CyberArk Integration with Duo - Implementation Guide

The Cyber-Ark Password Vault
Version 9.x

Introduction

This guide is designed to help implement Duo integration with CyberArk's Privileged Account Security solution. CyberArk's Enterprise Password Vault and Duo can be integrated using CyberArk and Duo's support for the RADIUS protocol.

This guide is intended to lead you through the integration process using Duo's Authentication Proxy to act as a RADIUS server, with CyberArk's Enterprise Password Vault configured as a RADIUS client. Duo's Authentication Proxy is also configured to perform primary authentication against Active Directory. This integration has been tested on version 9.1 of CyberArk's Privileged Account Security solution.

Duo Setup

1. Set up a Duo account : https://www.duosecurity.com/docs/getting_started
2. Login to the Duo Admin Panel : https://admin.duosecurity.com/login
3. Protecting Applications https://www.duosecurity.com/docs/protecting_applications
   - Locate RADIUS in the application list and click **Protect this application**
4. Set up a Duo Authentication Proxy : https://www.duosecurity.com/docs/radius
   a. Follow instructions in section: **Install the Duo Authentication Proxy**

      The machine you are installing on should have access to your AD server

   b. Follow instructions in section: **Configure the Proxy for Your Primary Authenticator - Active Directory**
      - Configure everything under the "REQUIRED" subsection

   c. Follow instructions in section: **Configure the Proxy for Your RADIUS device**
      - Configure everything under the "REQUIRED" subsection
      - search_dn – Configure a query that will include all the AD users that will authenticate through Duo. (It is recommended that the list be as minimal as possible while still including the necessary users)
      - radius_ip_1 – Configure this to the IP of your vault server
      - radius_secret_1 – Should not be more than 16 characters (CyberArk limit)
      - client – choose "ad_client"
      - server mode (section in the configuration file) -
        a. `[radius_server_auto]` – This setting will make the server work in push mode, in which the user will need to accept the Duo request on their mobile device.
        b. `[radius_server_challenge]` – Will make the server work in challenge mode where a challenge screen will be displayed after the login screen, in which the user should enter a Duo passcode. This is the mode you should use if you are going to configure multiple Duo Proxies for High-Availability
      - See "Appendix A – Duo Authentication Proxy configuration file" in this document for a template configuration file and examples

   d. Follow instructions in section: **"Start the Proxy"**

5. Enroll users : https://www.duosecurity.com/docs/enrolling_users
    - User names should match their AD names.

CyberArk Setup

1. Before beginning these steps, LDAP Integration for CyberArk Enterprise Password Vault should be configured
2. Refer to the **Privileged Account Security Installation Guide**:

   Go to: Installing the Privileged Account Security Solution -> Authenticating to the Privileged Account Security Solution -> Radius authentication.

   The 3 main parts are:

   a. Radius server – This has been covered by the “Duo Setup” section in this document

   b. Certificate – optional , but recommended – see instructions under **Configuring RADIUS Authentication , step 1**

   c. Vault setup for RADIUS : **Configuring RADIUS Authentication , steps 2-5**

      Notes regarding the DBParm.ini configuration in these steps:

      - Use file `radiusauth.dat` where `c:\RadiusSecret.dat` is mentioned
      - IP address of the RADIUS server – should be the IP of the server where the Duo Authentication Proxy is set up
      - Port – same as the one in the Duo Authentication Proxy configuration file (default is 1812)
      - Vaulthostname – your vault host name or IP (however the Duo Authentication Proxy server will be able to recognize it)
      - `radiusauth.dat -` the file where the radius secret is encrypted and stored (created in step 3)
      - High-Availability may be configured as documented, but in this case make sure the Duo Proxy is configured to work in challenge mode (`radius_server_challenge`) . See Appendix A for examples.

   d. **Configuring the User Account –** Follow these directions for users that will use the Duo authentication

   e. **Configuring Access through the PVWA -** Follow these directions once per PVWA server

