SafeNet Authentication Service

Integration Guide

Using RADIUS Protocol for CyberArk Privileged Account Security Suite

Document Information

Document Part Number	007-012987-001, Rev. A
Release Date	April 2015

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as CyberArk Privileged Account Security Suite.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

SafeNet Authentication Service (SAS) delivers a fully automated, versatile, and strong authentication-as-a-service solution.

With no infrastructure required, SafeNet Authentication Service provides smooth management processes and 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 multi-factor authentication (MFA) options in CyberArk Privileged Account Security Suite using SafeNet one-time password (OTP) authenticators managed by SafeNet Authentication Service.
- Configure CyberArk Privileged Account Security Suite to work with SafeNet Authentication Service in RADIUS mode.

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

CyberArk Privileged Account Security Suite can be configured to support multi-factor authentication in several modes. The RADIUS protocol will be used for the purpose of working with SafeNet Authentication Service.

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—SafeNet's cloud-based authentication service
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—A server version that is used by service providers to deploy instances of SafeNet Authentication Service
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—A server version that is used to deploy the solution on-premises in the organization

Environment

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

- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**
- **CyberArk Privileged Account Security Suite—**Version 9.0.1

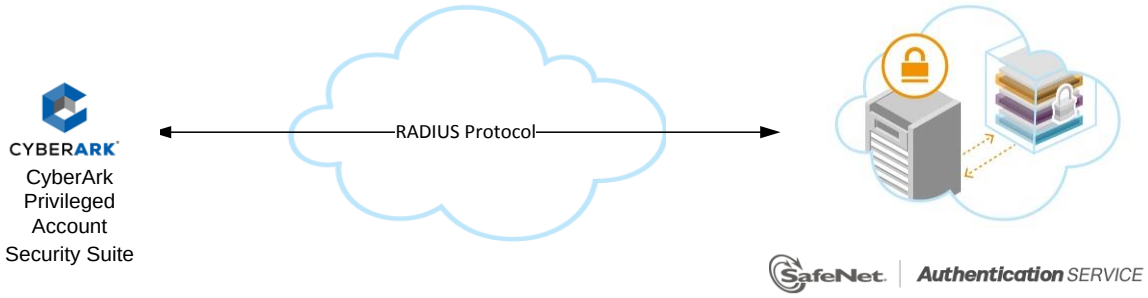
Audience

This document is targeted to system administrators who are familiar with CyberArk Privileged Account Security Suite, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

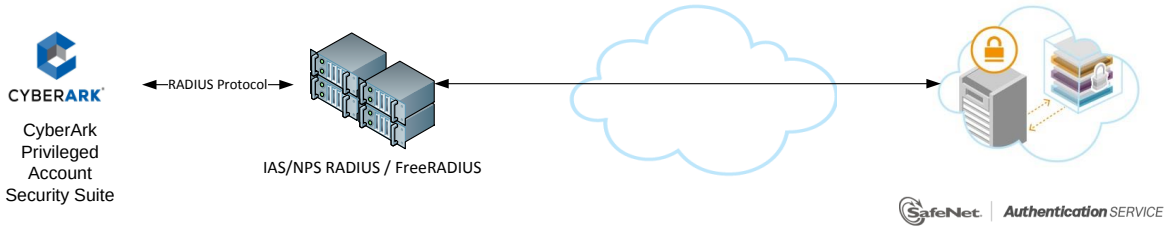
RADIUS-based Authentication using SAS Cloud

SAS Cloud provides two RADIUS mode topologies:

- **SAS cloud hosted RADIUS service—**A RADIUS service is already implemented in the SAS cloud environment, and can be used without any installation or configuration requirements.



- **Local RADIUS hosted on-premises**—A RADIUS agent is implemented in the customer's existing RADIUS environment. The agent forwards the RADIUS authentication requests to the SAS cloud environment. The RADIUS agent can be implemented on a Microsoft NPS/IAS or FreeRADIUS server.



This document demonstrates the solution using the SAS cloud-hosted RADIUS service.

For more information on how to install and configure the SafeNet Authentication Service Agent for IAS/NPS, refer to: http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf

For more information on how to install and configure FreeRADIUS, refer to the *SafeNet Authentication Service FreeRADIUS Agent Configuration Guide*.

RADIUS-based Authentication using SAS-SPE and SAS-PCE

For both on-premises versions, SAS can be integrated with the following solutions that serve as local RADIUS servers:

- **Microsoft Network Policy Server (MS-NPS)** or the legacy **Microsoft Internet Authentication Service (MS-IAS)**—SafeNet Authentication Service is integrated with the local RADIUS servers, using a special on-premises agent called SAS Agent for Microsoft IAS and NPS.

  For more information on how to install and configure the SAS Agent for Microsoft IAS and NPS, refer to:

  http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf

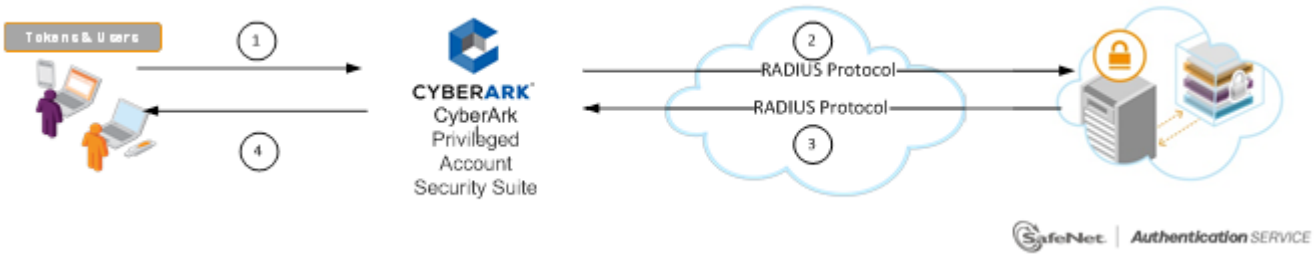
- **FreeRADIUS**—The SAS FreeRADIUS Agent is a strong authentication agent that is able to communicate with SAS through the RADIUS protocol.

