



MULTIFACTOR AUTHENTICATION

MFA INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: *EZMCOM Inc.*

Website: *www.ezmcom.com*

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

Version: *v3.22.44 RC30*

Date: *15-09-2016*

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 defence-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. EZMCOM'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 Entity Behavior Analytics (UEBA) and Fusion Biometric protected authentication on CyberArk.

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

1. Integrations can be done through RADIUS and SAML protocols.
2. End User flexibility of choosing the type of authenticator on SAML integration.
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 & DESCRIPTION OF PRODUCT INTEGRATION

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 how to:

1. Deploy Ezmcom's EzIdentity™ multi-factor authentication (MFA) options in CyberArk Privileged Account Security Suite using Multifactor authenticators, including Biometric and Behavioral Authentications.
2. Configure CyberArk Privileged Account Security Suite to work with EZMCOM Multifactor Authentication Solution through RADIUS and SAML protocols.

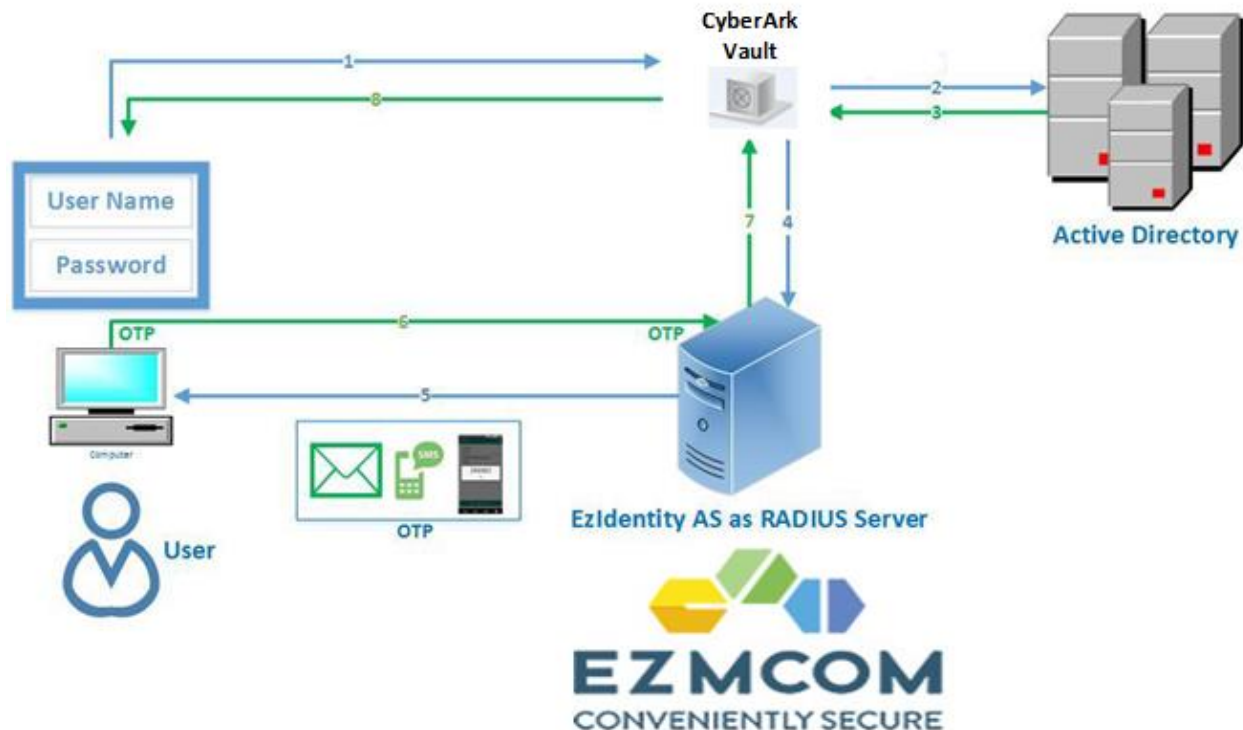
It is assumed that the CyberArk Privileged Account Security Suite environment is already configured and working with static passwords prior to implementing Ezmcom multi-factor Authentication Solution.

INTEGRATION USING RADIUS

CyberArk Privileged Account Security Suite can be configured to support Ezmcom MFA using the RADIUS protocol.

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.



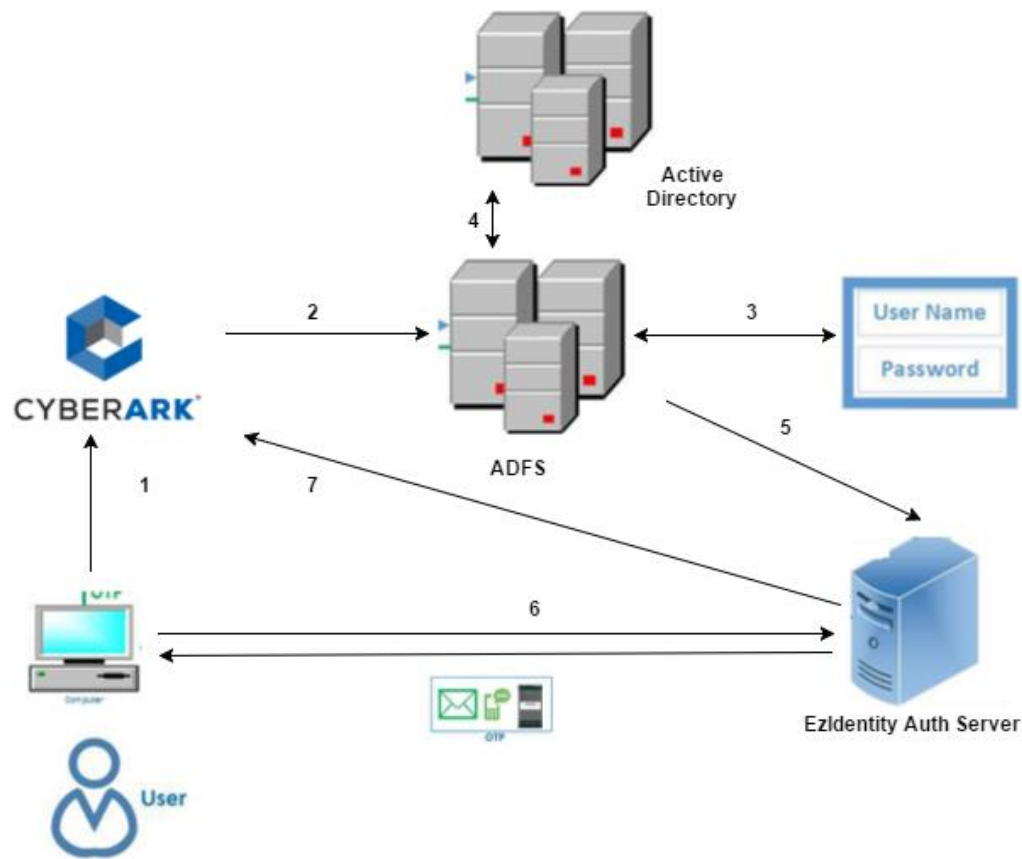
The Flow diagram can be summarized as below:

1. Primary (1FA) authentication is initiated to CyberArk Vault Manager using user's User Name and Active Directory password.
2. CyberArk Vault Manager sends authentication request to Active Directory for 1FA verification.
3. Once the Active Directory authentication is successful, the CyberArk Vault Manager sends 2FA authentication request to EzIdentity™ Authentication server as a RADIUS client.
4. EzIdentity™ AS will prompt the user for two factor authentication. User can enter the OTP generated from Software Token or trigger the delivery of OTP via an SMS/Email/IVR to the user's registered phone number/E-Mail Address. A Hardware Token can, also, be used to generate a One Time Passcode.
5. EzIdentity™ AS receives authentication request for 2FA to validate OTP over Radius Protocol.
6. CyberArk Vault Manager grants access to user if the OTP is validated successfully.

INTEGRATION USING SAML

CyberArk Privileged Account Security Suite can be configured to support Ezmcom MFA using the SAML (ADFS) protocol.

Below Figure 2 illustrates a high level deployment architecture of CyberArk Account Security Suite with EzIdentity™ AS



The Flow diagram can be summarized as below:

1. User initiates the CyberArk Portal.
2. ADFS Connection is initiated from CyberArk and user is presented with 1FA verification with his username and password using Active Directory.
3. Once the Active Directory authentication is successful, the CyberArk Vault Manager sends 2FA challenge, providing various options that could be available for the user.
4. EzIdentity™ AS will prompt the user for two factor authentication using PUSH or OTP generated from Software Token or trigger the delivery of OTP via an SMS/Email/IVR to the user's registered phone number/E-Mail Address. A Hardware Token can, also, be used to generate a One Time Passcode.
5. EzIdentity™ AS receives authentication request for 2FA to validate the MFA challenge.
6. CyberArk Vault Manager grants access to user if the MFA challenge is validated successfully.

