



PASSWORD VAULT WEB ACCESS, PRIVILEGED SESSION MANAGER, PRIVILEGED SESSION MANAGER RDP PROXY

SILVERFORT AUTHENTICATION PLATFORM – CYBERARK PAS INTEGRATION

Name of Company	Silverfort
Website	www.silverfort.io
Name of Product	Silverfort Authentication Platform
Version	1.5
Date	September 5 th , 2018

SILVERFORT SOLUTION OVERVIEW

The Silverfort Authentication Platform enables strong authentication across entire corporate networks and cloud environments, without any modifications to endpoints and servers.

Silverfort protects every sensitive user, device, and asset throughout the organization, including systems that don't support Multi-Factor Authentication today (proprietary systems, legacy applications, critical infrastructure, shared folders and more). In addition, Silverfort offers advanced user behavior analytics that can be used for adaptive authentication and real-time prevention, allowing enterprises to protect all their sensitive assets, prevent data breaches and achieve compliance with GDPR, PCI, HIPAA and more.

The Silverfort Authentication Platform is provided as a virtual appliance and does not require any software agents or local configurations on corporate endpoints and servers. Its web-based admin console enables security admins to easily apply strong authentication policies across the organization, identify authentication vulnerabilities, and achieve broad visibility and auditing of authentication and access activity.

KEY BENEFITS

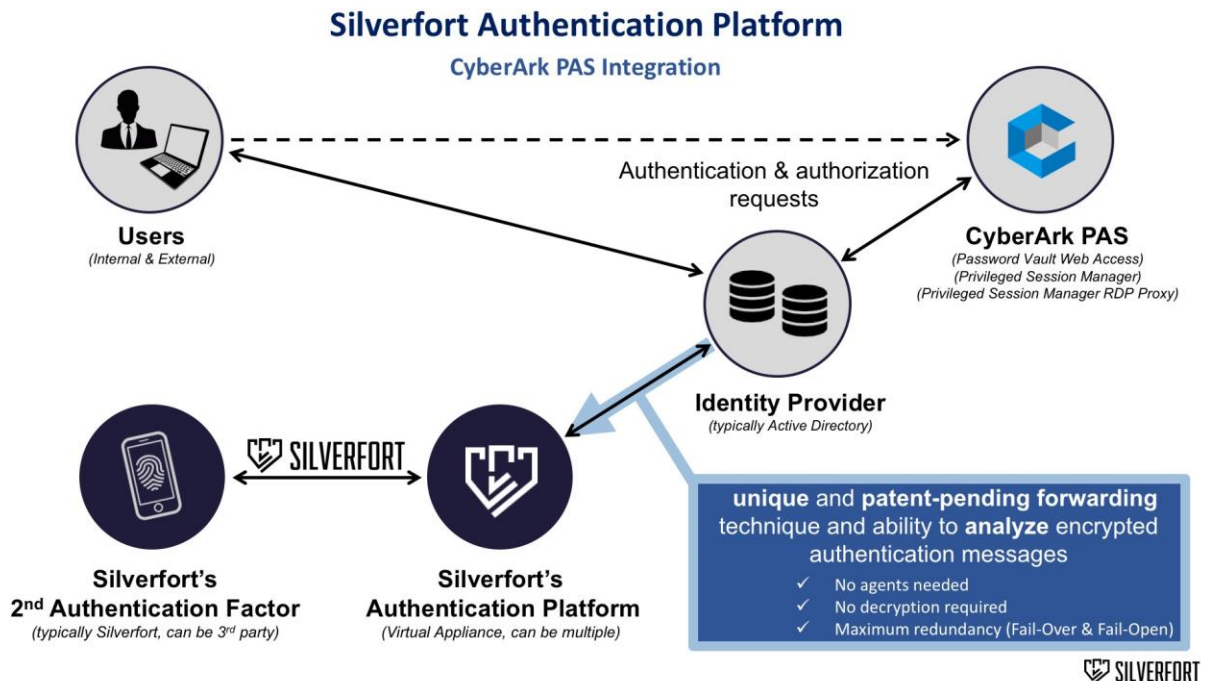
Silverfort provides non-intrusive Multi-Factor Authentication (MFA) for multiple authentication protocols, including Windows Authentication, LDAP Authentication, Radius Authentication and more.

Silverfort's minimum integration will allow agent-less MFA for accessing the CyberArk Password Vault Web Access (PVWA) and CyberArk Privileged Session Manager (PSM), including its Privileged Session Manager RDP Proxy (PSMP).

