EZIDENTITY MULTIFACTOR AUTHENTICATION

CYBERARK EZIDENTITY AUTHENTICATION INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: *EZMCOM Inc*.

Website: *www.ezmcom.com*

Name of Product: *EZMCOM EzIdentity™ Authentication Platform v3.1*

Version: *v1.00.00*

Date: 15-02-2017

TABLE OF CONTENTS

EZMCOM SOLUTION OVERVIEW

EZMCOM is a security access provider for innovative and easy-to-use technology that can be deployed to protect users, data, and applications from credential theft, account takeover and breaches. EZMCOM is working with companies worldwide to change the way we authenticate and authorize – across mobile

devices, servers, workstations within enterprise and cloud services. With over 50 million+ end users protected, EZMCOM's multilayer multi-factor "Common Criteria" and "FIDO-compliant Mobile SDKs" identity protection solution profiles online identities, self learns, tunes itself, and converts existing username and passwords into very strong credentials. All of this is done seamlessly, in real time, transparent to end-user. The solution comprises of a multi-layer defense-in-depth stack of User Entity Behaviour Analytics (UEBA), Risk based Fusion Biometric Authentication, Risk Based Adaptive Authentication and a comprehensive suite of strong authentication form factors comprising of Software & Hardware based OTP, eSignature Tokens, Software & Hardware PKI Tokens, Out-of-Band OTP Tokens over Text message | E-mail | Voice | Mobile Push notifications.

Few of the detailed collaterals can be found as below:

- EZMCOM's Fusion Biometric Authentication for looking beyond Two Factor authentication
- EZMCOM's Behavioural Authentication for looking beyond Risk Based authentication
- EZMCOM's Risk Based Authentication adding value on top of Two Factor authentication
- EZMCOM's Two Factor Authentication using Mobile device
- EZMCOM's wider range of Two Factor Authentication products (all form factors)

Few quick introductory videos can be found here and here.

KEY BENEFITS

A company's network and critical assets are its backbone of its daily business operations connecting employees, customers and partners from diverse physical locations. Allowing access to essential corporate assets is the core to every business today. EZMCOM's suite of security products provide strong authentication, along with CyberArk privileged access, which abidingly keeps your corporate assets safe from prowling intruders trying to access your critical corporate resources and data. EZMCOMS's Multifactor authentication services use a variety of factors of authentication to validate the end users. The primary factor being a username and password and a secondary which can be an Out-Of-Band token, SMS/Email/IVR, Desktop or Device App generated token.

For the first time, we are introducing powerful user convenient secure Ezmcom's User Behavior Analytics (UBA) and Fusion Biometric protected authentication on CyberArk.

Some of the key benefits of the solution can be summarized as below:

1. Direct integration with Cyberark so no multiple redirects etc.
2. User Behavior Analytics reports and Rule Based Authentication system, that can be configured how stringent or flexible as per client's network environment and requirement.
3. Ability to protect Mobile Soft Tokens with PIN, Biometric (TouchID, Face or Voice) and Behavioral (PIN based behavior) Authentication.
4. Support of various form factors such as Hardware Tokens, Out of Band, Soft Tokens, Desktop Tokens Display Cards etc.
5. Comprehensive Auditing for all Authentications.
6. Maker-Checker Module for Key administrative activities on the EzIdentity™ Management Portal.
7. "Common Criteria" Certified Authentication Platform.

PRODUCT DIAGRAM AND INTEGRATION DESCRIPTION

CyberArk Enterprise Password Vault®, part of the CyberArk Privileged Account Security Solution, enables organizations to secure, manage and track the use of privileged credentials, whether on-premise or in the cloud, across operating systems, databases, applications, hypervisors, network devices, and more.

This document describes:

1. How Ezmcom Ezidentity native integration with Cyberark would work?
2. How UBA plays its role in authenticating a user and how it is convenient and yet secure way to authenticate?
3. And How to configure this integration for this Cyberark setup?

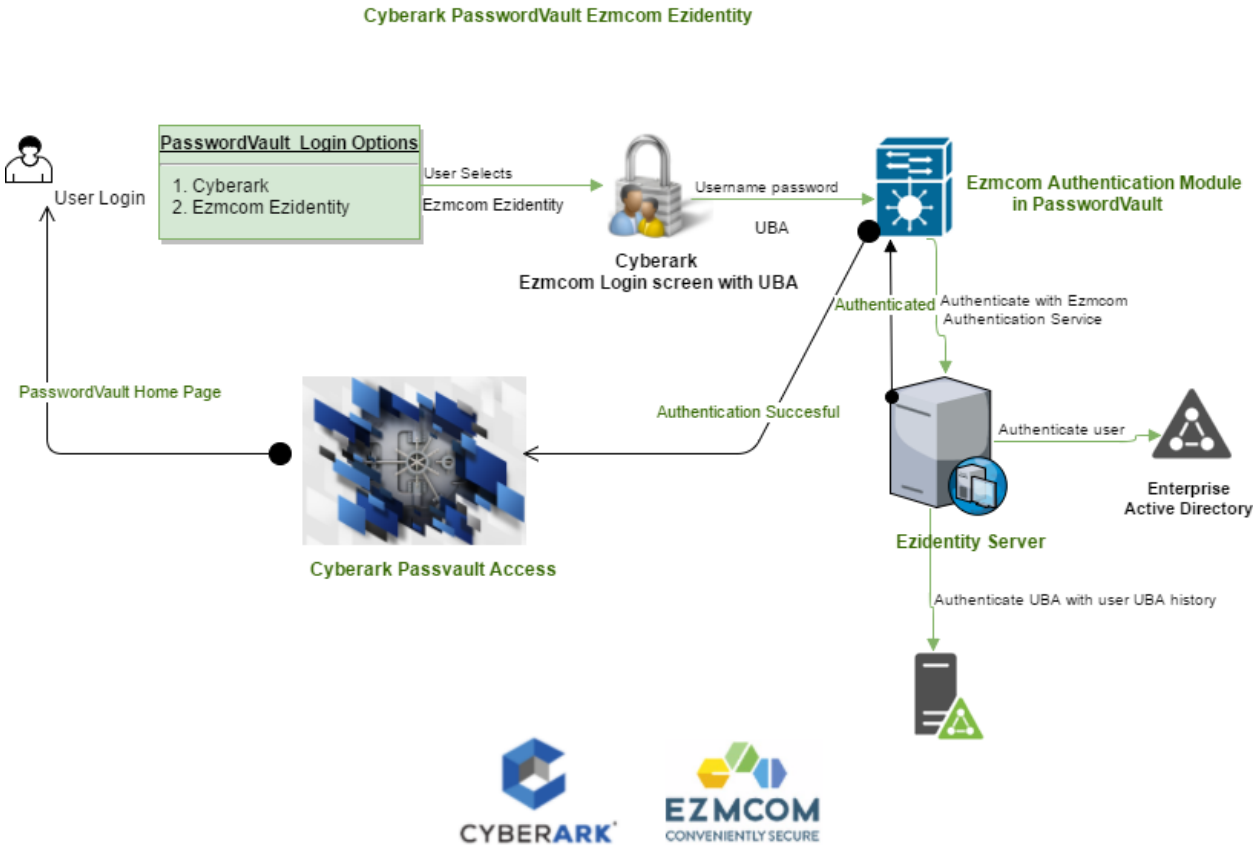
It is assumed that the CyberArk Privileged Account Security Suite environment is already configured and working with static passwords prior to implementing Ezmcom multi-factor Authentication Solution.

EZMCOM EZIDENTITY NATIVE INTEGRATION

CyberArk Privileged Account Security Suite can be configured to support Ezmcom MFA with UBA and RBA.

Below Figure 1 illustrates a high-level deployment architecture of CyberArk Account Security Suite with EzIdentity™ AS

Figure 1: High level integration architecture for EzIdentity™ AS with CyberArk.



The Flow diagram can be summarized as below:

1. Once user open CyberArk Vault Manager (Password Vault Web Access), user will get options to select authentication options based on Cyberark authentication configuration.
2. To choose EZMCOM Ezidentity authentication, Cyberark administrator must enable EZMCOM Ezidentity as one of the or default authentication option (after this setup).
3. Once user chooses EZMCOM Ezidentity option, user will see Cyberark EZMCOM authentication page for login.
4. After user types in username and password, EZMCOM authentication module will get a chance to authenticate username password through Ezidentity server which uses client's active directory server for authentication.
5. Once the Active Directory authentication is successful then Ezidentity server will also inspect User Behavioral information. And Rule based authentication will kick in.
6. If Ezidentity finds any anomaly in request like different typing pattern of user or user is using new machine to login, then user will get EZCOM MFA page for extra layer of authentication.
7. Once MFA is successful or User Behavior did not have any anomaly then user will be allowed to

go to Cyberark Password Vault Web Access home page.