EZIDENTITY™ INSTALLATION & INTEGRATION CONFIGURATION

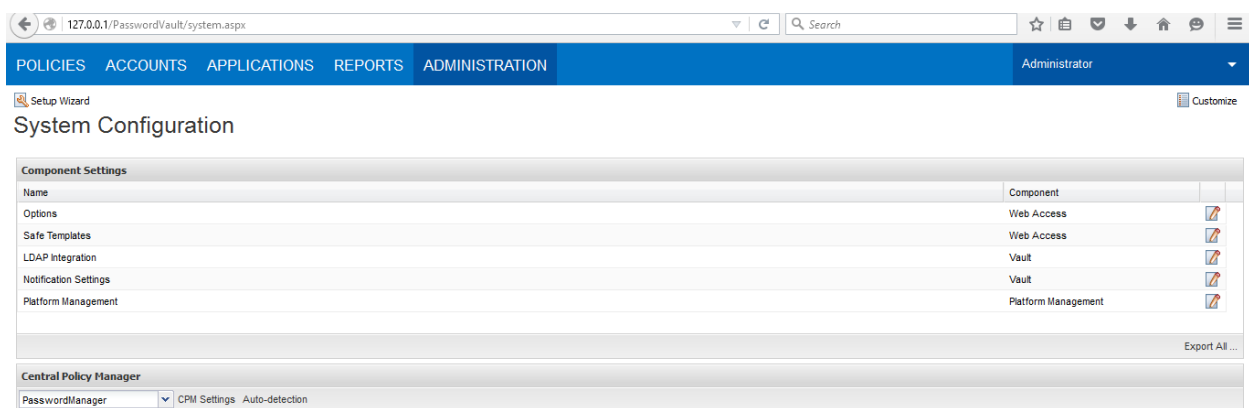
Please refer to the below documentations for EzIdentity Installation:

1. [EzIdentity™ Deployment Prerequisites](#)
2. [EzIdentity™ Authentication Server Quick Start Guide](#)

