CYBERARK®

The Identity Security Company™

PAM Administration

Privileged Session Management

Part 1

Agenda

By the end of this session, you will be able to describe the main features, architecture, and flow, as well as enable and use, the following session management solutions:

1. **Privileged Session Manager (PSM)**
   - PSM Ad-Hoc Connections
   - PSM via HTML5 Gateway
   - PSM for Windows

2. **PSM for SSH**

Overview

Privileged Session Management Provides 3 Main Benefits:

Isolation

Separate endpoints from critical target systems to prevent lateral movement

Monitoring

Detect and track suspicious activities in privileged sessions and events in real time

Recording

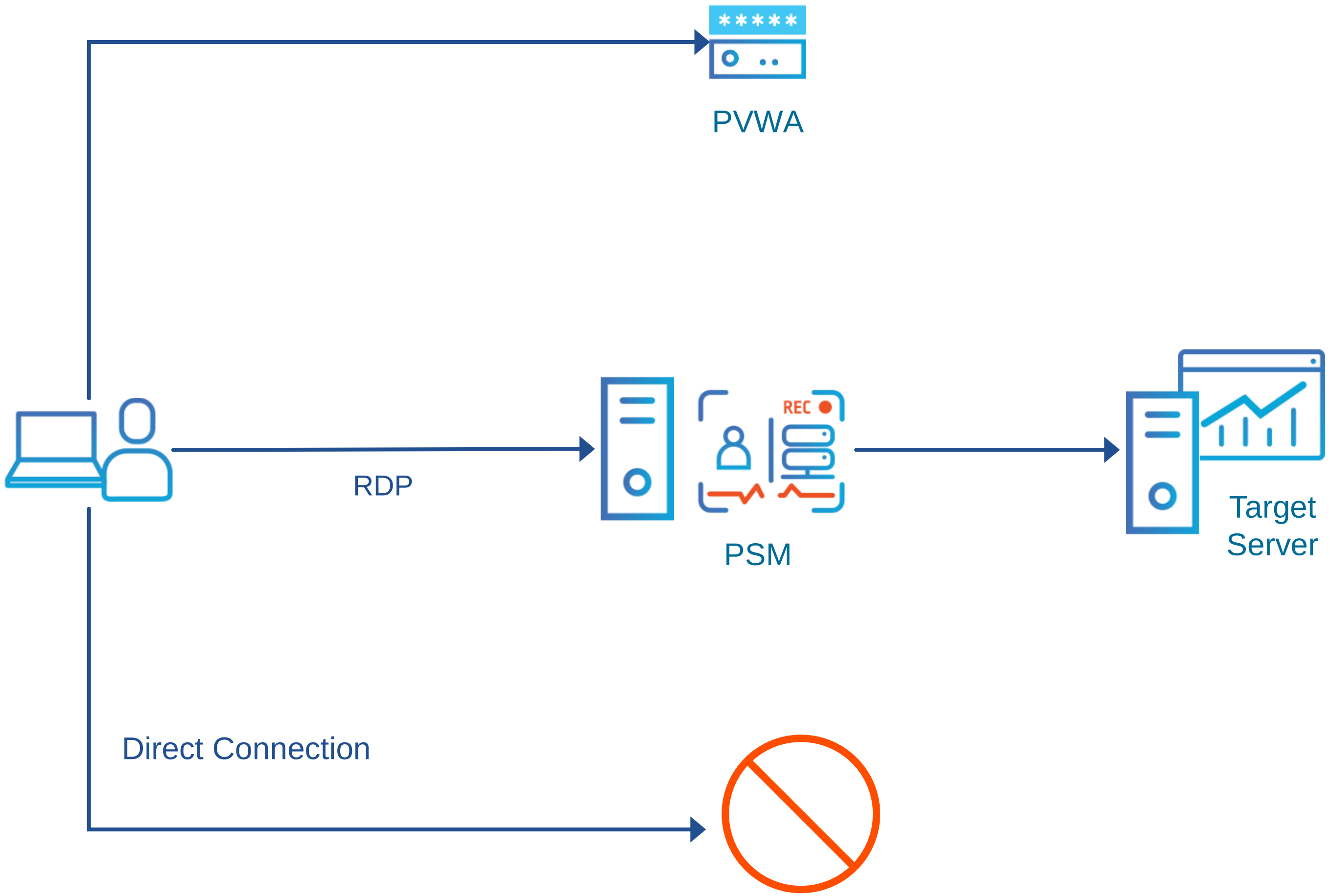
Support forensic analysis and audit with detailed records of privileged activity

Privileged Session Manager

The Privileged Session Manager

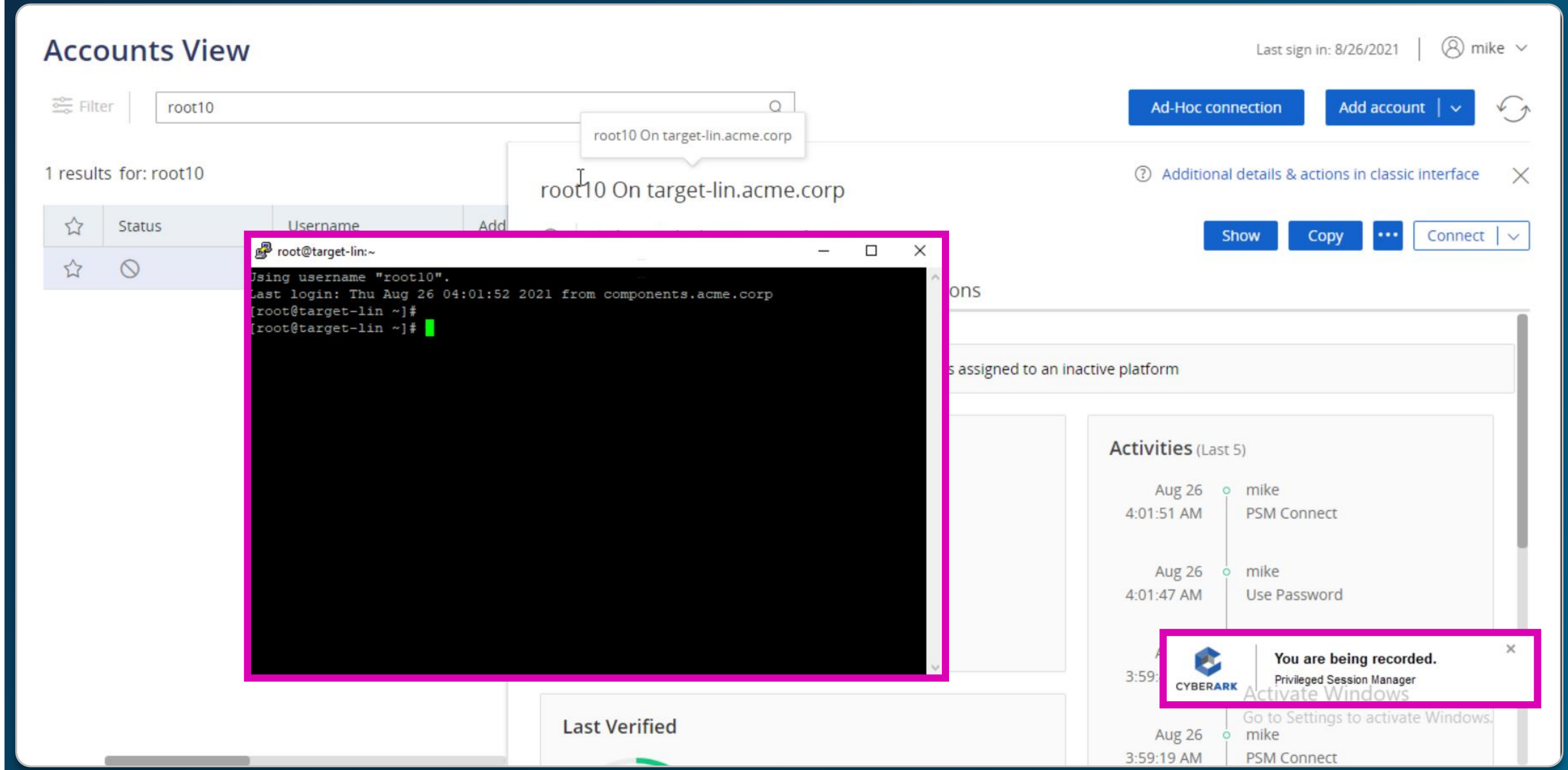
When we talk about **PSM**, the **Privileged Session Manager**, we are usually referring to the **PSM** installed on a Windows server.