  For more information on how to install and configure the SAS FreeRADIUS Agent, refer to the SafeNet Support Portal.

RADIUS Authentication Flow using SAS

SafeNet Authentication Service communicates with a large number of VPN and access gateway solutions using the RADIUS protocol.

The image below describes the data flow of a multi-factor authentication transaction for CyberArk Privileged Account Security Suite.



1. A user attempts to log on to CyberArk Privileged Account Security Suite using an OTP authenticator.
2. CyberArk Privileged Account Security Suite sends a RADIUS request with the user's credentials to SafeNet Authentication Service for validation.
3. The SAS authentication reply is sent back to the CyberArk Privileged Account Security Suite.
4. The user is granted or denied access to the CyberArk Privileged Account Security Suite based on the OTP value calculation results from SAS.

RADIUS Prerequisites

To enable SafeNet Authentication Service 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 a static password, before configuring the CyberArk Privileged Account Security Suite to use RADIUS authentication.
- Ports 1812/1813 are open to and from CyberArk Privileged Account Security Suite.
- A shared secret key has been selected. A shared secret key provides an added layer of security between the RADIUS server and RADIUS client for encryption, decryption, and digital signatures.

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with CyberArk Privileged Account Security Suite using RADIUS protocol requires:

- Synchronizing User Stores with SAS, page 7
- Assigning an Authenticator in SAS, page 8
- Adding CyberArk Privileged Account Security Suite as an Authentication Node in SAS, page 8
- Checking the SAS RADIUS Address, page 10

Synchronizing User Stores with SAS

Before SAS can authenticate any user in your organization, you must create a user store in SAS that reflects the users who need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

- Manually, one user at a time, using the **Create User** shortcut
- Manually, by importing one or more user records via a flat file
- Automatically, by synchronizing with your Active Directory/LDAP server using the SAS Synchronization Agent

For additional details on importing users to SafeNet Authentication Service, refer to “Creating Users” in the *SafeNet Authentication Service Subscriber Account Operator Guide*:

http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-SPE-SubscriberAccountOperatorGuide.pdf

All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.

Assigning an Authenticator in SAS

SAS supports a number of authentication methods that can be used as a second authentication factor for users authenticating through CyberArk Privileged Account Security Suite.

The following authenticators are supported:

- eToken PASS
- SMS Token
- MP-1 Software Token
- MobilePASS

Authenticators can be assigned to users in two ways:

- **Manual provisioning—**Assign an authenticator to users, one at a time.
- **Provisioning rule**—The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change. An authenticator will be assigned automatically to the user.

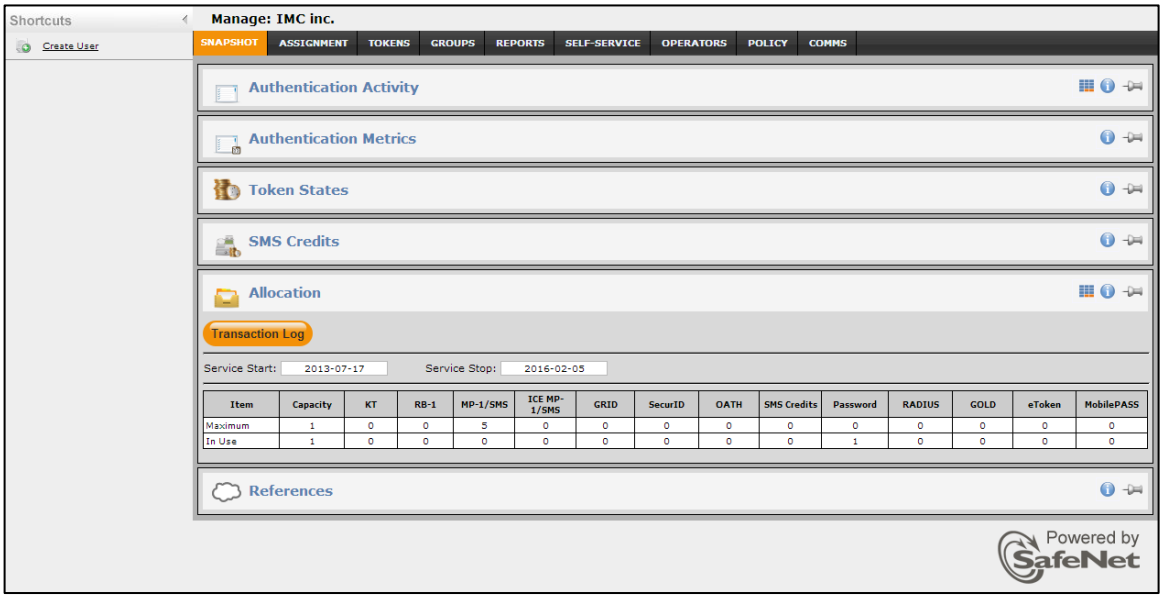
Refer to "Provisioning Rules" in the *SafeNet Authentication Service Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.