The standard MFA form factor is a Silverfort mobile application which provides push notifications to strongly authenticate. Because of Silverfort's unique support of providing MFA to Windows Single Sign-On and Active Directory based authentication, Silverfort can bring frictionless strong authentication to CyberArk's users by only setting up the required authentication policies in the Silverfort Management Console, and without any adaptation on CyberArk's side.

Silverfort allows CyberArk's Privileged Session Manager users to overcome the problem where MFA on the CyberArk Privileged Session Manager RDP Proxy becomes cumbersome and requires entering a one-time pin code at every single PSM connection. Silverfort's approach will be to only leverage MFA on PSM RDP Proxy sessions when needed, i.e. every time, at given intervals or when the network is at risk.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



The minimum integration to provide MFA to the CyberArk PVWA and PSM/PSMP only requires a policy configuration in the Silverfort Management Console, at which point the MFA will be instated automatically.

SILVERFORT INSTALLATION & INTEGRATION CONFIGURATION

For a minimum integration of the CyberArk Privileged Account Security environment with the Silverfort Authentication Platform, it is recommended to enable Silverfort's MFA on both the CyberArk Password Vault Web Access (PVWA) and the CyberArk Privileged Session Manager (PSM), including its Privileged Session Manager Remote Desktop Proxy (PSMP).

Example configuration 1: obtain Multi-Factor Authentication for accessing the CyberArk Password Vault Web Access using Windows Authentication

1. In the Silverfort Management Console, create a policy with a name that refers to the CyberArk Password Vault Web Access, e.g. "CyberArk (PVWA)". (see also PVWA Figure 1 below)
2. Off all protocols available on your Silverfort Authentication Platform, make sure to select both "Kerberos" and "NTLM" in the WITH section of the policy definition. (see also PVWA Figure 1 below)

3. In the WHO section of the definition, add the specific account names or account groups that will become subject to this policy. Typically for CyberArk, this will include your existing CyberArk groups such as “CyberArk Admins”, “CyberArk Auditors” and “CyberArk Users”. In case you only want to have a subset of your CyberArk users to have MFA enforced, you may need to create a specific group for this, e.g. “CyberArk MFA Users”. *(see also PVWA Figure 1 below)*
4. In case you want the policy to apply only to a specific set of source devices or IPs/Subnets, indicate those in the FROM section of the policy definition. *(see also PVWA Figure 1 below)*
5. In the TO section of the policy, add all CyberArk server resources that make part of the PVWA pool. In case a virtual SPN (Service Principal Name) would be used for setting up a PVWA pool, please add it too. *(see also PVWA Figure 1 below)*

For each PVWA server/SPN, select the “http” service (click on the CHANGE button, select the service). *(see also PVWA Figure 2 below)*
6. Unless the policy should become active when a certain risk is detected, select the “Any” option in the RISK section of the policy definition. *(see also PVWA Figure 1 below)*
7. To ensure Multi-Factor Authentication becomes active on the CyberArk Password Vault Web Access, select the “Require MFA” Action option in the DO section of the policy definition. You can optionally set the Resource Display Name which will appear in the Silverfort mobile application when MFA is triggered, and when MFA will be required. Don’t forget to make sure the policy is enabled by checking the switch icon on top. *(see also PVWA Figure 1 below)*
8. Verify the result by connecting to the CyberArk PVWA with a user that has a Silverfort MFA soft token configured. *(see also PVWA Figures 3, 4, 5, 6 below)*

CyberArk (PVWA) (#10)

Policy Name: CyberArk (PVWA)

For any authentication request that meets the following conditions:

WITH	Protocols ☒ Kerberos ☒ NTLM
WHO	Accounts CyberArk Admins, CyberArk Auditors and 1 more Change
FROM	Devices By Hostname: <u>All Devices</u> Change By IP/Subnet: Not Selected Change
TO	Resources <u>DR-AZ-PVWA</u> Change
RISK	☒ Any ☐ Risk level is <u>Medium</u> or higher.

Enforce this policy:

DO	Action: <u>Require MFA</u> Resource Display Name: <u>CyberArk (PVWA)</u> Require MFA: ☒ Every time ☐ Once every 10 hours
-----------	---

[Discard Changes](#) [Save](#)

PVWA Figure 1 - Silverfort example policy definition for adding agentless MFA to the CyberArk PVWA.

