Datablink Management Server Integration Guide

Using RADIUS protocol for CyberArk Privileged Account Security Suite

datablink

Document Information

Document Revision	Rev 1.1
Release Date	August 2016

USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com

CONTENTS

USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com

Description

Datablink Management Server (DMS) provides management processes using highly flexible security policies, token choice, and integration APIs.

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:

- Deploy the multi-factor authentication (MFA) option in CyberArk Privileged Account Security Suite using Datablink authenticators managed by DMS.
- Configure CyberArk Privileged Account Security Suite to work with DMS in RADIUS mode.

It is assumed that the CyberArk Privileged Account Security Suite environment is already configured and deployed to meet the environment's needs prior to implementing MFA using DMS.

CyberArk Privileged Account Security Suite can be configured to support MFA in several modes. The RADIUS protocol will be used for working with DMS.

Environment

The integration environment that was used in this document is based on the following software versions:

Datablink Management Server (DMS) – Version 5.3

Datablink Mobile Management Plug-in – Version 5.3

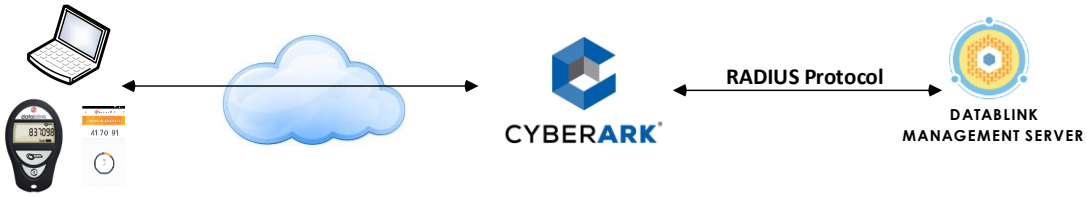
CyberArk Privileged Account Security Suite – Version 9.6

USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com

CyberArk Privileged Account Security Suite RADIUS authentication flow using DMS

DMS communicates with a number of various Virtual Private Network (VPN) and access gateway solutions using the RADIUS protocol.

The following diagram depicts the data flow of a MFA transaction for CyberArk Privileged Account Security Suite.



For more information on how to install the DMS and Datablink Mobile Management Plug-in, refer to *Datablink Management Server 5.3 Setup Manual* and *Datablink Mobile Management Plug-in 5.3 Setup Manual*.

USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com

Prerequisites

To enable DMS to receive RADIUS requests from CyberArk Privileged Account Security Suite, ensure the following:

- End users can authenticate through the CyberArk Privileged Account Security Suite environment with the CyberArk native protocol.
- Port 1812 is open between CyberArk Privileged Account Security Suite and DMS in both directions.
- A shared secret key has been chosen. A shared secret key provides an added layer of security by supplying an indirect reference to a shared secret key. The RADIUS server and the RADIUS client use it by mutual agreement between them for encryption, decryption, and digital signatures.
- A token is enrolled to a user in DMS.
- To enable a Push authentication, confirm the following ports are open between the Mobile Plug-in and the Internet:
  For iOS:
  - TCP port 5223
  - TCP port 2195-2196
  - TCP port 443

  For Android:
  - TCP port 5228-5230
  - TCP port 443

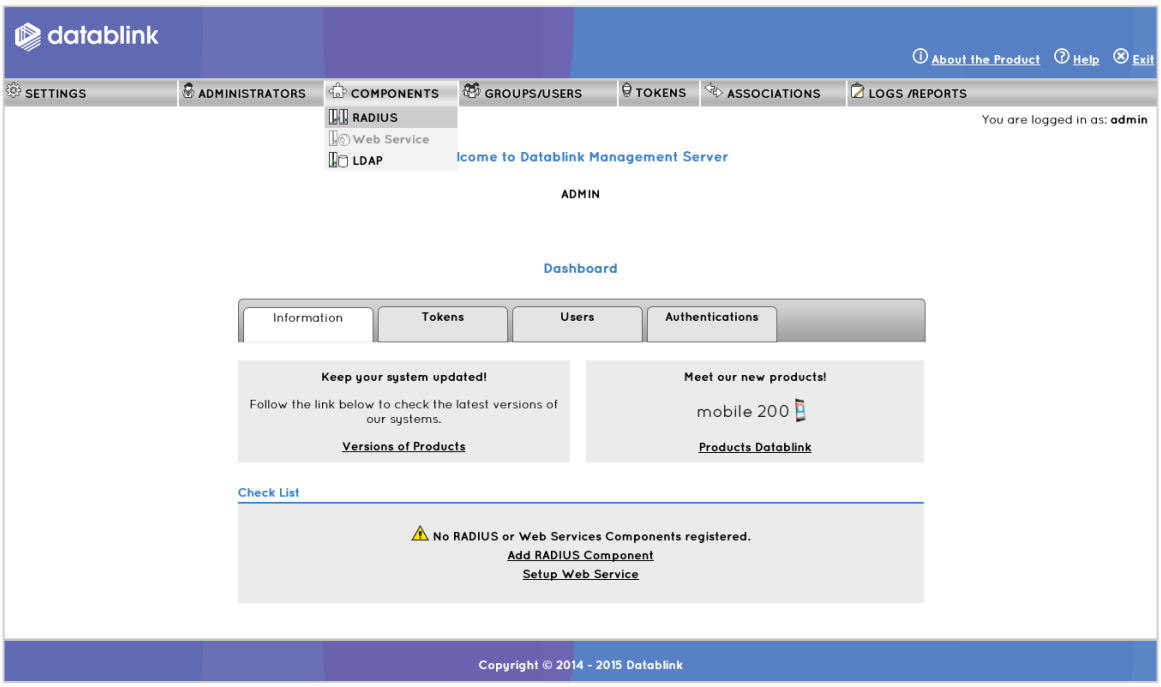
USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com

Configuring the DMS

To receive RADIUS authentication requests from the CyberArk Privileged Account Security Suite, define the CyberArk Privileged Account Security Suite as a RADIUS client in the DMS.
Please note that when the CyberArk Privileged Account Security Suite is defined as a RADIUS client in the DMS, it has to be assigned to the user's group that will use the CyberArk Privileged Account Security Suite.