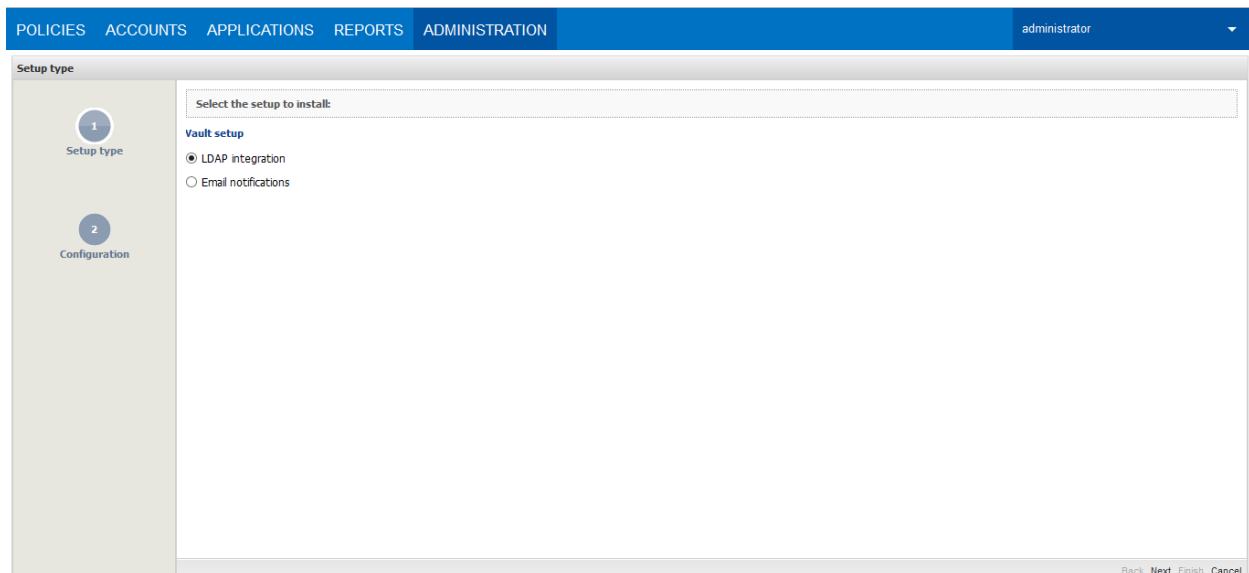
CYBERARK INTEGRATION GUIDE

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

POLICIES ACCOUNTS APPLICATIONS REPORTS ADMINISTRATION administrator

Configuration

1 Setup type

2 Configuration

LDAP Configuration Setup

Name: ezmcom.com

Directory Type: MicrosoftADProfile.ini

Address: owa.ezmcom.com

Port: 3268

LDAP Bind User: cn=Administrator,cn=users,dc=ezmcom,dc=com

LDAP Bind Password: *****

LDAP Base Context: cn=users,dc=ezmcom,dc=com

Test

Back Next Save and Continue Cancel

3. Click **Save and Continue**

POLICIES ACCOUNTS APPLICATIONS REPORTS ADMINISTRATION administrator

Configuration

1 Setup type

2 Configuration

LDAP Configuration Setup

Name: ezmcom.com

Directory Type: MicrosoftADProfile.ini

Address: owa.ezmcom.com

Port: 3268

LDAP Bind User: cn=Administrator,cn=users,dc=ezmcom,dc=com

LDAP Bind Password: *****

LDAP Base Context: cn=users,dc=ezmcom,dc=com

Test

Back Next Save and Continue Cancel

Add LDAP directory - Test configuration

Directory: ezmcom.com

Status: Successfully connected to directory

Host: owa.ezmcom.com

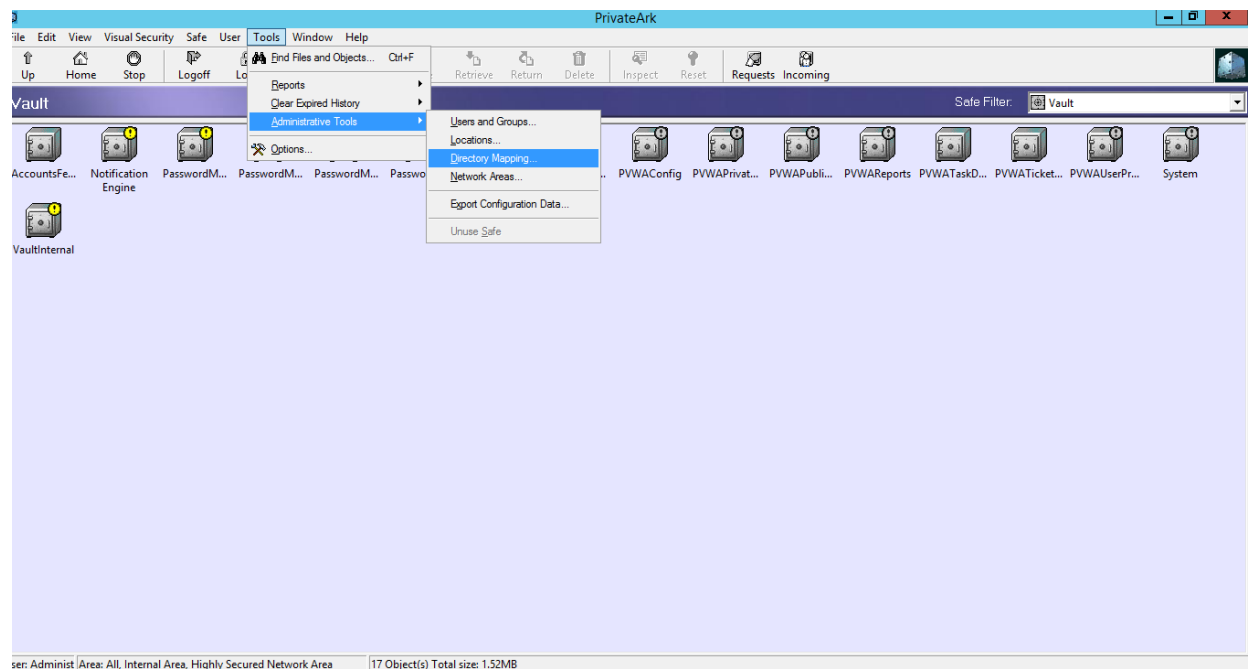
Status: Successfully connected

LDAP verify check ended successfully

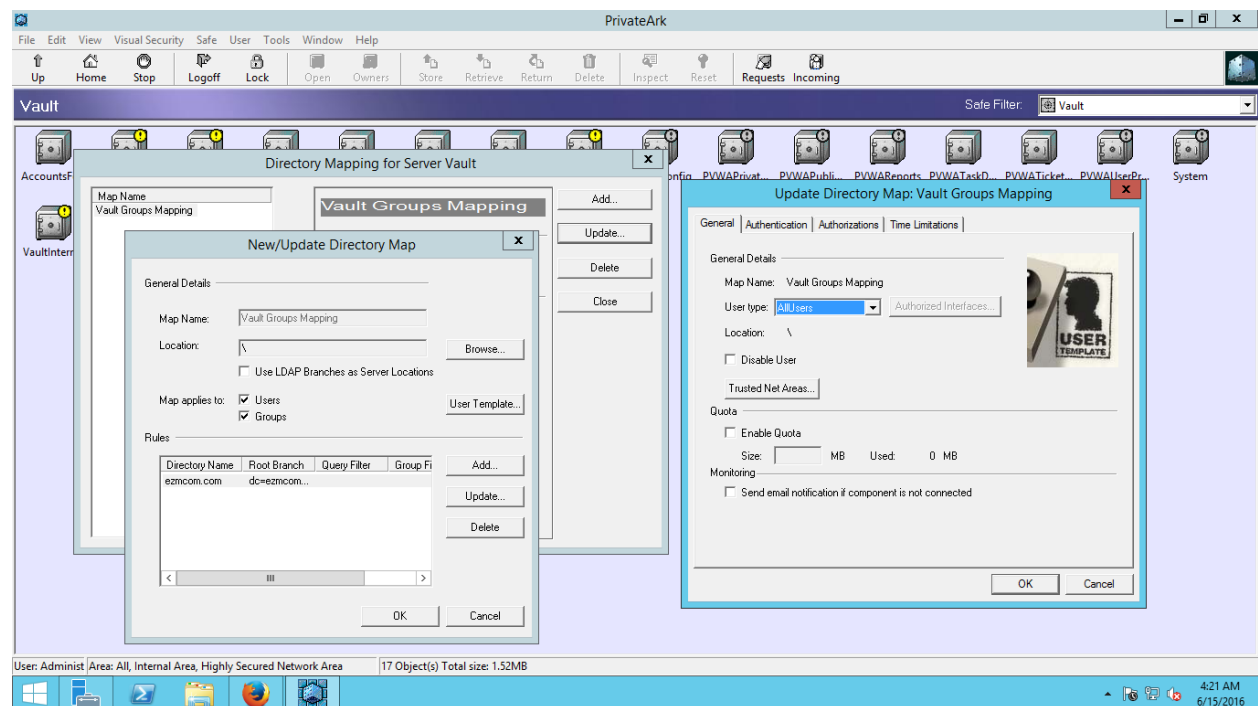
OK

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

On the PrivateArk Client:

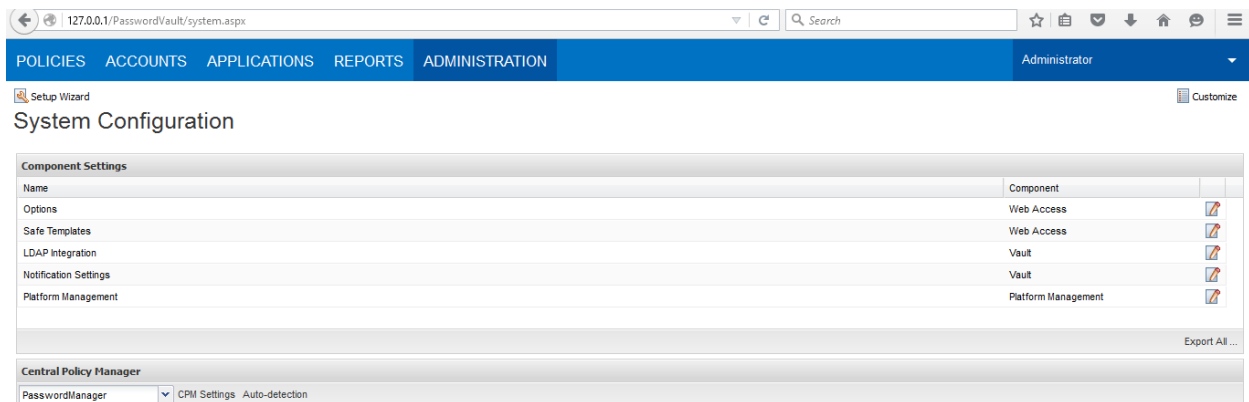


5. Map the LDAP configuration in PrivateArk. **Login into PrivateArk > Tools > Administrative Tools > Directory Mapping.**

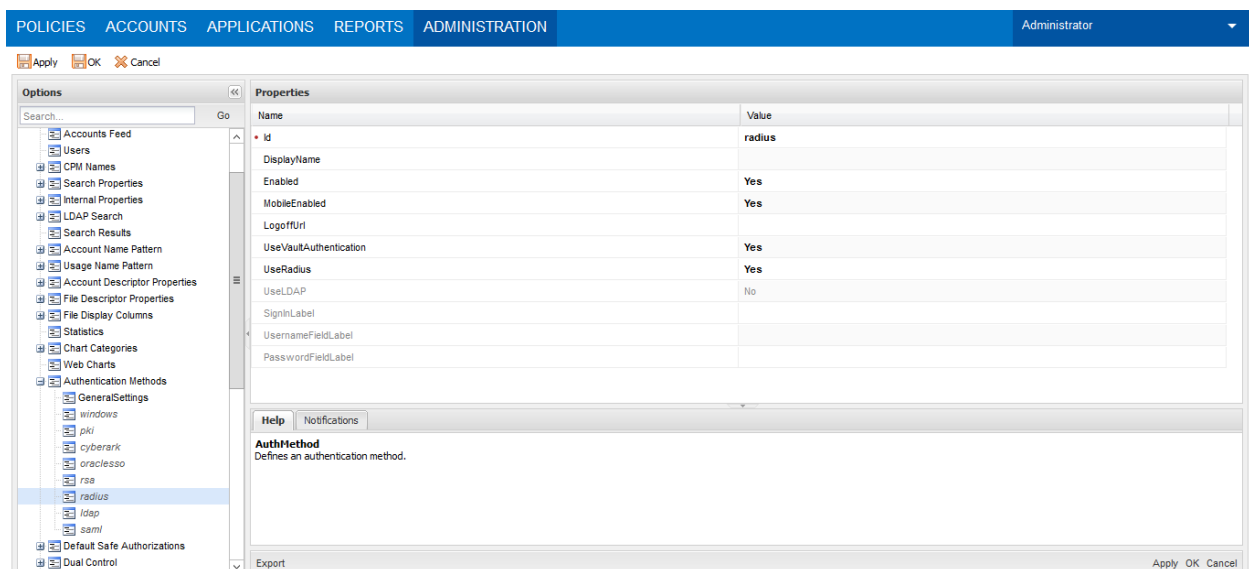


6. Under Directory Mapping, configure the Idap appropriately to match the Idap server. **Click Update > Update Directory Mapping > Configure Vault Groups Mapping.**

RADIUS CONFIGURATION



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

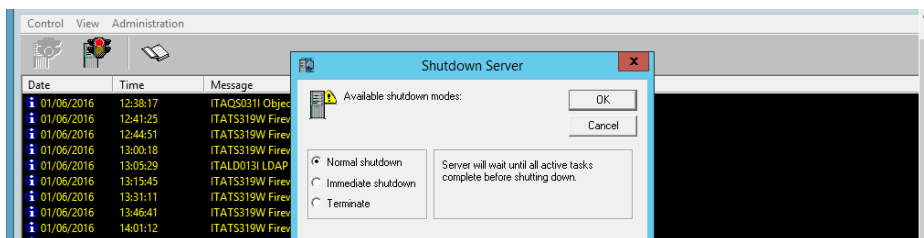


2. Select **RADIUS** under **Authentication Methods**

3. Select **Yes** from the **Enabled** options to enable RADIUS

4. Click **Apply**

5. To configure the RADIUS settings, stop the Password Vault Server

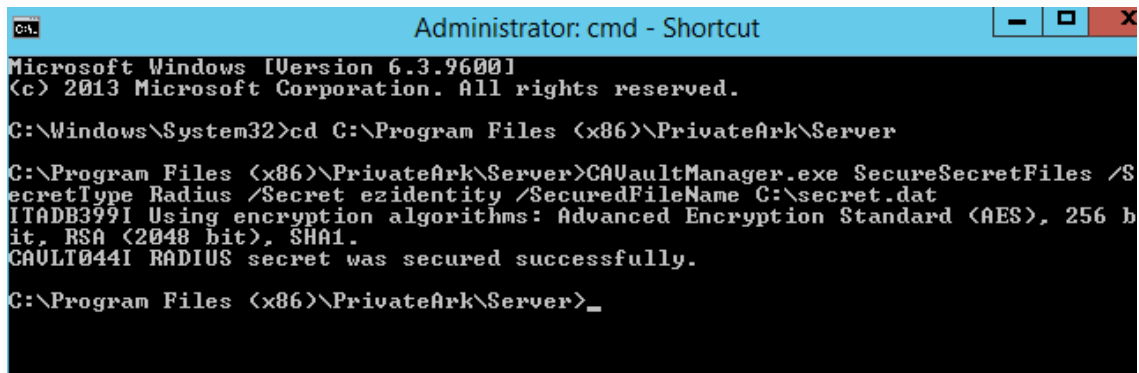


6. Generate the RADIUS shared secret file by opening the CMD as an administrator and running **CAVaultManager** to create an encryptedRADIUS shared secret file

