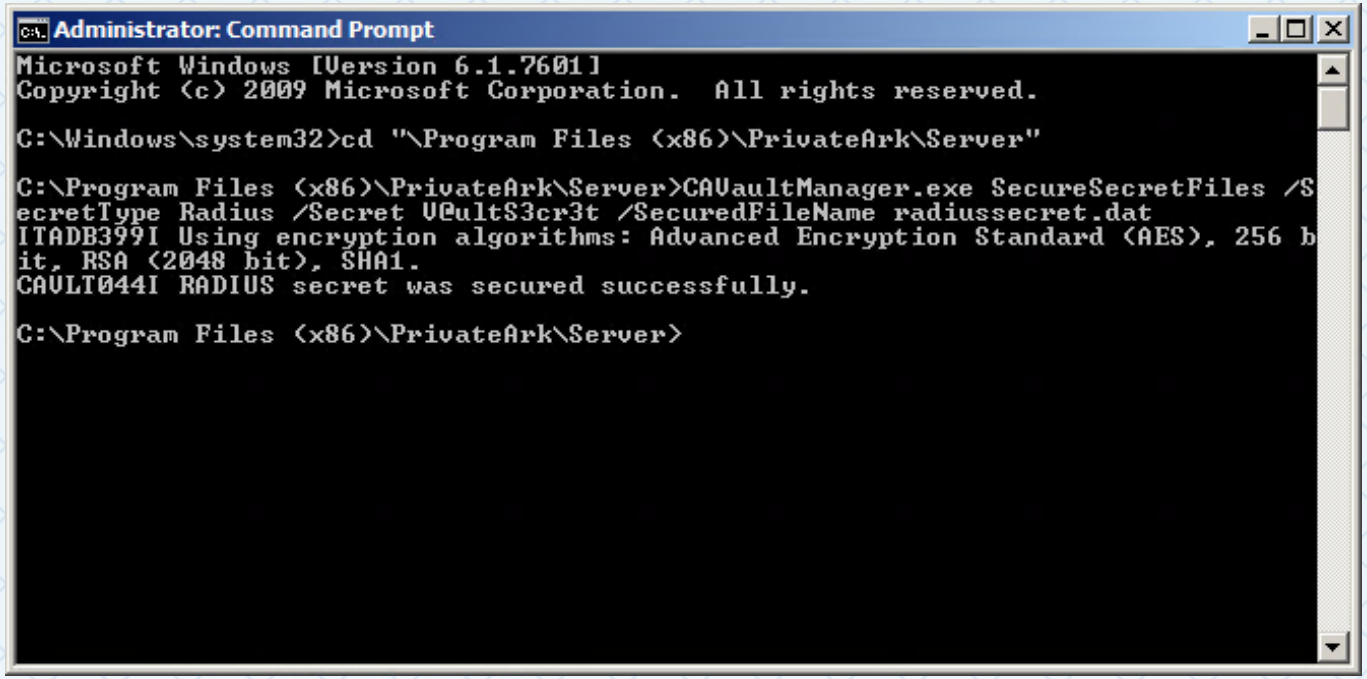
RADIUS AUTHENTICATION

- Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized authentication, Authorization and Accounting (AAA).
- The Vault allows users to log on through RADIUS authentication using logon credentials that are stored in the RADIUS server.
- The Vault also supports RADIUS challenge-response authentication if enabled by the RADIUS Administrator.



RADIUS CONFIGURATION

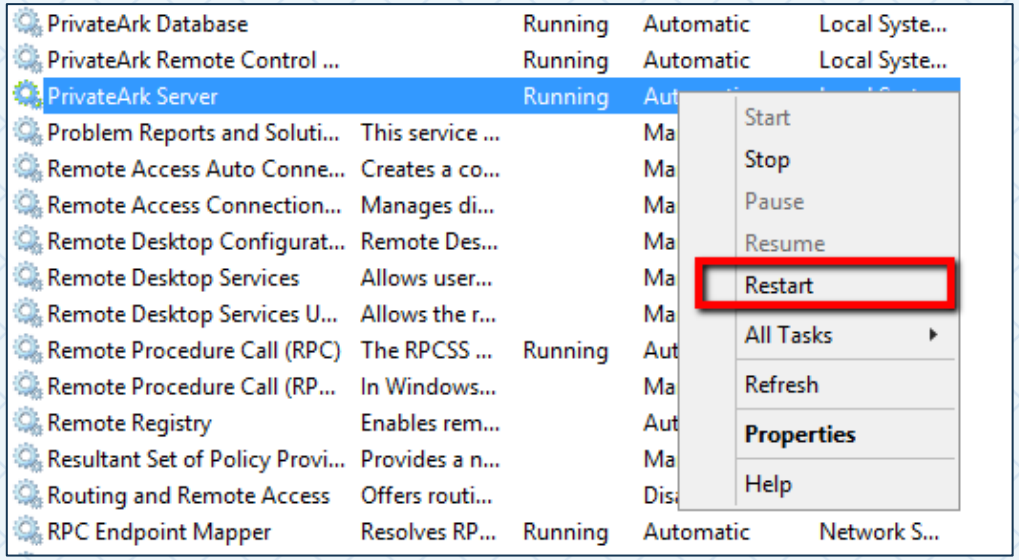
1. Create a file to store the RADIUS shared secret using the CAVaultManager utility.
2. In multiple vault configurations, each Digital Vault should have a unique RADIUS secret