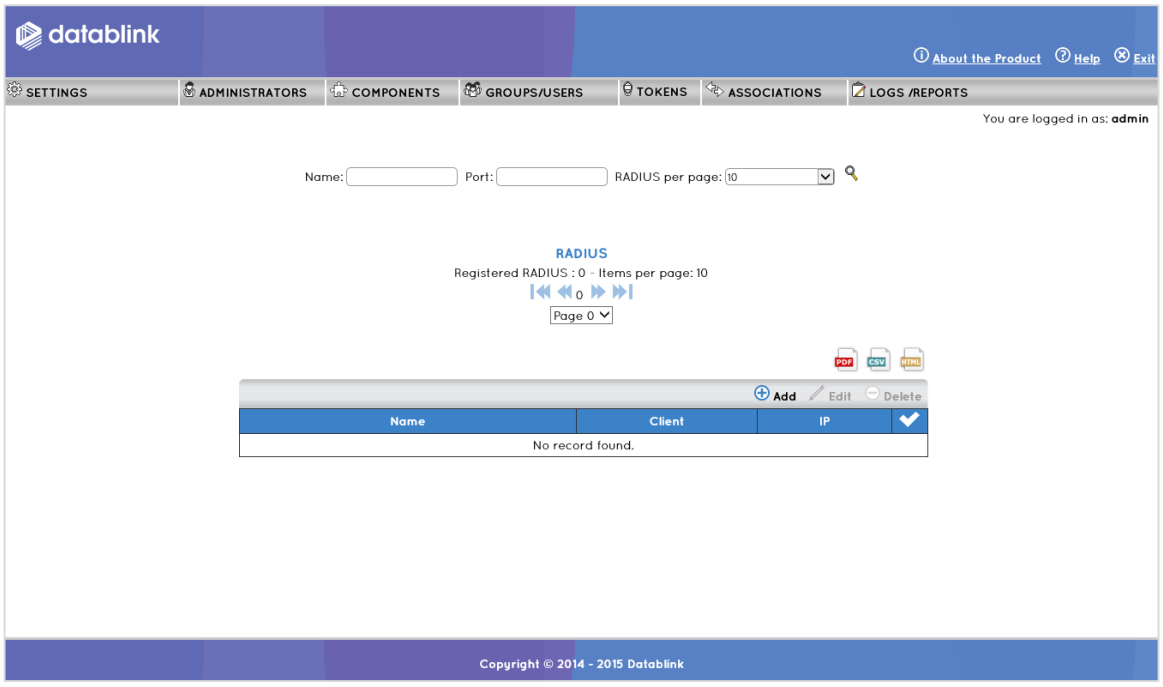
Adding CyberArk Privileged Account Security Suite as a RADIUS client in DMS

1. In the DMS web administration, on the toolbar, click on **COMPONENTS > RADIUS.**



USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com

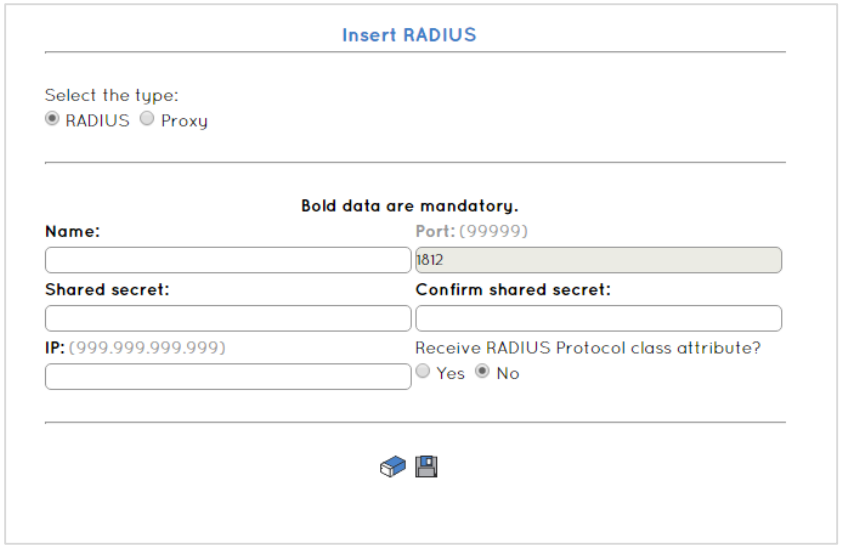
2. Click the **Add** icon.



3. In the **Insert RADIUS** window**,** complete the following fields and then click the save icon ( ).

Select the type	Select **RADIUS**
Name	Enter a name for the CyberArk Privileged Account Security Suite (e.g., **CyberArk**)
Shared secret	Enter a shared secret
Confirm shared secret	Enter the same shared secret
IP	Enter the internal server name or the IP address of the CyberArk Privileged Account Security Suite

USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com

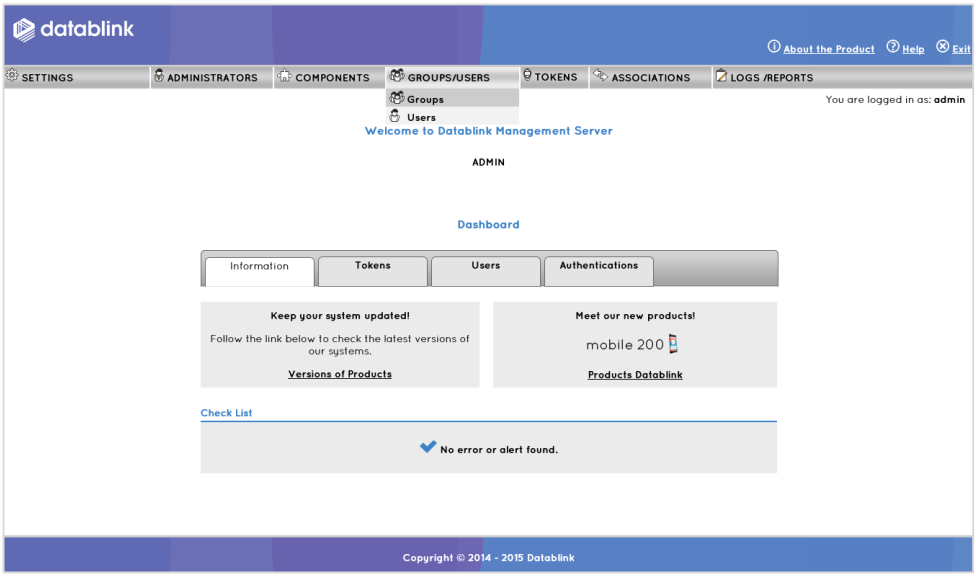


USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com

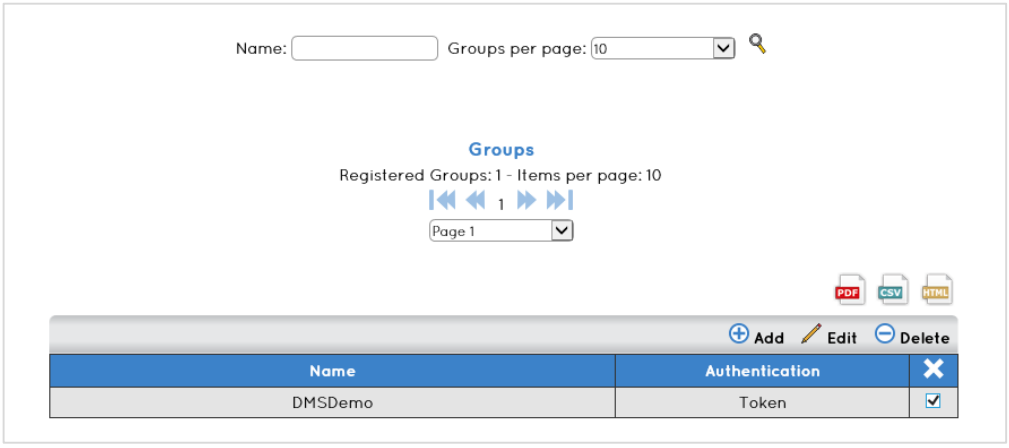
Configuring a user's group for a RADIUS authentication

Users should be set to authenticate using the CyberArk Privileged Account Security Suite RADIUS client that was added to the DMS. The user's group will be defined to use this RADIUS client.