Appendix A – Duo Authentication Proxy configuration file

Template configuration file:

```
[ad_client]
host=<YOUR_AD_SERVER_HERE>
service_account_username=<YOUR_BIND_USER_HERE>
service_account_password=<YOUR_BIND_PASSWORD_HERE>
search_dn=<YOUR_DN_SEARCH_HERE>

[<RADIUS_SERVER_MODE>]
ikey=<Get from the Duo integration setup>
skey=<Get from the Duo integration setup>
api_host=<Get from the Duo integration setup>
radius_ip_1=<YOUR_VAULT_SERVER_HERE>
radius_secret_1=<YOUR_RADIUS_SECRET_HERE>
client=ad_client
port=<PROXY_PORT – default is 1812>
```

Example configuration file for Duo auto method:

```
[ad_client]
host=1.2.3.4
service_account_username=bind
service_account_password=password1234
search_dn=cn=Users,dc=my-lab,dc=com

[radius_server_auto]
ikey=DIJXXXXXXXXXXXX16UO
skey=LAAGFDASFRSERFVRFWEddddfsfsfrefDGDG83
api_host=api-1234.duosecurity.com
radius_ip_1=1.2.3.5
radius_secret_1=myRadiusSecret
client=ad_client
port=1812
```

Example configuration file for Duo challenge method:

(Difference from auto method highlighted)

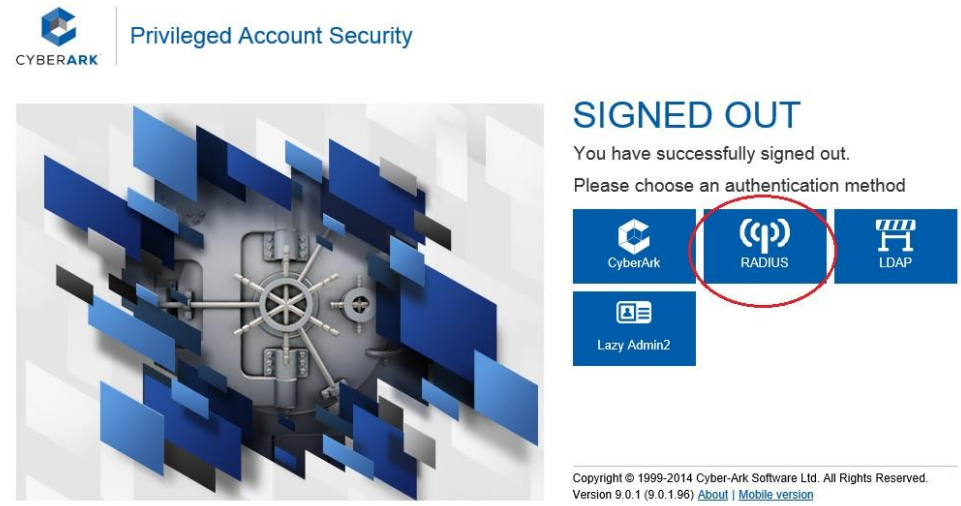
```
[ad_client]
host=1.2.3.4
service_account_username=bind
service_account_password=password1234
search_dn=cn=Users,dc=my-lab,dc=com

[radius_server_challenge]
ikey=DIJXXXXXXXXXXXX16UO
skey=LAAGFDASFRSERFVRFWEddddfsfsfrefDGDG83
api_host=api-1234.duosecurity.com
radius_ip_1=1.2.3.5
radius_secret_1=myRadiusSecret
client=ad_client
port=1812
```

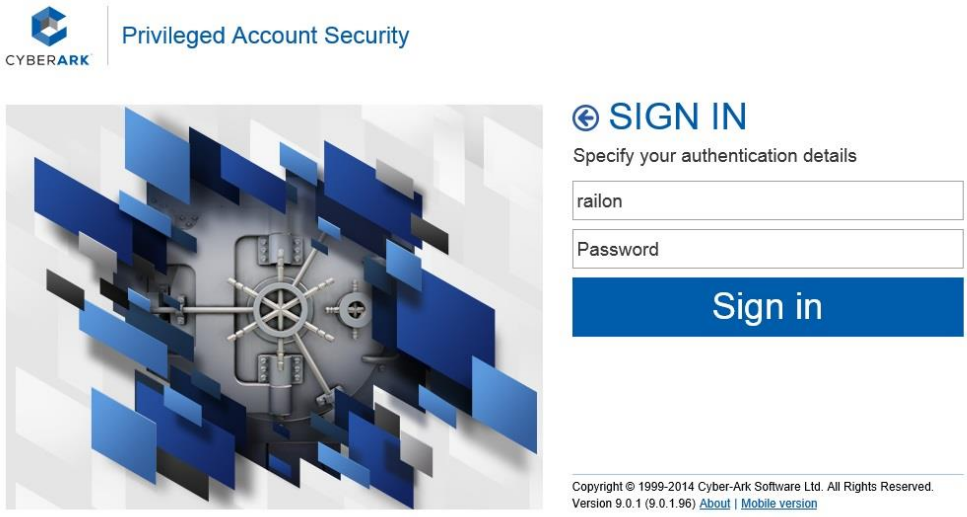
Appendix B – Example authentication processes