You can think of this as the "Universal PSM" because you can connect through it practically from any device to any device.



The Privileged Session Manager

- The **PSM** enables organizations to secure, control, and monitor privileged access to network devices
- It creates detailed session audits and video recordings of all IT administrator privileged sessions on remote machines
- Sessions on the target systems are fully isolated and the privileged account credentials are never exposed to the end-users or their client applications and devices



1 results for: root10

root10 On target-lin.acme.corp

root@target-lin:~

```
Jsing username "root10".
Last login: Thu Aug 26 04:01:52 2021 from components.acme.corp
[root@target-lin ~]#
[root@target-lin ~]#
```

s assigned to an inactive platform

Activities (Last 5)

Aug 26 4:01:51 AM — mike — PSM Connect

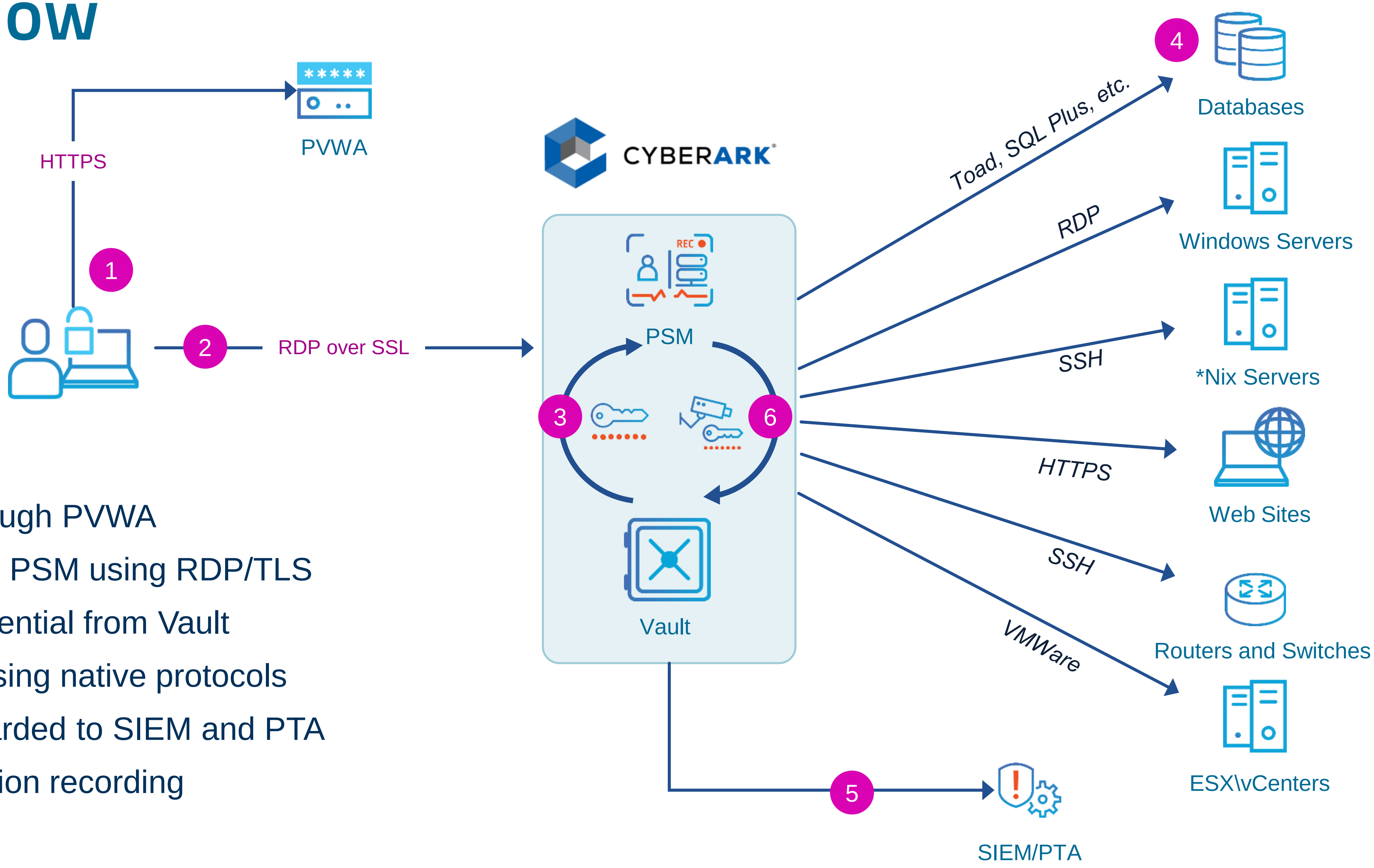
Aug 26 4:01:47 AM — mike — Use Password

3:59:

Aug 26 3:59:19 AM — mike — PSM Connect

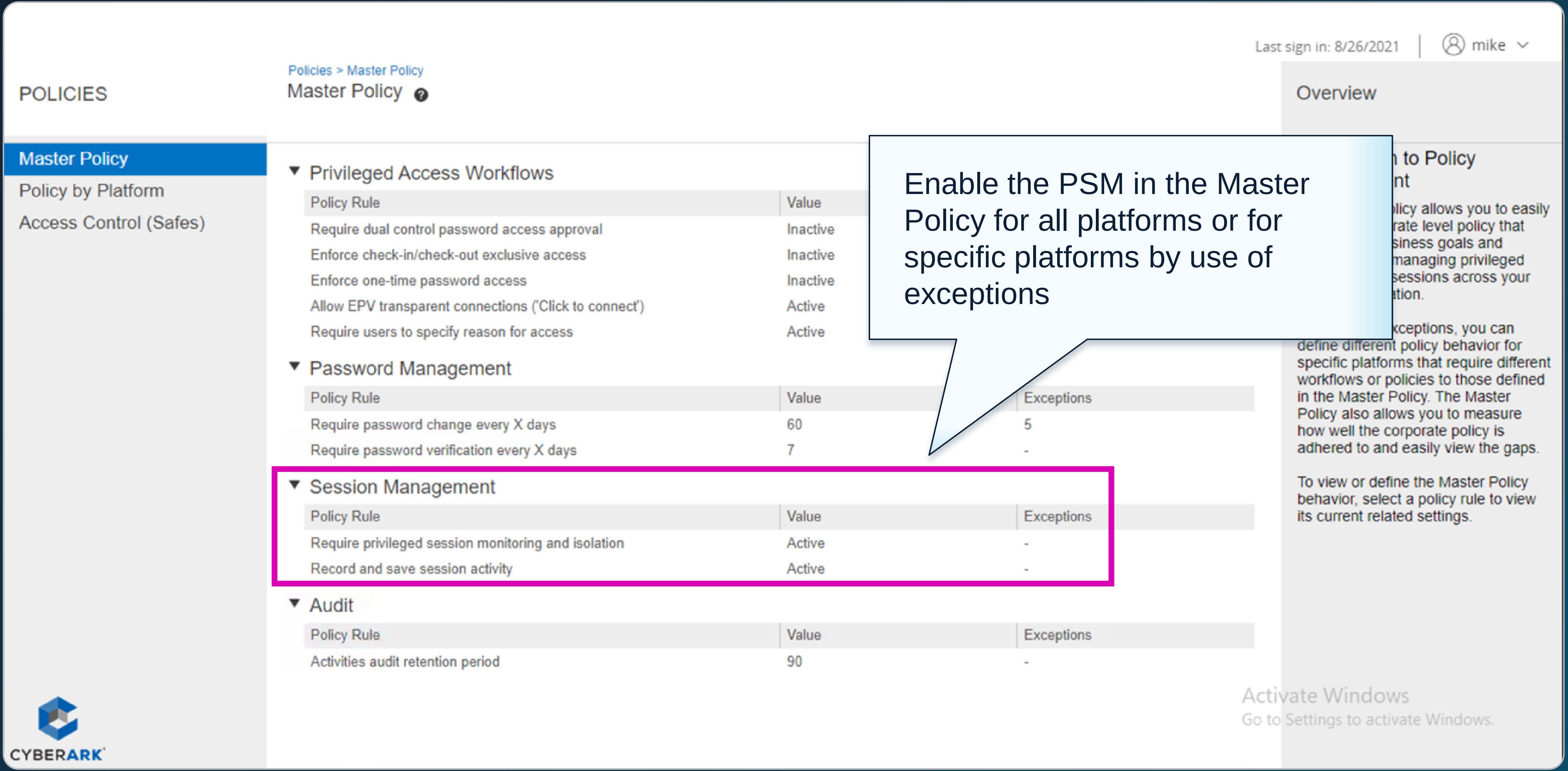
You are being recorded.
Privileged Session Manager

PSM Flow



1. Logon through PVWA
2. Connect to PSM using RDP/TLS
3. Fetch credential from Vault
4. Connect using native protocols
5. Logs forwarded to SIEM and PTA
6. Store session recording

Enable PSM: Master Policy



Last sign in: 8/26/2021 | mike

POLICIES

- Master Policy
- Policy by Platform
- Access Control (Safes)

Policies > Master Policy

Master Policy

▼ Privileged Access Workflows

Policy Rule	Value
Require dual control password access approval	Inactive
Enforce check-in/check-out exclusive access	Inactive
Enforce one-time password access	Inactive
Allow EPV transparent connections ('Click to connect')	Active
Require users to specify reason for access	Active

▼ Password Management

Policy Rule	Value	Exceptions
Require password change every X days	60	5
Require password verification every X days	7	-

▼ Session Management

Policy Rule	Value	Exceptions
Require privileged session monitoring and isolation	Active	-
Record and save session activity	Active	-

▼ Audit

Policy Rule	Value	Exceptions
Activities audit retention period	90	-

Overview

n to Policy
nt

licy allows you to easily
rate level policy that
siness goals and
managing privileged
sessions across your
ation.

xceptions, you can define different policy behavior for specific platforms that require different workflows or policies to those defined in the Master Policy. The Master Policy also allows you to measure how well the corporate policy is adhered to and easily view the gaps.

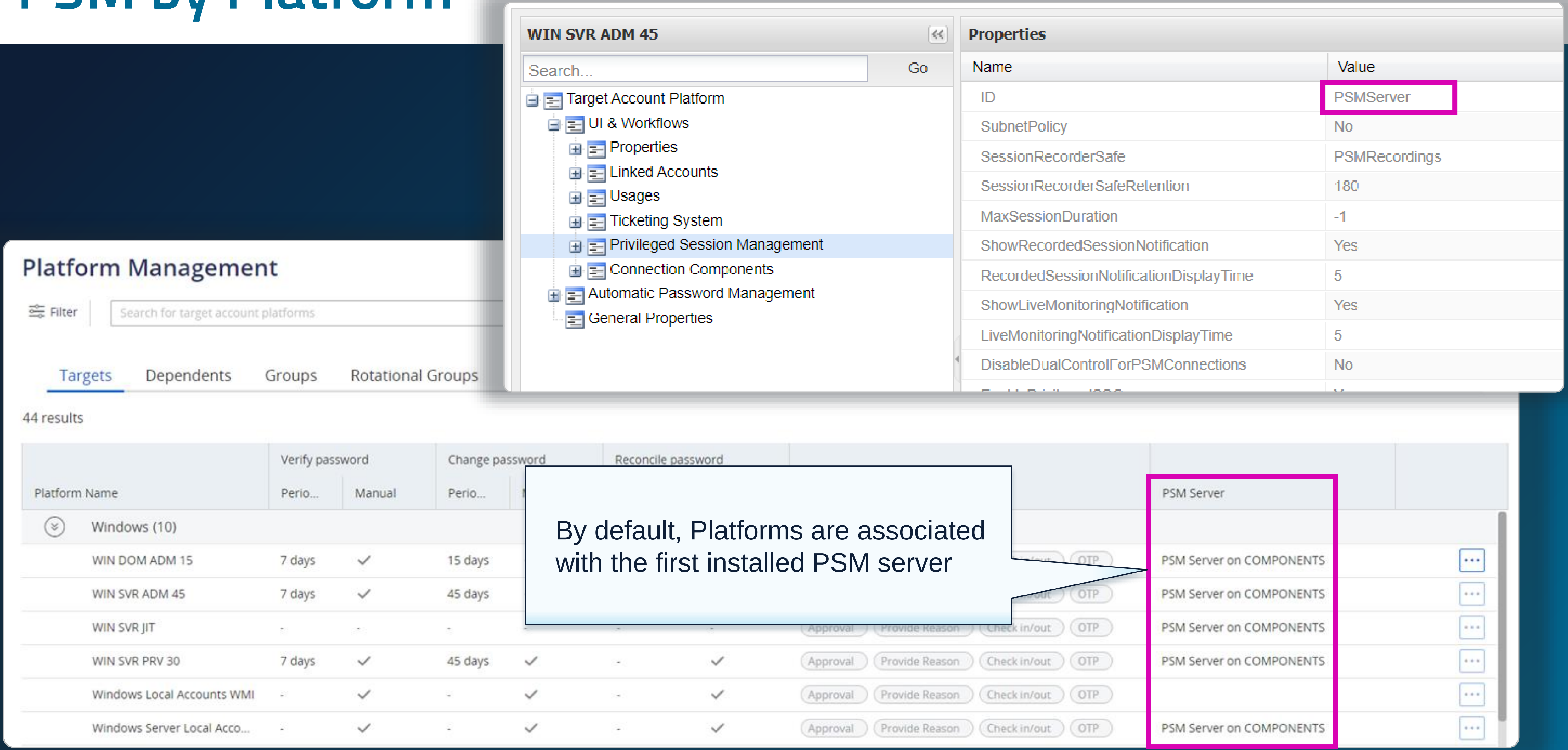
To view or define the Master Policy behavior, select a policy rule to view its current related settings.