Run this command: **CAVaultManager SecureSecretFiles /SecretType Radius /Secret VaultSecretKey /SecuredFileName c:\RadiusSecret.dat**

This is a sample of generating a shared secret file with ezidentity as the shared secret: **C:\Program Files (x86)\PrivateArk\Server>CAVaultManager.exe SecureSecretFiles /SecretType Radius /Secret ezidentity /SecuredFileName C:\secret.dat**

Move **secret.dat** to **C:\Program Files (x86)\PrivateArk\Server**



```
Administrator: cmd - Shortcut
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd C:\Program Files (x86)\PrivateArk\Server

C:\Program Files (x86)\PrivateArk\Server>CAVaultManager.exe SecureSecretFiles /S
ecretType Radius /Secret ezidentity /SecuredFileName C:\secret.dat
ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 b
it, RSA (2048 bit), SHA1.
CAULT044I RADIUS secret was secured successfully.

C:\Program Files (x86)\PrivateArk\Server>_
```

Please note that the **RADIUS Secret** has a 14 character limit

Ensure that the shared secret used for the CyberArk Configuration is the same as in the EzIdentity RADIUS Server settings

7. Locate the Password Vault Server **DBParm.ini** file at **C:\Program Files (x86)\PrivateArk\Server**, and take a backup of the file.

8. Open the **DBParm.ini** file, and add the RadiusServerInfo key under the [MAIN] section:

CyberArk DBParm.ini Configuration Values

RadiusServersInfo=RADIUS_Server_IP;RADIUS_Port;EzIdentitygroupid;secret.dat

where;

RADIUS_Server_IP = The IP of the RADIUS server

RADIUS_Port = Port number of the RADIUS

EzIdentitygroupid = The id of customer domain

secret.dat = The shared secret file, created in the previous section

Example: RadiusServersInfo=192.168.2.32;1645;52;secret.dat

Note:

Replace the **RadiusServersInfo**, **RADIUS_Server_IP**, **RADIUS_Port**, **EzIdentitygroupid**, and **secret.dat** placeholder values with the actual values

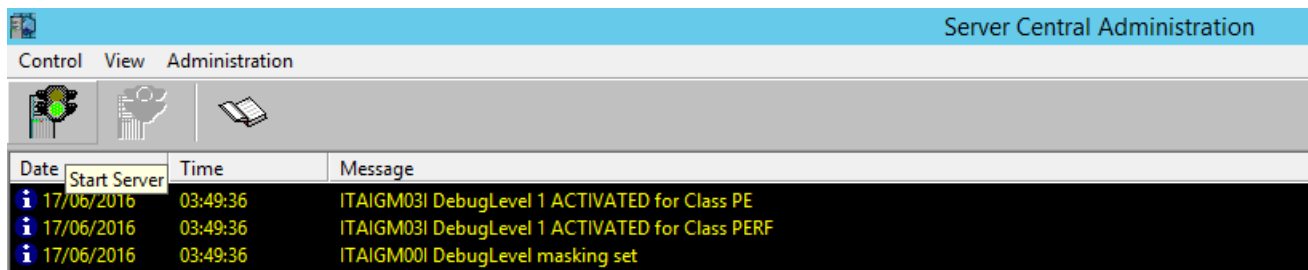
Ensure that there is an additional RADIUS Server for authentication (set up an additional RADIUS Server following step 8)

Example of two RADIUS Servers:

RadiusServersInfo=192.168.2.32;1645;32;secret1.dat,10.50.50.10;1645;33;secret2.dat

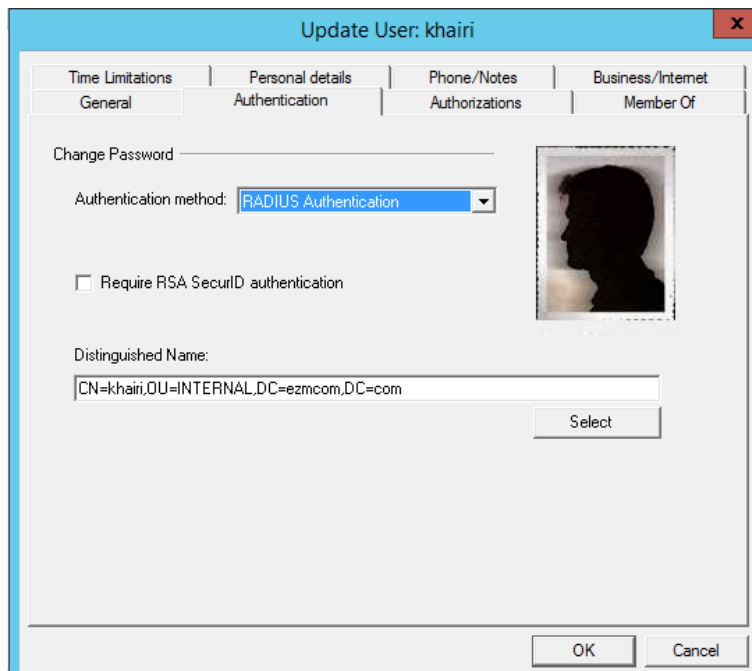
9. Save the **DBParm.ini** file

10. Start the Password Vault Server



SETTING RADIUS FOR USER'S AUTHENTICATION METHOD

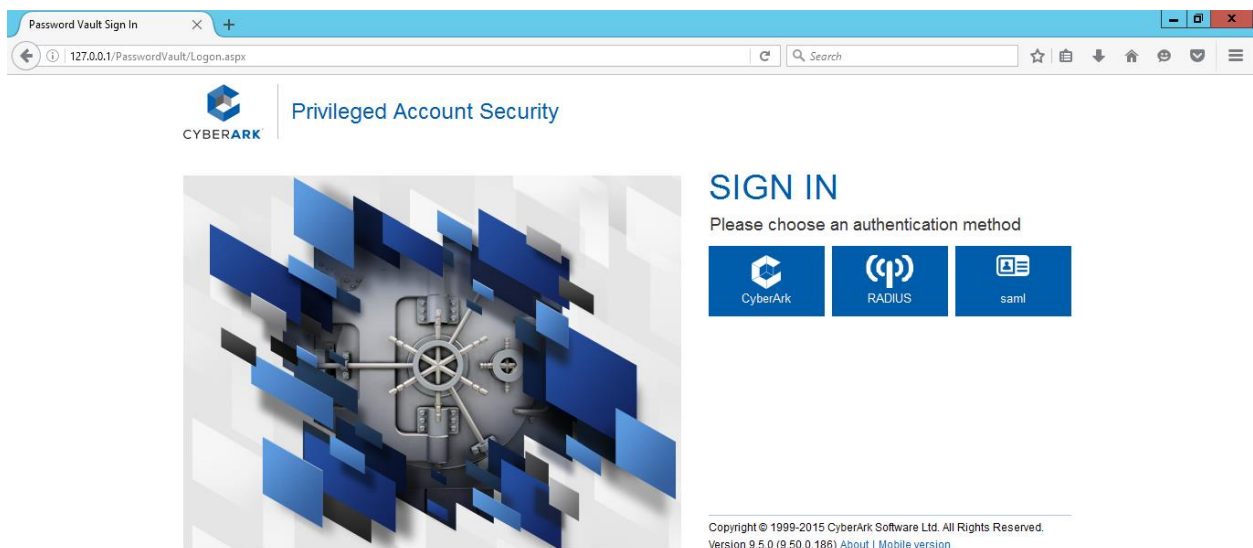
1. Login into PrivateArk > Tools > Administrative Tools > Users and Groups.