1. On the toolbar in the DMS web administration, click on **GROUPS/USERS > Groups.**

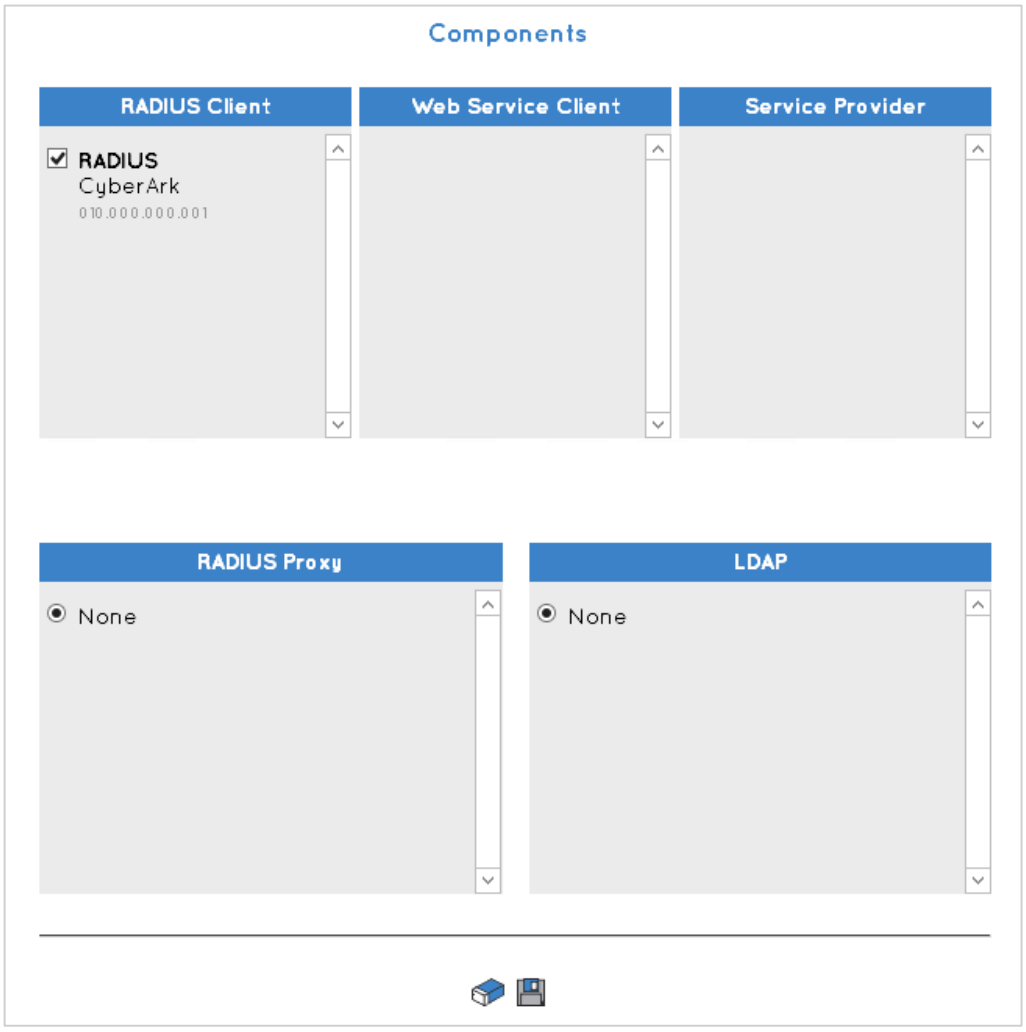


2. Select and enable the checkbox on the right of the desired group name, and click on **Edit**.



USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com

3. Under the **Components**, in the **RADIUS Client** list, select the RADIUS client of the CyberArk Privileged Account Security Suite.



4. Click on the save icon ( ).

USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com

Configuring CyberArk Privileged Account Security Suite

To set up CyberArk Privileged Account Security Suite using the RADIUS protocol with DMS, the following should be performed:

- Configuring a Shared Secret Key
- Configuring a RADIUS Server on the Vault
- Adding RADIUS Authentication to the CyberArk Privileged Account Security Suite
- Setting the User Authentication as RADIUS

For additional information on configuring RADIUS authentication, please refer to the "RADIUS Authentication" section in the *CyberArk Privileged Account Security Installation Guide*.

Configuring a Shared Secret Key

A shared secret key should be created and be stored in an encrypted file.

On the Vault server, run **CAVaultManager** to create an encrypted RADIUS shared secret key and store it as a file. Use the following example:

CAVaultManager SecureSecretFiles /SecretType Radius /Secret *<VaultSecret>* /SecuredFileName *<location>RadiusSecret.dat***

Configuring a RADIUS Server on the Vault

1. On the Vault server, open **Server Central Administration**.
2. Shut down the PrivateVault server by clicking on the stoplight () icon.
3. Edit the **DBParm.ini** file in **C:\Program Files (x86)\PrivateArk\Server** and add the **RadiusServerInfo** key under the **[MAIN]** section:
   RadiusServerInfo=*<RADIUS_Server_IP/Hostname>*;<RADIUS_Port>;<Vault_Hostname>;<RADIUS shared secret file>

RADIUS_Server_IP/Hostname	The DMS IP or hostname
RADIUS_Port	Port number of the RADIUS (DMS default 1812)

USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com

Vault_Hostname	The name or IP of the RADIUS client
RADIUS shared secret file	The location and filename of the shared secret key file that was previously created

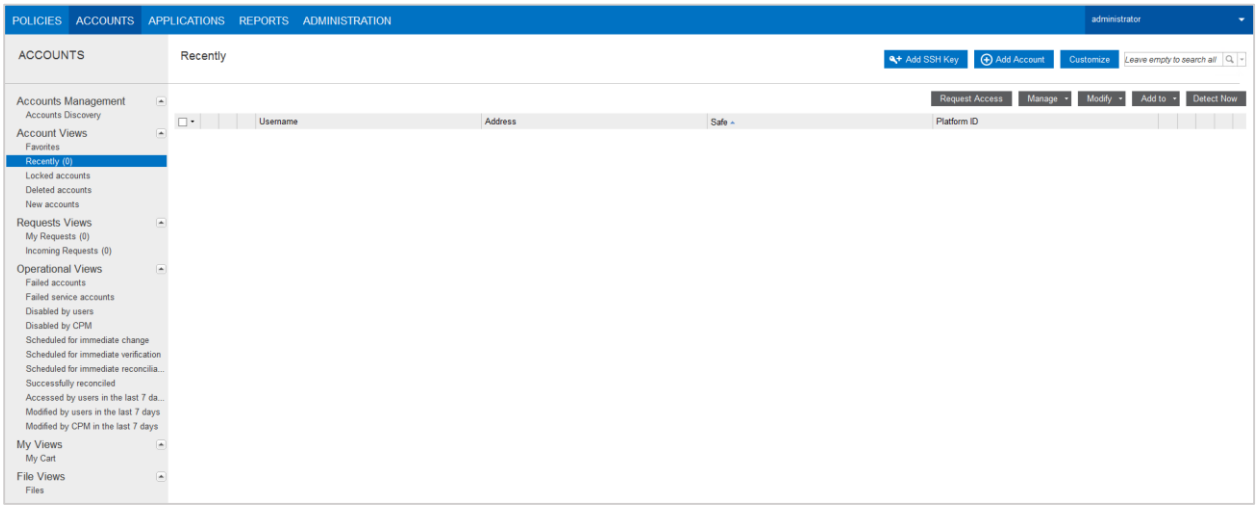
```
[MAIN]
RadiusServersInfo=10.0.0.2;1812;DMS;RadiusSecret.dat
TasksCount=20
DateFormat=DD.MM.YY
TimeFormat=HH:MM:SS
...
...
ASymCipherAlg=RSA-2048
[SYSLOG]
UseLegacySyslogFormat=Yes
```

4. On the Vault server, open **Server Central Administration**.
5. Start the PrivateVault server but clicking on the  icon.