http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-SPE-SubscriberAccountOperatorGuide.pdf

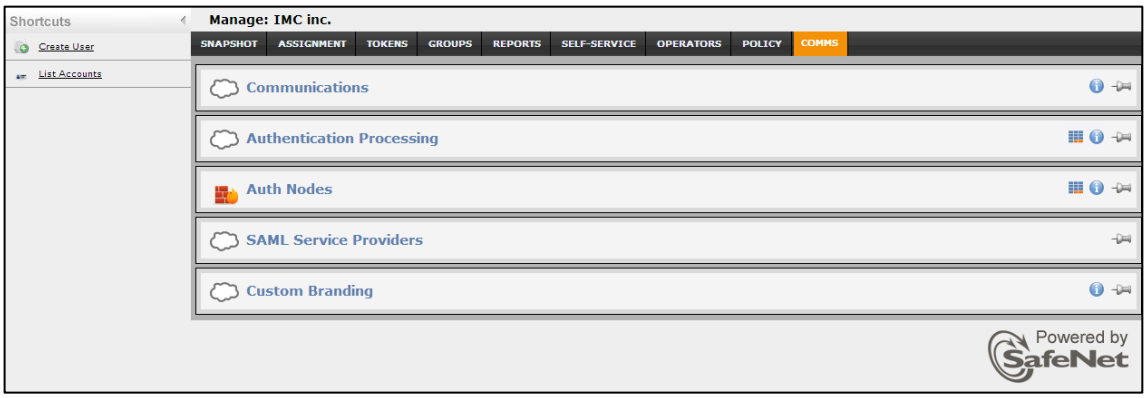
Adding CyberArk Privileged Account Security Suite as an Authentication Node in SAS

Add a RADIUS entry in the SAS **Auth Nodes** module to prepare it to receive RADIUS authentication requests from CyberArk Privileged Account Security Suite. You will need the IP address of CyberArk Privileged Account Security Suite and the shared secret to be used by SAS and CyberArk Privileged Account Security Suite.

1. Log in to the SAS console with an Operator account.



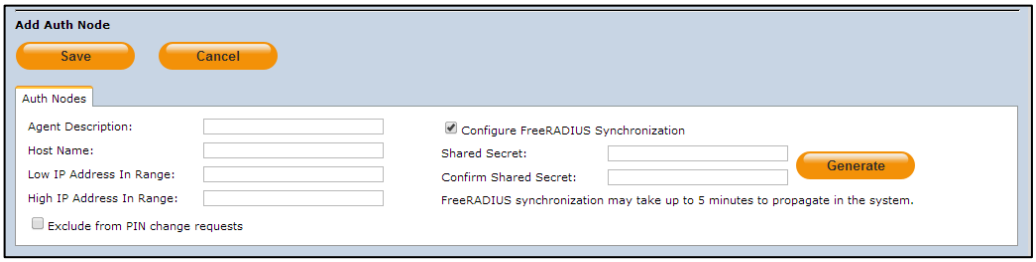
2. Click the **COMMS** tab, and then select **Auth Nodes**.



3. In the **Auth Nodes** module, click the **Auth Nodes** link.

4. Under **Auth Nodes**, click **Add**.
5. In the **Add Auth Nodes** section, complete the following fields, and then click **Save**:

Agent Description	Enter a host description.
Host Name	Enter the name of the host that will authenticate with SAS.
Low IP Address In Range	Enter the IP address of the host or the lowest IP address in a range of addresses that will authenticate with SAS.
High IP Address In Range	Enter the highest IP address in a range of IP addresses that will authenticate with SAS.
Configure FreeRADIUS Synchronization	Select this option.
Shared Secret	Enter the shared secret key.
Confirm Shared Secret	Re-enter the shared secret key.

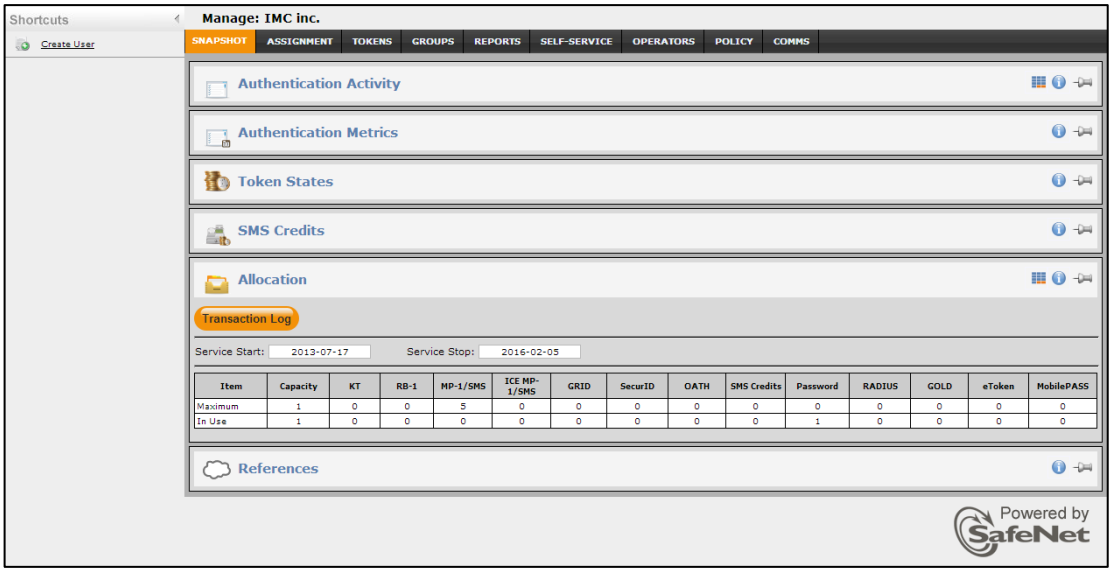


The Auth Node is added to the system.