RADIUS CONFIGURATION

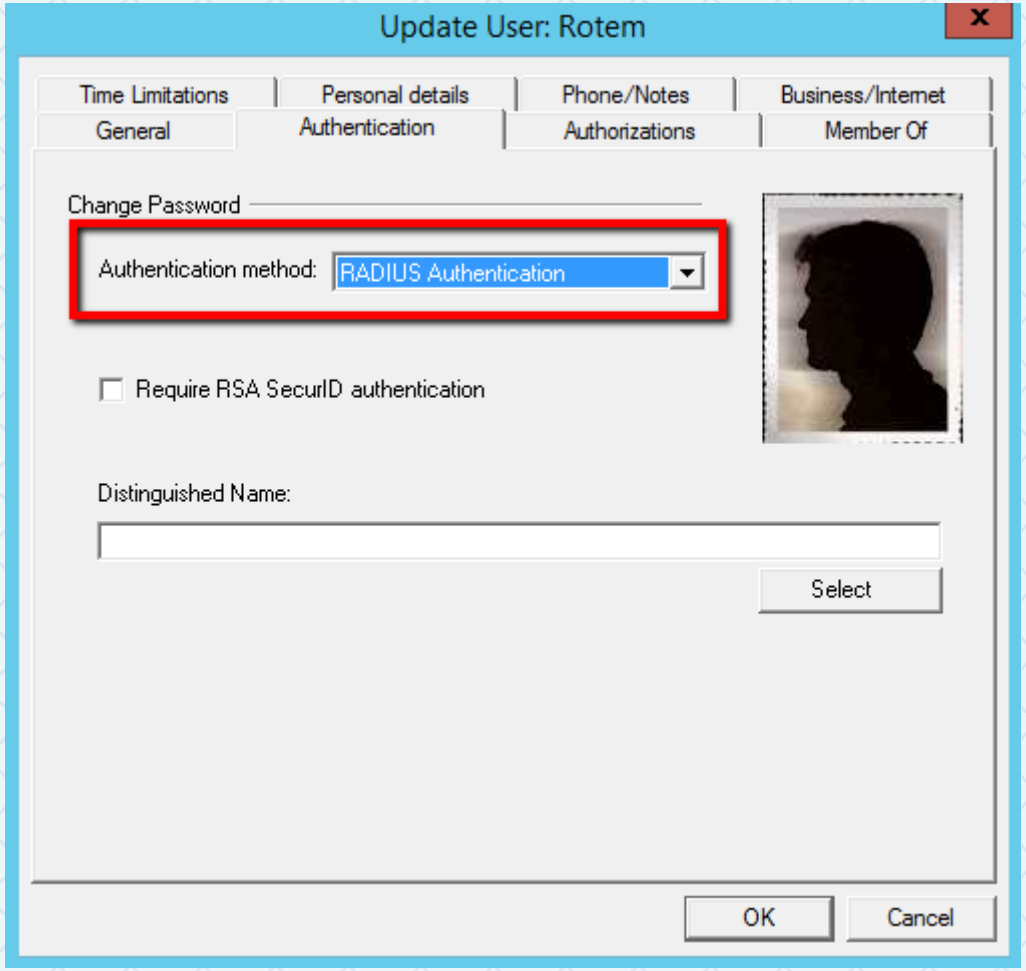
1. Add the RADIUS configuration in dbparm.ini and restart the PrivateArk Service using the Windows Services applet
2. Check the ITALOG.LOG for warnings or errors!

```
[MAIN]
TasksCount=20
DateFormat=DD.MM.YY
TimeFormat=HH:MM:SS
ResidentDelay=10
BasePort=1858
LogRetention=7
LockTimeOut=30
DaysForAutoClear=30
DaysForPicturesDistribution=Never
ClockSyncTolerance=600
TraceArchiveMaxSize=5120
RecoveryPubKey=C:\PrivateArk\Keys\RecPub.key
ServerKey=C:\PrivateArk\Keys\Server.key
...
[RADIUS]
RadiusServersInfo=1.1.1.1;1812;vault01;radiussecret.dat
```