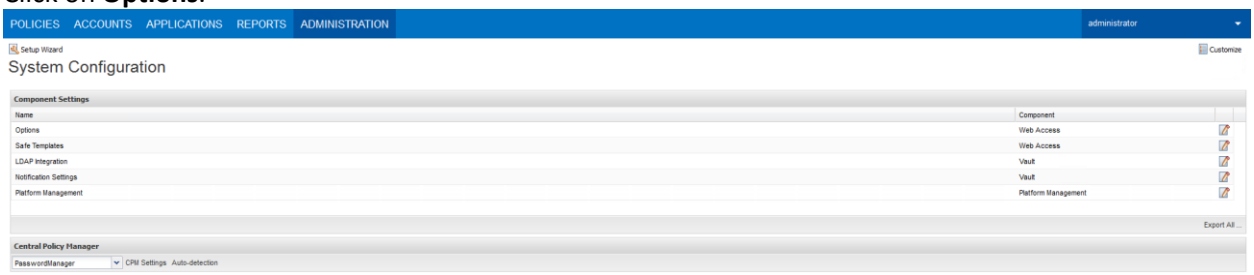
USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com

Adding RADIUS Authentication to the CyberArk Privileged Account Security Portal

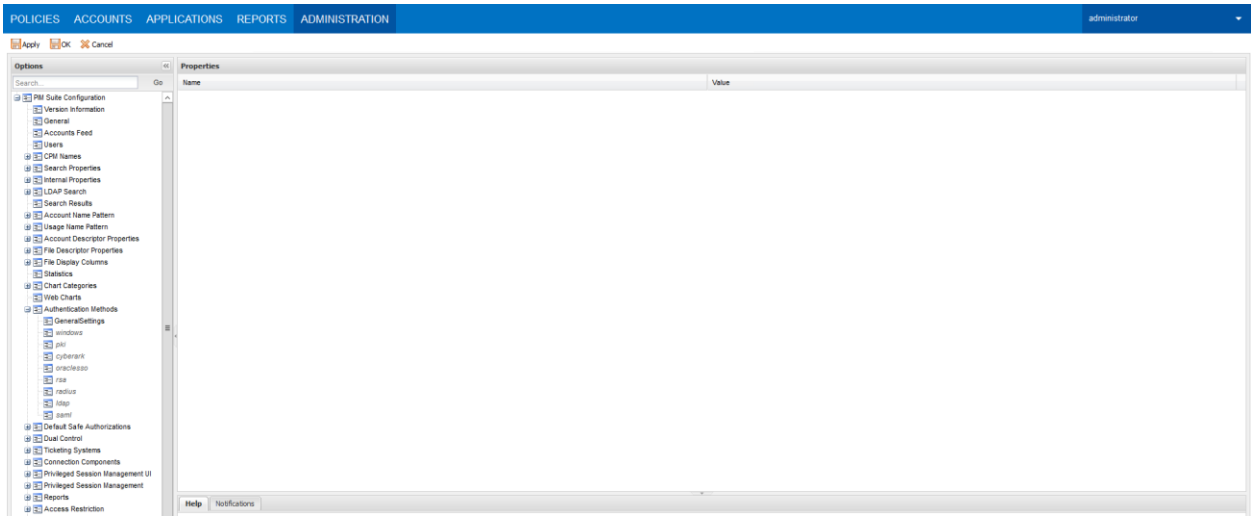
1. Log in to the Privileged Account Security portal as an Administrator.
2. Click on **ADMINISTRATION** tab.



3. Click on **Options**.



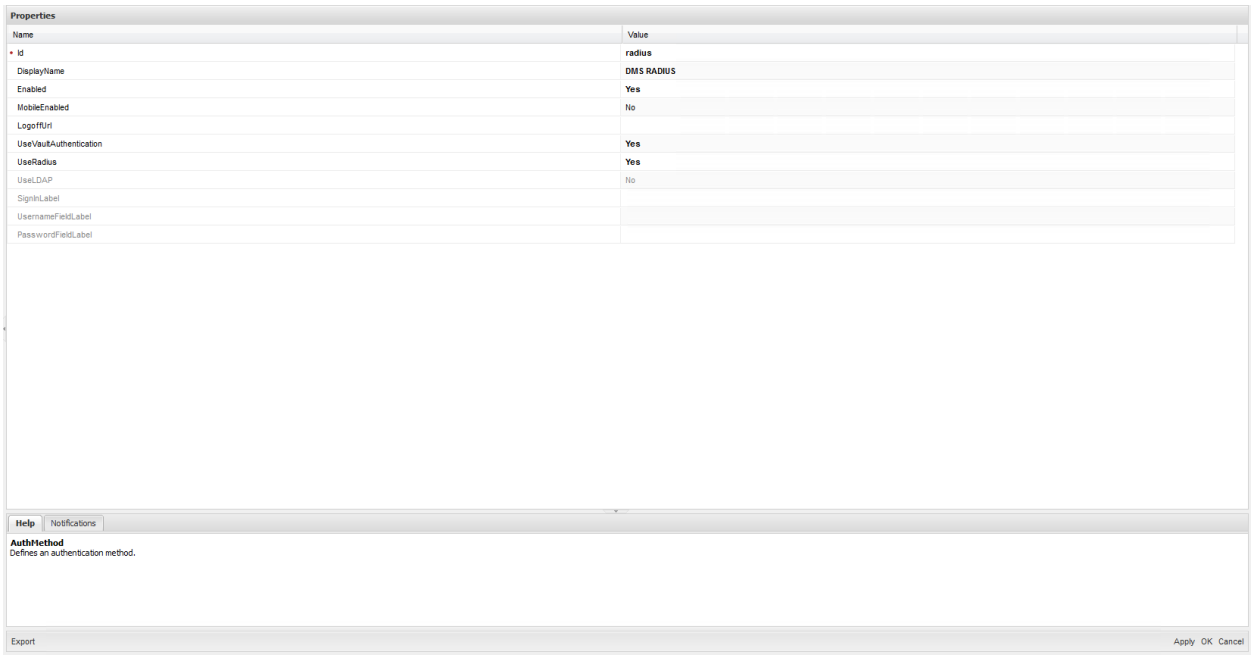
4. Click on **Authentication Methods > radius**.



USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com

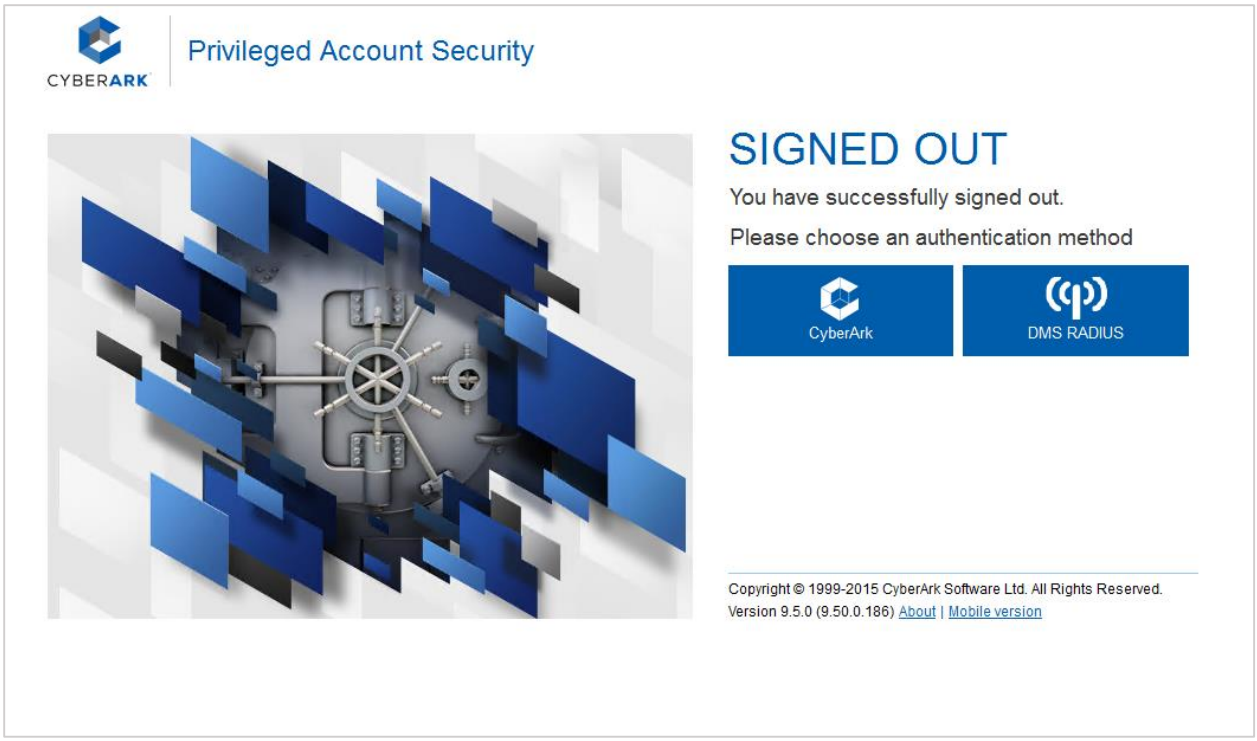
5. On the **Properties** pane, complete the following fields and click **Apply.**

DisplayName	Enter a friendly name for the policy. This name will be displayed on the Privileged Account Security portal login page.
Enabled	Select **Yes.**
UseRadius	Select **Yes**.



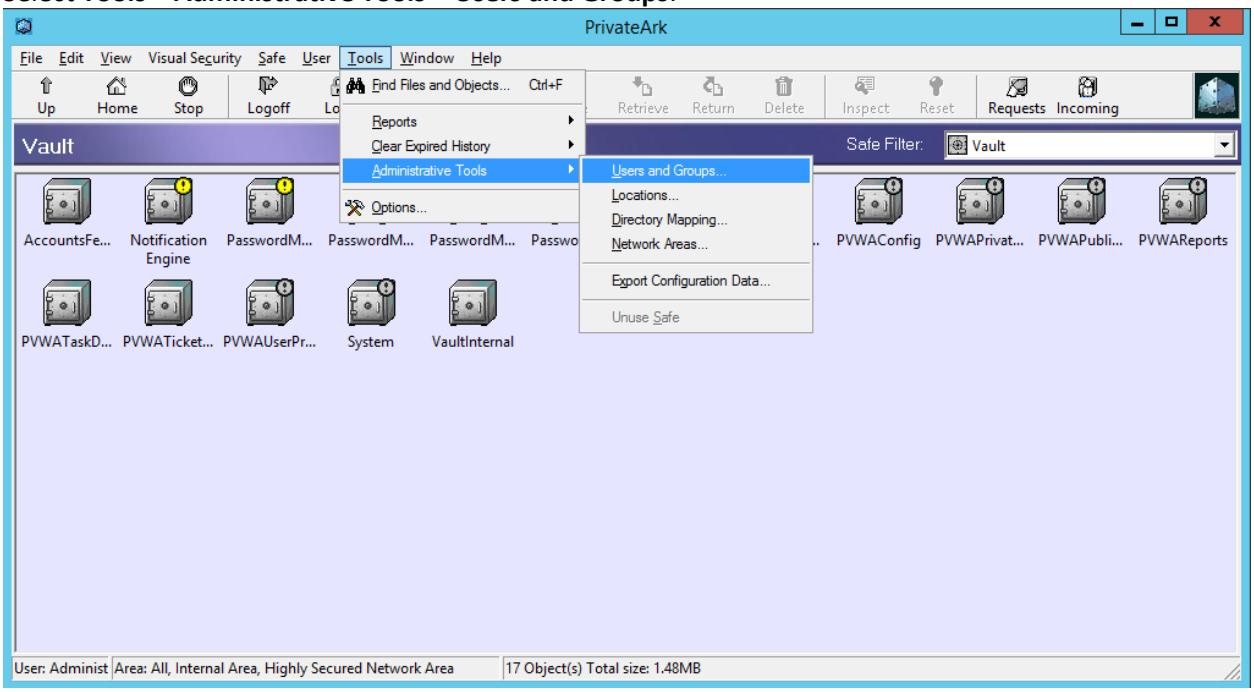
6. Sign out from the Privileged Account Security portal. The newly added authentication method (e.g., DMS RADIUS) will appear on the sign out screen, verifying that it has been added successfully.

USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com



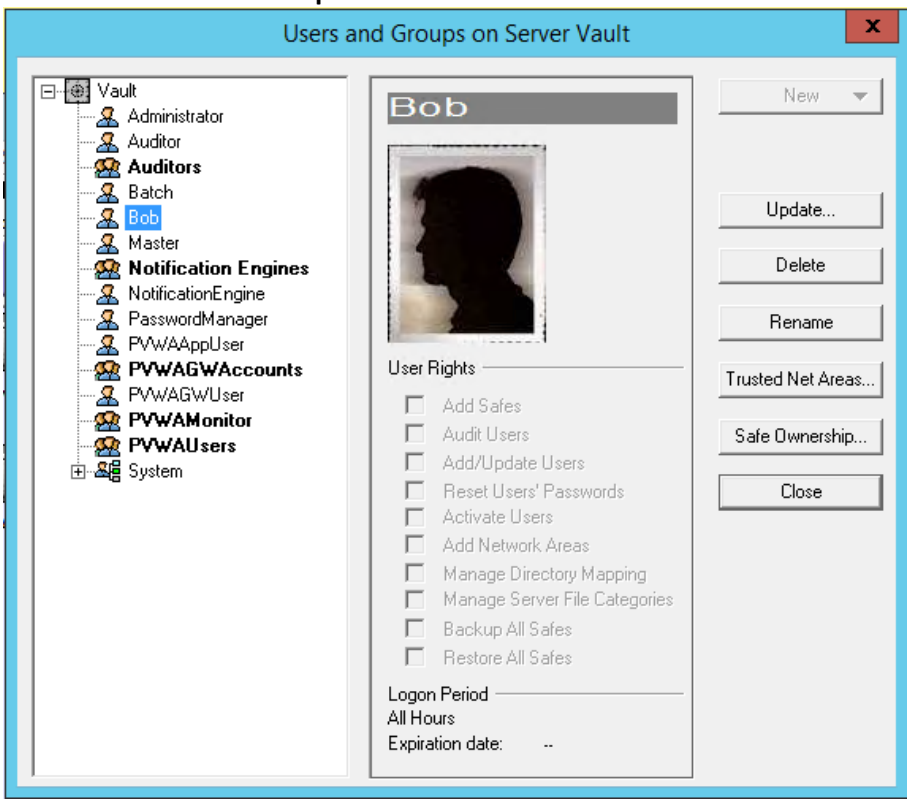
Setting the User Authentication as RADIUS