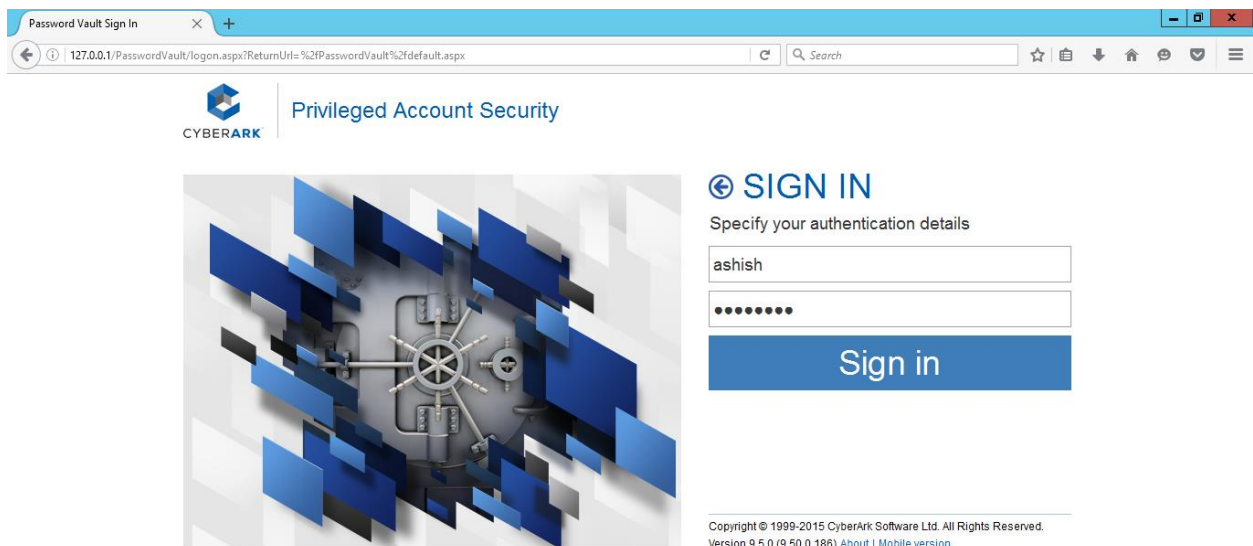
2. Change the Authentication method to RADIUS Authentication > Click OK.

TESTING RADIUS AUTHENTICATION

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



2. For test purposes, please use username in the 1FA login.



Click **Sign in** > Enter OTP in RADIUS challenge to login (Using Soft Token, protected by Biometric Authentication (TouchID))

Browser window: Password Vault Sign In
URL: 127.0.0.1/PasswordVault/login.aspx?ReturnUrl=%2FPasswordVault%2Fdefault.aspx

CYBERARK Privileged Account Security



RADIUS CHALLENGE

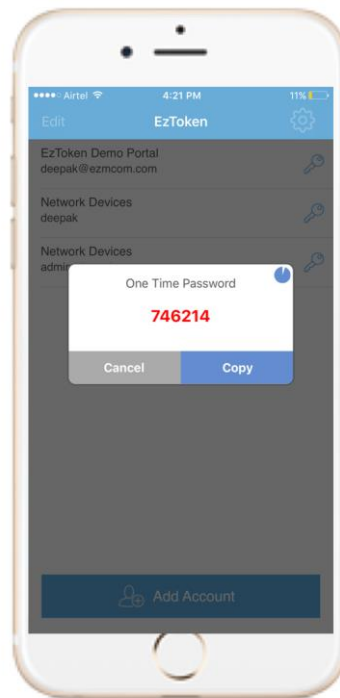
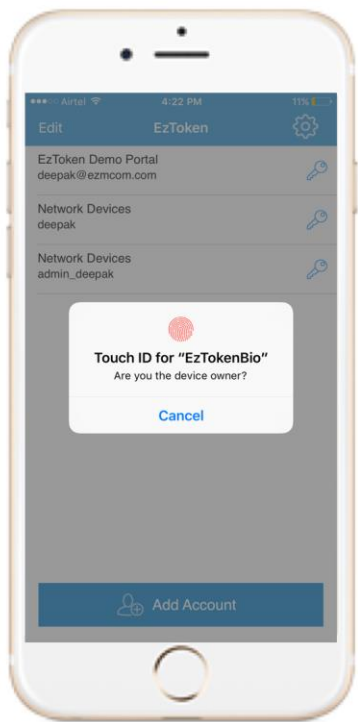
ITATS542I Passcode

ashish

Response

Post Answer

Copyright © 1999-2015 CyberArk Software Ltd. All Rights Reserved.
Version 9.5.0 (9.50.0.186) [About](#) | [Mobile version](#)



You can use the following mechanisms to generate the OTP and use it in the RADIUS challenge:

- 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 Behavioral PIN
- Soft Token OTP, protected by Biometric Authentication (Face, Voice, TouchID)

CONFIGURING SAML

Step 1: Configure Identity Provider for SAML (in this case EzIdentity integrated 2FA ADFS)

1. Configure ADFS for relying party. **Login into ADFS** as Administrator > Open the Active Directory Federation Services (AD FS) Management console.
2. In the navigation pane, expand **Trust Relationships**, then double-click **Relying Party Trusts** folder.
3. In the right pane, click **Add Relying Party Trust**. -This opens the Active Directory Federation Services (AD FS) 2.0 configuration wizard.

On the Welcome to the Add Relying Party Trust Wizard page, click **Start** > Select **Enter data about the relying party manually**, and then click **next** > Type a relying party name and then click **Next**. > Select **Active Directory Federation Services (AD FS) 2.0 Profile** > click **Next** > Do not use an encryption certificate. Click **Next**.

Click to select the **Enable support for the SAML** check box. >In the **SAML URL** field, type the name of the web application URL (for example, **https://<Cyberark IP>/PasswordVault**) > Click **Next** > Type the name of the relying party trust identifier (must be a unique name, for example, **CyberArk1**), and then click **Add**. Click **Next**. Note that this will be the realm value when you configure a new Issuer in Step 2.

Select **Permit all users to access this relying party** > Click **Next**.

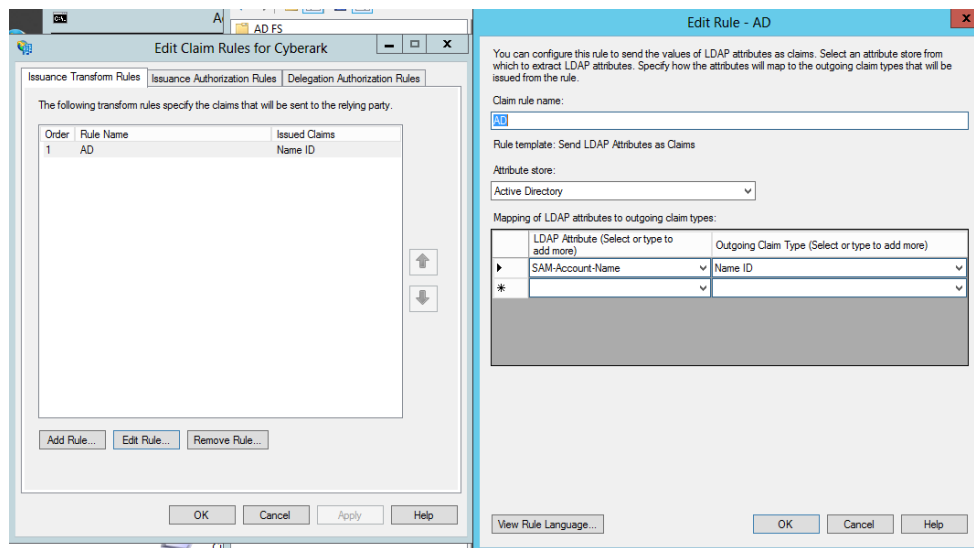
On the Ready to Add Trust page, there is no action required > click **Next**.

On the Finish page > click **Close**.

This opens the Rules Editor Management console. Use this console and the next procedure to configure the mapping of claims from your chosen directory source.

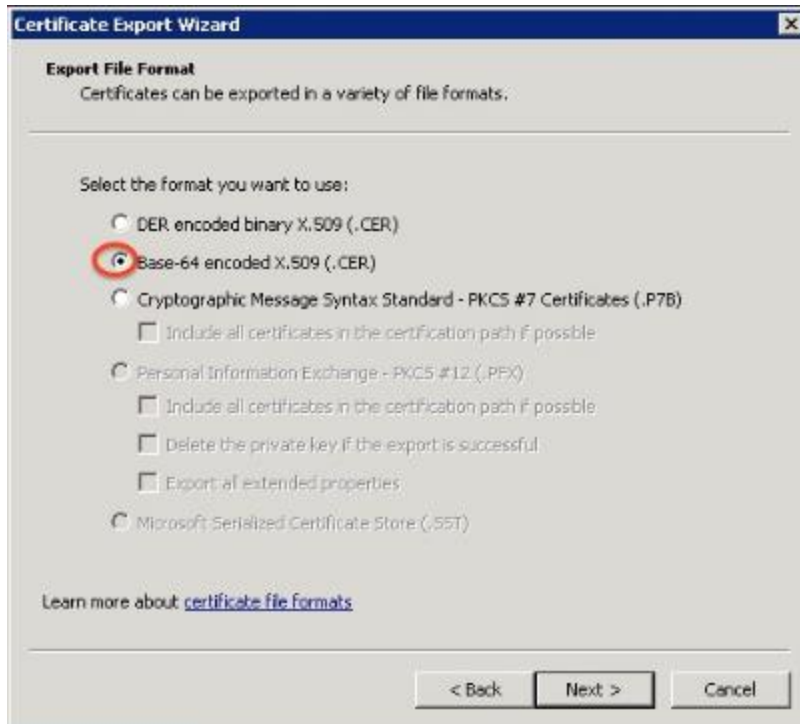
To configure a claim rule

1. On the **Issuance Transform Rules** tab, click **Add Rule**.
2. On the Select Rule Template page, select **Send LDAP Attributes as Claims**. Click **Next**.
3. On the Configure Rule page, type the name of the claim rule in the **Claim rule name** field.
4. From the **Attribute Store** drop-down list, select **Active Directory**.
5. In the **Mapping of LDAP attributes to outgoing claim types** section, under **LDAP Attribute**, select **SAM-Account-Name**.
6. Under **Outgoing Claim Type**, select **Name ID**.
7. Click **Finish**, and then click **OK**.