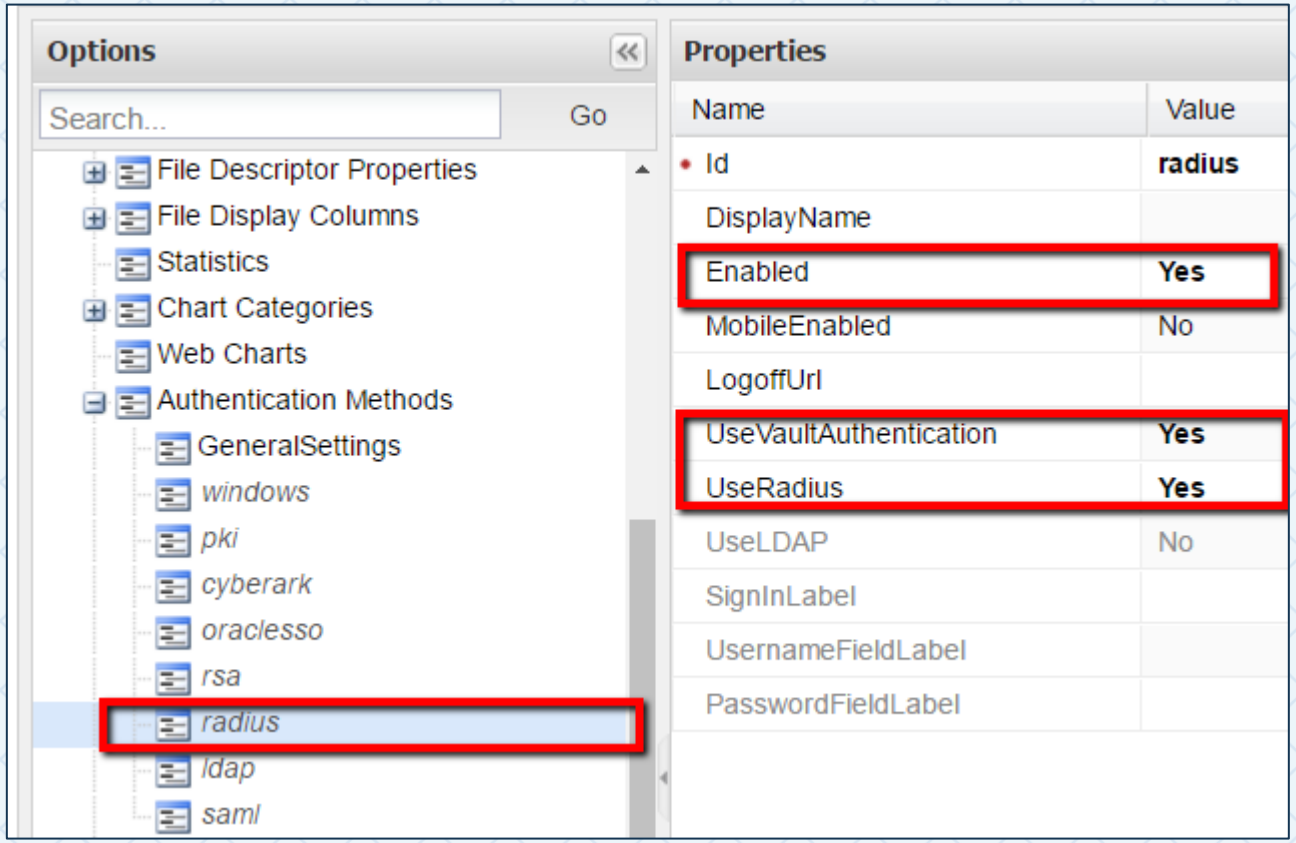
RADIUS CONFIGURATION

1. Set the user's Authentication Method as "RADIUS"



RADIUS CONFIGURATION

1. Enable “RADIUS” Authentication in the PVWA



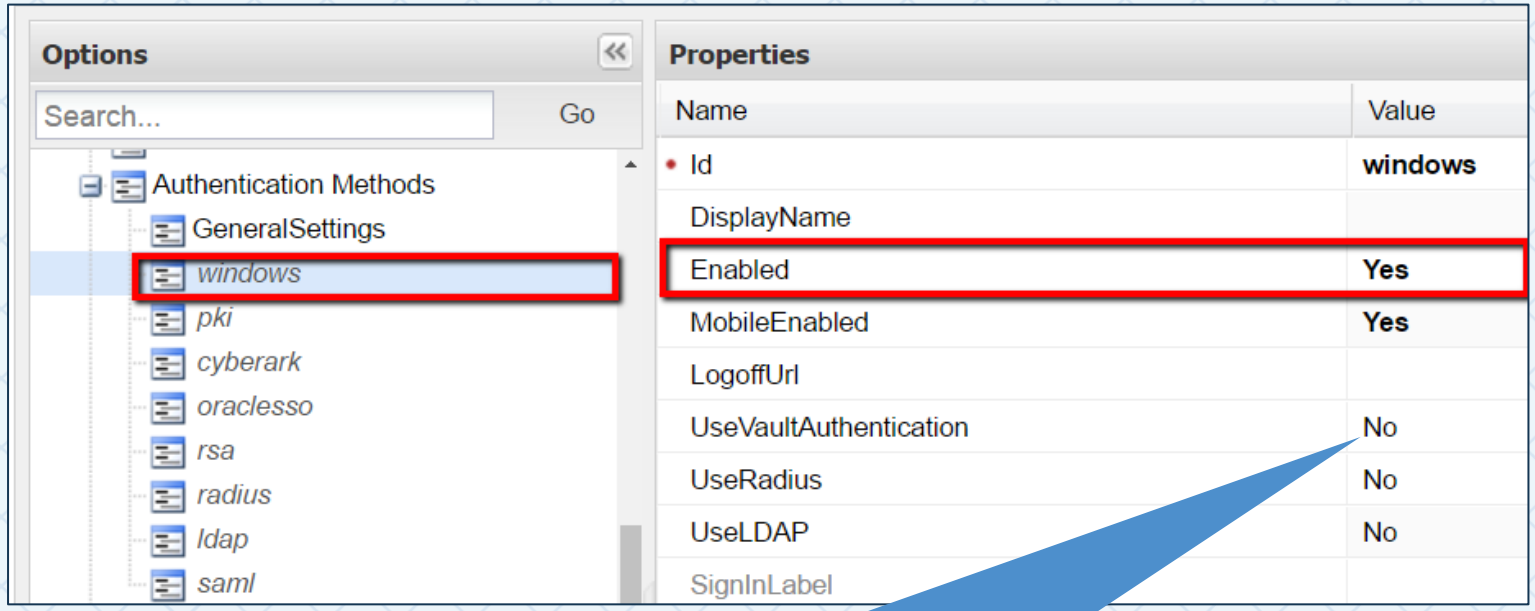
WINDOWS AUTHENTICATION

WINDOWS AUTHENTICATION

- In Windows authentication, the client browser sends a strongly hashed version of the password in a cryptographic exchange to the web server.
- In CyberArk, Windows Authentication allows a Single Sign On solution for PVWA by authenticating to the vault via the user's Windows credentials.

WINDOWS AUTHENTICATION

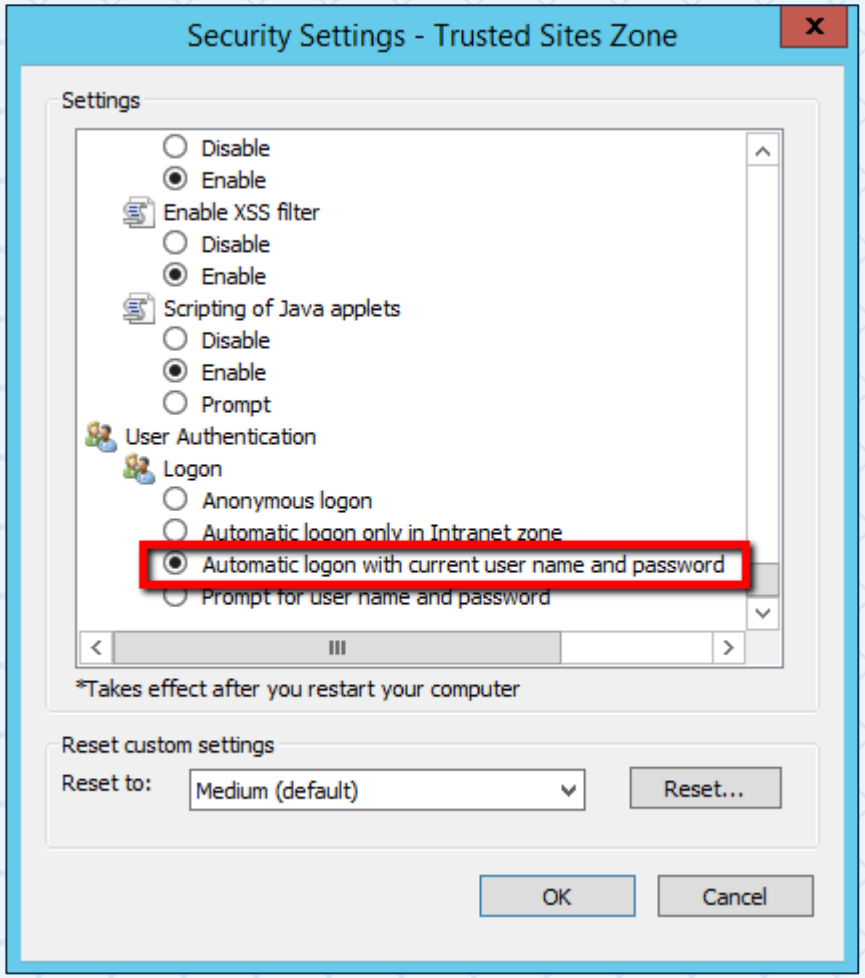
1. Enable “Windows” authentication in the PVWA



When “UseVaultAuthentication” is set to **NO**, the authentication method set for the user in the vault is ignored