CYBERARK

Enable the PSM in the Master Policy for all platforms or for specific platforms by use of exceptions

CYBERARK®

PSM by Platform



WIN SVR ADM 45

Search... Go

- Target Account Platform
  - UI & Workflows
    - Properties
    - Linked Accounts
    - Usages
    - Ticketing System
    - Privileged Session Management
    - Connection Components
  - Automatic Password Management
  - General Properties

Properties

Name	Value
ID	PSMServer
SubnetPolicy	No
SessionRecorderSafe	PSMRecordings
SessionRecorderSafeRetention	180
MaxSessionDuration	-1
ShowRecordedSessionNotification	Yes
RecordedSessionNotificationDisplayTime	5
ShowLiveMonitoringNotification	Yes
LiveMonitoringNotificationDisplayTime	5
DisableDualControlForPSMConnections	No

Platform Management

Filter | Search for target account platforms

Targets | Dependents | Groups | Rotational Groups

44 results

	Verify password		Change password		Reconcile password			
Platform Name	Perio...	Manual	Perio...					PSM Server
Windows (10)								
WIN DOM ADM 15	7 days	✓	15 days				OTP	PSM Server on COMPONENTS
WIN SVR ADM 45	7 days	✓	45 days				OTP	PSM Server on COMPONENTS
WIN SVR JIT	-	-	-	-	-	-	Approval Provide Reason Check in/out OTP	PSM Server on COMPONENTS
WIN SVR PRV 30	7 days	✓	45 days	✓	-	✓	Approval Provide Reason Check in/out OTP	PSM Server on COMPONENTS
Windows Local Accounts WMI	-	✓	-	✓	-	✓	Approval Provide Reason Check in/out OTP	
Windows Server Local Acco...	-	✓	-	✓	-	✓	Approval Provide Reason Check in/out OTP	PSM Server on COMPONENTS

By default, Platforms are associated with the first installed PSM server

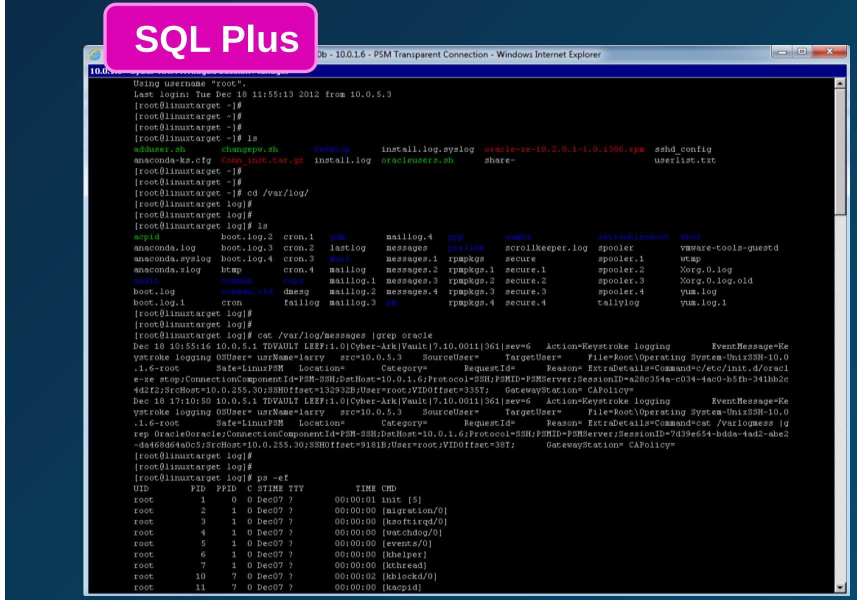
PSM Connection Components

Connection Components/ Connectors

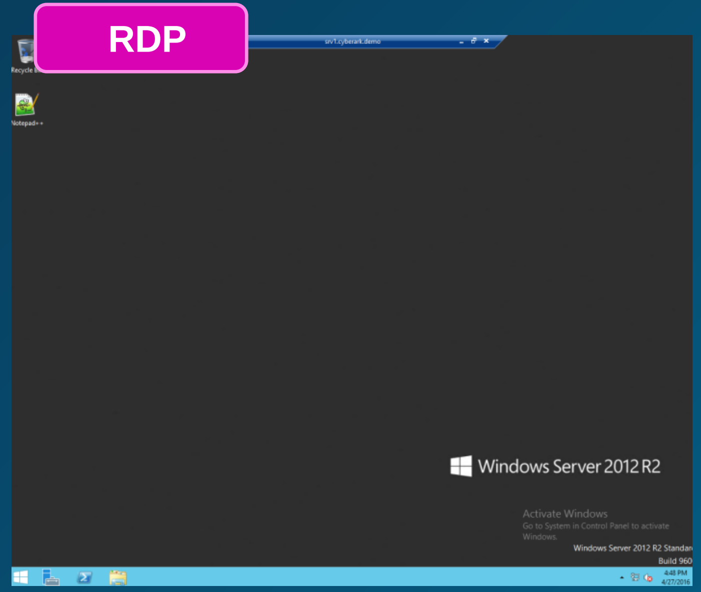
Connection Components (aka Connectors) define the configuration settings for using a given third-party client to connect to a target platform.

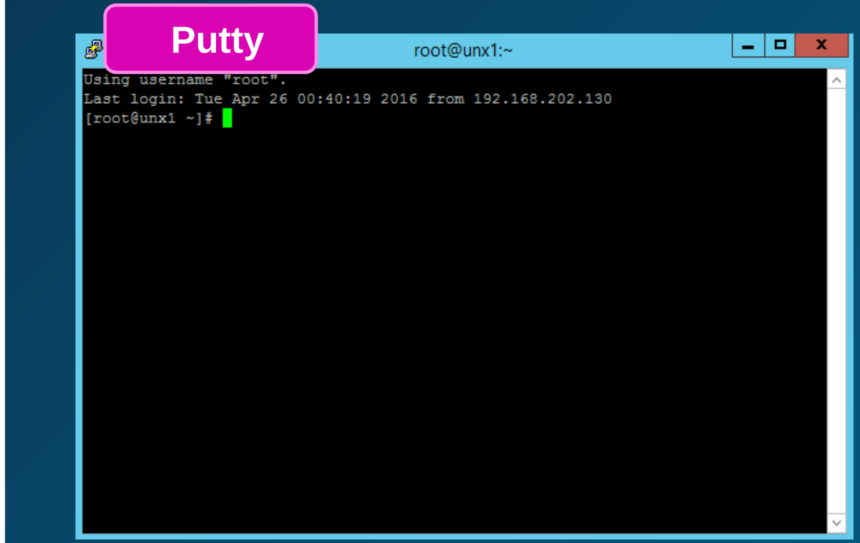
A few common ones are:

- SQLPlus
- RDP
- Putty
- WinSCP

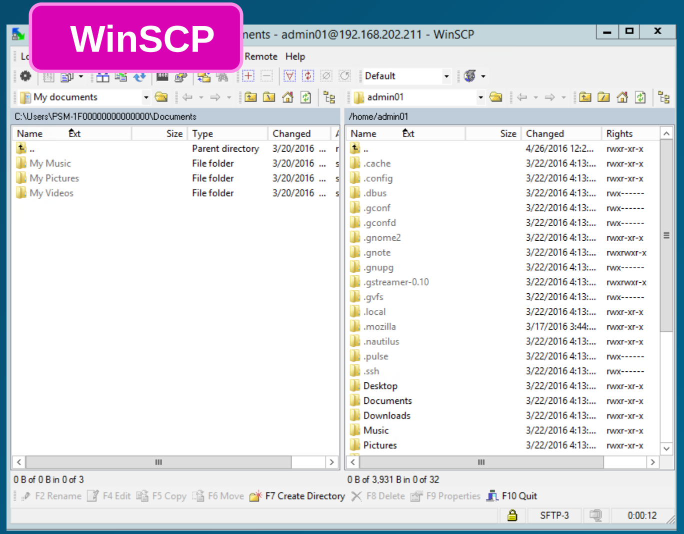

SQL Plus
0b - 10.0.1.6 - PSM Transparent Connection - Windows Internet Explorer

```
Using username "root".
Last login: Tue Dec 18 11:55:13 2012 from 10.0.5.3
[root@linuxtarget ~]#
[root@linuxtarget ~]#
[root@linuxtarget ~]#
[root@linuxtarget ~]# ls
adduser.sh       changepw.sh       Desktop      install.log.syslog  oracle-xe-10.2.0.1-1.0.i386.rpm  sshd_config
anaconda-ks.cfg  Conn_inst.tar.gz  install.log  oracleusers.sh      share~                           userlist.txt
[root@linuxtarget ~]#
[root@linuxtarget ~]#
[root@linuxtarget ~]# cd /var/log/
[root@linuxtarget log]#
[root@linuxtarget log]#
[root@linuxtarget log]# ls
acpid            boot.log.2  cron.1   gdm        maillog.4   ppp         samba              setroubleshoot  vbox
anaconda.log     boot.log.3  cron.2   lastlog    messages    prelink     scrollkeeper.log   spooler         vmware-tools-guestd
anaconda.syslog  boot.log.4  cron.3   mail       messages.1  rpmpkgs     secure             spooler.1       wtmp
anaconda.xlog    btmp        cron.4   maillog    messages.2  rpmpkgs.1   secure.1           spooler.2       Xorg.0.log
audit            conman      cups     maillog.1  messages.3  rpmpkgs.2   secure.2           spooler.3       Xorg.0.log.old
boot.log         conman.old  dmesg    maillog.2  messages.4  rpmpkgs.3   secure.3           spooler.4       yum.log
boot.log.1       cron        faillog  maillog.3  pm          rpmpkgs.4   secure.4           tallylog        yum.log.1
[root@linuxtarget log]#
[root@linuxtarget log]#
[root@linuxtarget log]# cat /var/log/messages |grep oracle
Dec 18 10:55:16 10.0.5.1 TDVAULT LEEF:1.0|Cyber-Ark|Vault|7.10.0011|361|sev=6   Action=Keystroke logging        EventMessage=Ke
ystroke logging OSUser= usrName=larry   src=10.0.5.3    SourceUser=     TargetUser=     File=Root\Operating System-UnixSSH-10.0
.1.6-root       Safe=LinuxPSM   Location=       Category=       RequestId=      Reason= ExtraDetails=Command=c/etc/init.d/oracl
e-xe stop;ConnectionComponentId=PSM-SSH;DstHost=10.0.1.6;Protocol=SSH;PSMID=PSMServer;SessionID=a28c354a-c034-4ac0-b5fb-341bb2c
4d2f2;SrcHost=10.0.255.30;SSHOffset=132932B;User=root;VIDOffset=335T;   GatewayStation= CAPolicy=
Dec 18 17:10:50 10.0.5.1 TDVAULT LEEF:1.0|Cyber-Ark|Vault|7.10.0011|361|sev=6   Action=Keystroke logging        EventMessage=Ke
ystroke logging OSUser= usrName=larry   src=10.0.5.3    SourceUser=     TargetUser=     File=Root\Operating System-UnixSSH-10.0
.1.6-root       Safe=LinuxPSM   Location=       Category=       RequestId=      Reason= ExtraDetails=Command=cat /varlogmess |g
rep Oracle0oracle;ConnectionComponentId=PSM-SSH;DstHost=10.0.1.6;Protocol=SSH;PSMID=PSMServer;SessionID=7d39e654-bdda-4ad2-abe2
-da468d64a0c5;SrcHost=10.0.255.30;SSHOffset=9181B;User=root;VIDOffset=38T;      GatewayStation= CAPolicy=
[root@linuxtarget log]#
[root@linuxtarget log]#
[root@linuxtarget log]# ps -ef
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 Dec07 ?        00:00:01 init [5]
root         2     1  0 Dec07 ?        00:00:00 [migration/0]
root         3     1  0 Dec07 ?        00:00:00 [ksoftirqd/0]
root         4     1  0 Dec07 ?        00:00:00 [watchdog/0]
root         5     1  0 Dec07 ?        00:00:00 [events/0]
root         6     1  0 Dec07 ?        00:00:00 [khelper]
root         7     1  0 Dec07 ?        00:00:00 [kthread]
root        10     7  0 Dec07 ?        00:00:02 [kblockd/0]
root        11     7  0 Dec07 ?        00:00:00 [kacpid]
```





```
Using username "root".
Last login: Tue Apr 26 00:40:19 2016 from 192.168.202.130
[root@unx1 ~]#
```



C:\Users\PSM-1F00000000000000\Documents

Name	Ext	Size	Type	Changed
..			Parent directory	3/20/2016 ...
My Music			File folder	3/20/2016 ...
My Pictures			File folder	3/20/2016 ...
My Videos			File folder	3/20/2016 ...

