SafeNet Authentication Service Integration Guide

Using RADIUS Protocol for CyberArk Privileged Account Security Suite



THE DATA PROTECTION COMPANY

Document Information

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

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

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	4
Description	4
Applicability	4
Environment	5
Audience	5
RADIUS-based Authentication using SAS Cloud	5
RADIUS-based Authentication using SAS-SPE and SAS-PCE	6
RADIUS Authentication Flow using SAS	6
RADIUS Prerequisites	7
Configuring SafeNet Authentication Service	7
Synchronizing User Stores with SAS	7
Assigning an Authenticator in SAS	8
Adding CyberArk Privileged Account Security Suite as an Authentication Node in SAS	8
Checking the SAS RADIUS Address	10
Configuring CyberArk Privileged Account Security Suite	11
Configuring a RADIUS Shared Secret	11
Configuring a RADIUS Server on the Vault	12
Adding RADIUS Authentication to the Privileged Account Security Portal	13
Configuring a User for RADIUS Authentication	15
Running the Solution	17
Support Contacts	18

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 onpremises 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.

Shortcuts 4	Manage:	IMC inc.													
Create User	SNAPSHOT	ASSIGNMENT	TOKENS	GROUPS	REPOR	ats s	SELF-SERVICE	OPERA	TORS		OMMS				
	Aut	henticatior	Activity	/											III 🛈 ->=
	Aut	henticatior	Metrics												0 ->=
	🚹 Tok	en States													•
	SMS	6 Credits													0 🖓
	Allo	cation													III () 🚑
	Transaction	n Log													
	Service Start:	2013-07-	17	Service S	itop: 2	016-02	-05								
	Item	Capacity	кт	RB-1 MP	-1/SMS	ICE MP- 1/SMS	GRID	SecurID	OATH	SMS Credits	Password	RADIUS	GOLD	eToken	MobilePASS
	Maximum	1	0	0	5	0	0	0	0	0	0	0	0	0	0
	Inose				· · ·						•				
	C Ref	erences													•
													(Pov	vered by

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

Shortcuts 4	Manage	IMC inc.								
Create User	SNAPSHOT	ASSIGNMENT	TOKENS	GROUPS	REPORTS	SELF-SERVICE	OPERATORS	POLICY	COMMS	
List Accounts	Co Co	mmunicatior	IS							() - ,
	C Au	thentication	Processi	ng						III 🕜 - 🛏
	🔛 Au	th Nodes								III 🕜 ->=
	SA	ML Service I	Providers	;						-Q=
	Cu:	stom Brandi	ng							() ->=
										SafeNet

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

Auth Nodes III 🛈 🕂							
Auth Nodes:							
Task Description							
Auth Nodes	Create and configure SafeNet A	Authentication Service Authenticatio	n Nodes				
Auth Nodes: Using the RADIUS protocol over the and for alternatives to RADIUS traff Add Chang	e internet provides limited securi fic, please refer to the recomme ge Log Cancel	ity of the traffic between the organi endations included in the SafeNet Au	zation's data center and the authe thentication Service Administrator	ntication service. For ir r guide.	nproved security		
Primary RADIUS Server IP: 1	109.73.120.148:1812	Primary SafeNet Authentication Service Agent DNS:	agent1.safenet-inc.com:443	Max. Auth Nodes: 1	0		
Failover RADIUS Server IP: 6	59.20.230.201:1812	Failover SafeNet Authentication Service Agent DNS:	agent2.safenet-inc.com:443				
No Records							

- 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.

Add Auth Node Save Cancel Auth Nodes	
Agent Description:	Configure FreeRADIUS Synchronization Shared Secret: Confirm Shared Secret: FreeRADIUS synchronization may take up to 5 minutes to propagate in the system.

The Auth Node is added to the system.

Auth Nodes: Using the RADIU: and for alternativ	Nuth Nodes: Jsing the RADIUS protocol over the Internet provides limited security of the traffic between the organization's data center and the authentication service. For improved security ind for alternatives to RADIUS traffic, refer to the recommendations included in the SafeNet Authentication Service Administrator Guide. Add Change Log Cancel						
Primary RADIUS Failover RADIUS	Server IP: 109.73.120. Server IP: 69.20.230.20	148:1812 Primary S Service A D1:1812 Failover S Service A	afeNet Authentication gent DNS: afeNet Authentication gent DNS:	agent1.safenet-inc.c agent2.safenet-inc.c	om:443 Max. om:4 <mark>4</mark> 3	Auth Nodes: 1	LO
Index	Description	Host Name	IP Add	ress	FreeRADIUS Synchronization		
1	VMware Horizon 6	VMware Horizon 6	84.94.2	15.66	True	Edit	Remove
Displaying:	1 to 6 of 6						

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.