WINDOWS AUTHENTICATION

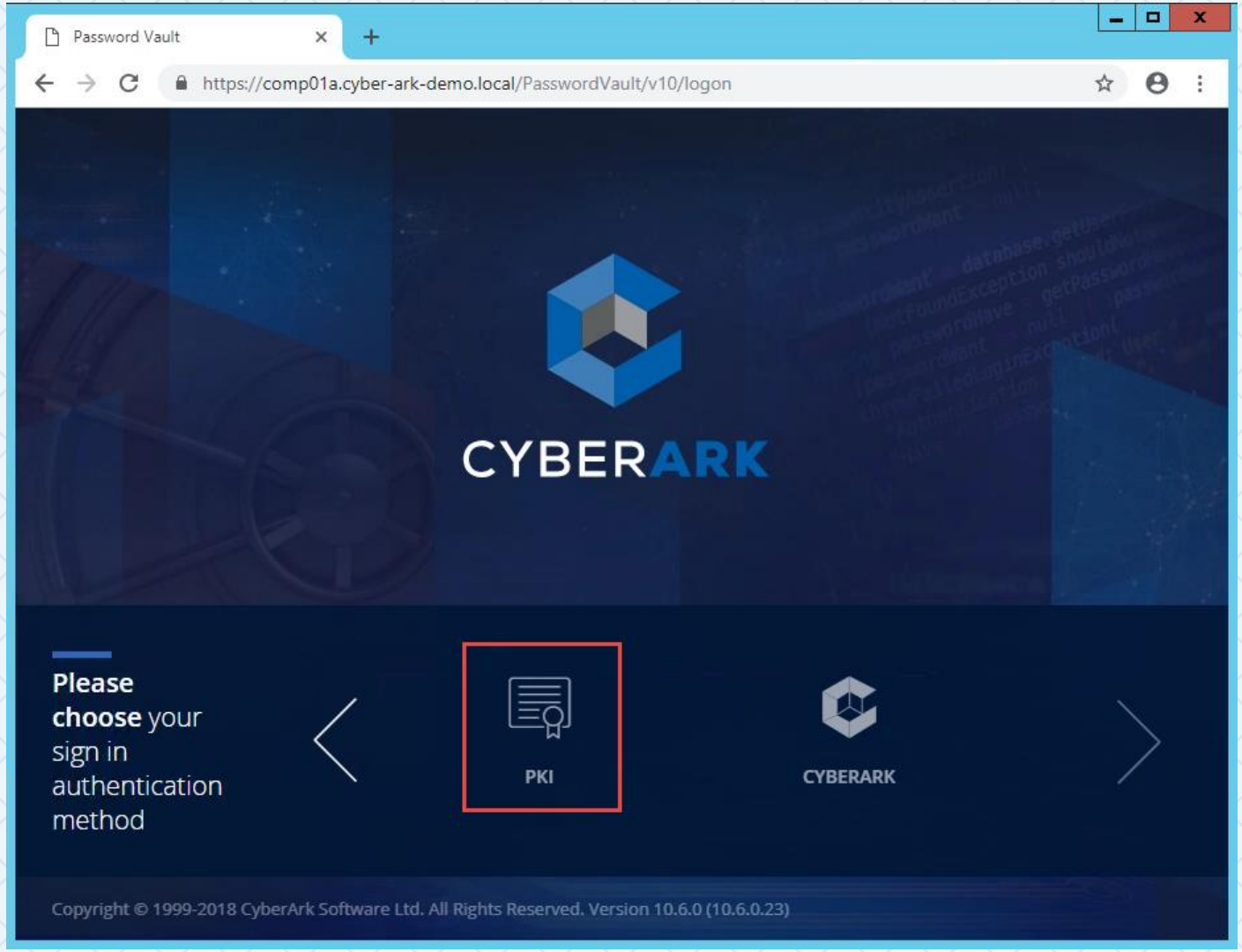
1. Enable “Windows” authentication in the PVWA
2. For Single Sign-On (SSO) add the PVWA URL to the trusted sites and enable ‘Automatic logon with current username and password” in the browser security settings.



PKI AUTHENTICATION

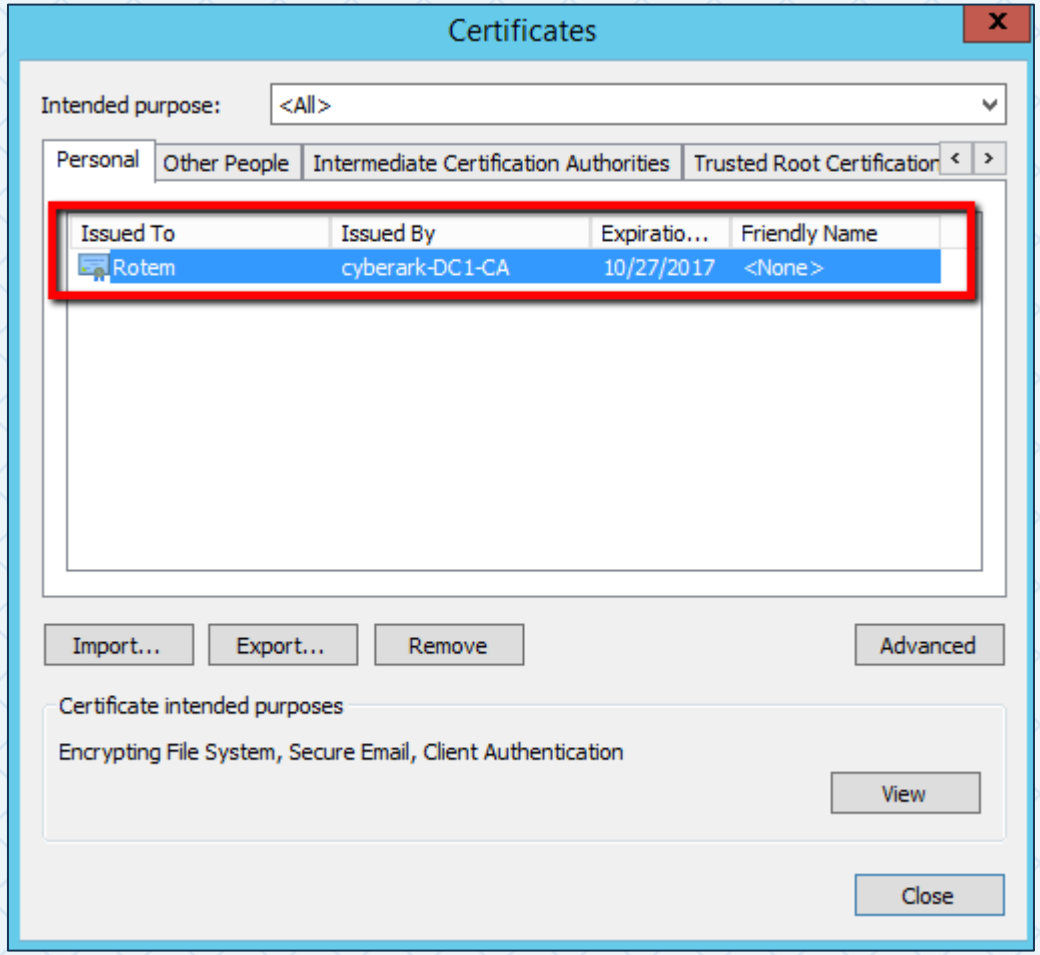
PKI CONFIGURATION

- PKI (Public Key Infrastructure) enables the use of certificates for applications, servers and users to identify each other and establish a secure connection
- PKI Authentication for CyberArk allows users to authenticate using a Digital Certificate that can stored on a Smart card, USB device or Windows Certificate store