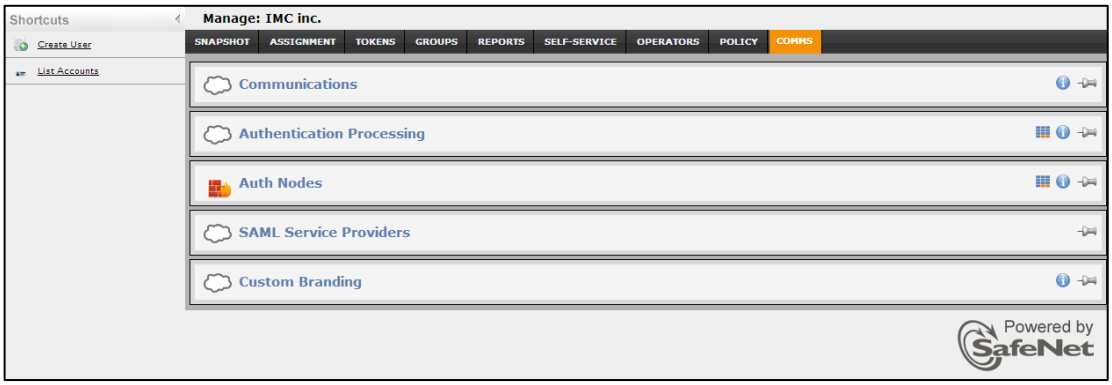
Checking the SAS RADIUS Address

Before adding SAS as a RADIUS server in CyberArk Privileged Account Security Suite, check its IP address. The IP address will be added to CyberArk Privileged Account Security Suite as a RADIUS server later in this document.

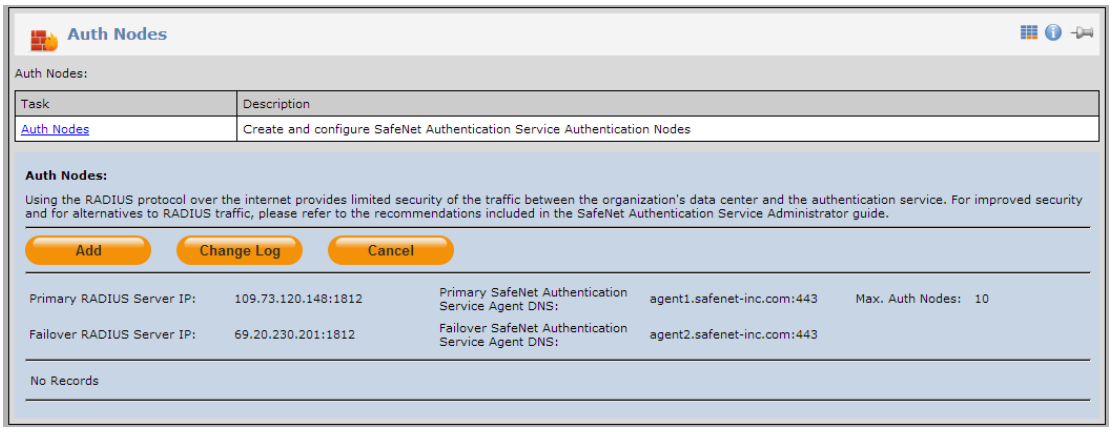
1. Log in to the SAS console with an Operator account.



2. Click the **COMMS** tab, and then select **Auth Nodes**.



3. In the **Auth Nodes** module, click the **Auth Nodes** link. The SAS RADIUS server details are displayed.



Configuring CyberArk Privileged Account Security Suite

Configuring CyberArk Privileged Account Security Suite to use RADIUS authentication requires the following:

- Configuring a RADIUS Shared Secret, page 11
- Configuring a RADIUS Server on the Vault, page 12
- Adding RADIUS Authentication to the Privileged Account Security Portal, page 13
- Configuring a User for RADIUS Authentication, page 15

