YUBIKEY AUTHENTICATION FOR CYBERARK PAS

Name of Company: Yubico
Website: www.yubico.com
Name of Product: YubiKey 4 / YubiKey NEO

YUBICO SOLUTION OVERVIEW

Businesses are challenged with protecting company data and systems in a continually evolving landscape. Stolen credentials cost companies billions of dollars each year — and hackers are targeting everyone, from small businesses to large enterprises. Yubico's products help protect access to both data and resources critical for operations, with a simple touch

A YubiKey is a small hardware device that offers two-factor authentication with a simple touch of a button. YubiKeys are built strong enough for the largest enterprises, while remaining simple enough for anyone to use. YubiKeys are used by 8 of the top 10 internet enterprises and by millions of users in over 150 countries

PREREQUISITES

- CyberArk Private Account Security [*]
- Microsoft Windows Active Directory domain
- Certification Authority
- Microsoft Internet Explorer or Google Chrome (for PVWA Authentication)
- YubiKey PIV Manager

[*] for the purpose of this document, the integration was tested with v9.7, but it should be supported from v7.x and upwards.

STORING YOUR PERSONAL CERTIFICATE IN THE YUBIKEY

You will need to follow the *YubiKey PIV Deployment Guide* in order to configure your Certification Authority for Login with a YubiKey. Then follow the *YubiKey PIV Manager User's Guide* in order to setup you YubiKey and store your personal certificate.

CONFIGURING THE PVWA TO AUTHENTICATE USING THE YUBIKEY

ENABLE PKI AUTHENTICATION

During installation, the PVWA is automatically configured to support PKI authentication for users who select this authentication method. However, if these authentication configurations have been changed and the PVWA currently doesn't support PKI authentication, you can configure it using the procedure in the *Configuring PKI Authentication for the PrivateArk Client* section of the *Privilege Account Security Installation guide* v9.7.

REQUIREMENTS

SSL Certificate – A web server certificate that has been certified by a Certificate Authority (CA).

IN THE IIS:

1. Make sure that you have installed an SSL certificate on the web server.
2. In the Default Web Site Properties window on the web site that will host the PVWA, display the Directory Security window, and click **Edit** to display the Secure Communications Properties window.
Note: This is relevant for IIS 6 only.
3. In the Secure Communications window, select **Enable certificate trust list**.
4. If an IIS message appears indicating that the CA is not trusted, do the following:

   i. Click **New** to create a new CTL,
   Or,
   Click **Edit** to modify an existing CTL list.
   A certificate trust list wizard appears.
   ii. Click **Next** to begin the wizard.
   iii. In the Certificates in the CTL window, select the Trusted CA that created the certificate and then complete the wizard.
   Note: If the CA doesn’t appear in the Certificates list, add it to the local computer store then repeat this step.
   To Add a CA to the Local Computer Certificate Store

      i. Display the Microsoft Management Console.
      ii. From the **File** menu, select **Add/Remove Snap-in**; the Add/Remove Snap-in window appears.
      iii. Click **Add**; the Add Standalone Snap-in window appears.
      iv. Select **Certificates**, then click **Add**; the Certificates snap-in window appears.
      v. Select **Computer Account**, then click **Next**; the Select Computer window appears.
      vi. Select **Local Computer**, then click **Finish**; the Add Standalone Snap-in window appears.
      vii. Click **Close**; the Add/Remove Snap-in window appears and displays Certificates (Local Computer).
      viii. Click **OK**; the main Console window appears.
      ix. Expand **Certificates (Local Computer)**, then expand **Trusted Root Certification Authorities**; the Certificates folder appears.
      x. Select **Certificates**, then from the **Action** menu, select **All Tasks**, then **Import …**; the Certificates Import Wizard appears.
      xi. Click **Next**; the File to Import window appears.
      xii. Select the certificate file to import, then click **Next**; the Certificate Store window appears.
      xiii. Select **Place all certificates in the following store**, then click **Next**; the Completing the Certificate Import Wizard window appears and displays the details of the selected certificate.
      xiv. Click **Finish**; the selected certificate is imported to the local computer account.

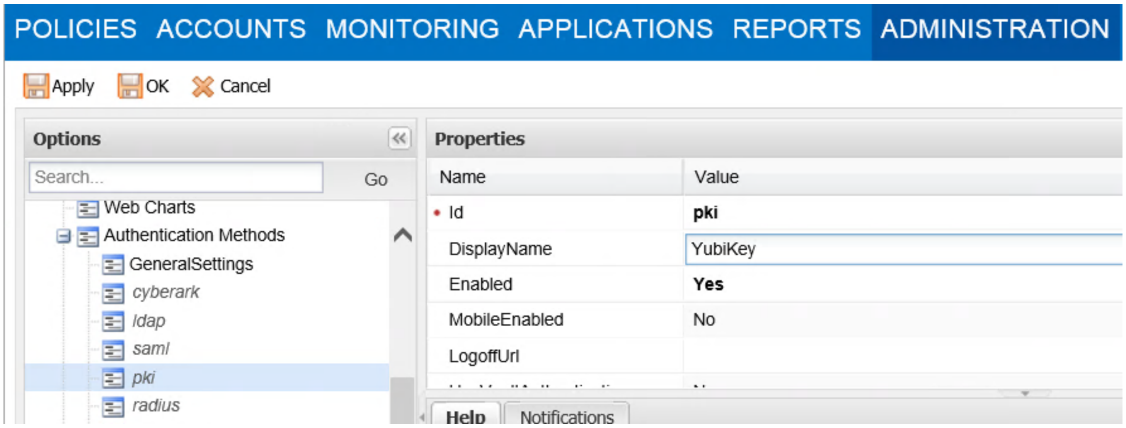
5. Open the PasswordVault/auth/pki subfolder, and display the Properties window.
6. Make sure that **Require client certificates** is selected, then click **OK**.