Example #1 – Duo auto method with push

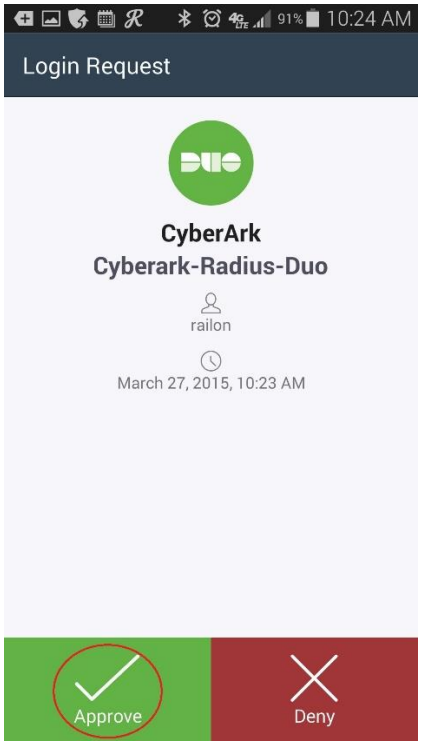
1. Open PVWA and select “RADIUS”



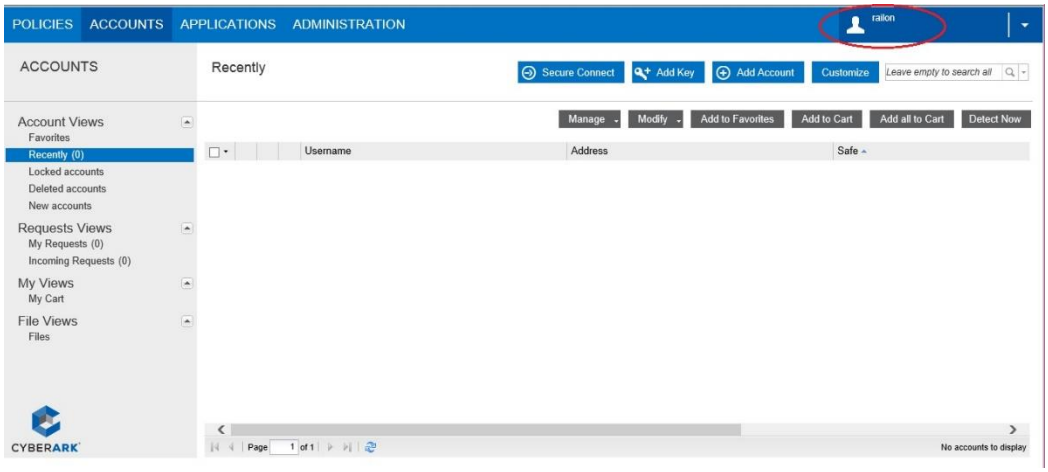
2. Enter AD user and password, then click “Sign in”, the login process will wait