To export a token signing certificate

1. On the ADFS server, open the Active Directory Federation Services (AD FS) 2.0 Management console.
2. In the navigation pane, expand **Service**, and then click the **Certificates** folder.
3. Under **Token signing**, click the primary token certificate as indicated in the Primary column.
4. In the right pane, click **View Certificate link**. This displays the properties of the certificate.
5. Click the **Details** tab.
6. Click **Copy to File**. This starts the Certificate Export Wizard.
7. On the Welcome to the Certificate Export Wizard page, click **Next**.
8. On the Export Private Key page, click **No, do not export the private key**, and then click **Next**.
9. On the Export File Format page, select **DER encoded binary X.509 (.CER)**, and then click **Next**.



10. On the File to Export page, type the name and location of the file that you want to export, and then click **Next**. For example, enter **C:\ADFS.cer**.
11. On the Completing the Certificate Export Wizard page, click **Finish**.

Step 2: Implementing User Entity Behavior Analytics (UEBA) into ADFS

In addition to above changes please find the ezmcom package/folder that includes all necessary script to run the snippet and copy to the domain home directory.

- Locate the Master page <ADFS Home>/MasterPages/MasterPage.master
 - a. Reference the jquery script, by putting the tag below just before the `</body>`.


```
<script src="<% = Request.ApplicationPath + "/ezmcom/js/lib/jquery/jquery-1.11.3.min.js" %>"></script>
```
- Then locate the form page <ADFS Home>/FormsSignIn.aspx then append the scripts below to the page just before the `</asp:Content>` tag.
 - b. Reference the UEBA script

```
<script src="<% = Request.ApplicationPath + "/ezmcom/js/ezuba.min.js" %>"></script>
```

```

<script type="text/javascript" >

EzUBAnalytics.init();

// ID of element to be bind with UEBA.

var elem_id = "PasswordTextBox";

// Bind and register element field to UEBA analytics.
EzUBAnalytics.bind(document.getElementById(elem_id));

// Let Get ReferenceID from UEBA analytic Server.

document.forms[0].onsubmit = function () {

// UBA Web Server URL.

//var domain_url = 'https://211.25.18.246:9843';(SAMPLE)

var domain_url = 'https://Server IP Address:9843';

var api_path = '/uba-webservice/uba/v1/ubastore/put';

var url_path = domain_url + api_path;

var ubadata = JSON.stringify(EzUBAnalytics.ubaJson(document.getElementById(elem_id)));

$.ajax({type: 'POST',

        async: false,

        timeout: 30000,

        contentType: 'application/json',

        datatype: 'json',

        crossDomain: true,

        url: _url,

        data:ubadata,

        error: function (json) {

            console.log("error: "+json);

        },

        success: function (resultdata) {

            if(resultdata != null && resultdata.key != null) {

// Let store the key to the cookie

            document.cookie = "ubarefid=" + resultdata.key;

            }

        }

    });

```

```

// Allow form submission continue

document.forms[0].submit();

}

});

}

</script>

```

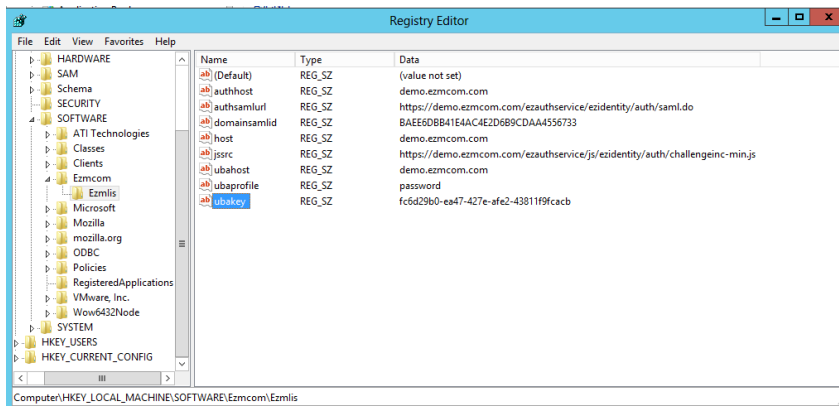
For the agent, add these 3 keys into the registry subkey

HKEY_LOCAL_MACHINE\Software\Ezmcom\Ezmlis (Path where the Ezmcom

i. ubahost – Host name of the server

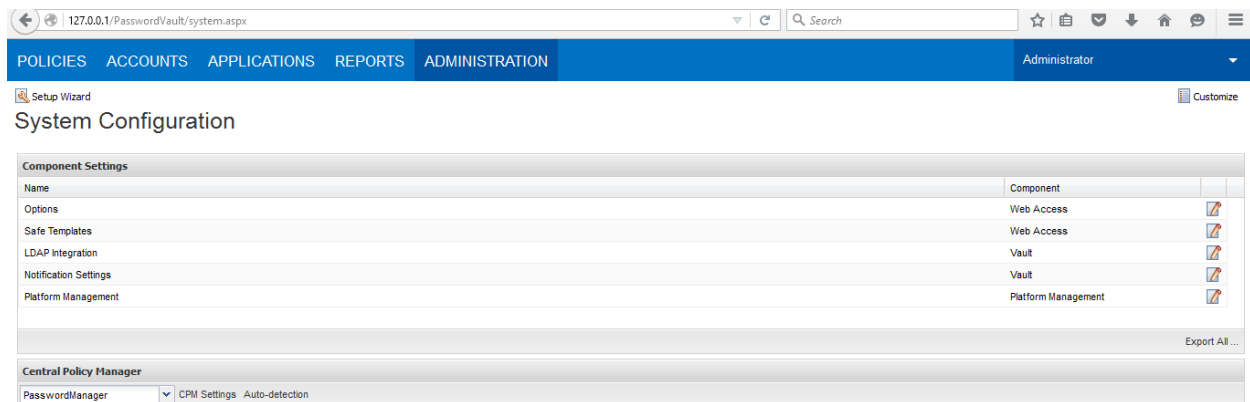
ii. ubakey - fc6d29b0-ea47-427e-afe2-43811f9fcacb (Sample Key) (Please Note : UBA key is unique across each application (or per-say client). The UBA key is essentially an API master key that is required by the RESTful API calls, and yes it will be provided by EZMCOM Team)

iii. ubaprofile - password

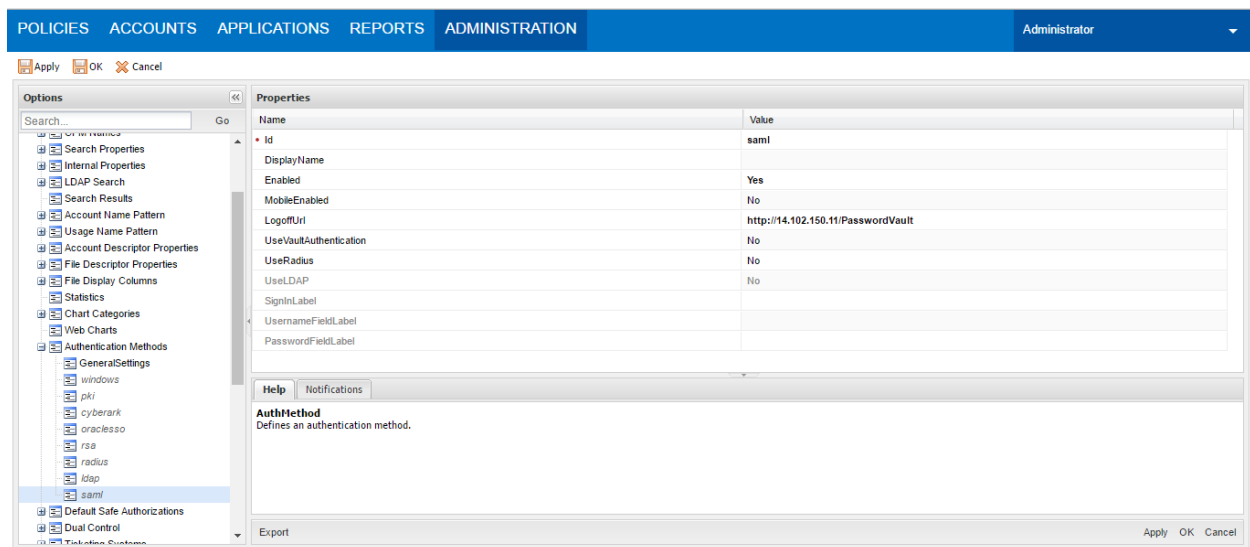


To disable UEBA, just blank the ubahost key's value

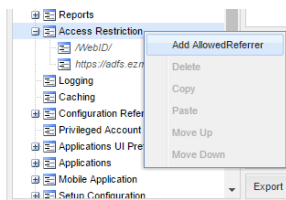
Step 3: Configure CyberArk PVWA for SAML