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

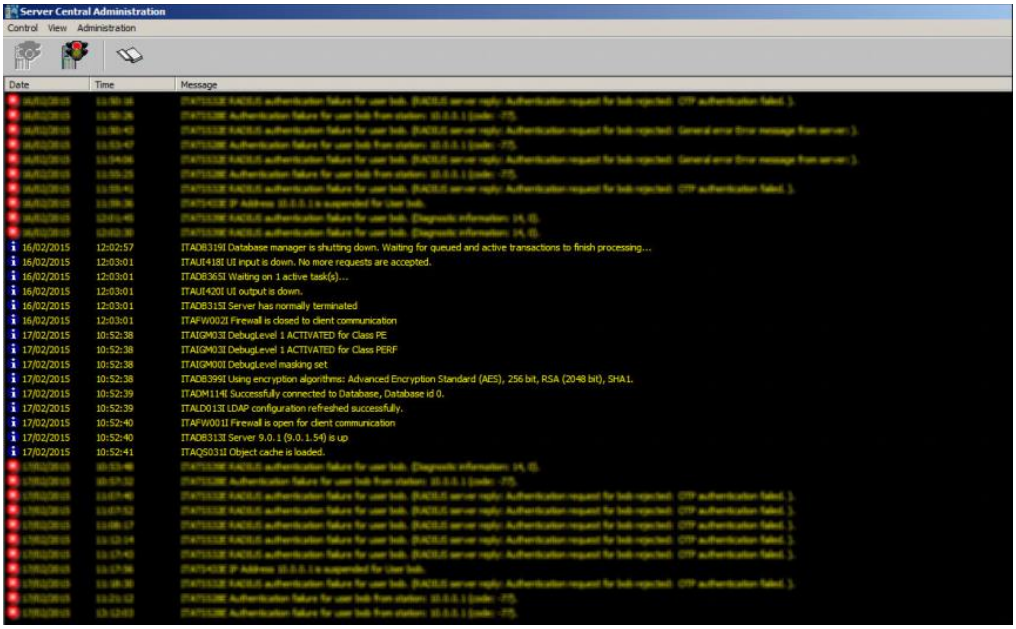
Configuring a RADIUS Shared Secret

1. Create a certificate for the vault (if needed).
2. On the RADIUS server, run **CAVaultManager** to create an encrypted RADIUS shared secret file. Refer to the following example:

   CAVaultManager SecureSecretFiles /SecretType Radius /Secret VaultSecret /SecuredFileName c:\RadiusSecret.dat

Configuring a RADIUS Server on the Vault

1. On the vault server, open **Server Central Administration**.
2. Click  to shut down the PrivateVault server.



(The screen image above is from CyberArk®. Trademarks are the property of their respective owners.)

3. Navigate to **C:\Program Files (x86)\PrivateArk\Server**.
4. Locate and open **DBParm.ini**, and add the **RadiusServerInfo** key under the **[MAIN]** section:

   RadiusServersInfo=RADIUS_Server_IP;RADIUS_Port;vaulthostname;radiusauth.dat

   Values are defined below.

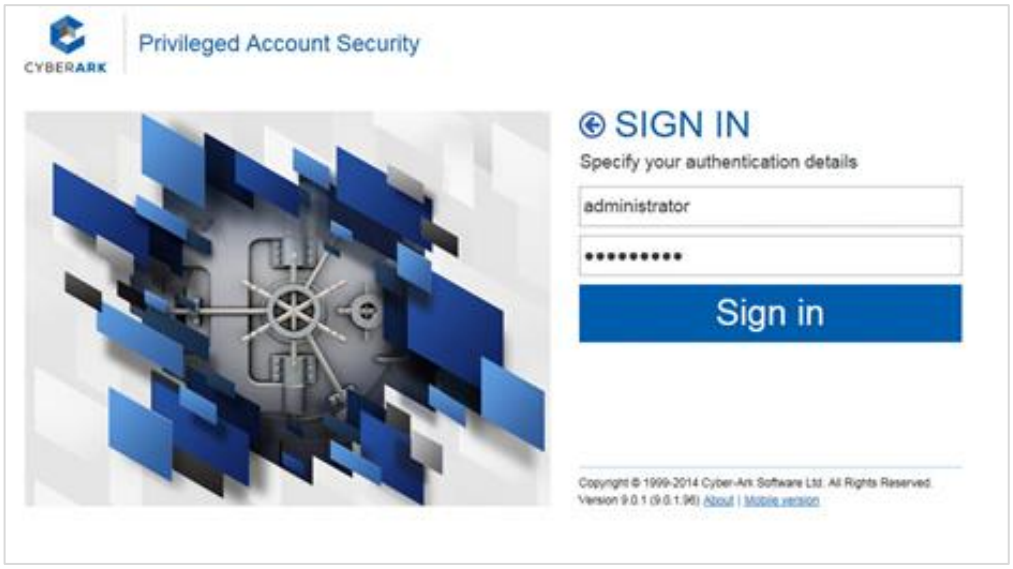
RADIUS_Server_IP	The IP of the RADIUS server
RADIUS_Port	Port number of the RADIUS
vaulthostname	The name of the RADIUS client
radiusauth.dat	The shared secret file, created in the previous section

(The screen image above is from CyberArk®. Trademarks are the property of their respective owners.)