0 B of 0 B in 0 of 3

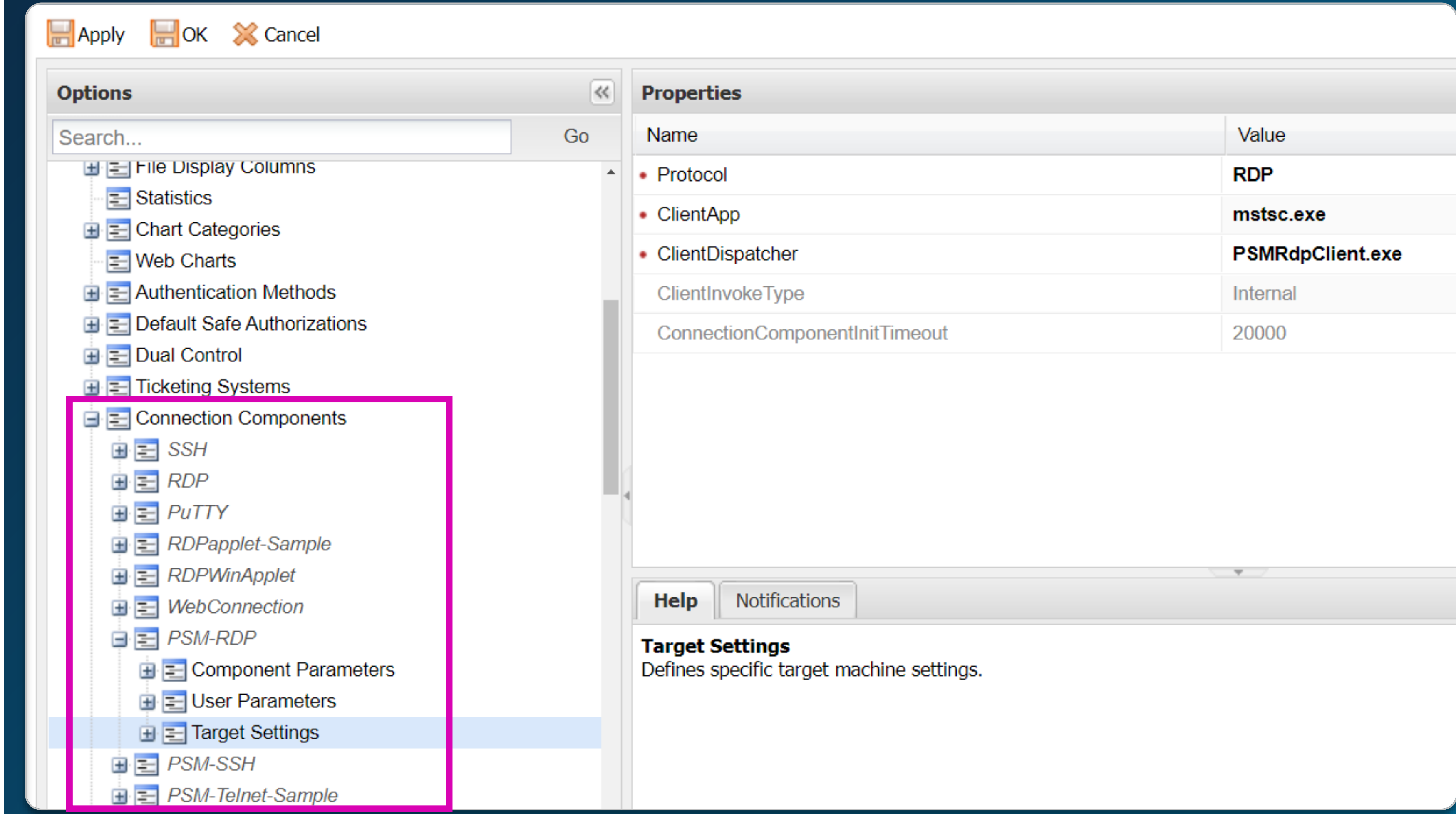
/home/admin01

Name	Ext	Size	Changed	Rights
..			4/26/2016 12:2...	rwxr-xr-x
.cache			3/22/2016 4:13:...	rwxr-xr-x
.config			3/22/2016 4:13:...	rwxr-xr-x
.dbus			3/22/2016 4:13:...	rwx------
.gconf			3/22/2016 4:13:...	rwx------
.gconfd			3/22/2016 4:13:...	rwx------
.gnome2			3/22/2016 4:13:...	rwxr-xr-x
.gnote			3/22/2016 4:13:...	rwxrwxr-x
.gnupg			3/22/2016 4:13:...	rwx------
.gstreamer-0.10			3/22/2016 4:13:...	rwxrwxr-x
.gvfs			3/22/2016 4:13:...	rwx------
.local			3/22/2016 4:13:...	rwxr-xr-x
.mozilla			3/17/2016 3:44:...	rwxr-xr-x
.nautilus			3/22/2016 4:13:...	rwxr-xr-x
.pulse			3/22/2016 4:13:...	rwx------
.ssh			3/22/2016 4:13:...	rwx------
Desktop			3/22/2016 4:13:...	rwxr-xr-x
Documents			3/22/2016 4:13:...	rwxr-xr-x
Downloads			3/22/2016 4:13:...	rwxr-xr-x
Music			3/22/2016 4:13:...	rwxr-xr-x
Pictures			3/22/2016 4:13:...	rwxr-xr-x

0 B of 3,931 B in 0 of 32

Connection Components/ Connectors

- There are many connection components available out of the box
- Additional connection components can be found in the **CyberArk Marketplace**
- Organizations can also build and add custom connection components to the **PAM** solution