CONFIGURING THE USER ACCOUNT

1. Log on to the PrivateArk Client as the predefined Administrator user.
2. Display the User properties of the user to configure, and display the Authentication tab.
3. From the Authentication method drop-down list, select **Password**, then click **OK**. This is a dummy setting that has no value as users connecting through the PVWA are required to provide a certificate.
4. Log off the Vault.

CONFIGURING ACCESS THROUGH THE PVWA

1. Log onto the PVWA as the predefined Administrator user.
2. Click **ADMINISTRATION** to display the **System Configuration** page, then click **Options**; the main system configuration editor appears.
3. Expand **Authentication Methods**; a list of the supported configuration methods is displayed.
4. Select **pki** and make sure the **Enabled** property is set to **Yes**.
5. Set DisplayName to YubiKey.

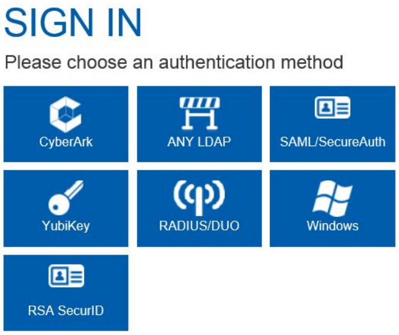


Name	Value
• Id	**pki**
DisplayName	YubiKey
Enabled	**Yes**
MobileEnabled	No
LogoffUrl	

6. Click **Apply** to save the new configurations and apply them immediately,
   or,
   Click **Save** to save the new configurations and apply them after the period of time specified in the **RefreshPeriod** parameter.

TESTING THE YUBIKEY AUTHENTICATION IN THE PVWA

After your personal certificate is stored in the YubiKey, insert it when ready to authenticate to the PVWA. In the PVWA, in the list of available authentication methods, click **YubiKey**:

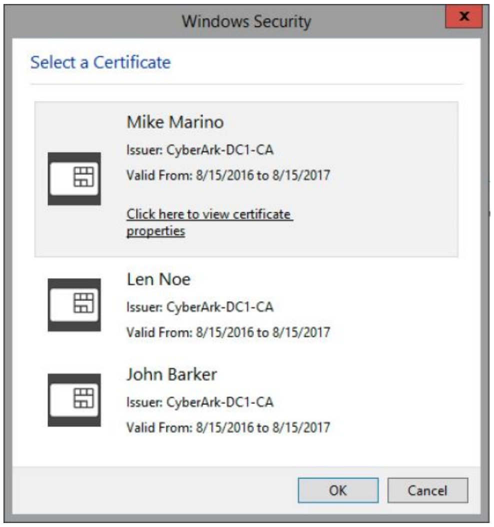


SIGN IN

Please choose an authentication method

Depending on your browser and the security configurations, either of the following scenarios will happen:

- The PVWA will automatically locate the user's certificate and log the user onto the Vault,
  or,
  A list of certificates will be displayed where the user can select a certificate and be logged on to the Vault.



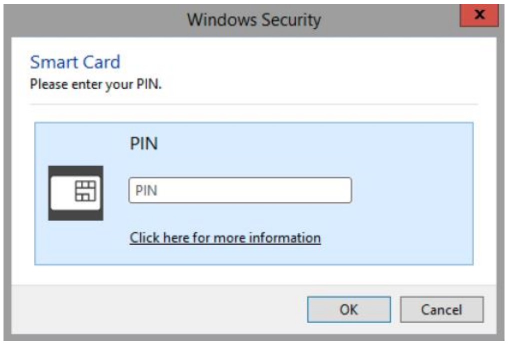
Windows Security

Select a Certificate

Mike Marino
Issuer: CyberArk-DC1-CA
Valid From: 8/15/2016 to 8/15/2017
Click here to view certificate properties

Len Noe
Issuer: CyberArk-DC1-CA
Valid From: 8/15/2016 to 8/15/2017

John Barker
Issuer: CyberArk-DC1-CA
Valid From: 8/15/2016 to 8/15/2017



Windows Security

Smart Card

Please enter your PIN.