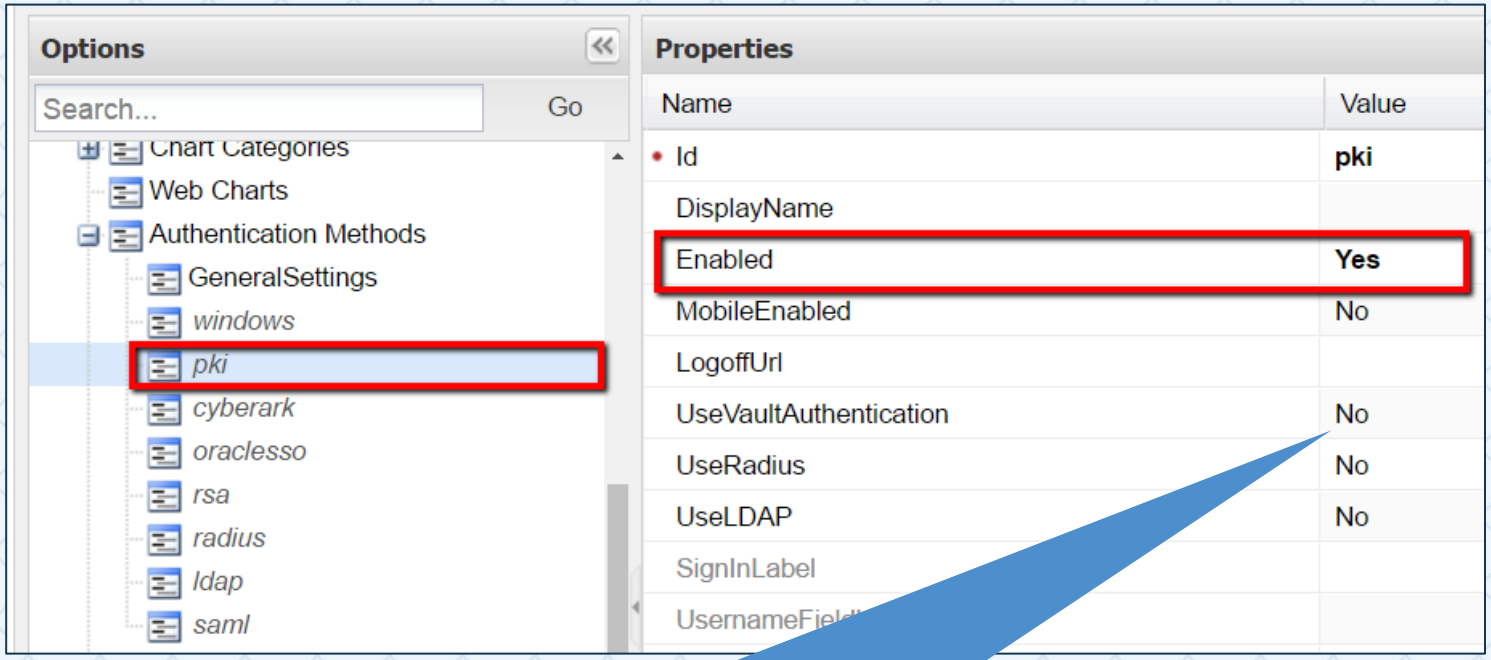
PKI CONFIGURATION

1. The infrastructure for PKI must be in place and users must be issued personal certificates



PKI CONFIGURATION

1. Enable “PKI” authentication in the PVWA



When “UseVaultAuthentication” is set to **NO**, the authentication method set for the user in the vault is ignored

PKI CONFIGURATION

1. The final step to enabling PKI requires an update to the **applicationHost.config** file
2. Update the location path as shown below, then run IISRESET to apply the change

From:

```
<location path="Default Web Site/PasswordVault/auth/pki">
    <system.webServer>
        <security>
            <access sslFlags="Ssl, SslNegotiateCert, SslRequireCert" />
        </security>
    </system.webServer>
</location>
```

To:

```
<location path="Default Web Site/PasswordVault/api/auth/pki/logon">
    <system.webServer>
        <security>
            <access sslFlags="Ssl, SslNegotiateCert, SslRequireCert" />
        </security>
    </system.webServer>
</location>
```

CYBERARK

RSA SECURID

ORACLE SSO

SAML

GOOGLE AUTH

AMAZON COGNITO

RSA SECURID

- RSA SecurID authentication uses a token, either hardware (key fob) or software (soft token), which generates an authentication code at fixed intervals.
- RSA SecureID can provide native 2FA to the PVWA

Prerequisites**:**

- Install and configure RSA Web Agent on PVWA server.
- Enable RSA authentication in PVWA

ORACLE SSO

- Oracle SSO Authentication enables PVWA users to authenticate to the Vault using SSO with the same identity they use across the enterprise.

Prerequisites:

- Install and Configure OracleSSO on the PVWA Server.
- Enable OracleSSO Authentication in PVWA

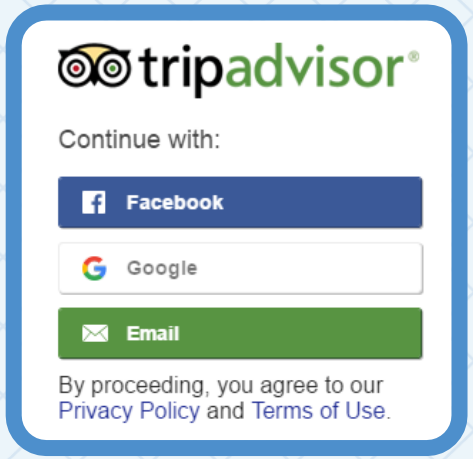
ORACLE
Identity Management

SAML

- SAML authentication enables PVWA users to benefit from an SSO workflow across multiple domains.
- Services are provided by the Identity Provider (IdP).
  - The IdP handles authentication via its login page.
  - Authentication occurs at the IdP (not the Vault).