3. Duo message received on mobile device for approval

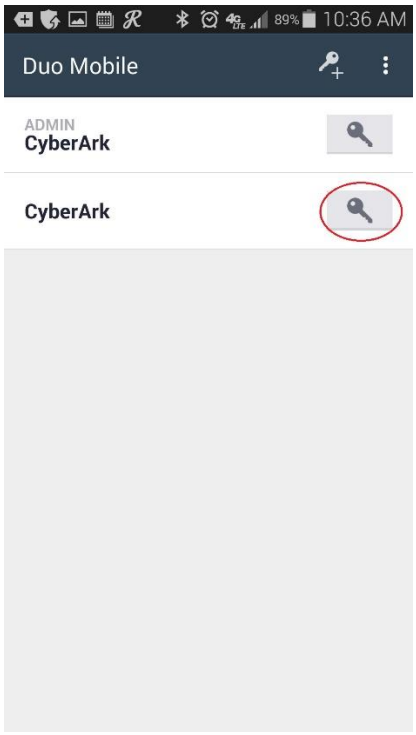


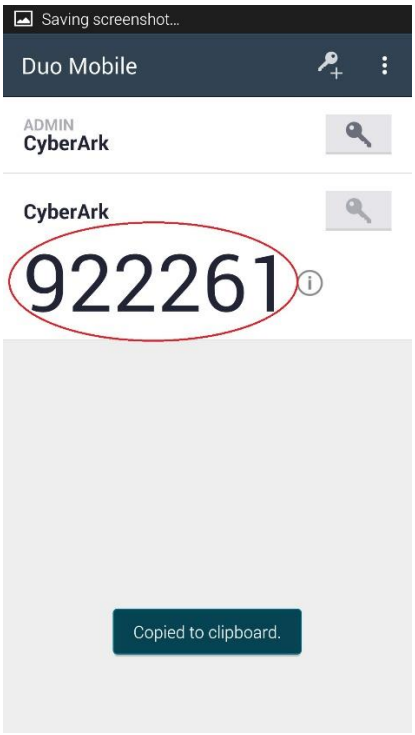
4. PVWA authentication complete



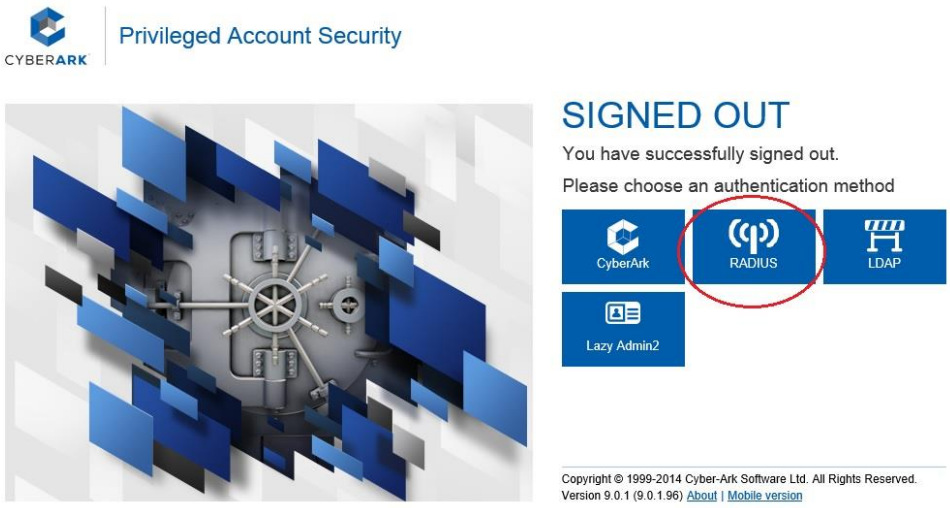
Example #1 – Duo auto method with passcode