5. Open Server Central Administration and click  to start the PrivateVault server.

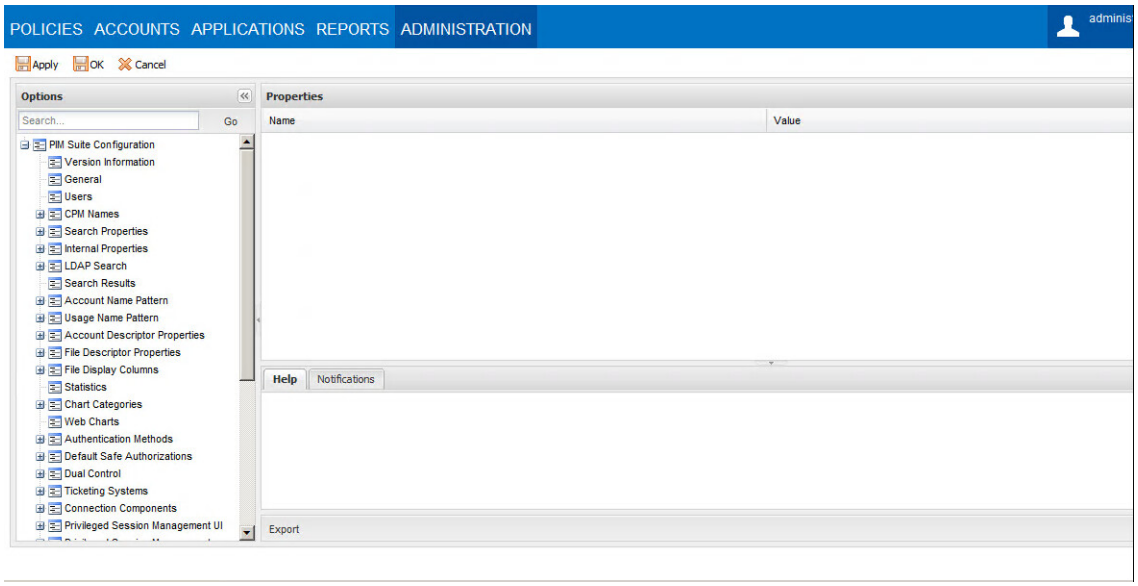
Adding RADIUS Authentication to the Privileged Account Security Portal

1. Log in to the Privileged Account Security portal as **administrator**.



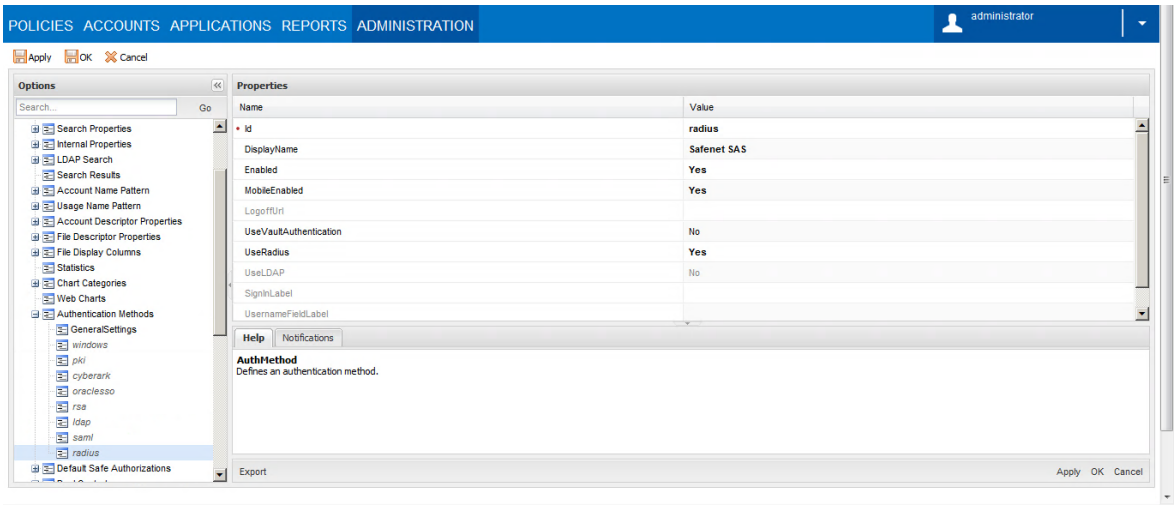
(The screen image above is from CyberArk®. Trademarks are the property of their respective owners.)

2. Click the **ADMINISTRATION** tab, and then select **Options**.



(The screen image above is from CyberArk®. Trademarks are the property of their respective owners.)

3. Expand **Authentication Methods**, and then select **radius**.

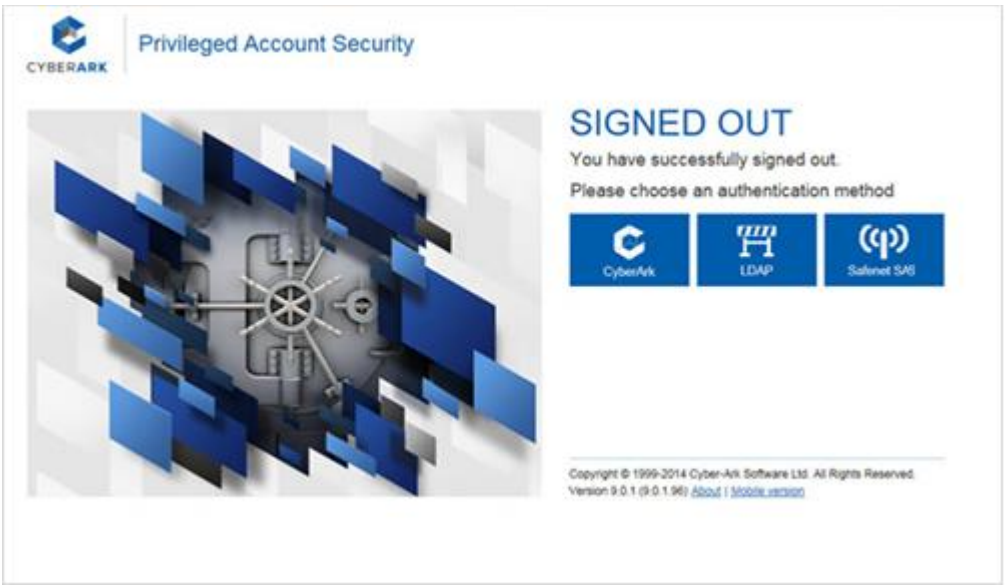


(The screen image above is from CyberArk®. Trademarks are the property of their respective owners.)