CyberArk (PVWA) (#10)

SELECT RESOURCES

Q Type Server name...

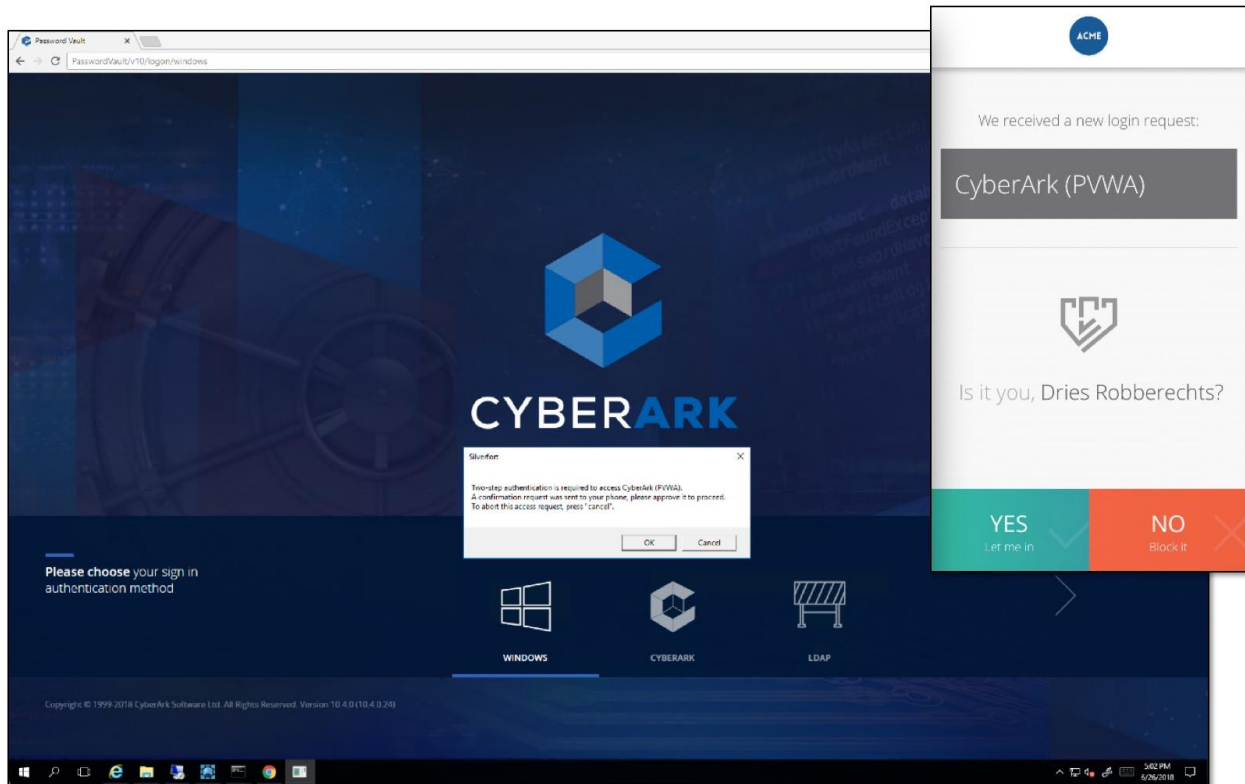
- ☒ http/dr-az-pvwa
- ☒ http/dr-az-pvwa.ad.draz.silverfort.io
- ☐ ias/dr-az-pvwa
- ☐ ias/dr-az-pvwa.ad.draz.silverfort.io
- ☐ iisad/dr-az-pvwa
- ☐ iisad/dr-az-pvwa.ad.draz.silverfort.io
- ☐ mcsvc/dr-az-pvwa
- ☐ mcsvc/dr-az-pvwa.ad.draz.silverfort.io
- ☐ messenger/dr-az-pvwa
- ☐ messenger/dr-az-pvwa.ad.draz.silverfort.io
- ☐ min/dr-az-pvwa
- ☐ min/dr-az-pvwa.ad.draz.silverfort.io
- ☐ msiserver/dr-az-pvwa

[Cancel](#) [Done](#)