1. Open the Duo app and click the key icon to get a passcode:

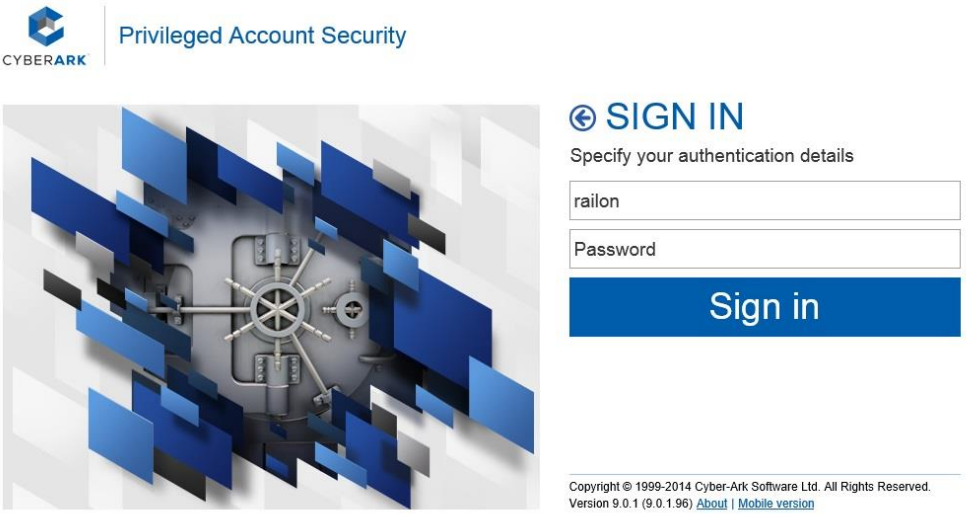




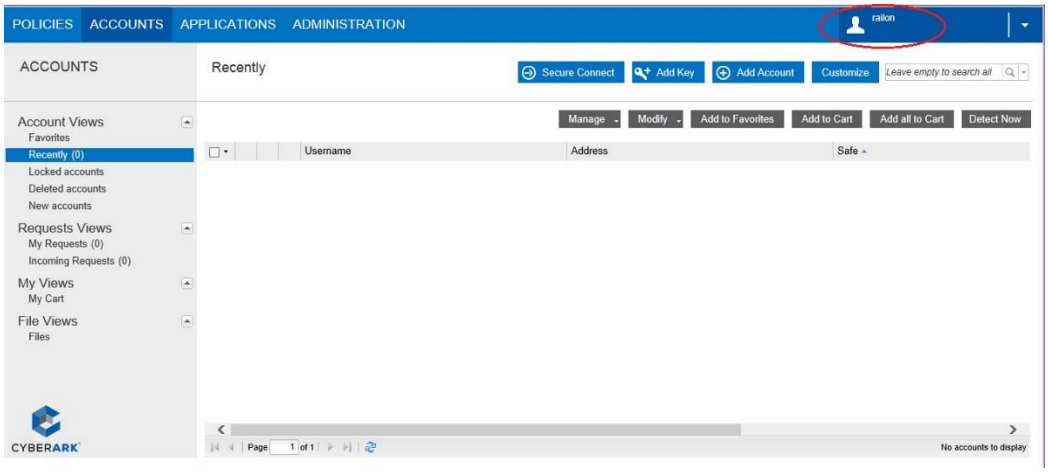
2. Open PVWA and select “RADIUS”



2. Enter AD user. Enter AD password followed by a comma (“,”) and then the Duo passcode from step 1 to your password (e,g mypassword,922261). Click “Sign in”.