Prerequisites:

- Enable SAML auth in the PVWA → Options → Authentication Methods → SAML
- Add BaseURL to AllowedReferrer in Options → Access Restrictions
- Edit saml.config found in \Inetpub\wwwroot\PasswordVault
- More information can be found online at Configure SAML authentication in PAM



GOOGLE AUTHENTICATION

- Google authentication enables users to authenticate to the Vault with a predefined Google account, according to the organizational policy
- Services are provided by Google Identity Platform
  - Uses secure OAuth 2.0

Prerequisites:

- Configure in In Google's Developers Console
- Install Google authentication and configure oauth
- Configure access through the PVWA

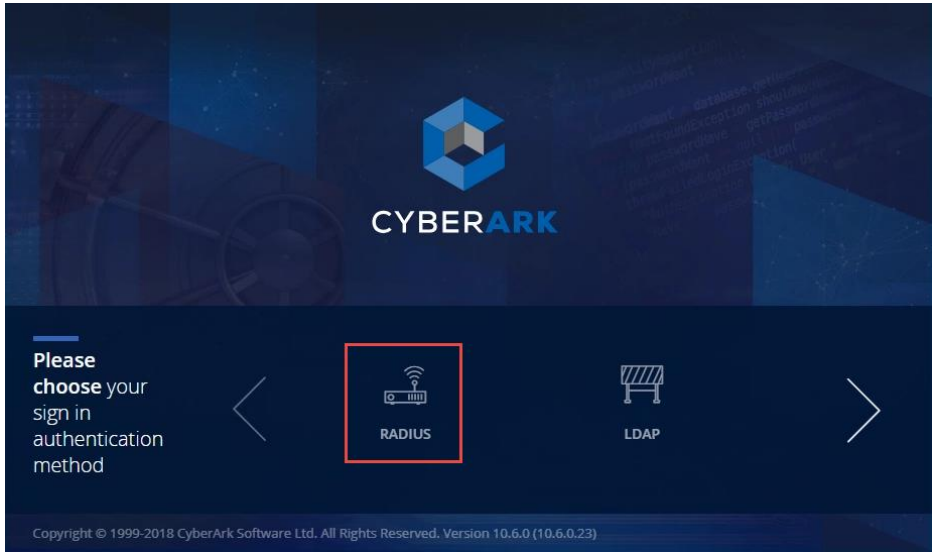
AMAZON COGNITO AUTHENTICATION

- Using Amazon Cognito you can configure multiple IdPs (SAML) for multiple domains
- Amazon Cognito serves as a gateway between the PVWA and the different IdPs by routing the authentication request to the specific IdP based on the user's domain
- Before you configure Amazon Cognito in PVWA you must first configure it in AWS
- Prerequisites:
- Create a user pool in Amazon Cognito
- Configure the IdPs
- Configure Amazon Cognito in PVWA
- See Amazon Cognito Authentication online

TWO FACTOR AUTHENTICATION (2FA)

TWO FACTOR AUTHENTICATION

- **Two-factor authentication** (also known as **2FA**) is a method of confirming a user's claimed identity by utilizing a combination of *two* different components (something a user knows; and something a user has)
- Using two-factor authentication enables you to mitigate common credential theft techniques, such as basic key loggers or more advanced attack tools that are capable of harvesting plaintext passwords
- CyberArk recommends that customers deploy two-factor authentication to the CyberArk Digital Vault, preferably over RADIUS protocol

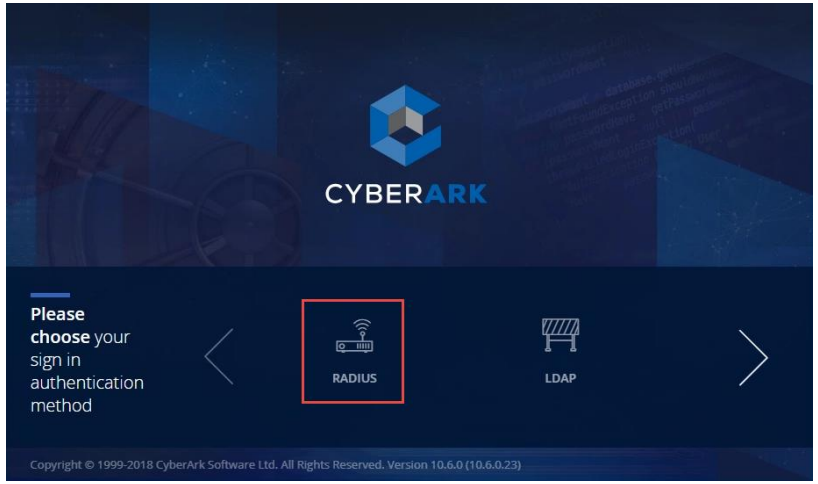


USING 2FA IN CYBERARK

- In the PVWA you can combine ONE PVWA method with ONE Vault Method to create a multi-factor authentication, as shown in the table

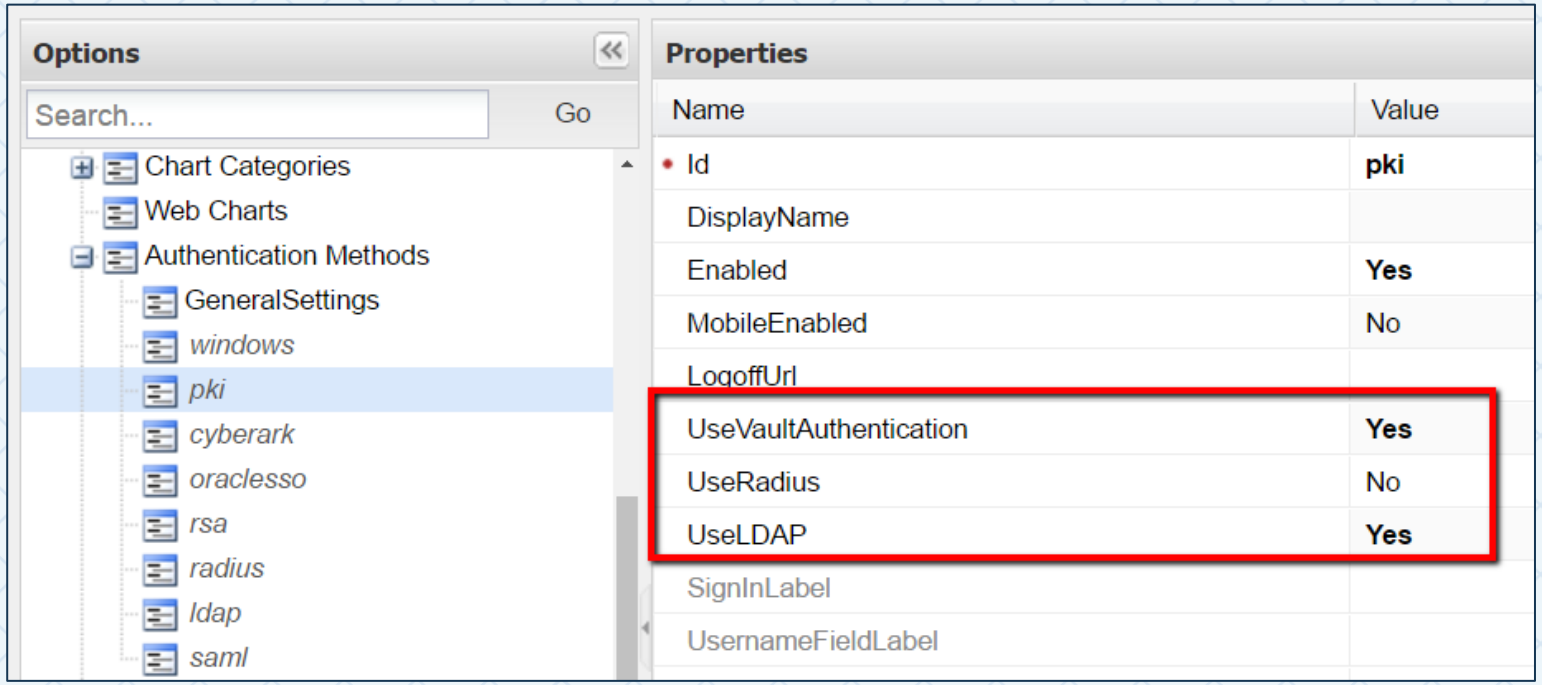
IIS	Vault
PKI (certificate)	LDAP (password)
Windows (password)	RADIUS (token)
RSA (token)	CyberArk (password)