4. On the **Properties** window, complete the following fields, click **Apply**, and then click **Save**:

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

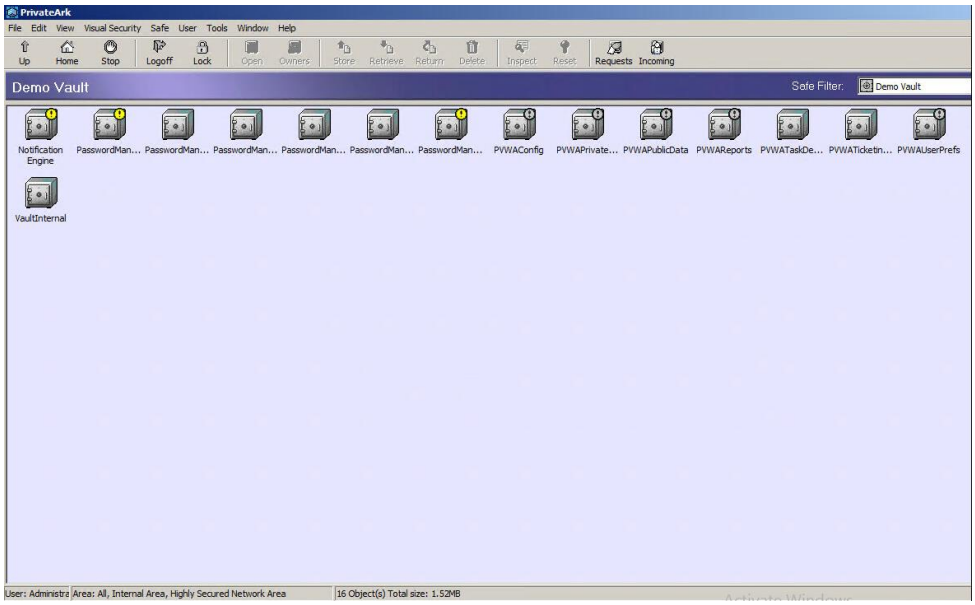
5. On the Privileged Account Security portal login page, verify that the new authentication policy has been added (for example, **Safenet SAS**).



(The screen image above is from CyberArk®. Trademarks are the property of their respective owners.)

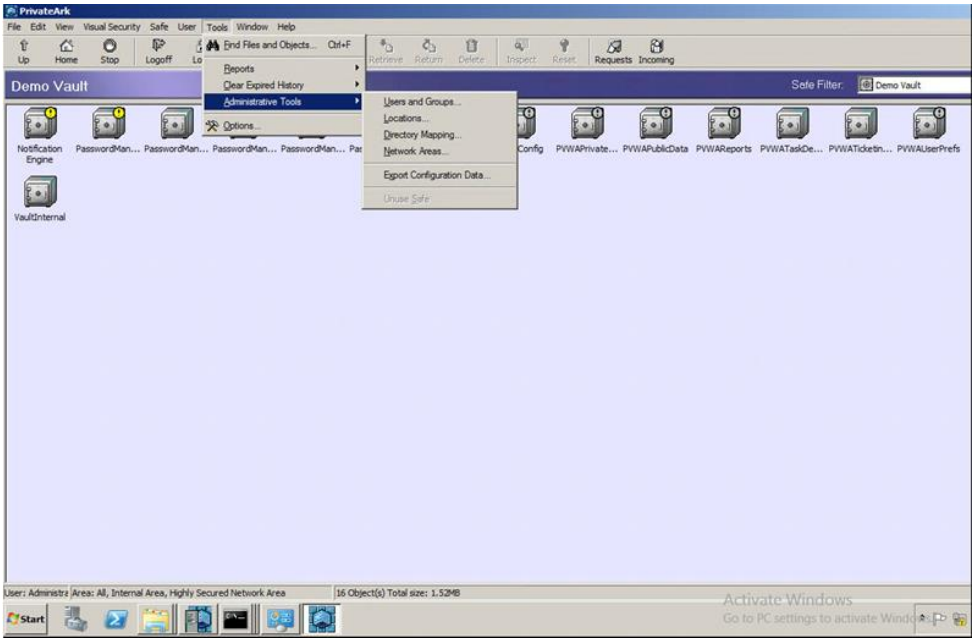
Configuring a User for RADIUS Authentication

1. Open the PrivateArk console and log in to the vault.



(The screen image above is from CyberArk®. Trademarks are the property of their respective owners.)

2. Select **Tools > Administrative Tools > Users and Groups**.



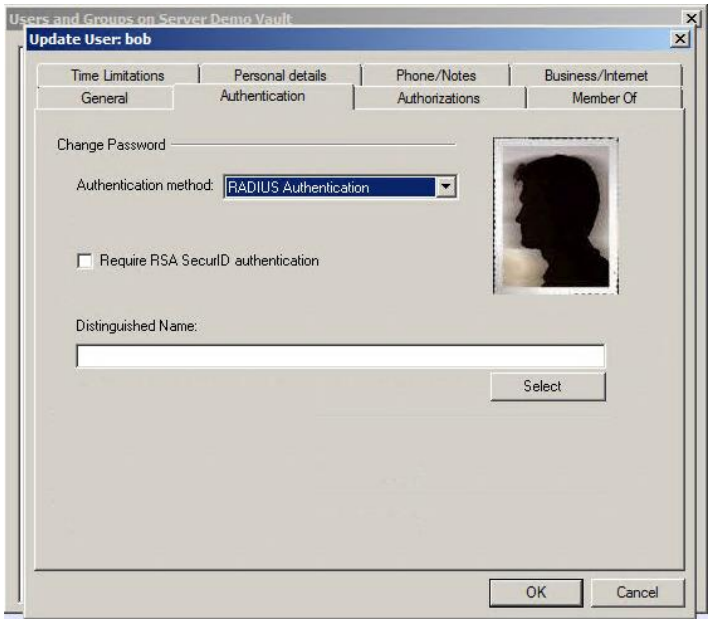
(The screen image above is from CyberArk®. Trademarks are the property of their respective owners.)