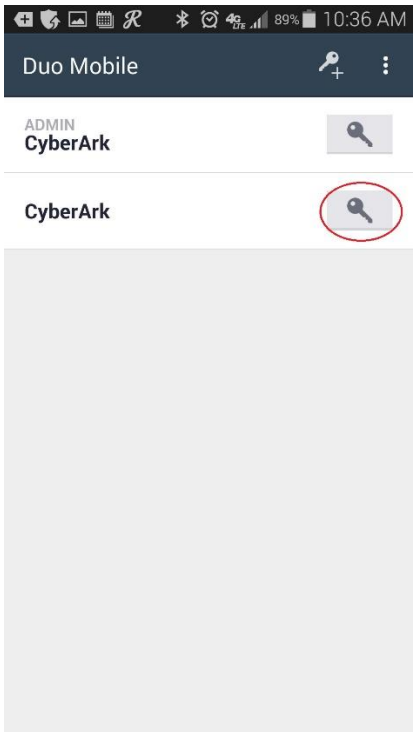
4. PVWA authentication complete

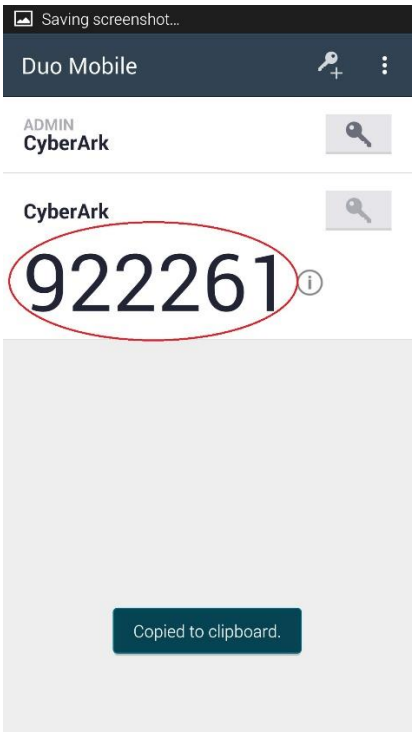


CYBERARK

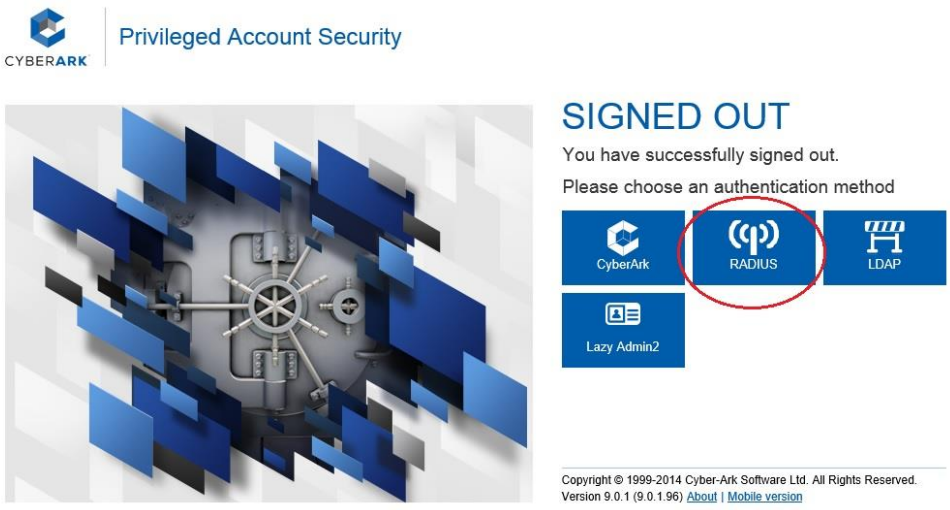
Example #3 – Duo challenge method

1. Open the Duo app and click the key icon to get a passcode:

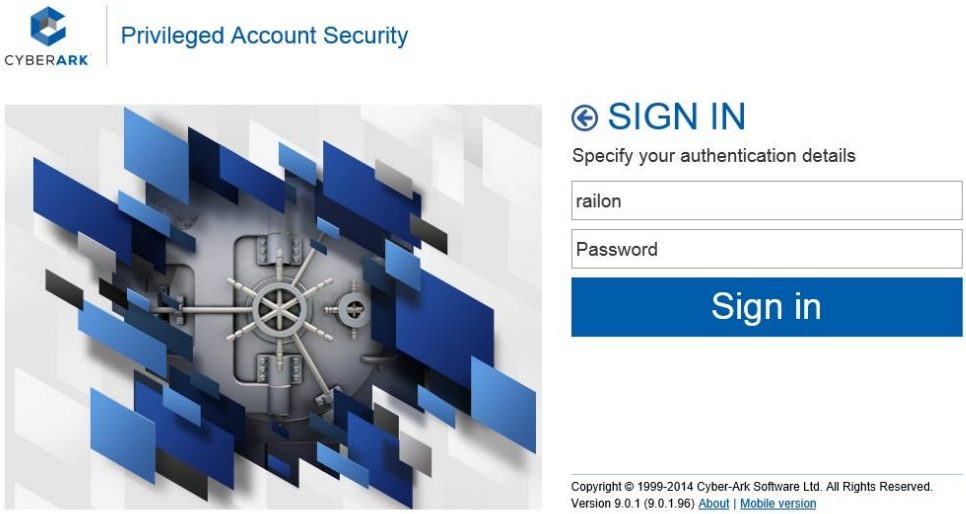




2. Open PVWA and select “RADIUS”



2. Enter AD user and password, then click “Sign in”



4. Challenge screen displayed in PVWA – enter Duo passcode from step 1, then click “Post Answer”

4. PVWA authentication complete