8. The above diagram does not provide full information about user's behavior history building flow but in that case user will be presented with MFA page each time until Ezidentity has full information about user's behavior (e.g. typing pattern, user browser information etc.).
9. For more information about User Behavioral Analytics and Risk based Authentication please visit:- https://www.ezmcom.com/

EZIDENTITY™ INSTALLATION

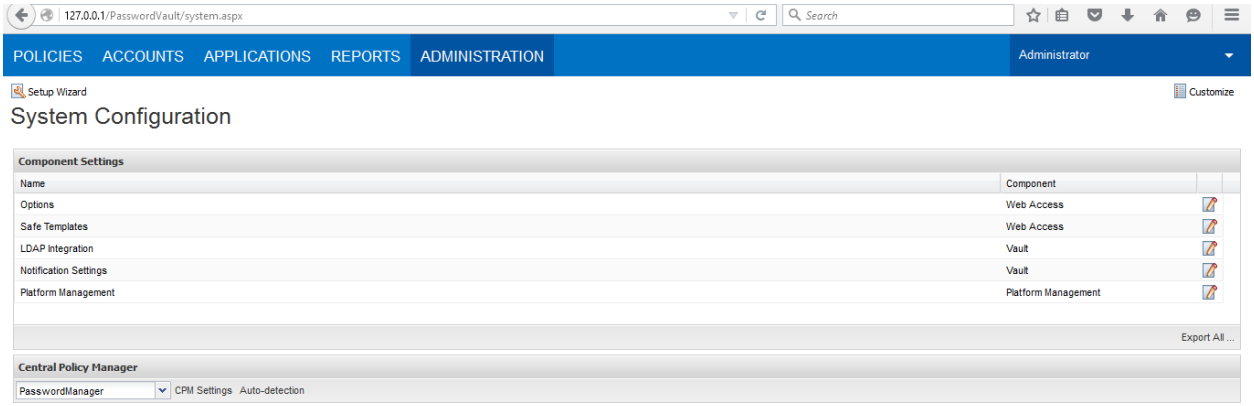
Please refer to the below documentations for EzIdentity Installation:

1. EzIdentityTM Deployment Prerequisites
2. EzIdentityTM Authentication Server Quick Start Guide

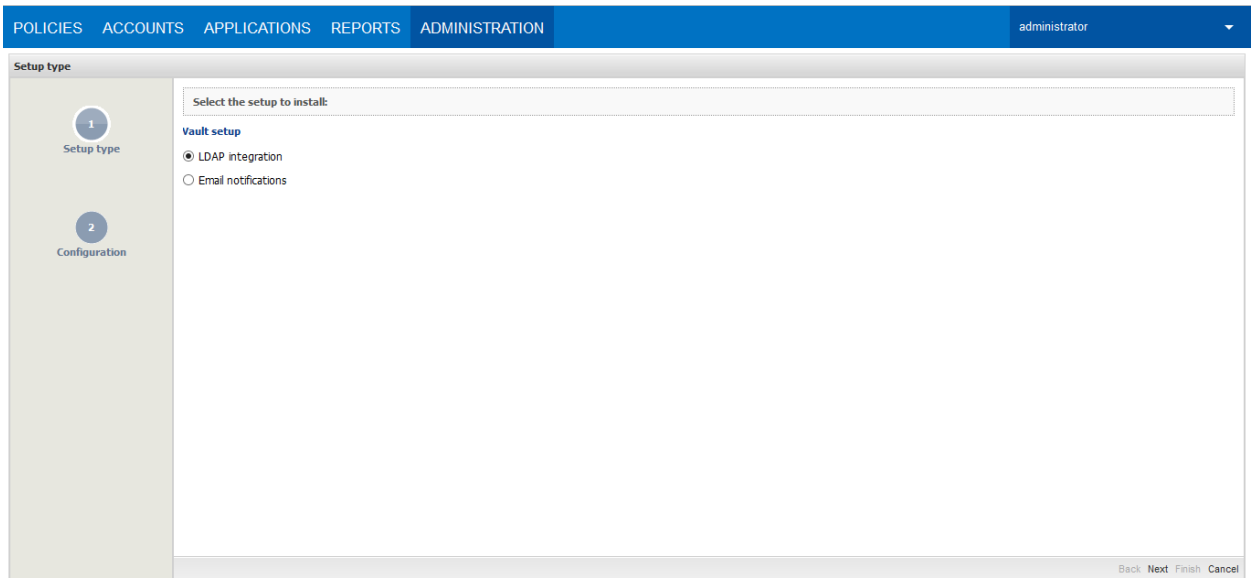
CYBERARK INTEGRATION

LDAP CONFIGURATION

This step is optional and can be skipped in case the LDAP has, already, been integrated.