1. Open the PrivateArk console and log in to the Vault.
2. Select **Tools > Administrative Tools > Users and Groups**.

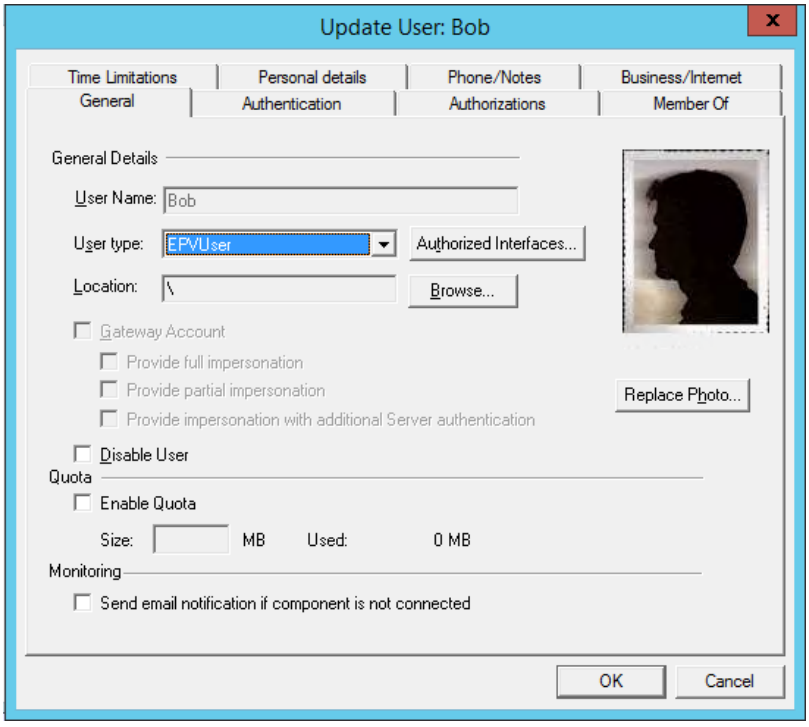


USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com

3. Select the user and click **Update**.

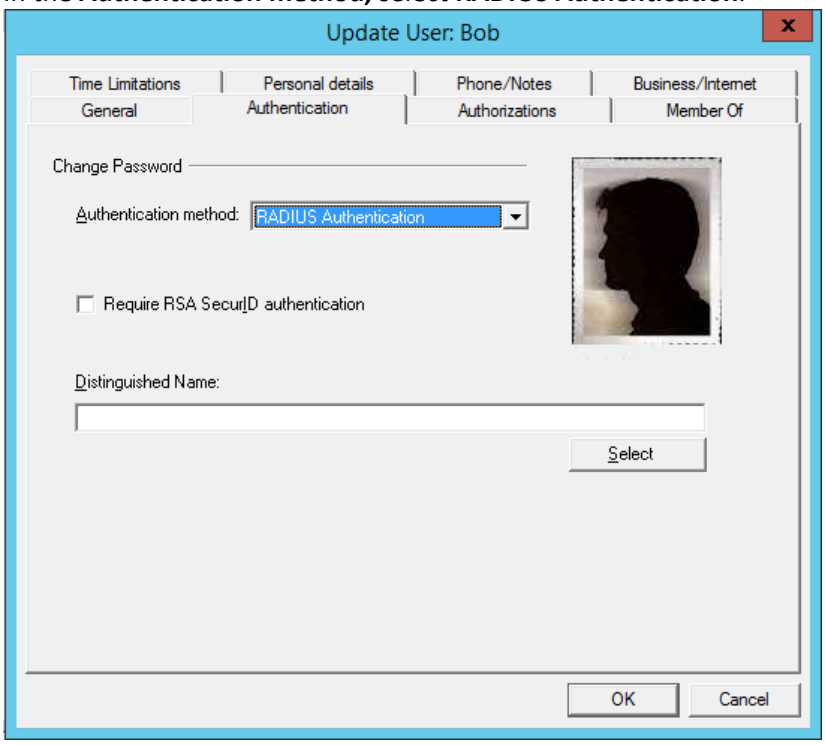


4. Click the **Authentication** tab.



USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com

5. In the **Authentication method,** select **RADIUS Authentication**.



6. Click **OK** and then click **Close**.

USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com

Running the Solution

The authentication can be performed with either a hardware token or a mobile token that is installed on a mobile device.

When using the mobile token, the authentication can be performed with a one-time password (OTP) or with a push authentication method, where the user receives a push notification that enables the user to approve the connection using the mobile application.

This example demonstrates configuration and use of the push authentication method.

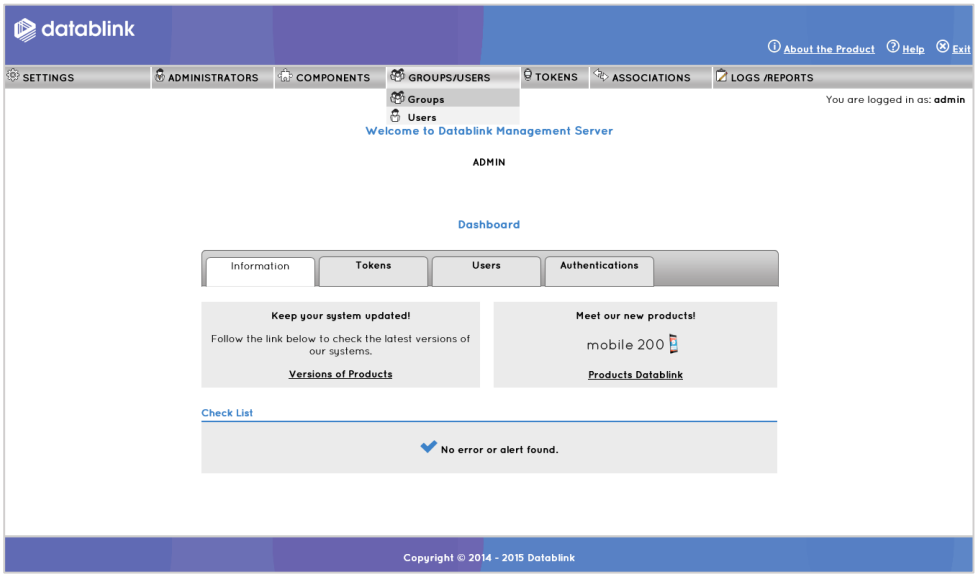
In this chapter, the following will be explained:

- Configuring Push Authentication in DMS
- Connecting Using Privileged Account Security Portal

Configuring Push Authentication in DMS

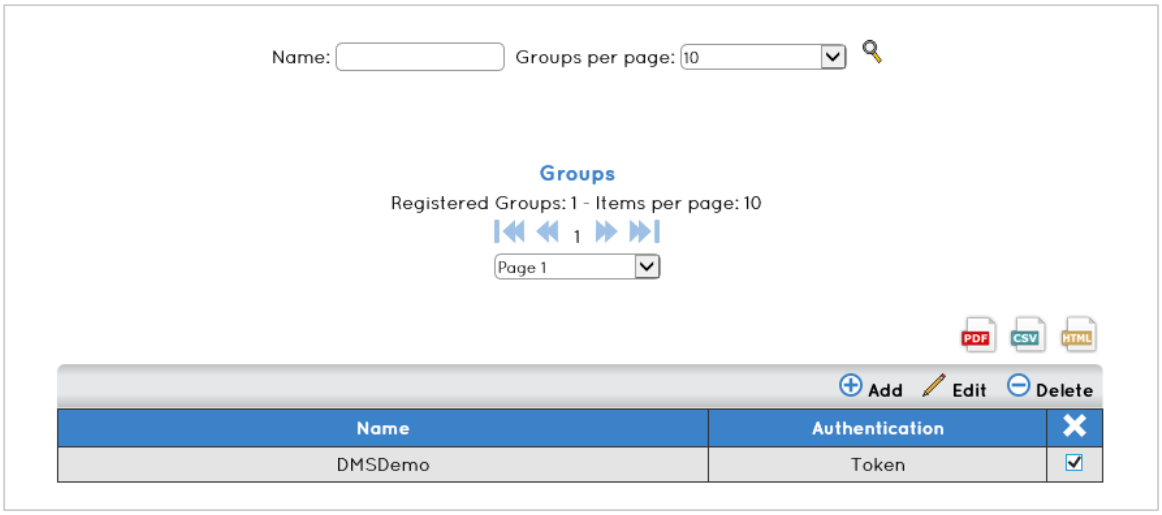
The push authentication method enables the user to approve the authentication by clicking on the mobile token instead of typing an OTP.

1. In the DMS web administration, on the toolbar, click on **GROUPS/USERS > Groups.**



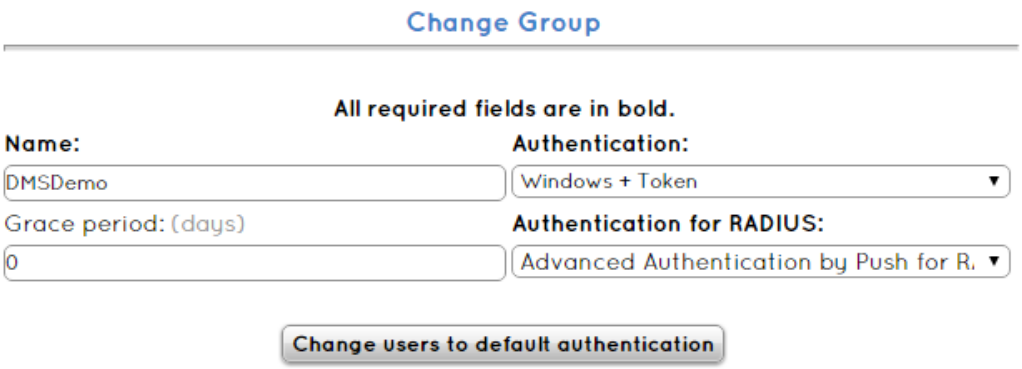
2. Select and enable the checkbox on the right of the desired group name, and click on **Edit**.

USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com



3. In the first section, set the following:

Authentication	Select one of the following: • **Password + Token** • **Windows + Token** • **LDAP + Token** In this example, **Windows + Token** was chosen
Authentication for RADIUS	Select **Advanced Authentication by Push**



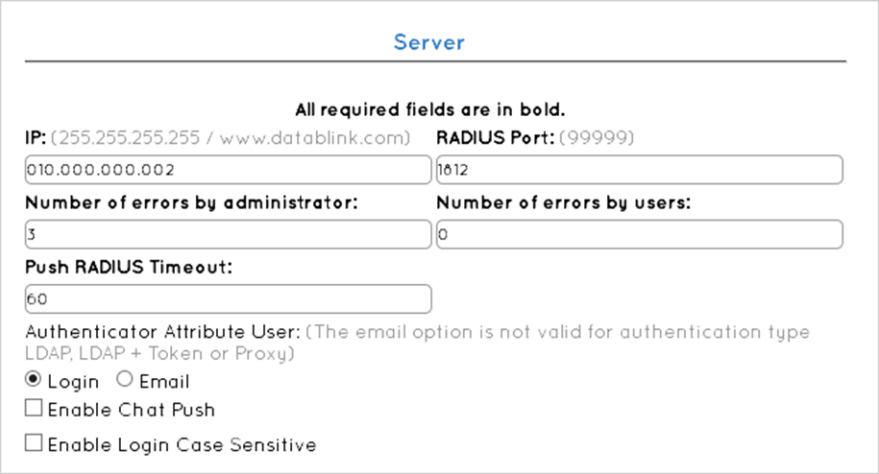
4. Click on the save icon ( ) on the bottom of the page.

USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com

***NOTE**: It is highly recommended to increase the default authentication timeout when using push authentication.*

Changing the authentication timeout in DMS

1. In the DMS web administration, on the toolbar, click on **SETTINGS > Server.**
2. On the upper section, change the **Push RADIUS Timeout** field to 60.