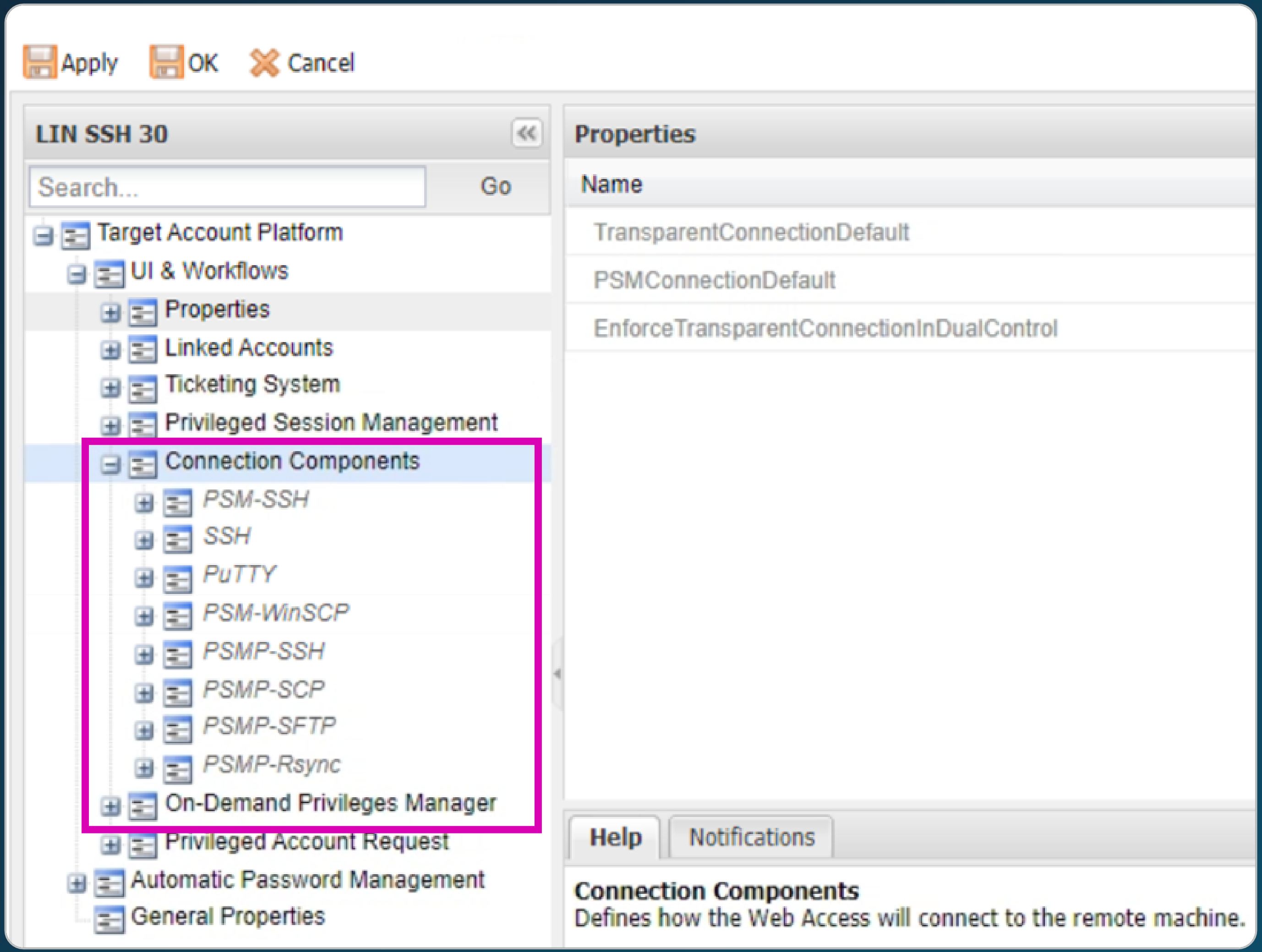


Name	Value
• Protocol	**RDP**
• ClientApp	**mstsc.exe**
• ClientDispatcher	**PSMRdpClient.exe**
ClientInvokeType	Internal
ConnectionComponentInitTimeout	20000

Target Settings
Defines specific target machine settings.

Platform Settings

To enable the use of a particular third-party client to connect to a given account, the appropriate ***Connection Component*** needs to be assigned to the ***Platform*** that manages that account



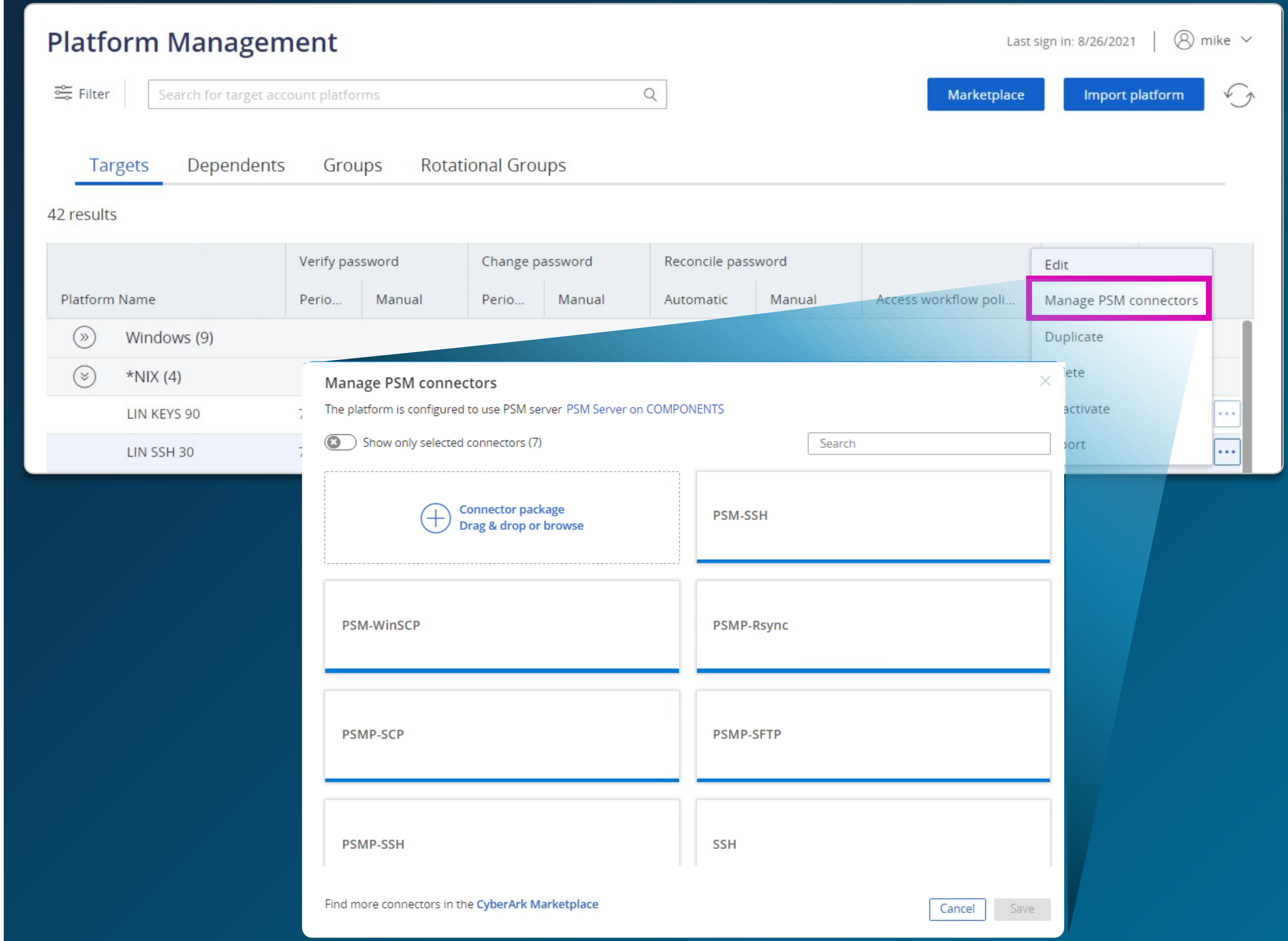
Properties

Name
TransparentConnectionDefault
PSMConnectionDefault
EnforceTransparentConnectionInDualControl

Connection Components
Defines how the Web Access will connect to the remote machine.