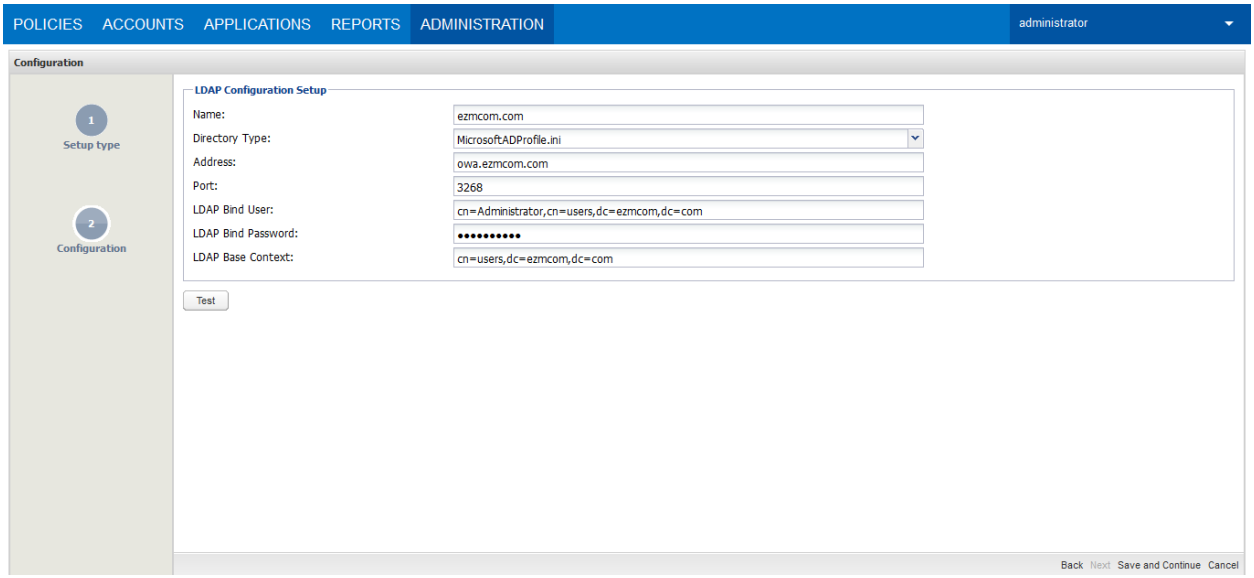


1. Log into the CyberArk Password Vault Web Access, and select **Setup Wizard** under **Administration.**

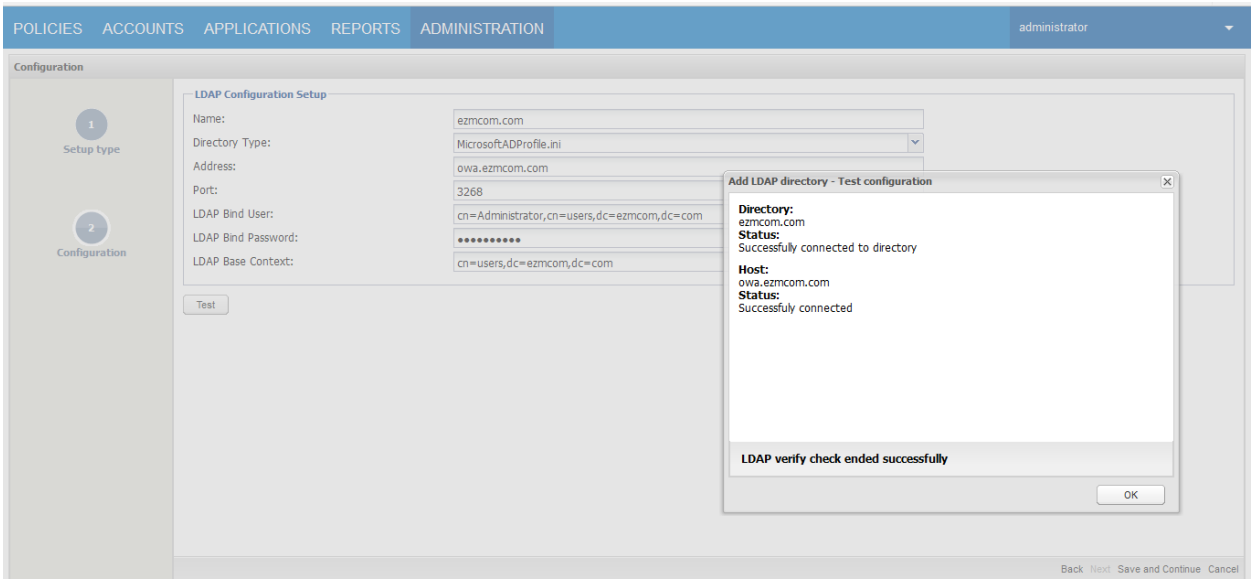


2. Select **LDAP Integration** under **Vault** setup and click **Next**

3. Fill in LDAP configurations

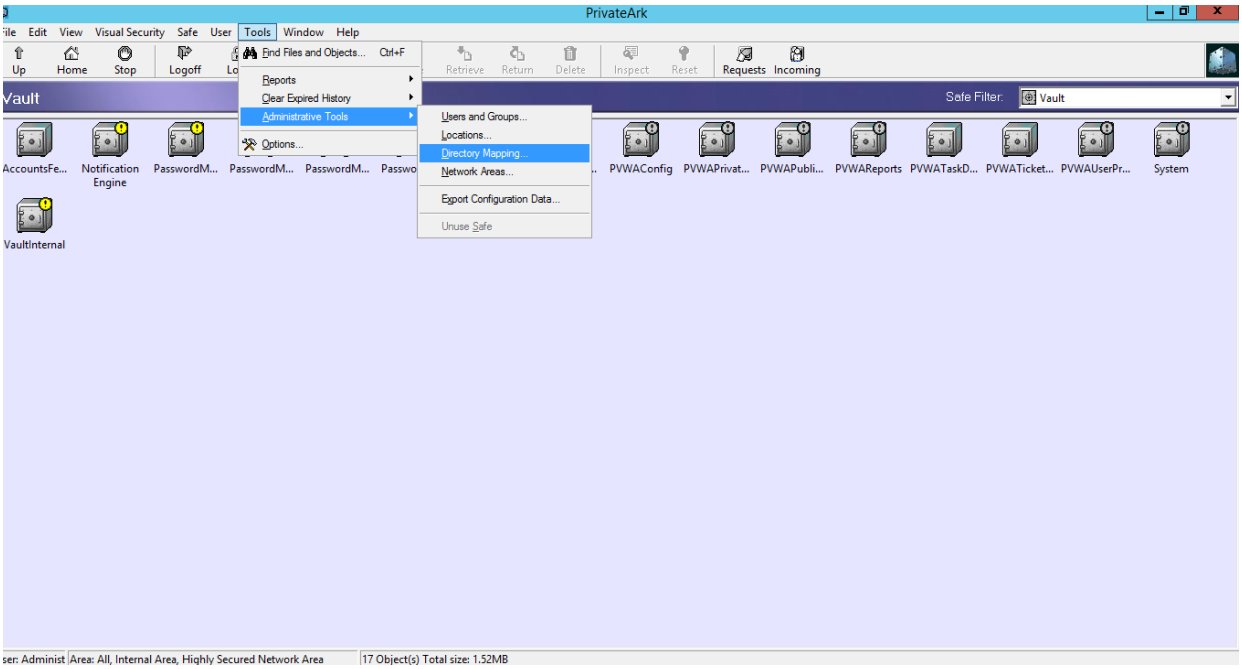


3. Click **Save and Continue**

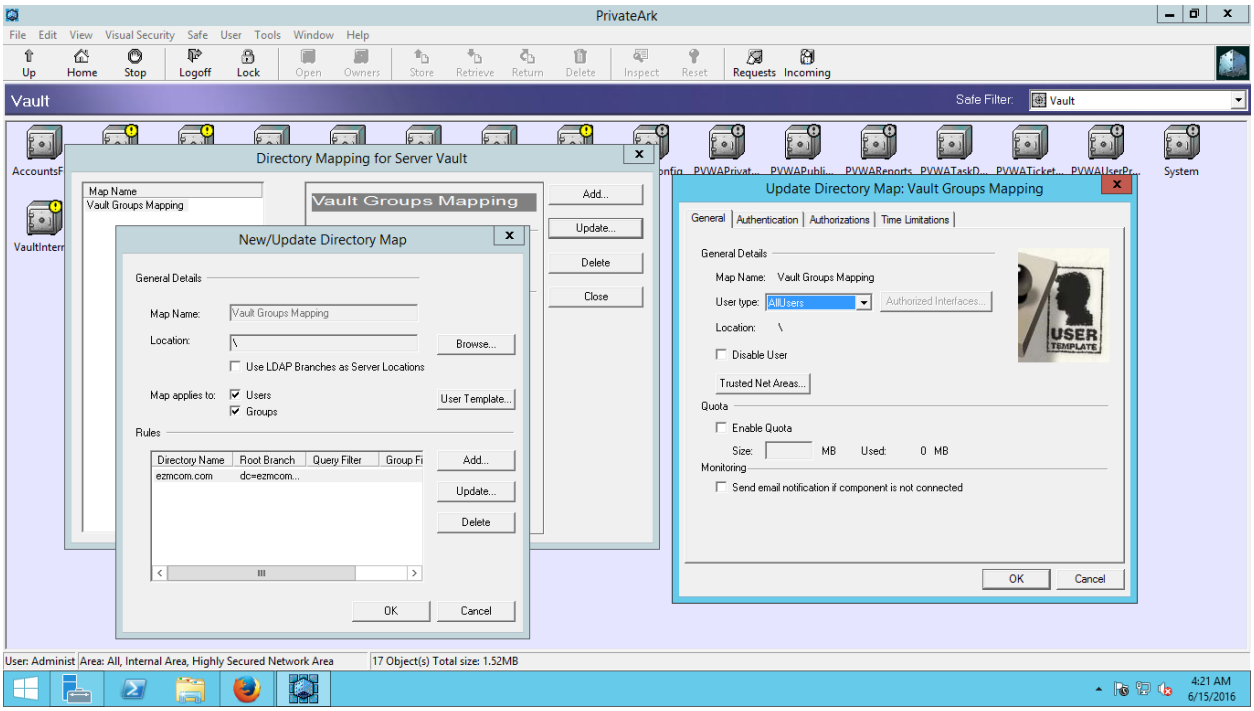


4. **If LDAP verify check ended successfully. Then, Click Finish.** You can view the configuration again under LDAP integration**.**

On the PrivateArk Client:



5. Map the LDAP configuration in PrivateArk**. Login into PrivateArk > Tools > Administrative Tools > Directory Mapping.**



1. Under Directory Mapping, configure the ldap appropriately to match the ldap server. **Click Update > Update Directory Mapping > Configure Vault Groups Mapping.**

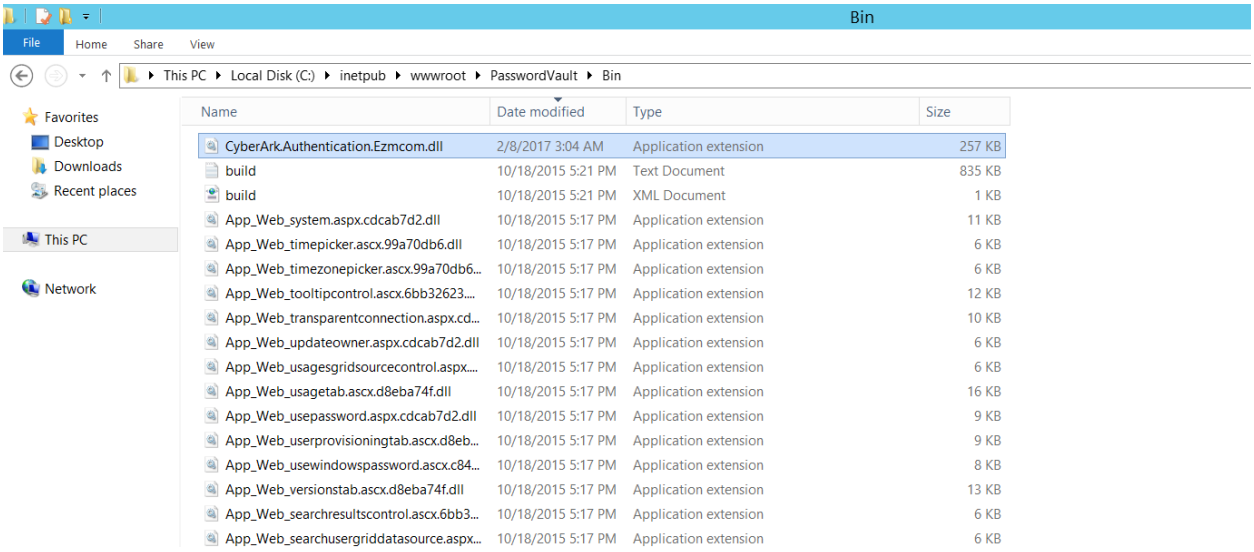
ENABLE EZMCOM EZIDENTITY AUTHENTICATION

Configuration Assumption:

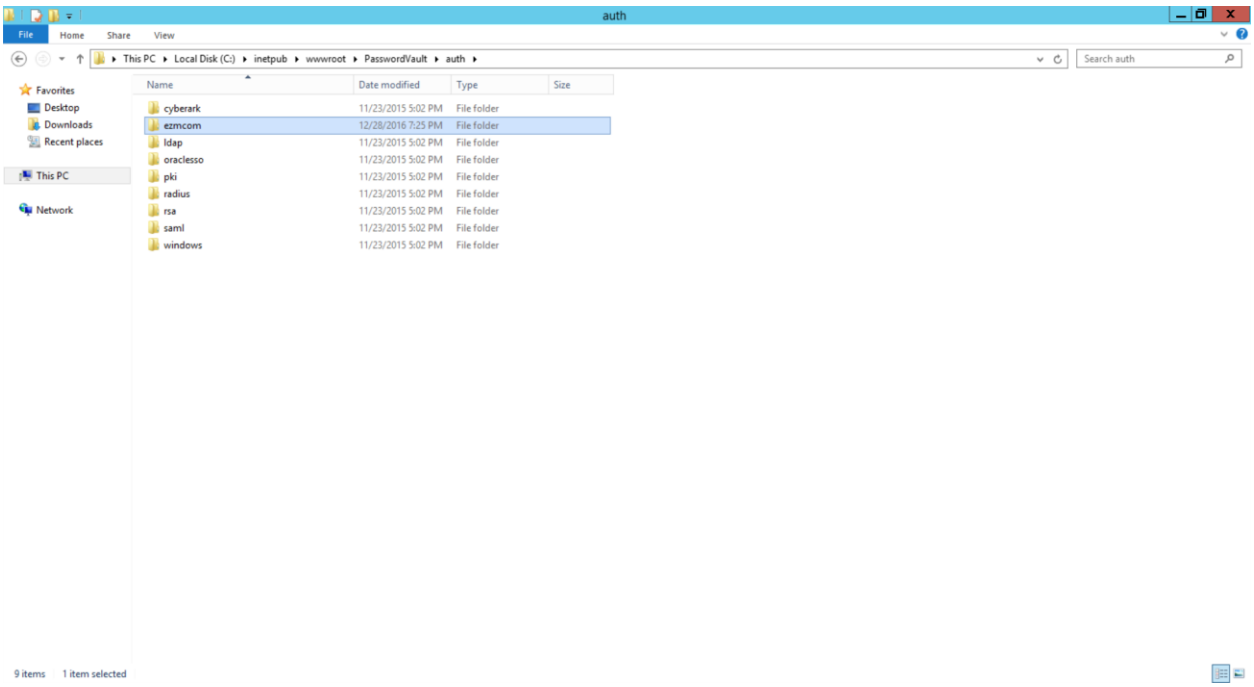
1. Location where PasswordVault Web Manager application is installed at "**C:\inetpub\wwwroot\PasswordVault\auth**" with the name PasswordVault. Change this path as per where your PaswordVault Web Manager(PVWA) application is installed.
2. User has administrative privileges on the PVWA machines and PVWA application as well.

Configuration Steps: -

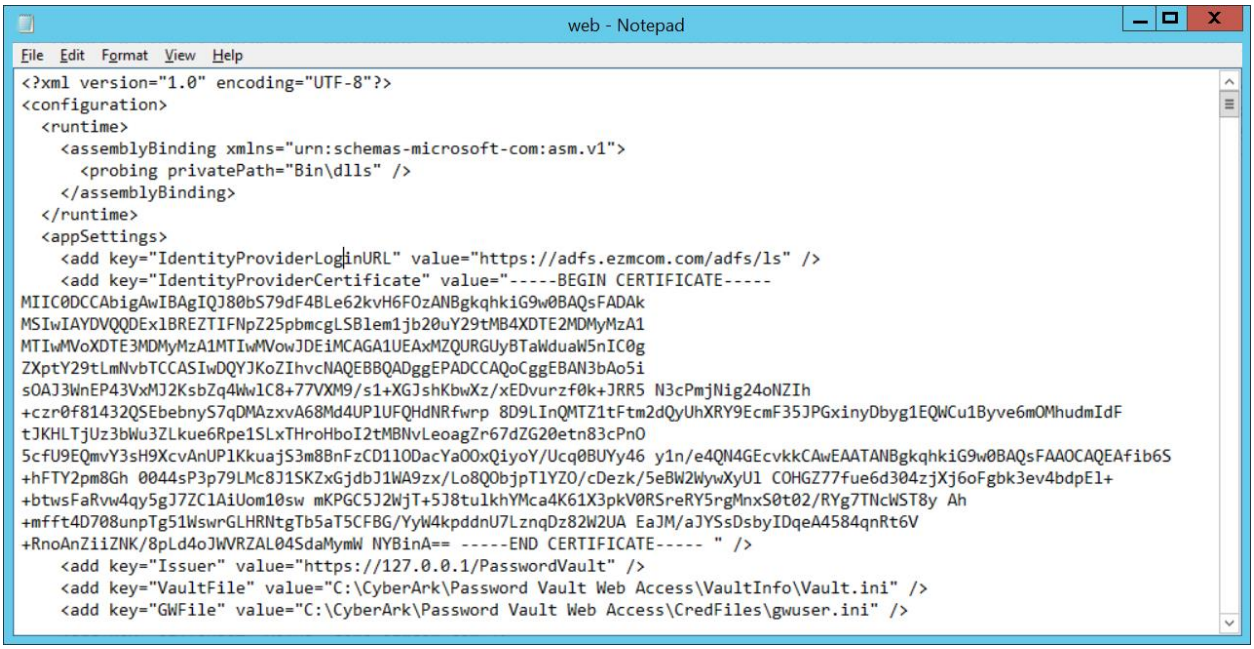
1. Copy "CyberArk.Authentication.Ezmcom.dll" (provided in Ezmcom package) in bin folder of PasswordVault Web Manager application. By default, it is present in IIS "inetpub" folder.



2. Open Auth folder of PasswordVault application by default it should be at "**C:\inetpub\wwwroot\PasswordVault\auth**". Copy "**ezmcom**" folder given with the Ezmcom package inside this folder.



3. Open "web.config" file from the same application folder "C:\inetpub\wwwroot\PasswordVault\"



4. And paste following configuration key and values in the file inside "<appSettings>" xml node-

There are 10 app settings that need to be carefully configured in the web.config file. This setting will look like –

```
    <add key="ezmcomdomainsamlid"
value="XXXXXXXXXXX4AC4E2D6B9XXXX45567XX"/>
    <add key="ezmcomhost" value="cyberarkdemo.xxxx.com"/>
    <add key="ezmcombypass" value="0"/>
    <add key="ezmcomgid" value="xx"/>
    <add key="ezmcom1faHost" value=" cyberarkdemo.xxxx.com"/>
    <add key="ezmcomubahost" value=" cyberarkdemo.xxxx.com"/>
    <add key="ezmcomrbahost" value=" cyberarkdemo.xxxx.com"/>
    <add key="ezmcomapplicationname" value="/passwordvault"/>
    <add key="ezmcomubaapikey" value="xxxxxx-6596-xxxx-af0f-xxxxxc7cd87e"/>
    <add key="ezmcomdisableuba" value="0"/>
```

Value for “**ezmcomapplicationname**” key would be name of the PaswordVault Web Manager in IIS. In above example, it is “passwordvault”. In configuration Add “/” in front of this name.