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



2. Select **SAML** under **Authentication Methods**
3. Select **Yes** from the **Enabled** options to enable SAML
4. Set the **LogoffURL** to any preferred URL, e.g. the Integrated IdP logoff page (<https://adfs.ezmcom.com/adfs/ls>) or the company homepage
5. Click **Apply**



Properties	
Name	Value
BaseUrl	https://adfs.ezmcom.com
RegularExpression	No

Help
Notifications

AllowedReferrer
Defines a URL in another web application through which the PVWA can be accessed.

Export
Apply
OK
Cancel

6. Select **Options** > Right-click **Access Restriction** and select **Add AllowedReferrer**

7. Set the **BaseUrl** value to the base URL of the **IdentityProviderLoginURL**

For example, if the **IdentityProviderLoginURL** is **https://adfs.ezmcom.com/adfs/ls**, then the **BaseUrl** would be **https://adfs.ezmcom.com**

8. Click **OK**

Step 4: Configure CyberArk SAML settings

9. To configure the SAML settings, stop the Password Vault Web Access by using **iisreset /start** or **iisreset /stop** via command line

10. Locate the Password Vault Server **web.config** file at **C:\inetpub\wwwroot\PasswordVault**, and take a backup of the file

11. Open the **web.config** file (located in **..\Password Vault Web Access\Env**), and add these three (3) keys to the **<appSettings>** section of the file:

CyberArk web.config SAML Configuration Values

```
<add key="IdentityProviderLoginURL" value=" https://adfs.ezmcom.com/adfs/ls" />
```

```
<add key="IdentityProviderCertificate" value="<FULL CERT VALUE>" />
```

```
<add key="Issuer" value="UniqueName" />
```

Replace **https://adfs.ezmcom.com/adfs/ls** with the actual Fully Qualified Domain Name (FQDN) of the Integrated Identity provider appliance, and the CyberArk-integrated realm name

Replace **<FULL CERT VALUE>** with the actual certificate value from the **Assertion Signing Certificate** from Identity Provider

Replace **UniqueName** with the actual **WSFed/SAML Issuer** value set in the Web Admin (step 7)

The certificate value must be in base64 format and pasted as a single line. Example:

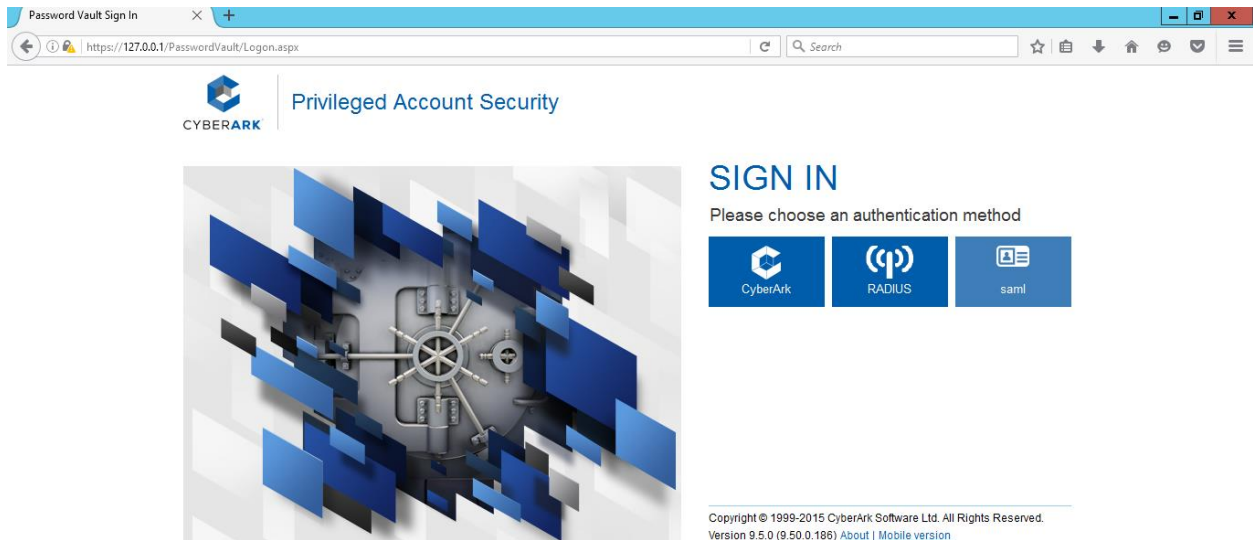
```
<add key="IdentityProviderCertificate" value="-----BEGIN CERTIFICATE-----
MIIC0DCCAbigAwIBAgIQJ80bS79dF4BL62kvH6FOzANBgkqhkiG9w0BAQsFADAK
MSIwIAYDVQQDElBREZTIFNpZ25pbmcgLSBlem1jb20uY29tMB4XDTE2MDMyMzA1
MTIwMVowXDTE3MDMyMzA1MTIwMVowJDEiMCAGA1UEAxMZQURGUyBTaWduaW5nIC0g
ZXptY29tLmNvbTCCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAN3bAo5i
sOAJ3WnEP43VxMJ2KsbZq4WwIC8+77VXM9/s1+XGJshKbwXz/xEDvurzf0k+JRR5
N3cPmjNig24oNZlh+czr0f81432QSEbebnys7qDMAzxa68Md4UPIUFQHdNRfwrp
8D9LInQMTZ1tFtm2dQyUhXRY9EcmF35JPGxinyDbyg1EQWCu1Byve6mOMhudmIdF
tJKHLTjUz3bWu3ZLkue6Rpe1SLxTHroHbol2tMBNvLeoagZr67dZG20etn83cPnO
5cfU9EQmvY3sH9XcvAnUPlKkuajS3m8BnFzCD1IODacYaOOxQiyoY/Ucq0BUyy46
y1n/e4QN4GEcvkkCAWEAATANBgkqhkiG9w0BAQsFAAOCAQEAfib6S+hFTY2pm8Gh
0044sP3p79LMc8J1SKZxGjdbJ1WA9zx/Lo8QObjpTIYZO/cDezk/5eBW2WyywXyUI
COHGZ77fue6d304zjXj6oFgbk3ev4bdpEI++btwsFaRww4qy5gJ7ZCIAiUom10sw
mKPGC5J2WjT+5J8tulkhYMca4K61X3pkV0RSreRY5rgMnxS0t02/Ryg7TNcWST8y
Ah+mfft4D708unpTg51WswrGLHRNtgTb5aT5CFBG/YyW4kpdndU7LznqDz82W2UA
EaJM/aJYSsDsbylDqeA4584qnRt6V+RnoAnZiiZnK/8pLd4oJWVRZAL04SdaMymW
NYBinA==
-----END CERTIFICATE-----
"/>
```