- **RADIUS, SAML** and **RSA secureID** can provide native 2FA without having to combine two authentication methods



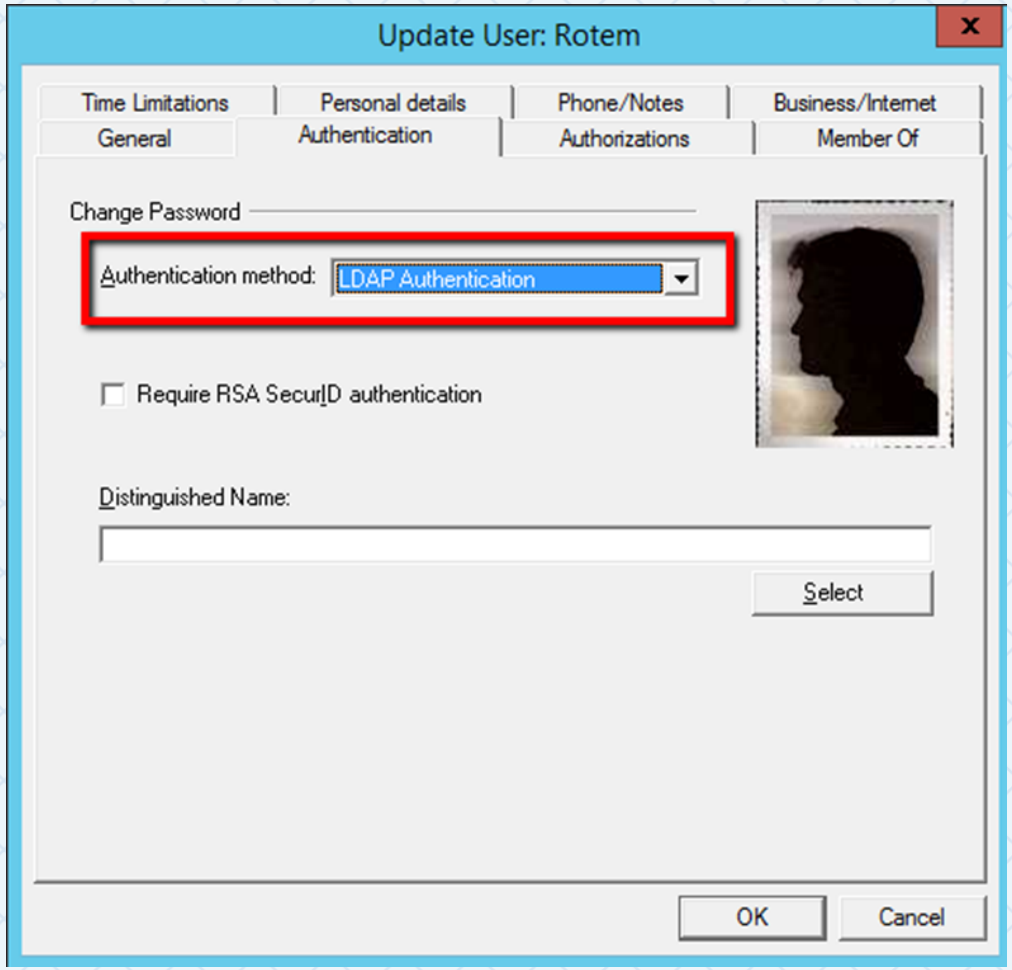
EXAMPLE: PKI + LDAP

Configure PKI as primary authentication method and LDAP as secondary authentication method