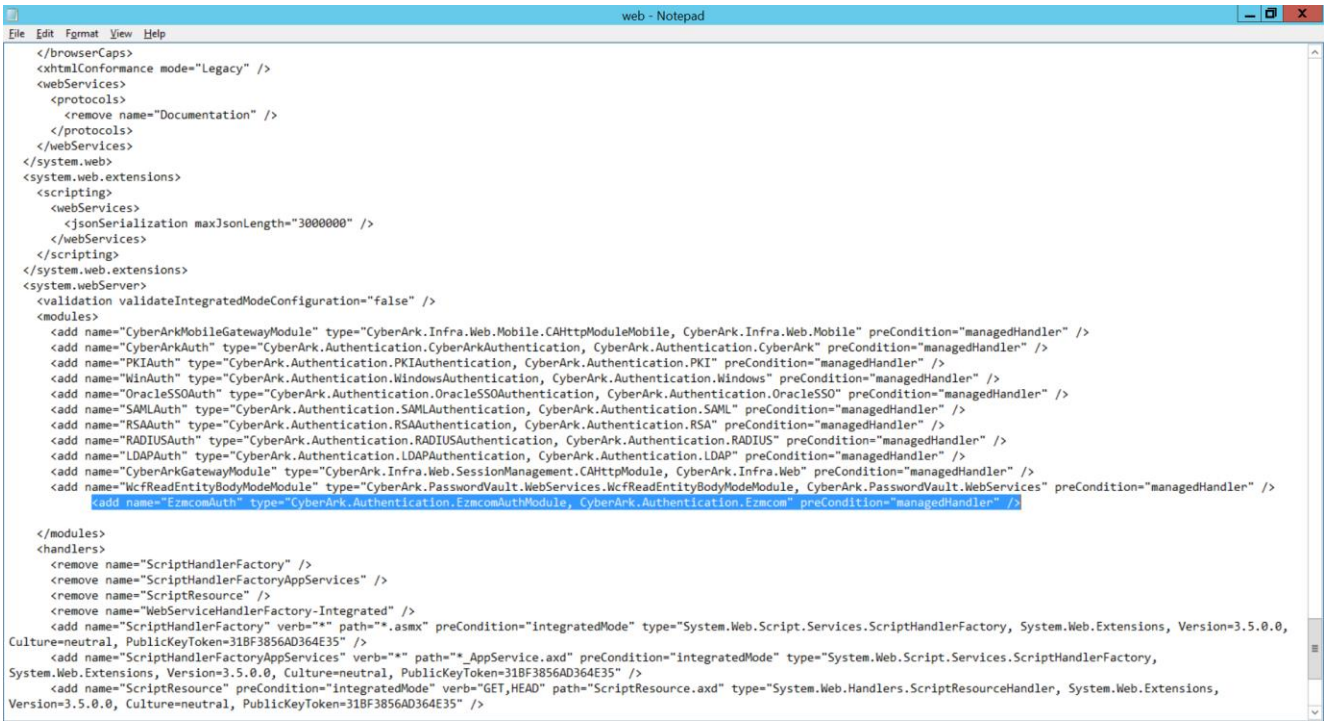
Note: For all these configuration values, contact Ezmcom support team or Ezmcom partner in your region. They will be happy to assist you for this configuration, based on your server and deployment.

5. After adding appSetting configuration, you will need to add Ezmcom Authentication module configuration in Web.config.
   This setting will go inside "<modules>" section of web.config file under "<system.webServer>"

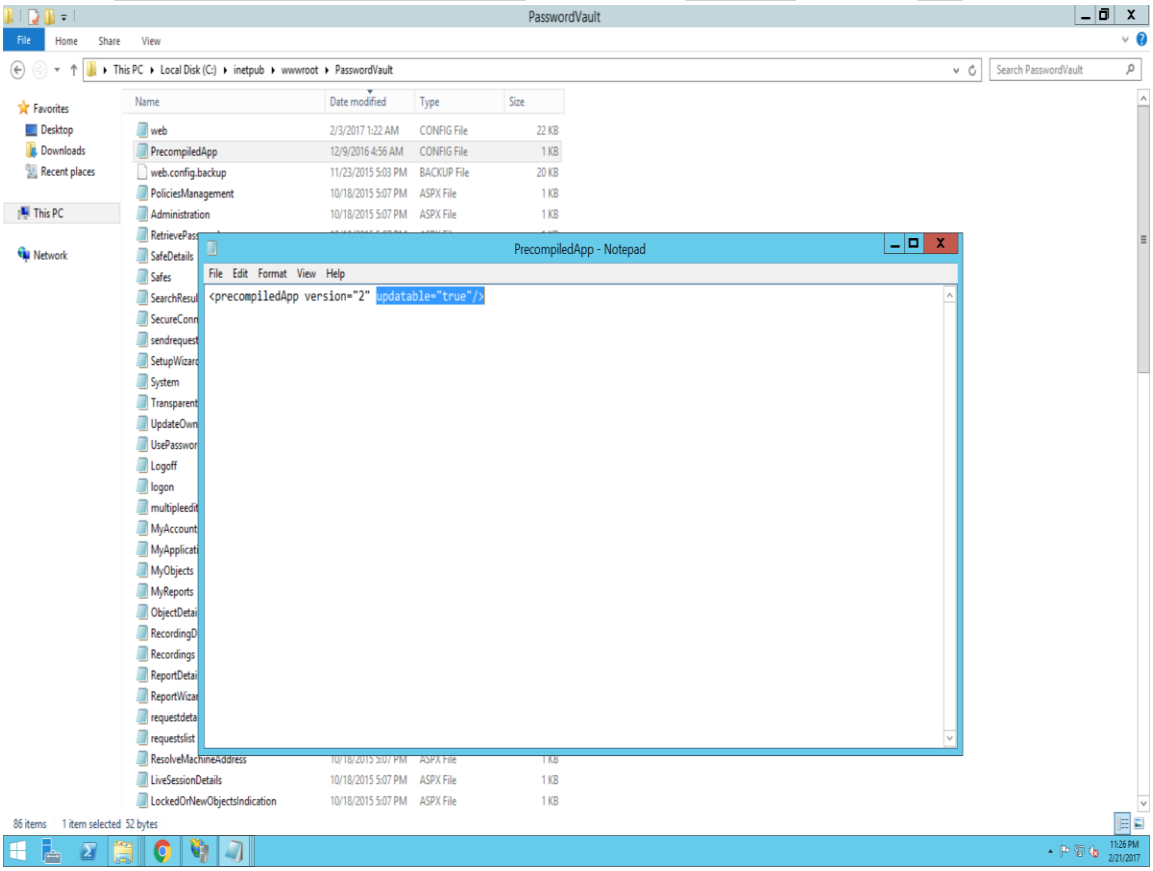
   Setting is-

```
<add name="EzmcomAuth"
type="CyberArk.Authentication.EzmcomAuthModule,
CyberArk.Authentication.Ezmcom" preCondition="managedHandler" />
```

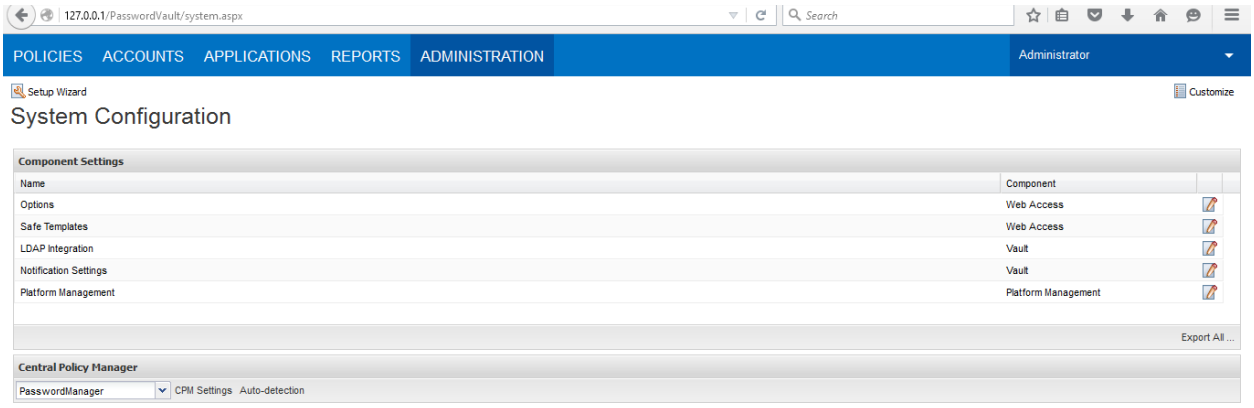
   Below screenshot should give an idea about its location in web.config.