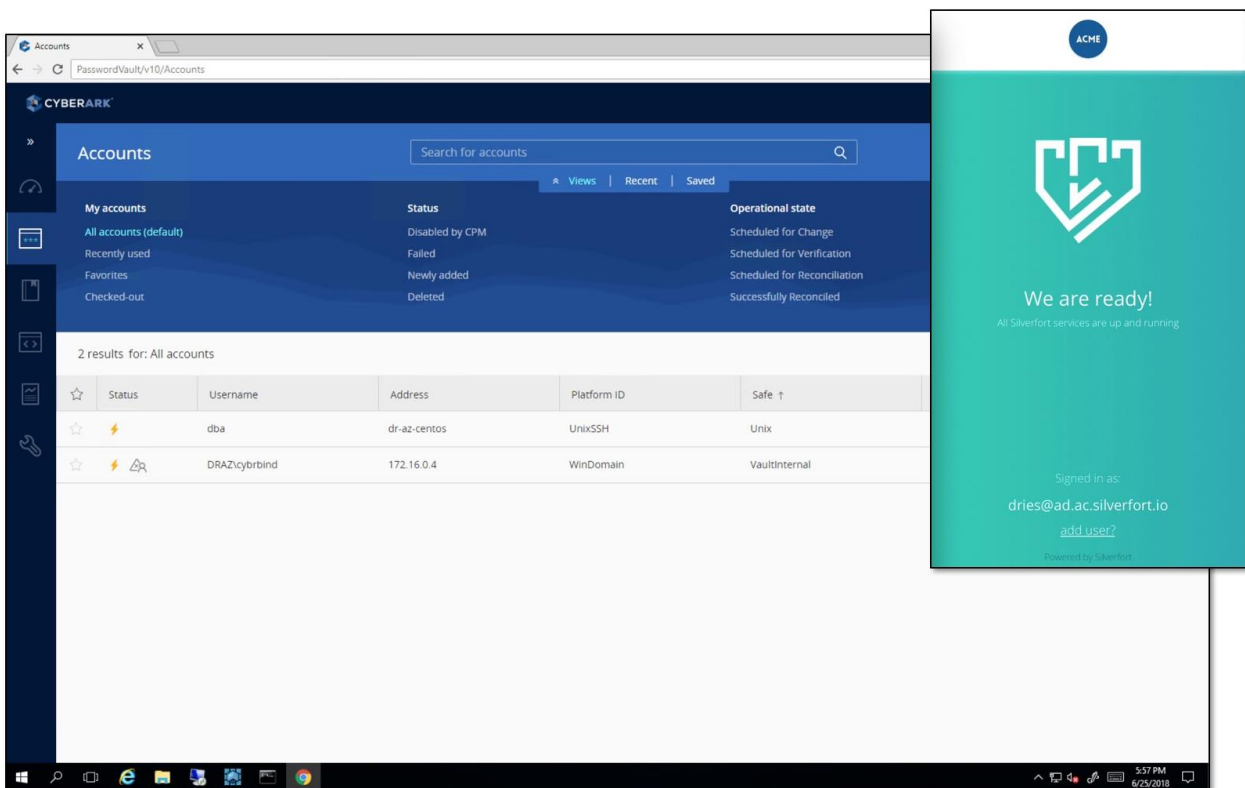
Require MFA: ☒ Every time ☐ Once every 10 hours

[Discard Changes](#) [Save](#)

PVWA Figure 2 - Select the "http" service linked to the CyberArk PVWA server(s).



PVWA Figure 3: The result before confirming the PVWA authentication in the Silverfort mobile app.



PVWA Figure 4: The result after confirming the PVWA authentication in the Silverfort mobile app.

Dries Robberechts
dries@ad.draz.silverfort.io
ad.draz.silverfort.io
1
1
Protected

TOKENS (1)

#	TOKEN ID	TYPE	DEVICE	STATUS
1	cOOC1fw9Qn4:APA91bEkdhCeZpLGd4vXjAV--hS_286xcb95bWFn4YQF...	Mobile token	iOS	Active

IDENTITIES (1)

#	APPLICATION KEY	USERNAME
1	ad.draz.silverfort.io	dries

Main Identity (AD)

+ Add Identity

PVWA Figure 5: The user has at least one active soft token in the Silverfort Authentication Platform.