Shortcuts 1	Manage: 1	EMC inc.													
Create User	SNAPSHOT	ASSIGNMENT	ТОКЕ	NS GRO	DUPS REI	PORTS SI	ELF-SERVIO	CE OPERA	TORS P	OLICY CO	MMS				
	Auti	nenticatio	on Activ	rity											III 🛈 🚧
	Auti	nenticatio	n Metr	ics											() ->=
	toko	en States	;												0 ->=
	SMS	Credits													0 ->=
		cation													III 🛈 🚧
	Transaction	Log													
	Service Start:	2013-07	-17	Serv	ice Stop:	2016-02-0	05								
	Item	Capacity	кт	RB-1	MP-1/SMS	ICE MP- 1/SMS	GRID	SecurID	ОАТН	SMS Credits	Password	RADIUS	GOLD	eToken	MobilePASS
	Maximum	1	0	0	5	0	0	0	0	0	0	0	0	0	0
	In Use	1	0	0	0	0	0	0	0	0	1	0	0	0	•
	C Refe	erences													() -µ
													(Pov	vered by

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.

Auth Nodes					III 🛈 ->=
Auth Nodes:					
Task	Description				
Auth Nodes	Create and configure SafeNet A	Authentication Service Authenticatio	n Nodes		
Auth Nodes: Using the RADIUS protocol over the and for alternatives to RADIUS traf Add Chang	e internet provides limited securi fic, please refer to the recomme ge Log Cancel	ty of the traffic between the organi ndations included in the SafeNet Au	zation's data center and the author thentication Service Administrate	entication service. For r guide.	improved security
Primary RADIUS Server IP: :	109.73.120.148:1812	Primary SafeNet Authentication Service Agent DNS:	agent1.safenet-inc.com:443	Max. Auth Nodes:	10
Failover RADIUS Server IP: 6	59.20.230.201:1812	Failover SafeNet Authentication Service Agent DNS:	agent2.safenet-inc.com:443		
No Records					

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.

Server Cen	tral Administratio	
Control View	Administration	
122	~~ %	
HF N		
Date	Time	Message
autocas es	E.S. Mills Lak	CATELINE AUDILE authoritization Taken Tar user both. DADLE server regire Authoritization request for both rejected. CTV authoritization fields).
14,00,00 ct	11,000,000	20172228 Authentication failure for user tell from stationy 10.0.0.1 (code: -275.
and the later of t	11/30/42	20423332 FACEULE authentication failure for user hole. EAREULE server reply: Authentication request for hell reported. General error Error message from server:).
INVIGORIS	13.53.47	278/25200 Authentication failure fail from stations 30.0.0.1 (solit) -775.
Interference	111044-046	TATISTER AUDIT authentication failure for user beils. (SARDUS per-ow-raphy Authentication-request for beil reported). General error Error message from server;).
C INVICTION OF	11.55-25	2019:022 Aufbertikation failure für uner heit Fran station: 10.0.0.1 (onler: 27).
04/03/0053	11-11-11-11	CONSECTABLES authoritization failure for user balls. (EACE):5 service registy: Authoritization-request for ball reported). CPP authoritization failed, 5.
100/102/08/05	11,799,365	EXT_CER P Address 10.0.0.1 is supported for their hole.
California (California)	12410-48	20070000 MACOLE authentication Splace for user Indo. Eliagrandiz enformation: 14, (1),
146/03/08/05	1214121.30	214715330 fullEl.cli authentication failure fair une balt. Elagrandre information: 14, (1).
16/02/2015	12:02:57	ITAD8319I Database manager is shutting down. Waiting for queued and active transactions to finish processing
16/02/2015	12:03:01	ITAUI418[UI input is down. No more requests are accepted.
16/02/2015	12:03:01	ITAD83651 Waiting on 1 active task(s)
16/02/2015	12:03:01	TFAUI-4201 UI output is down.
16/02/2015	12:03:01	ITAD8315I Server has normally terminated
16/02/2015	12:03:01	ITAFW002I Finewal is closed to client communication
17/02/2015	10:52:38	ITAIGM03I DebugLevel 1 ACTIVATED for Class PE
17/02/2015	10:52:38	ITAIGM03I DebugLevel 1 ACTIVATED for Class PERF
17/02/2015	10:52:38	ITAIGM001 DebugLevel masking set
17/02/2015	10:52:38	ITAD8399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit, RSA (2048 bit), SHA1.
17/02/2015	10:52:39	ITADM114I Successfully connected to Database id 0.
17/02/2015	10:52:39	ITALD0131 LDAP configuration refreshed successfully.
17/02/2015	10:52:40	ITAFW0011 Frewal is open for client communication
17/02/2015	10:52:40	ITA08313I Server 9.0.1 (9.0.1.54) is up
17/02/2015	10:52:41	ITAQS0311 Object cache is loaded.
 Environmente 	101-1-11-100	CATACHER AND A
 Checkbergs 	10.57.52	204/35288 Authoritization failure for user hub from stations (0.0.0.1 (online -27).
1.0002/2014/5	1107-00	2003332 MADLE authentication failure for user India. BADLE server replic Authentication request for both reported. CPP authentication failed. 3.
 Links/Sects 	1.1.407-92	CENTERE AUDIT authentication failors for user look. (EADLID server reply: Authentication respect for hole rejected). (CP authentication failed.).
L Mig Gerste	11444-127	PATELEX NUMER automitation failure for user links. [NALLIZ server reply: Automitation-request for bolt-reported. OTP automitation failed.].
End.2/28105		25475538 AADLD authentication failure for user helix. (IADLD server regist: Authentication regards for helix opecied: (219 authentication failed:).
C MALLOWING	11.1240	20423332 foldtut authentication failure for user lolls. (IADUS server reply: Authentication-request for loll rejected). (2019 authentication failed.) .
1.1462/06-08	11.17.96	25475428 Dr Address 10.5.6.1 a augurdief fo Unor Isla.
 Intraction 	11.08.30	PERSUE FACILIT authentication failure for user losis. (FACILIT server reply: Authentication request for both reported. (279 authentication failed.)).
 L'MELETARIST 	13.29.12	EXPECTION Authoritization failure for user habitrary attribute attribute 228.
 Instatutest 	13 1249	27.875.2282 Auditoritization failure for part help from stations (E. S. J.) (solar 275).