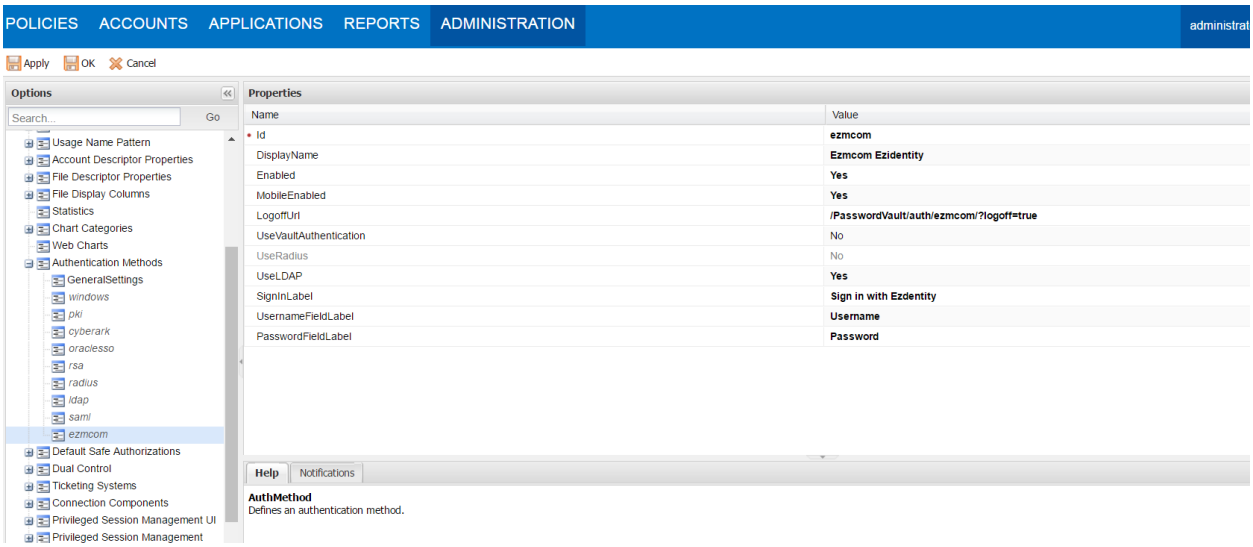
6. Now open “PrecompiledApp.config” file from same application folder location which is in our case at location: “C:\inetpub\wwwroot\PasswordVault\” and change “updatable” value to “true”.



7. After completing all the previous steps from 1 to 6,
Log into the CyberArk Password Vault Web Access with administrator role, and select **Options** under **Administration**



2. Select **ezmcom** under **Authentication Methods**



3. Select **Yes** from the **Enabled** options to enable "ezmcom"

4. Click **Apply**

5. Other Values for this configuration will be as per the screenshot-

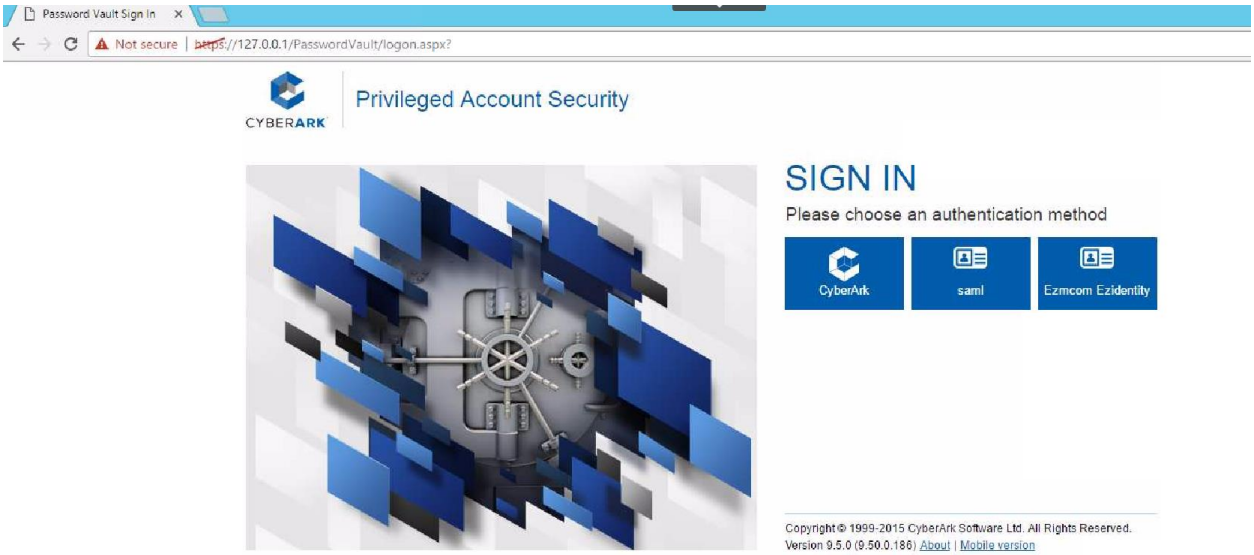
Id: ezmcom
Display Name: Ezmcom Ezidentity
Enabled: Yes
Mobile Enabled: Yes
LogoffUrl: /PasswordVault/auth/ezmcom/?logoff=true
UseVaultAuthentication: No
UseRadius: No
UseLDAP: Yes
SignInLabel: Sign in with Ezdentity
Username field Label: Username
Password Label: Password

After completing all above steps, Password Vault Web Access is all integrated with Ezidentity Authentication, provided Ezidentity server setting is done and completed.

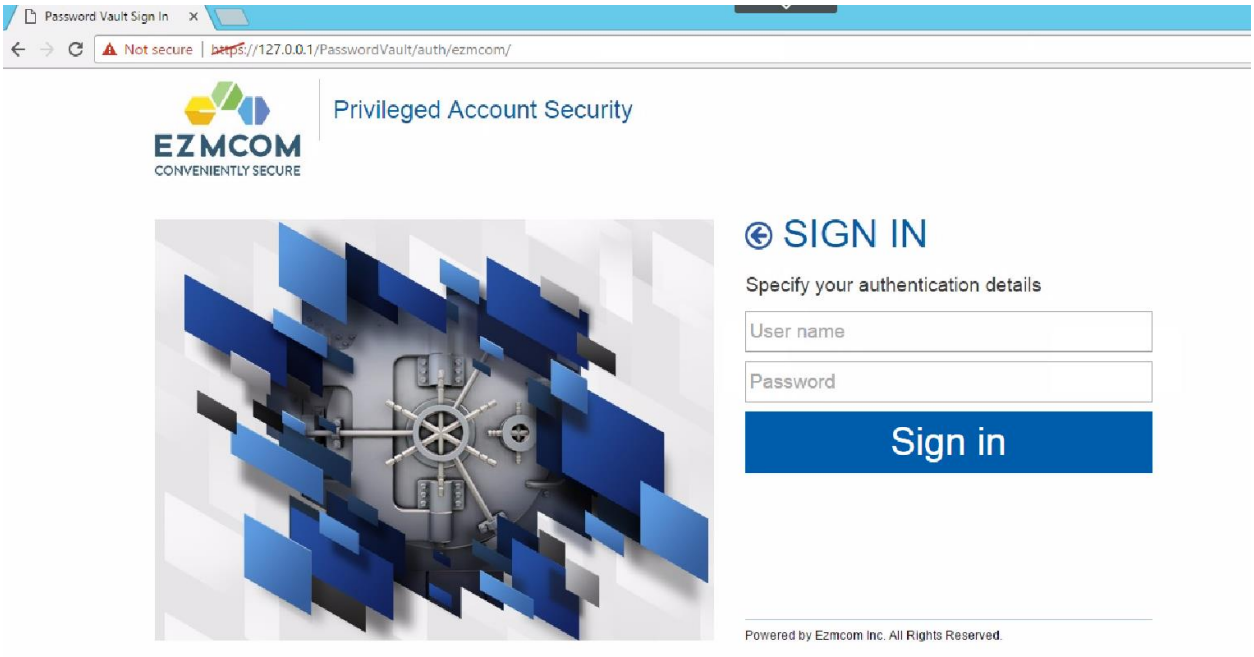
Note: Also make sure to get the Ezidentity server public certificate installed in this Cyberark component server so that the communication between Cyberark Vault Manager with Ezidentity server is secure and runs without any issue.