SILVERFORT DASHBOARD

34 DENY
321K AUTH REQUESTS
304 MFA

Dashboard

LOGS

LOGS FILTER

☒ FILTER BY USERS

Selected Users: Dries Robberechts

☒ FILTER BY DATES

From: 25/06/2018 19:57:00
To: 25/06/2018 19:58:00

☒ ADVANCED FILTER

Field: MFA Response
Equal: Approved

Apply

Reset

LOGS TABLE

CUSTOMIZE COLUMNS (11) | EXPORT

TIME	ACCOUNT	DEVICE	RESOURCE		POLICY			RISK	PROTOCOL	RESULT
	USERNAME	DEVICE NAME	SERVICE	SERVER	ACTION	EXECUTED POLICY	MFA RESPONSE			
25/06/2018 19:57:49.470	dries	dr-az-dt16	termarv	dr-az-psm	MFA	(11)	Approved	Low	Kerberos	Allowed
25/06/2018 19:57:02.527	dries	dr-az-dt16	http	dr-az-pvwa	MFA	(10)	Approved	Low	Kerberos	Allowed

Settings

Logout

9 Domains

15 Domain Admins

230 Organizational Units

470 Security Groups

PVWA Figure 6: The Silverfort Authentication Platform logs indicate that the user accessed the PVWA "http" service with MFA.

7

Example configuration 2: obtain Multi-Factor Authentication for accessing the CyberArk Privileged Session Manager RDP Proxy using Windows Authentication

1. In the Silverfort Management Console, create a policy with a name that refers to the CyberArk Privileged Session Manager RDP Proxy, e.g. “CyberArk (PSM RDP Proxy)”. *(see also PSM Figure 1 below)*
2. Off all protocols available on your Silverfort Authentication Platform, make sure to select both “Kerberos” and “NTLM” in the WITH section of the policy definition. *(see also PSM Figure 1 below)*
3. In the WHO section of the definition, add the specific account names or account groups that will become subject to this policy. Typically for CyberArk, this will include your existing CyberArk groups such as “CyberArk Admins”, “CyberArk Auditors” and “CyberArk Users”. In case you only want to have a subset of your CyberArk users to have MFA enforced, you may need to create a specific group for this, e.g. “CyberArk MFA Users”. *(see also PSM Figure 1 below)*
4. In case you want the policy to apply only to a specific set of source devices or IPs/Subnets, indicate those in the FROM section of the policy definition. *(see also PSM Figure 1 below)*
5. In the TO section of the policy, add all CyberArk server resources that make part of the PSM pool. In case a virtual SPN (Service Principal Name) would be used for setting up a PSM pool, please add it too. *(see also PSM Figure 1 below)*

For each PSM server/SPN, select the “termsrv” service (click on the CHANGE button, select the service).
(see also PSM Figure 2 below)

6. Unless the policy should become active when a certain risk is detected, select the “Any” option in the RISK section of the policy definition. *(see also PSM Figure 1 below)*
7. To ensure Multi-Factor Authentication becomes active on the CyberArk Privileged Session Manager RDP Proxy, select the “Require MFA” Action option in the DO section of the policy definition. You can optionally set the Resource Display Name which will appear in the Silverfort mobile application when MFA is triggered, and when MFA will be required. Don’t forget to make sure the policy is enabled by checking the switch icon on top. *(see also PSM Figure 1 below)*
8. Verify the result by connecting to the CyberArk PSM RDP Proxy with a user that has a Silverfort MFA soft token configured. *(see also PSM Figures 3, 4, 5, 6, 7 below)*

CyberArk (PSM RDP Proxy) (#11) (Unsaved)

Policy Name: CyberArk (PSM RDP Proxy)

For any authentication request that meets the following conditions:

WITH Protocols
☒ Kerberos ☒ NTLM

WHO Accounts
 CyberArk Admins, CyberArk Auditors and 1 more [Change](#)

FROM Devices
 By Hostname: All Devices [Change](#)
 By IP\Subnet: Not Selected [Change](#)

TO Resources
 DR-AZ-PSM [Change](#)

RISK ☒ Any
☐ Risk level is Medium or higher.

Enforce this policy:

DO Action: Require MFA
 Resource Display Name: CyberArk (RDP Proxy)
 Require MFA: ☒ Every time ☐ Once every 10 hours

You have unsaved changes

[Discard Changes](#) [Save](#)

PSM Figure 1 - Silverfort example policy definition for adding agentless MFA to the CyberArk PSM RDP Proxy.

CyberArk (PSM RDP Proxy) (#11)

3 Any 1 Any

SELECT RESOURCES

Q Type Server name...