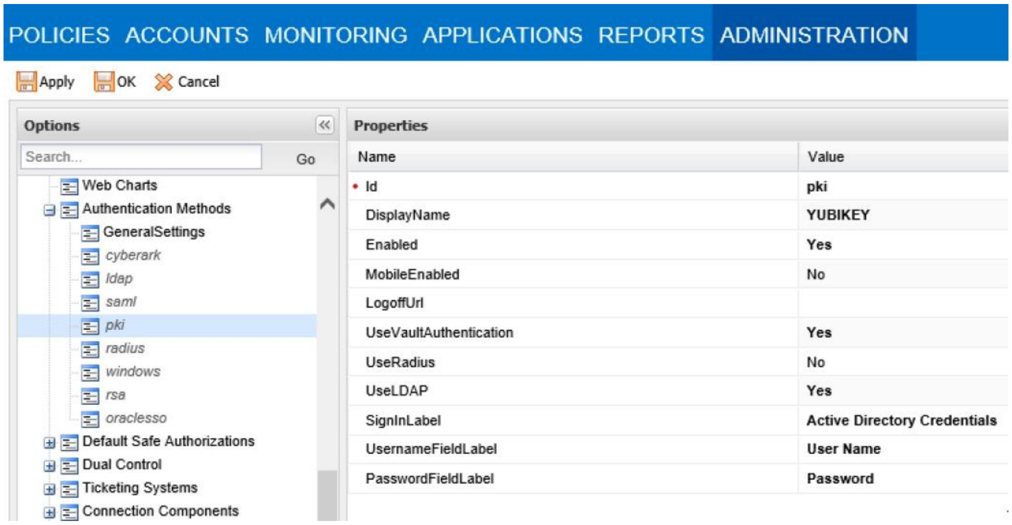
PIN

OPTIONAL: PRIVATEARK CLIENT TO AUTHENTICATION USING THE YUBIKEY

You need to enable PKI Authentication on the PrivateArk Client in order to authenticate using your YubiKey. Simply follow the steps on the *Appendix D: Configuring Additional Authentication for the PrivateArk Client* of the *Privilege Account Security Installation Guide*.

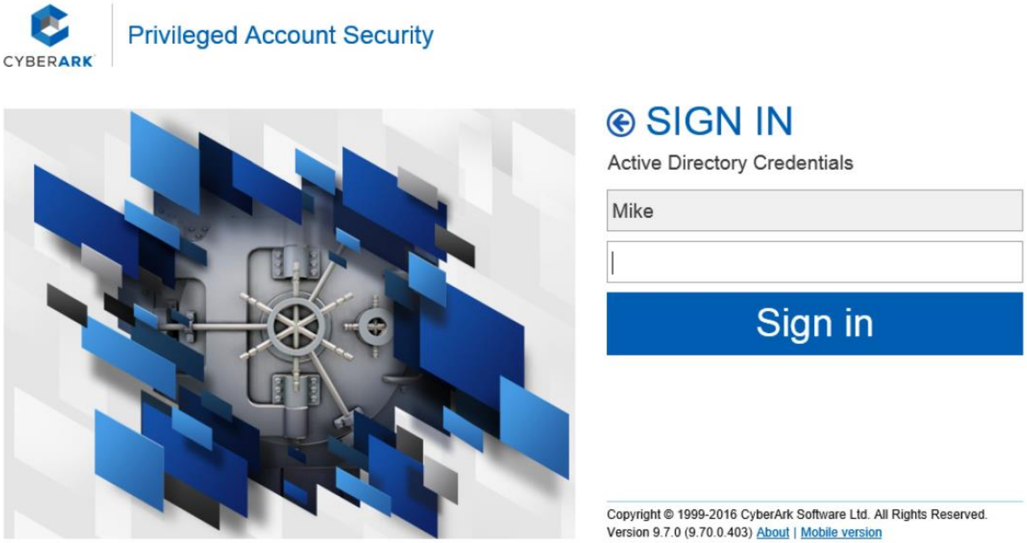
OPTIONAL: ENABLING ADDITIONAL AUTHENTICATION FACTORS

You can enable additional authentication factors, besides the YubiKey, such as Active Directory or Radius. In the PVWA go to ADMINISTRATION to display the System Configuration page, then click Options; the main system configuration editor appears. Expand Authentication Methods and select **pki**. Then set **UseVaultAuthentication** to Yes and select Yes on either **UseLDAP** or **UseRadius** and enter the appropriate labels:



Name	Value
Id	pki
DisplayName	YUBIKEY
Enabled	Yes
MobileEnabled	No
LogoffUrl	
UseVaultAuthentication	Yes
UseRadius	No
UseLDAP	Yes
SignInLabel	Active Directory Credentials
UsernameFieldLabel	User Name
PasswordFieldLabel	Password

The PVWA will request the additional authentication factors, after the YubiKey, during login:



Active Directory Credentials

Mike

Copyright © 1999-2016 CyberArk Software Ltd. All Rights Reserved.
Version 9.7.0 (9.70.0.403) About | Mobile version