TESTING EZIDENTITY MFA AUTHENTICATION

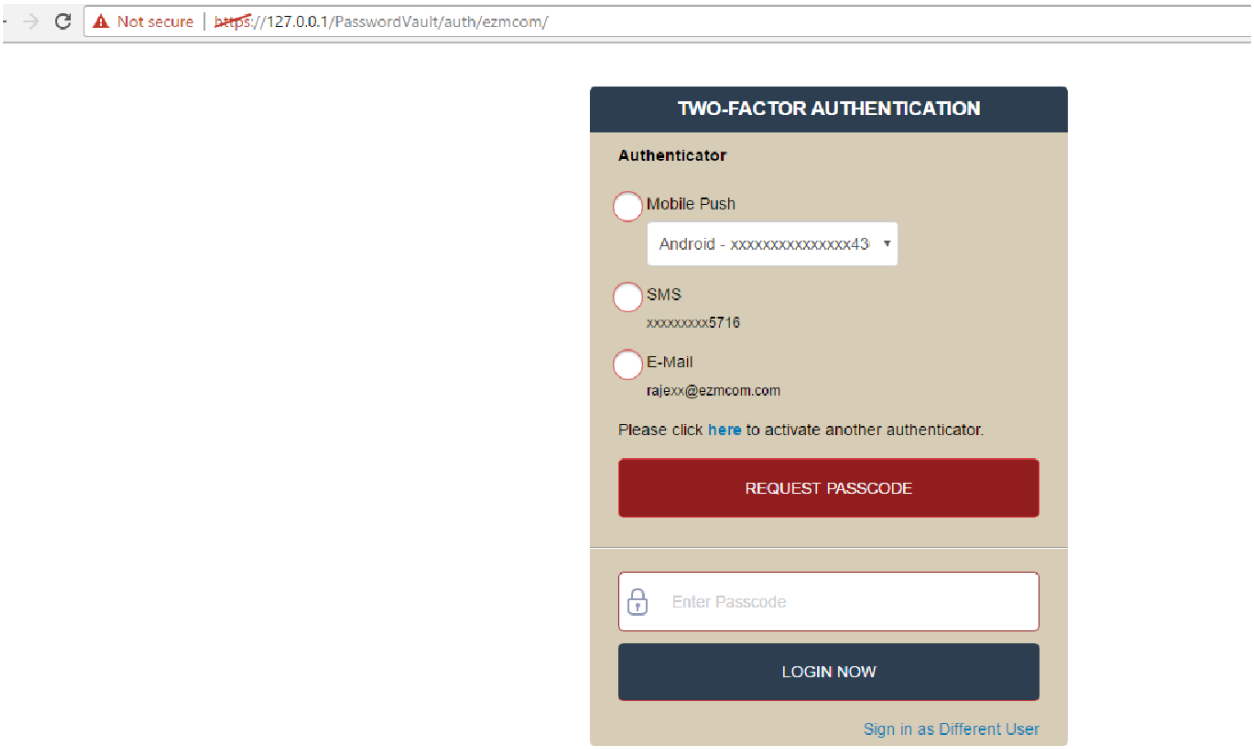
1. Log into the CyberArk Password Vault Web Access, choose Ezmcom Ezidentity as an authentication method.



2. User should see Ezmcom Cyberark primary authentication page.



3. After entering username and password Click **Sign in**

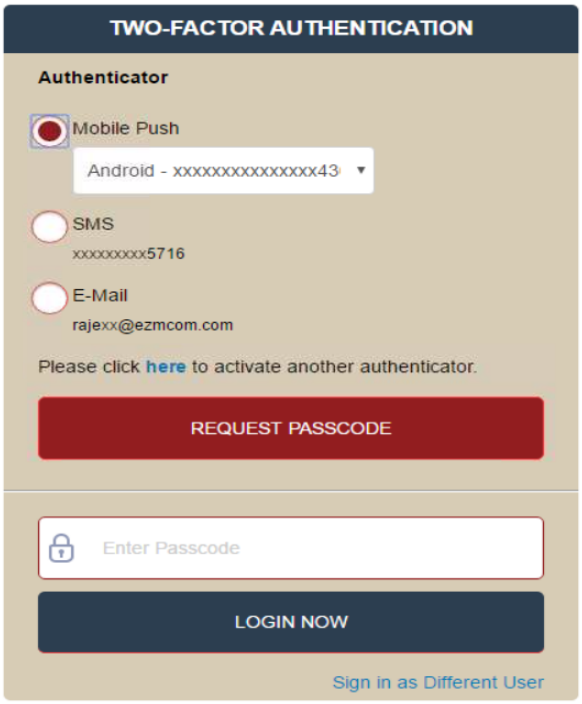


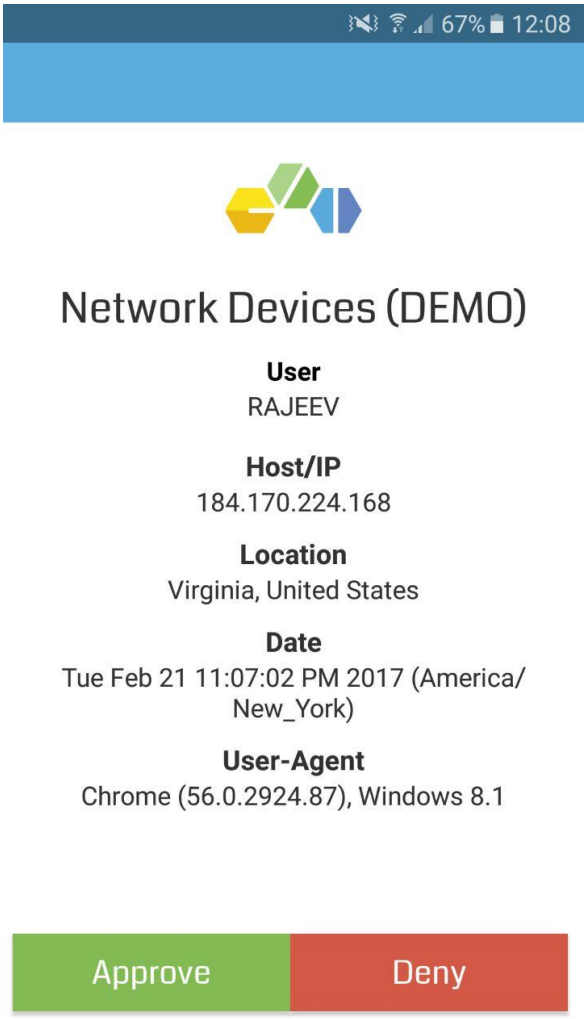
4. User should see Ezidentity MFA options based on soft tokens assigned to the user.

Supported MFA options

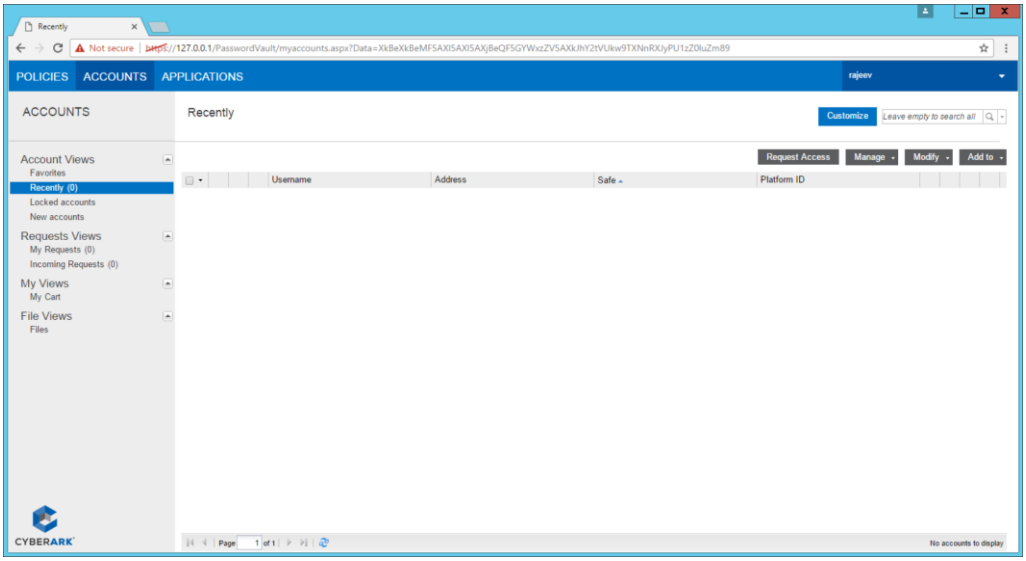
- PUSH based authentication
- Biometric Authentication (TouchID, Face, Voice)
- PIN based Authentication
- Behavioral PIN based Authentication
- OATH-Compliant Hardware Tokens
- SMS OTP
- Email OTP
- IVR OTP
- Both SMS and Email OTP
- Soft Token OTP
- Soft Token OTP, protected by PIN
- Soft Token OTP, protected by Behaviorial PIN
- Soft Token OTP, protected by Biometric Authentication (Face, Voice, TouchID)

5. Most convenient option is Mobile Push. Select mobile push if it is available for login to the user and click Request Passcode.


TWO-FACTOR AUTHENTICATION
Authenticator
Mobile Push
Android - xxxxxxxxxxxxxx43
SMS
xxxxxxxxx5716
E-Mail
rajexx@ezmcom.com
Please click here to activate another authenticator.
REQUEST PASSCODE
Enter Passcode
LOGIN NOW
Sign in as Different User



6. As you can see User should get mobile push notification on the registered mobile phone which has Eztoken app installed.