(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

1	(MAIN)
2	RadiusServersInfo=10.0.0.4;1812;host-1;RadiusSecret.dat
3	TasksCount-20
- 4	DateFormat=DD.MM.YY
5	TimeFormat=HH:MM:53
6	ResidentDelay-10
7	BasePort=1858
3	LogRetention=7
. 9	LockTimeOut=30
10	DaysForAutoClear=30
11	DaysForPicturesDistribution=Never
12	ClockSyncTolerance=600
-12	TraceArchiveMax51ze=5120
14	VaultEventNotifications=NotifyOnNevRequest,NotifyOnRejectRequest,NotifyOnConfirmRequestByAll,NotifyOnDeleteRequest
-15	RecoveryPubKey=C:\PAKeys\RecPub.key
1.6	ServerKey=C:\PAKeys\Server.key
17	StagingAreaDirectory=C:\PrivateArk\StagingArea
18	EntropyFile-C:\PrivateArk\Safes\entropy.rnd
1.9	DatabaseConnectionPasswordFile=C:\PAKeys\VaultUser.pass
20	ServerCertificateFile=C:\PAKeys\Server.pem
21	ServerPrivateKey=C:\PAKeys\Server.pvk
-	

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

5. Open Server Central Administration and click rot 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.

层 Apply 🛛 层 OK 💥 Cancel				
Options		Properties		
Search	Go	Name	Value	
PM Suite Configuration General Version Information General Users Search Properties CPM Names Search Properties CDAP Search Search Results Search Results Search Results Account Name Pattern Search Results Account Search Pattern Search Results Search	•			
Fie Display Columns Statistics Chart Categories Web Charts Authentication Methods Default Safe Authorizations Dual Control Ticketing Systems Connection Components Privileged Session Management U		Help Notifications		

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

3. Expand Authentication Methods, and then select radius.

Apply 🔚 OK 💥 Cancel	FLICA	HONO REPORTS ADMINISTRATION		
Options	«	Properties		
earch	Go	Name	Value	
Search Properties		• ld	radius	
🗉 🔁 Internal Properties		DisplayName	Safenet SAS	
LDAP Search Search Desuits		Enabled	Yes	
Search Results Account Name Pattern		MobileEnabled	Yes	
🗉 🔁 Usage Name Pattern		LogoffUrl		
Account Descriptor Properties		UseVaultAuthentication	No	
E File Display Columns		UseRadius	Yes	
E Statistics		UseLDAP	No	
🗄 🔁 Chart Categories		SignInLabel		
Web Charts Authentication Methods		UsernameField abe		
GeneralSettings		Help Notifications		
 pki cyberark cyclerark cyclesso rsa ldap sami sami cycline 		AuthHethod Defines an authentication method.		
E Default Safe Authorizations	-	Export	A	oply OK Cance

(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.

Time Linitations	Personal details	Phone/Notes	Business/Interne
General	Authentication	Authorizations	Member Of
hange Password —			
Authentication me	thod: RADIUS Authentica	tion	1
🗖 Require RSA :	SecurID authentication		
		- Per	
Distinguished Nam	1e:	- Deg	
Distinguished Nam	ie:		Select
Distinguished Nan	ne:		Select
Distinguished Nam	ne:		Select
Distinguished Nam	ne:		Select

(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.

ACCOUNTS									L pop
ACCOUNTS		Recen	itly					Custor	nize Le
Account Views Favorites	۲					Manage 🗸	Modify +	Add to Favorites	Add
Recently (0) Locked accounts New accounts			Usen	name	Address	Safe 🔺		Platform ID	
Requests Views My Requests (0) Incoming Requests (0)									
My Views My Cart									
File Views Files	۲								
8									
CYBERARK'		14 4 P	age 1 of 1	× >1 &					

(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		
Technical Support Customer Portal	International 1-410-931-7520 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.			