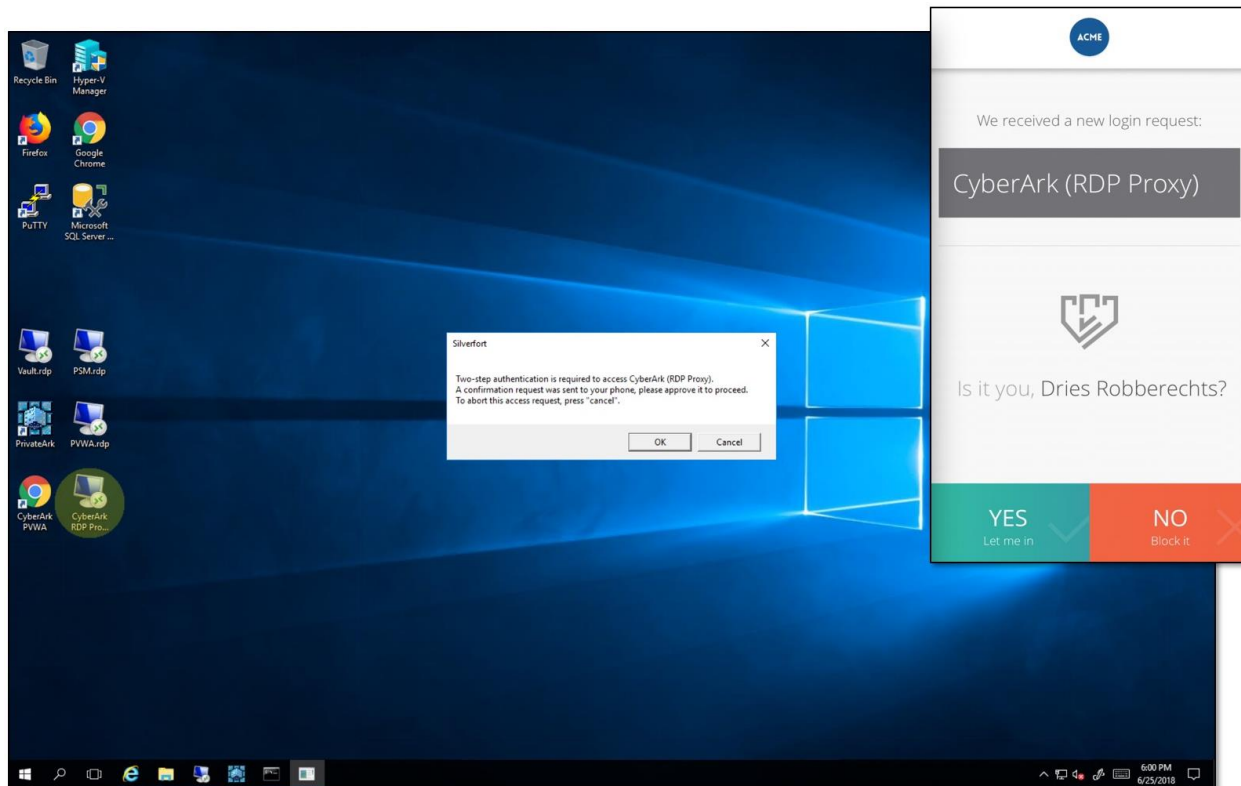
- ☒ termsrv/dr-az-psm
- ☒ termsrv/dr-az-psm.ad.draz.silverfort.io
- ☐ time/dr-az-psm
- ☐ time/dr-az-psm.ad.draz.silverfort.io
- ☐ trksvr/dr-az-psm
- ☐ trksvr/dr-az-psm.ad.draz.silverfort.io
- ☐ trkwks/dr-az-psm
- ☐ trkwks/dr-az-psm.ad.draz.silverfort.io
- ☐ ups/dr-az-psm
- ☐ ups/dr-az-psm.ad.draz.silverfort.io
- ☐ w3svc/dr-az-psm
- ☐ w3svc/dr-az-psm.ad.draz.silverfort.io
- ☐ wins/dr-az-psm

[Cancel](#) [Done](#)