12. Save the **web.config** file

13. Start the Password Vault Web Access by using **iisreset /start** or **iisreset /stop** via command line

TESTING SAML AUTHENTICATION

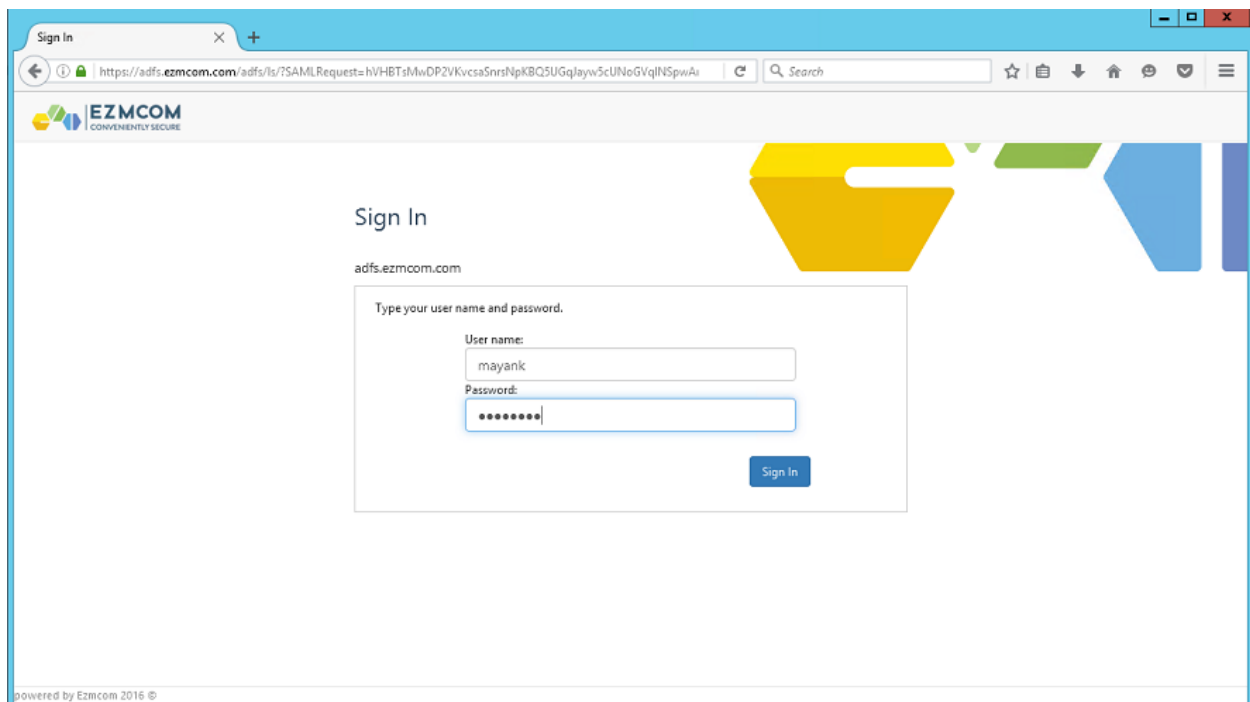
1. Log into the CyberArk Password Vault Web Access, choose SAML as an authentication method.



Click **saml** > redirect to ADFS 1FA page > Enter ADFS credentials

After completion of User Entity Behavior Analytics(UEBA) training following two cases will be there.

1. If UEBA confidence score is above threshold - It will allow user to login without MFA
2. If UEBA confidence score is below threshold - MFA will be challenged.

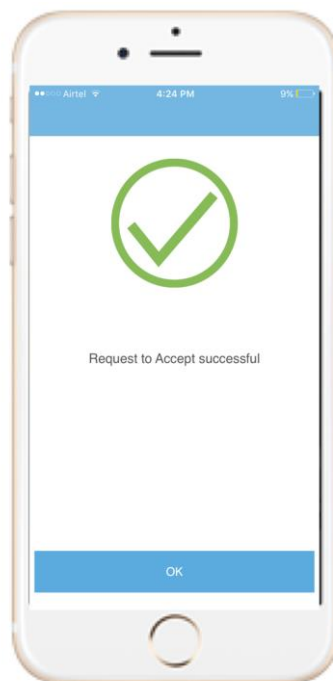
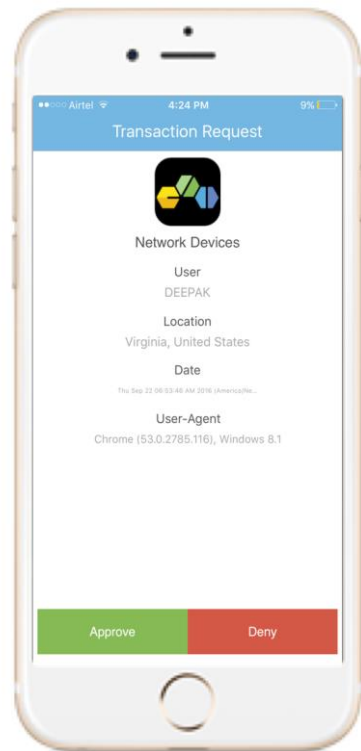
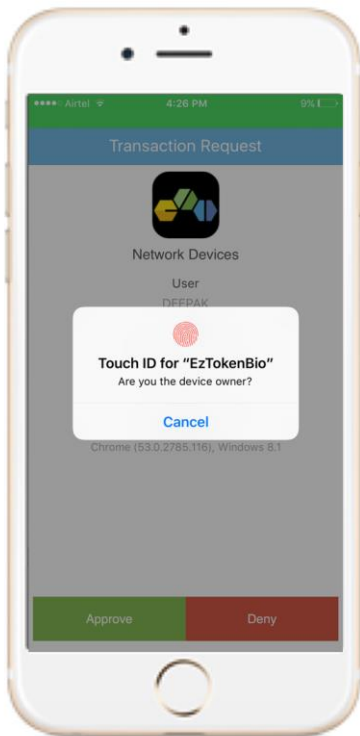


2FA page > Authenticate using PUSH or OTP

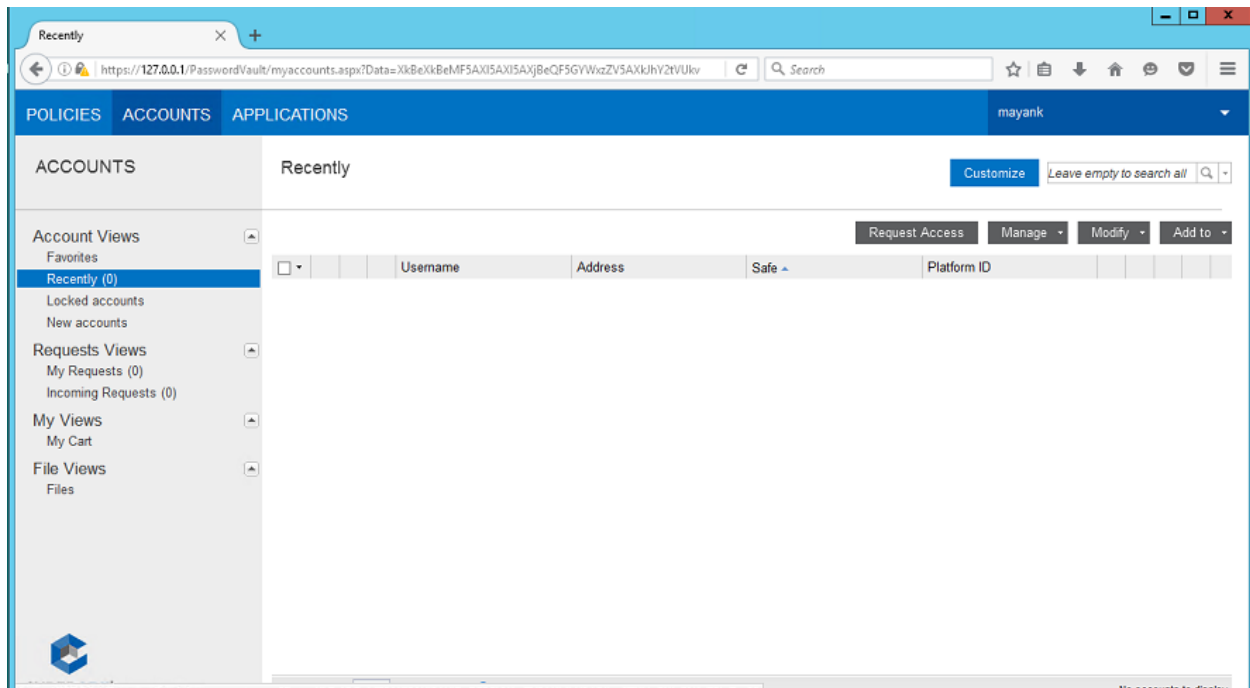
The screenshot displays a web browser window with the URL <https://adfs.ezmcom.com/ezmcom/ezmcom.aspx?params=c2lkPXBiB0NWRzMG5hZTM0eWVsZTNwdHVqaiZnaWQ9NDgmdl>. The page title is "Ezmcom". The main content area is titled "TWO-FACTOR AUTHENTICATION". Under the heading "Authenticator", there are three radio button options: "Mobile Push" (selected), "SMS", and "E-Mail". The "Mobile Push" option is expanded, showing a dropdown menu with the text "Android - xxxxxxxxxxxxxxxx2022". Below these options is a red button labeled "REQUEST PASSCODE". At the bottom of the form, there is a text input field with a lock icon and the placeholder text "Enter Passcode", and a dark blue button labeled "LOGIN NOW".

The following authentication mechanisms can be used to obtain the authentication:

- 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 Behavioral PIN
- Soft Token OTP, protected by Biometric Authentication (Face, Voice, TouchID)



3.



PARTNER CONTACT INFO

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