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

(The screen image above is from CyberArk®. Trademarks are the property of their respective owners.)

4. Click the **Authentication** tab.

5. Select **RADIUS Authentication** from the **Authentication method** menu.



(The screen image above is from CyberArk®. Trademarks are the property of their respective owners.)

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

Running the Solution

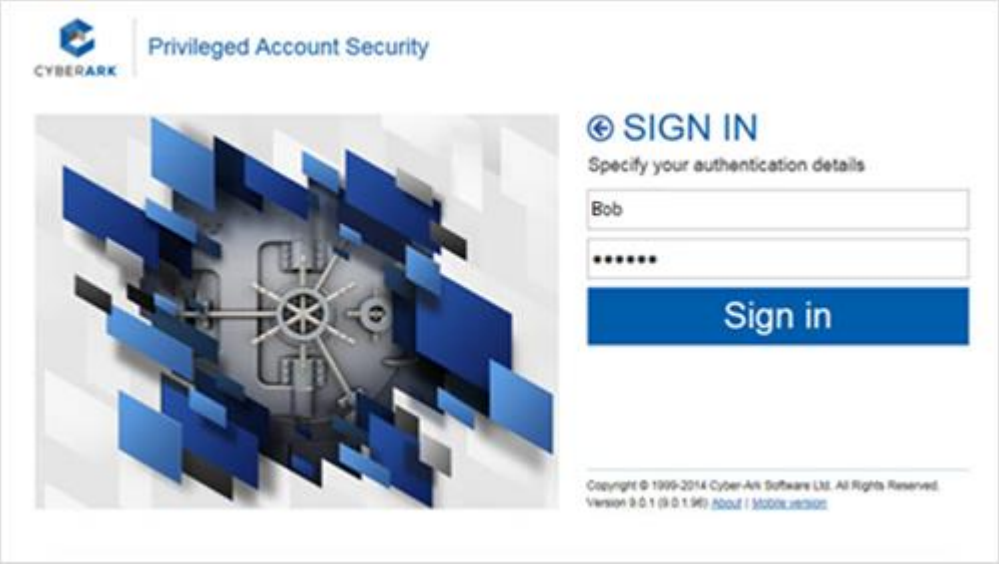
Verify the integration solution after you have successfully configured CyberArk Privileged Account Security Suite for SAS authentication.

For this integration, an SMS token is configured for authentication with the SAS solution.

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

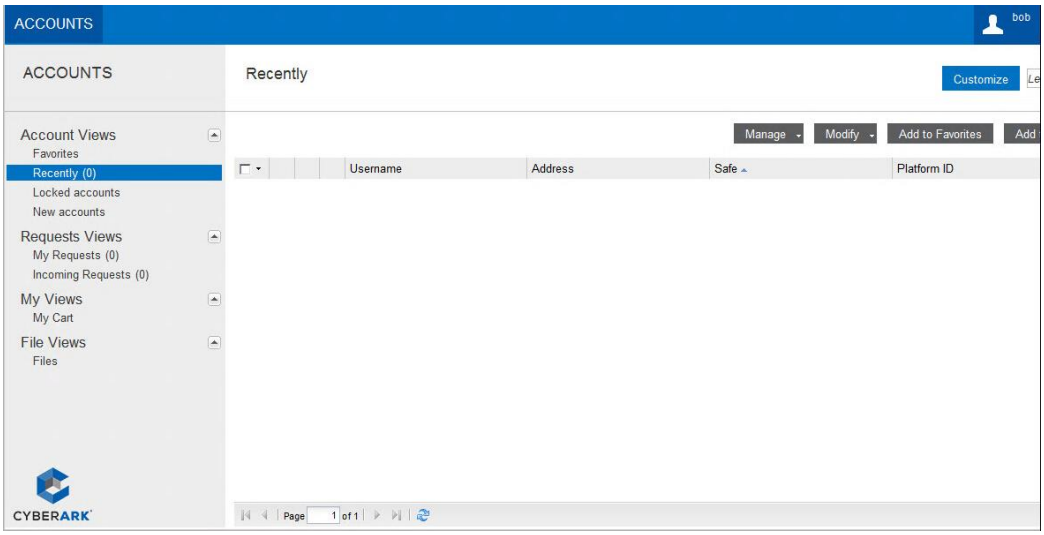
(The screen image above is from CyberArk®. Trademarks are the property of their respective owners.)

2. Type the username and the OTP, and then click **Sign in**.



(The screen image above is from CyberArk®. Trademarks are the property of their respective owners.)

After successful authentication, the user is logged in.



(The screen image above is from CyberArk®. Trademarks are the property of their respective owners.)

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	