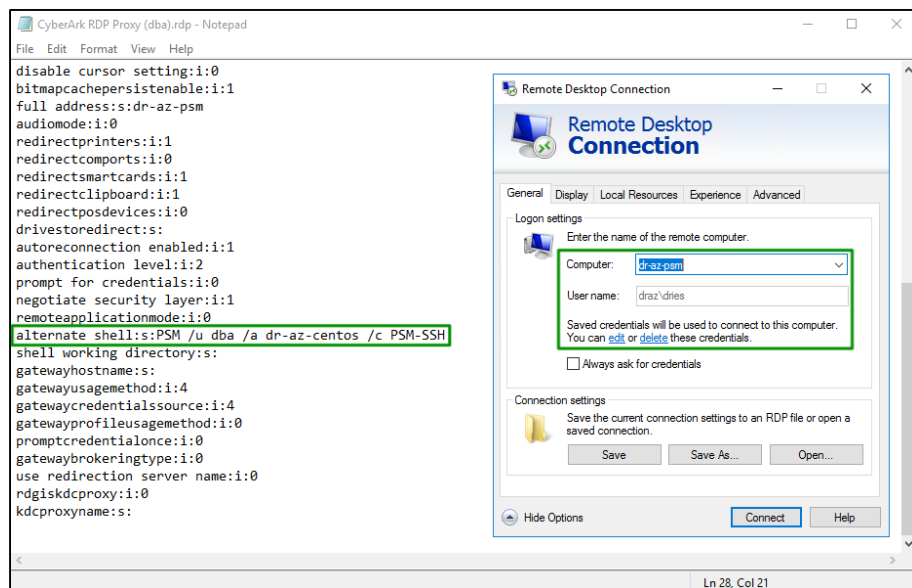
Require MFA: ☒ Every time ☐ Once every 10 hours

[Discard Changes](#) [Save](#)

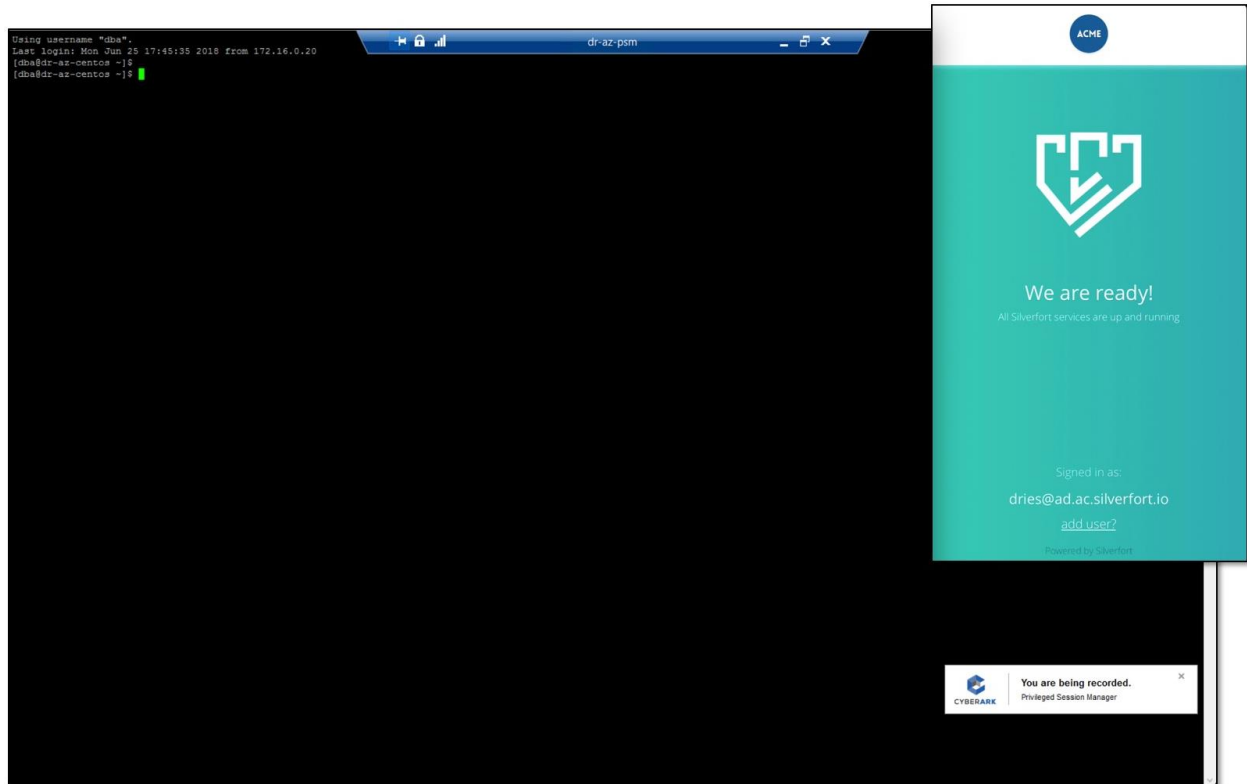
PSM Figure 2 - Select the "termsrv" service linked to the CyberArk PSM server(s).