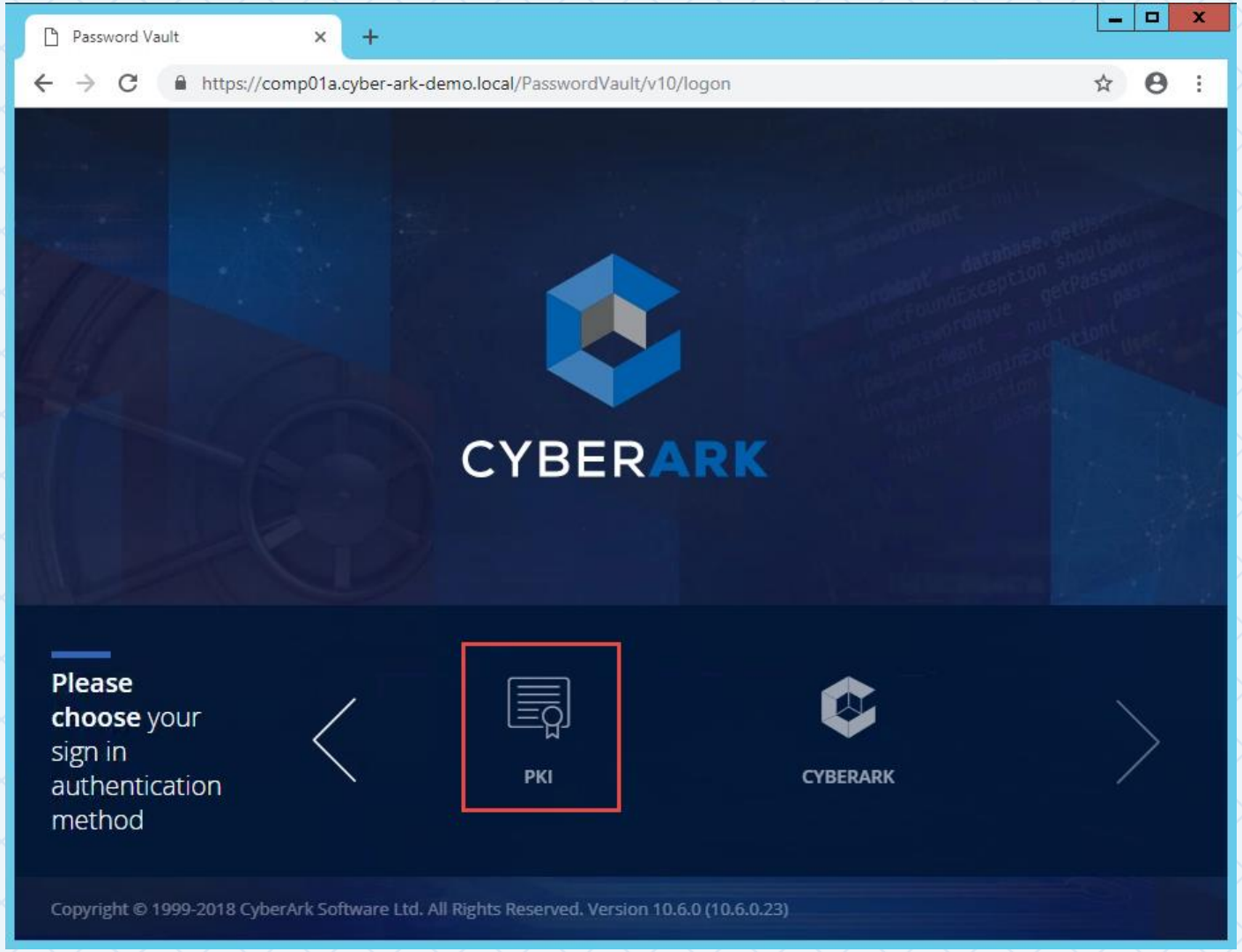
EXAMPLE: PKI + LDAP

- Set the user's authentication method as LDAP



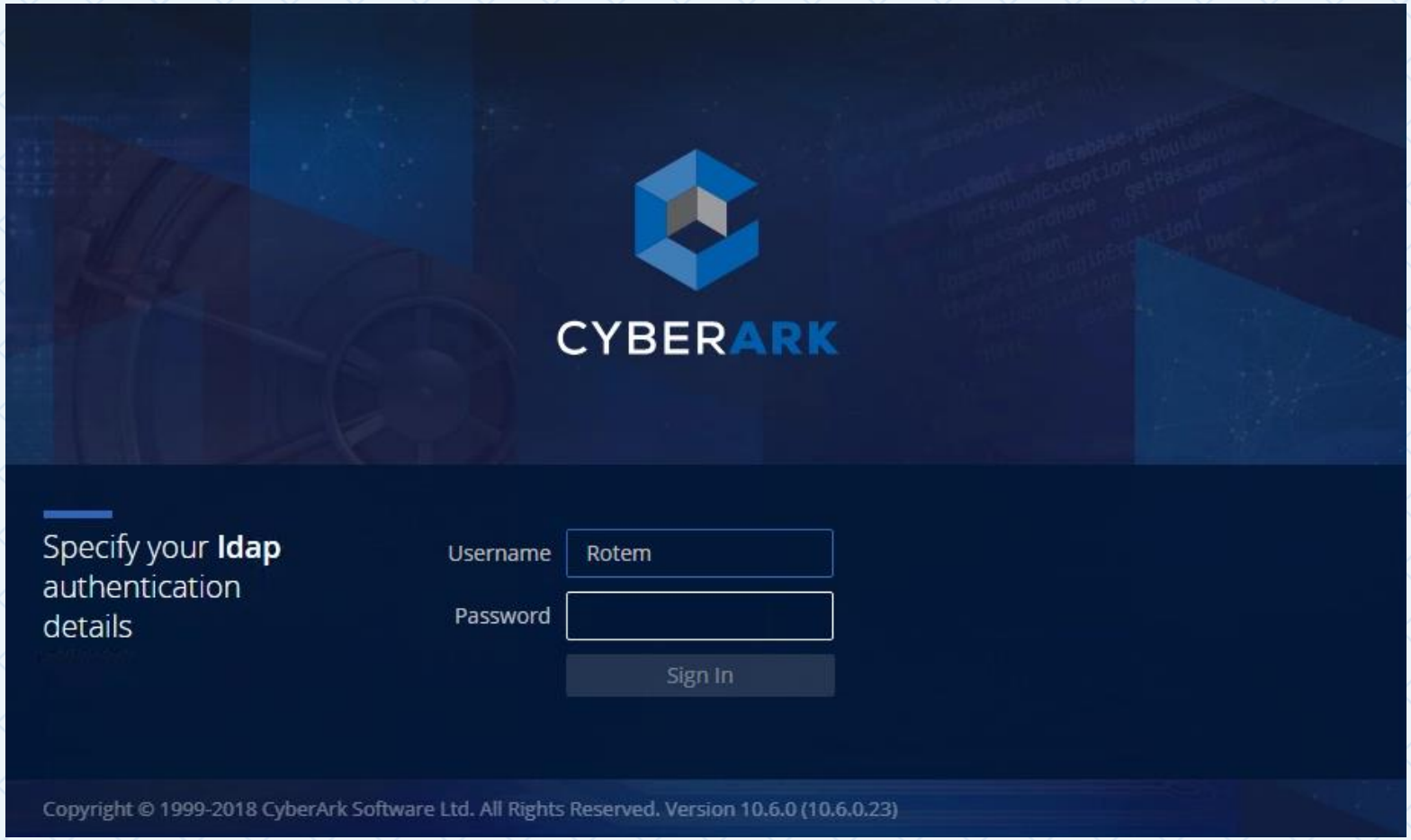
EXAMPLE: PKI + LDAP

- User chooses “PKI” as the authentication method



EXAMPLE: PKI + LDAP

- After IIS authenticates the user based on the user's personal certificate, the user is also prompted for their LDAP password
- See "Configure a secondary authentication method" online at docs.cyberark.com



SUMMARY

SUMMARY

This session has covered:

- The various authentication methods supported by CyberArk
- How two factor authentication works in CyberArk
- Integration of CyberArk with external Authentication systems

THANK YOU