3. Click on the save icon ( ) on the bottom of the page.

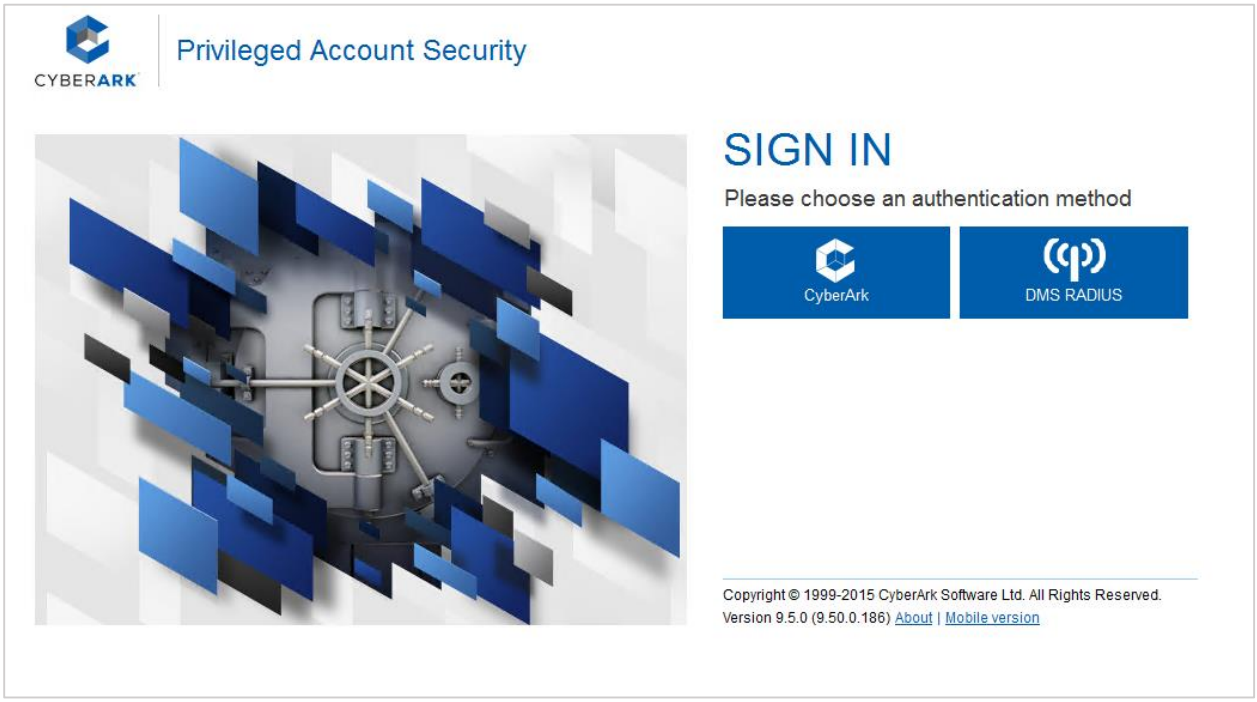
Changing the authentication timeout in CyberArk Privileged Account Security Suite

1. On the Password Vault Web Access server, edit the file ***<Installation directory>*\Password Vault Web Access\VaultInfo\Vault.ini**
2. Remove the **#** char before the **#TIMEOUT=30** and change the timeout to 60.
3. Save the file.
4. On the Vault server, edit the file ***<Installation directory>*\Server\dbparm.ini**
5. Change the **DefaultTimeout** value to 60.
6. Save the file.

USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com

Connecting Using Privileged Account Security Portal

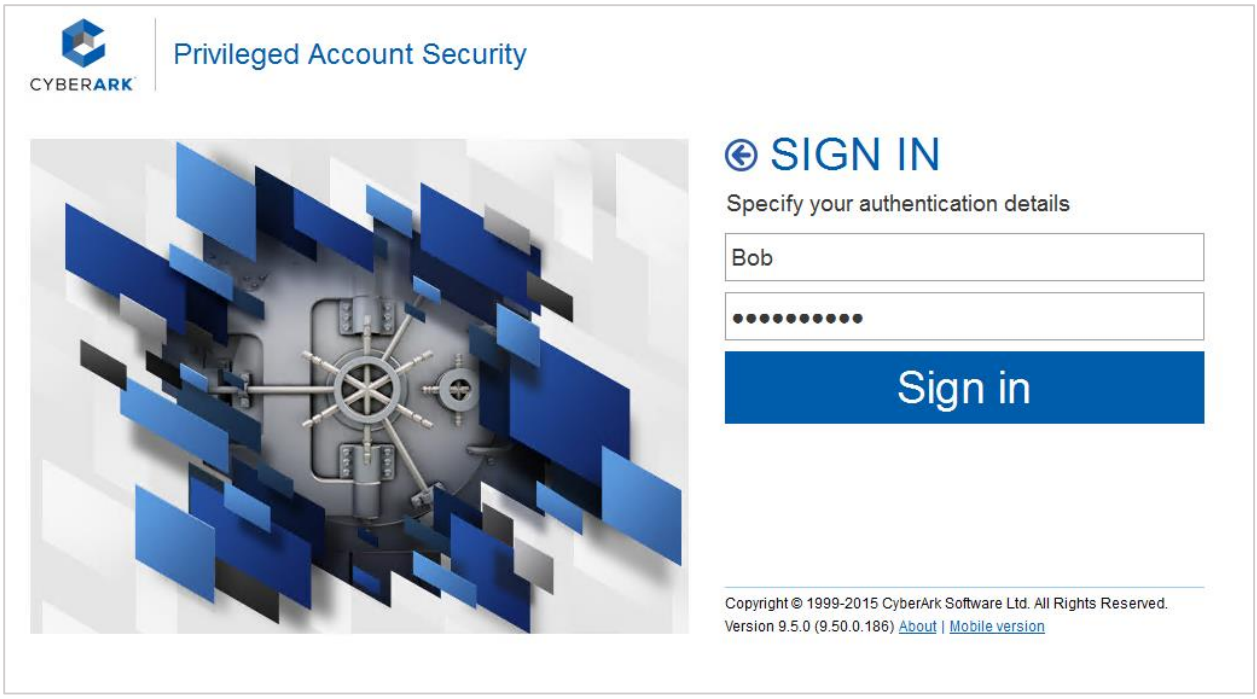
1. On the Privileged Account Security Portal login page, select the RADIUS authentication method (for example, **DMS RADIUS**).



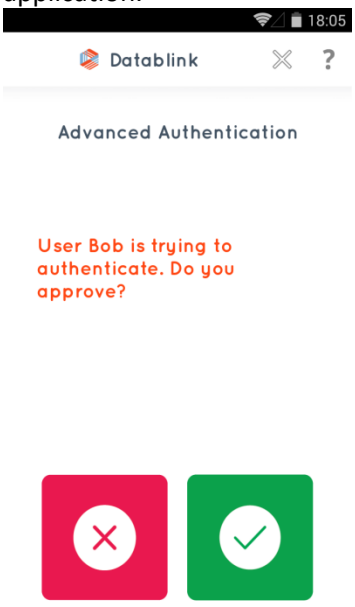
2. Complete the following fields and click **Sign in:**

User name	Enter the required user name
Password	Enter the windows password of the user

USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com

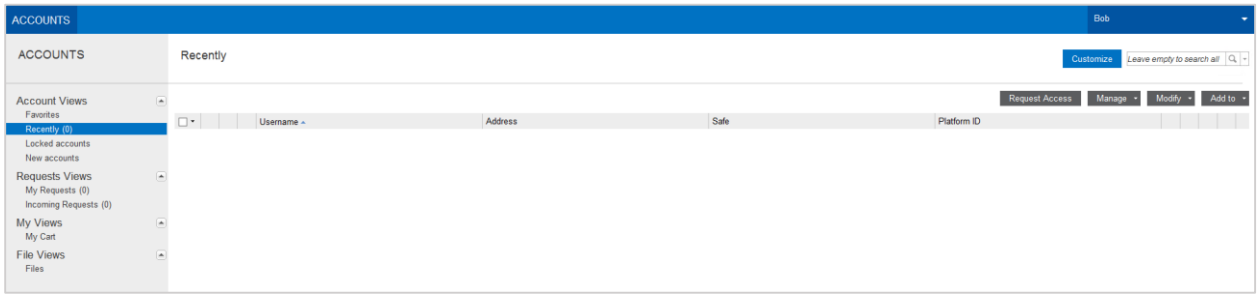


3. Click on the approval button in the authentication approval request that appears in the mobile application.



USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com

The user is logged in to the Privileged Account Security Portal.



USA: +1 703 639-0600
Brazil: +55 11 4612-8334
support@datablink.com
www.datablink.com