PSM Figure 3: The result before confirming the PSM authentication in the Silverfort mobile app. In the example, the connection was launched using a preconfigured PSM RDP Proxy connection marked in yellow.



PSM Figure 4: The details of the preconfigured PSM RDP Proxy connection marked in yellow in PSM Figure 3.



PSM Figure 5: The result after confirming the PSM authentication in the Silverfort mobile app.

Dries Robberechts

dries@ad.draz.silverfort.io

ad.draz.silverfort.io

1

1

Protected

TOKENS (1)

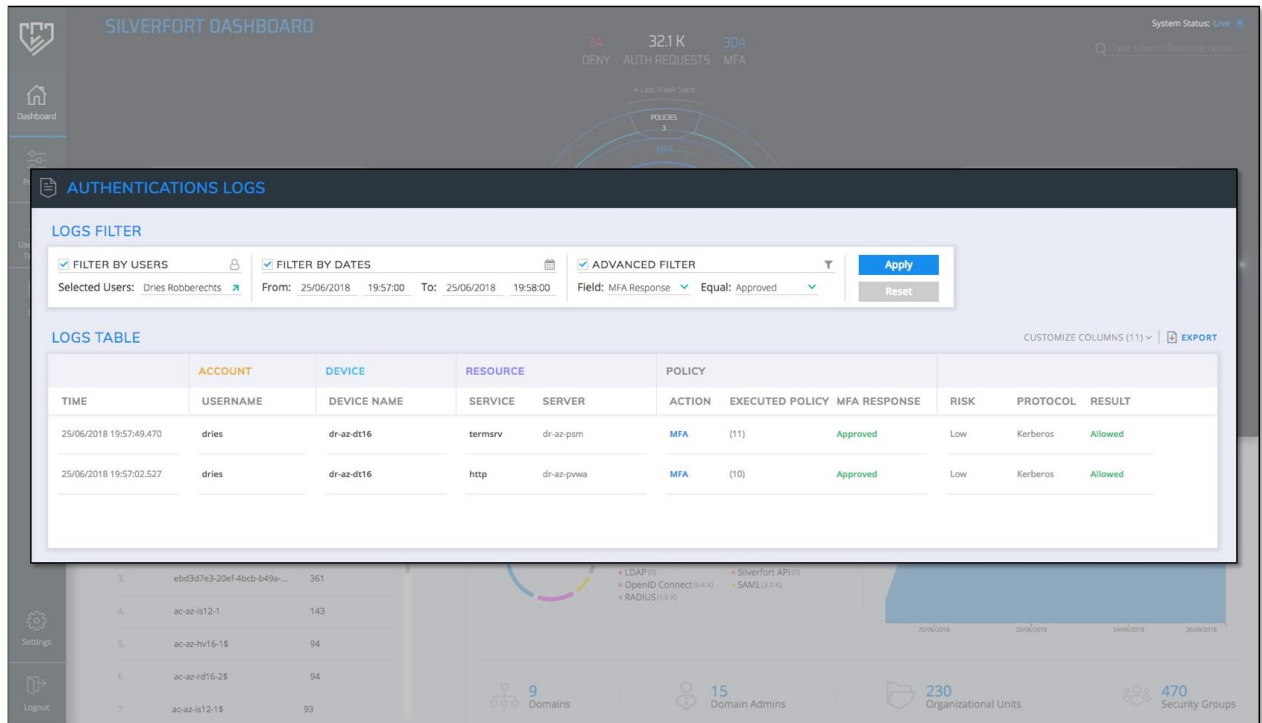
#	TOKEN ID	TYPE	DEVICE	STATUS	
1	cOOC1fw9Qn4:APA91bEkdhCeZpLGd4VxJAV-hS_286xcb9SbWFn4YQF...	Mobile token	iOS	Active	

IDENTITIES (1)

#	APPLICATION KEY	USERNAME	
1	ad.draz.silverfort.io	dries	Main Identity (AD)

+ Add Identity

PSM Figure 6: The user has at least one active soft token in the Silverfort Authentication Platform.



PSM Figure 7: The Silverfort Authentication Platform logs indicate that the user accessed the PSM RDP Proxy “termsrv” service with MFA.

PARTNER CONTACT INFO

Business Contact	Name	Dries Robberechts
	Email	dries@silverfort.io
	Tel	+32 474 53 03 02
Technical Contact	Name	
	Email	
	Tel	
Support Contact	Name	
	Email	
	Tel	