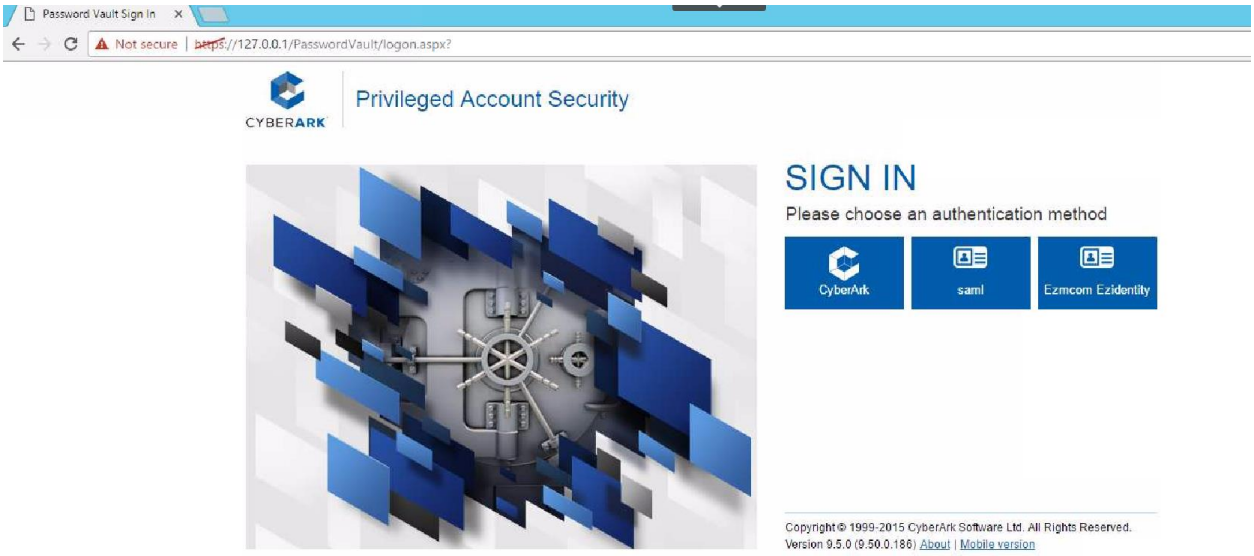
7. On click of Approve in mobile notification, user will get into Cyberark PasswordVault Manager application.

TESTING EZIDENTITY AUTHENTICATION WITH UBA

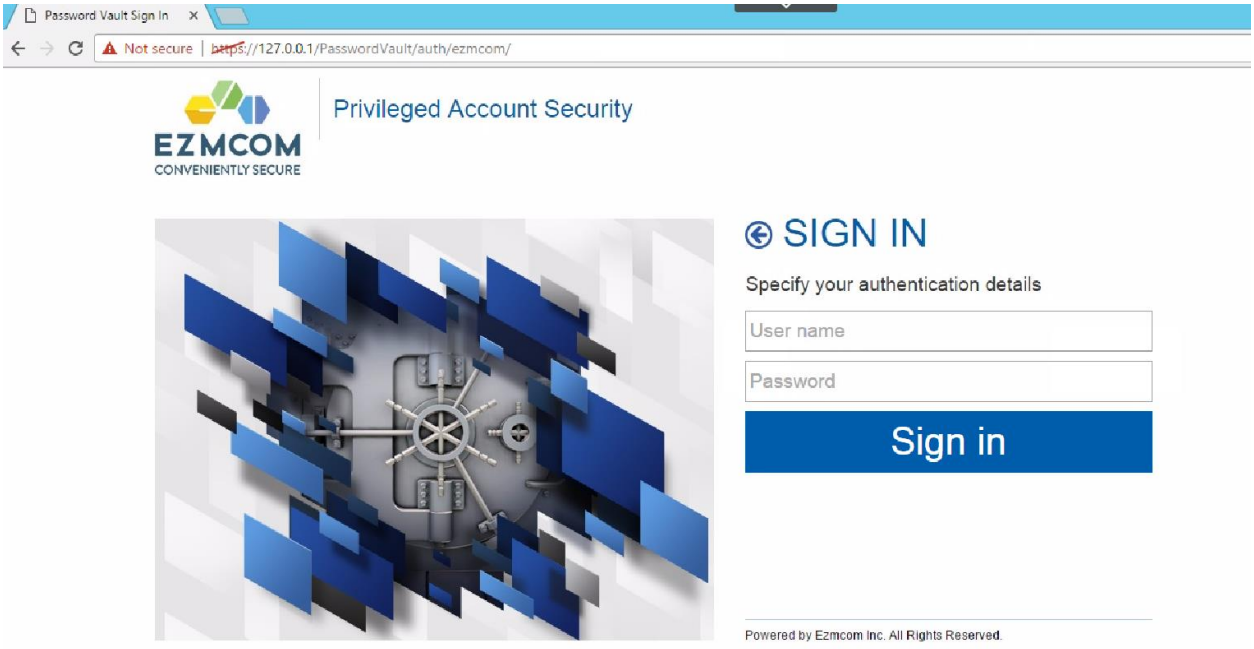
User Based Analytics based Authentication is powerful yet very secure way of authenticating any user to the application.

Most of the steps to test this flow will be same, only thing that would be missing would be MFA page provided user has typed in his password from his usual browser, machine, network etc.

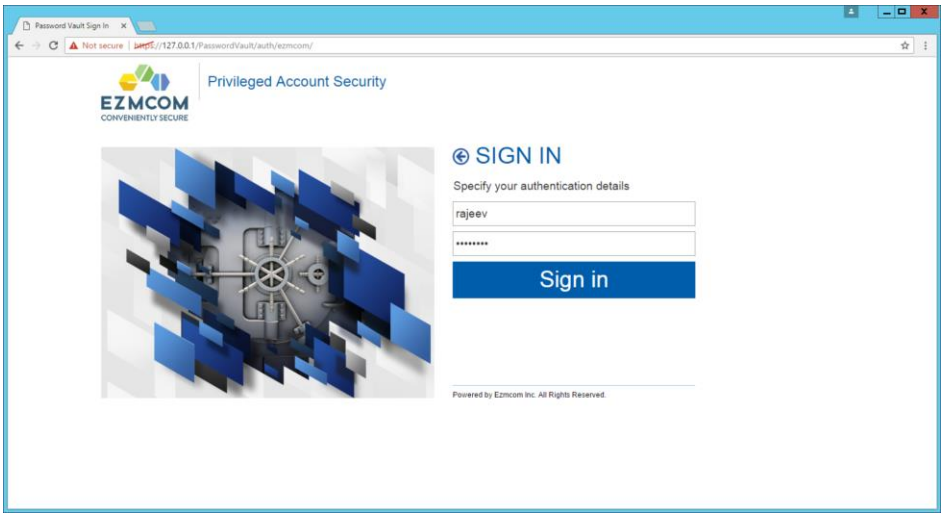
1. Log into the CyberArk Password Vault Web Access, choose Ezmcom Ezidentity as an authentication method.



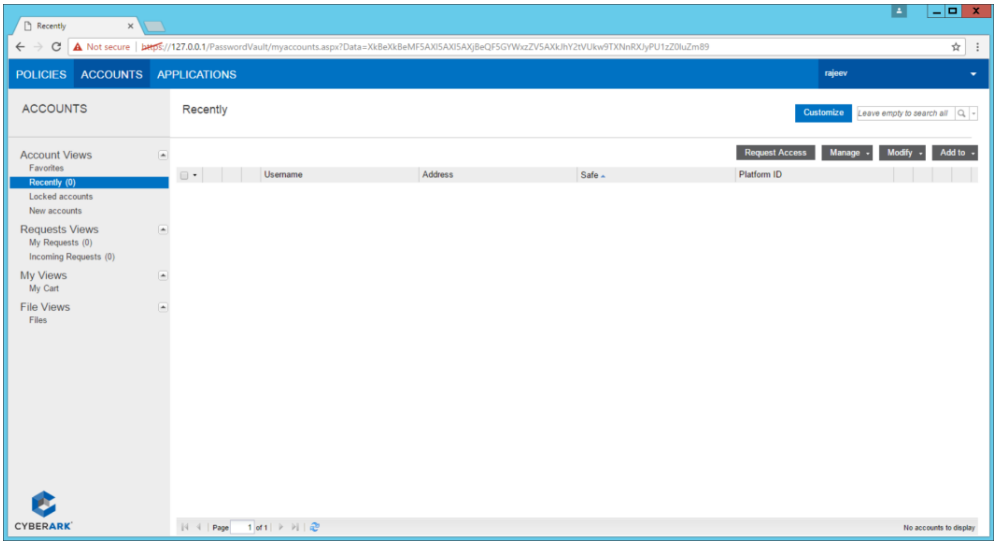
2. User should see Ezmcom Cyberark primary authentication page.



3. if user is in training mode (means until Ezidentity creates its historical information about particular user), user will see MFA page and it should follow previous Ezidentity MFA authentication to login.



4. Once the user types in his password, which is very familiar to him then Ezidentity may assume that the user's training has been completed and may allow the user to login directly to PasswordVault manager application without MFA which is very convenient and yet secure way to allow the user to login.



PARTNER CONTACT INFO

Business Contact	Name	Pravat Mishra
	Email	pravat@ezmcom.com
	Tel	+1 (510) 396 3894
Technical Contact	Name	Rajeev Verma
	Email	rajeev@ezmcom.com
	Tel	+91 (776) 082 5225
Support Contact	Name	Ashish Pati
	Email	support@ezmcom.com
	Tel	+60 (12) 279 1117