Importing and Managing Connectors

The new interface accelerates and simplifies **Vault** administration by allowing admins to import **PSM** connectors and link them to ***Platforms***, all from one location



Platform Management

Last sign in: 8/26/2021 | mike

Filter | Search for target account platforms

Marketplace | Import platform

Targets | Dependents | Groups | Rotational Groups

42 results

Platform Name	Verify password		Change password		Reconcile password		Access workflow poli...
	Perio...	Manual	Perio...	Manual	Automatic	Manual	
Windows (9)							
*NIX (4)							
LIN KEYS 90	7						
LIN SSH 30	7						

Edit
Manage PSM connectors
Duplicate
ete
activate
port

Manage PSM connectors

The platform is configured to use PSM server PSM Server on COMPONENTS

Show only selected connectors (7)

Search

Connector package
Drag & drop or browse

PSM-SSH

PSM-WinSCP

PSMP-Rsync

PSMP-SCP

PSMP-SFTP

PSMP-SSH

SSH

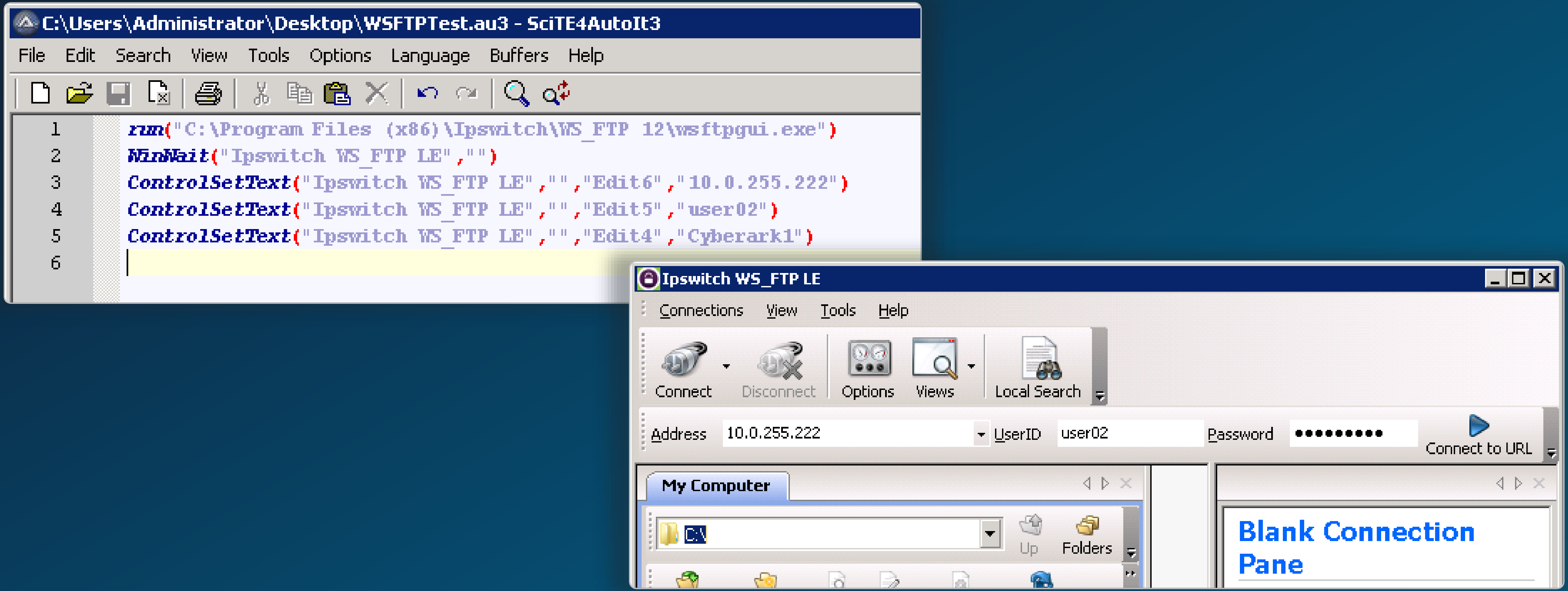
Find more connectors in the CyberArk Marketplace

Cancel | Save

CYBERARK®

Universal Connector

The Universal Connector framework facilitates the creation of custom connection components using a (relatively) simple, freeware programming language called AutoIT.



```
run("C:\Program Files (x86)\Ipswitch\WS_FTP 12\wsftpgui.exe")
WinWait("Ipswitch WS_FTP LE","")
ControlSetText("Ipswitch WS_FTP LE","","Edit6","10.0.255.222")
ControlSetText("Ipswitch WS_FTP LE","","Edit5","user02")
ControlSetText("Ipswitch WS_FTP LE","","Edit4","Cyberark1")
```

Address 10.0.255.222

UserID user02

Password •••••••••

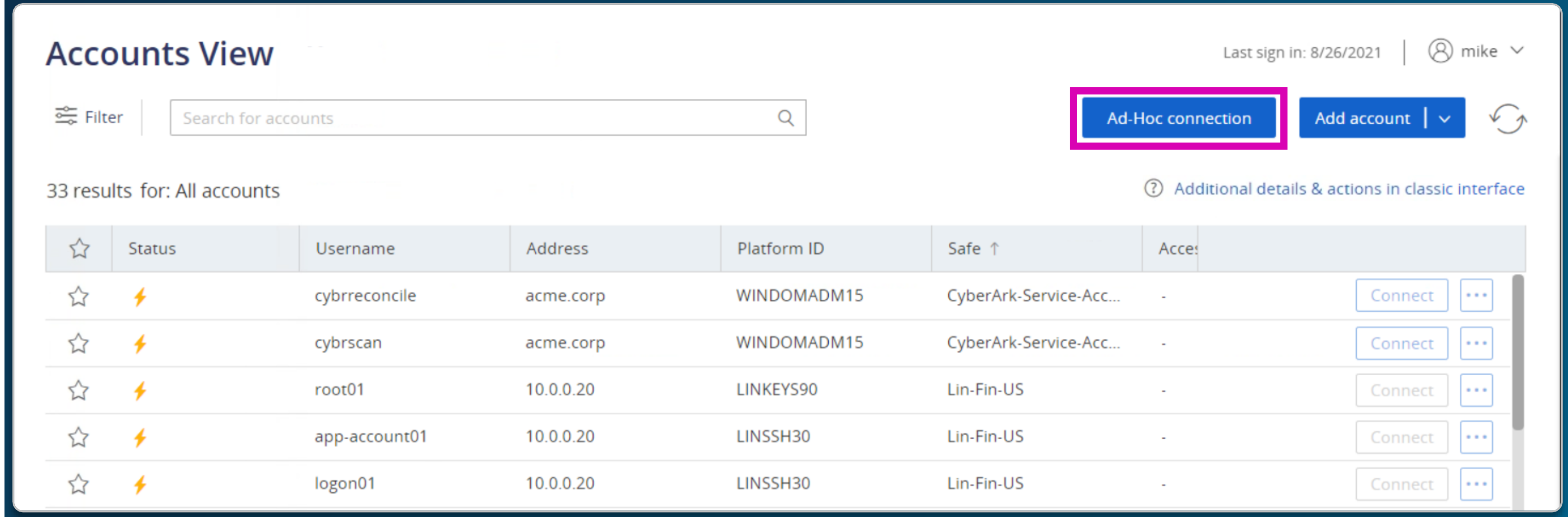
C:\Users\Administrator\Desktop\WSFTPTest.au3 - SciTE4AutoIt3
File Edit Search View Tools Options Language Buffers Help
Ipswitch WS_FTP LE
Connections View Tools Help
Connect
Disconnect
Options
Views
Local Search
Connect to URL
My Computer
C:\
Up
Folders
Blank Connection Pane

PSM Ad-hoc Sessions

PSM Ad-hoc Connection: Overview

With an **Ad-Hoc Connection**, users can connect securely to any machine supported by the PSM if they know the password

- Main use cases:
  - Connecting with accounts that are not stored in the CyberArk Vault
  - Connecting with personal accounts
- Provides all the benefits of PSM: isolation, monitoring, and recording



Accounts View

Last sign in: 8/26/2021 | mike

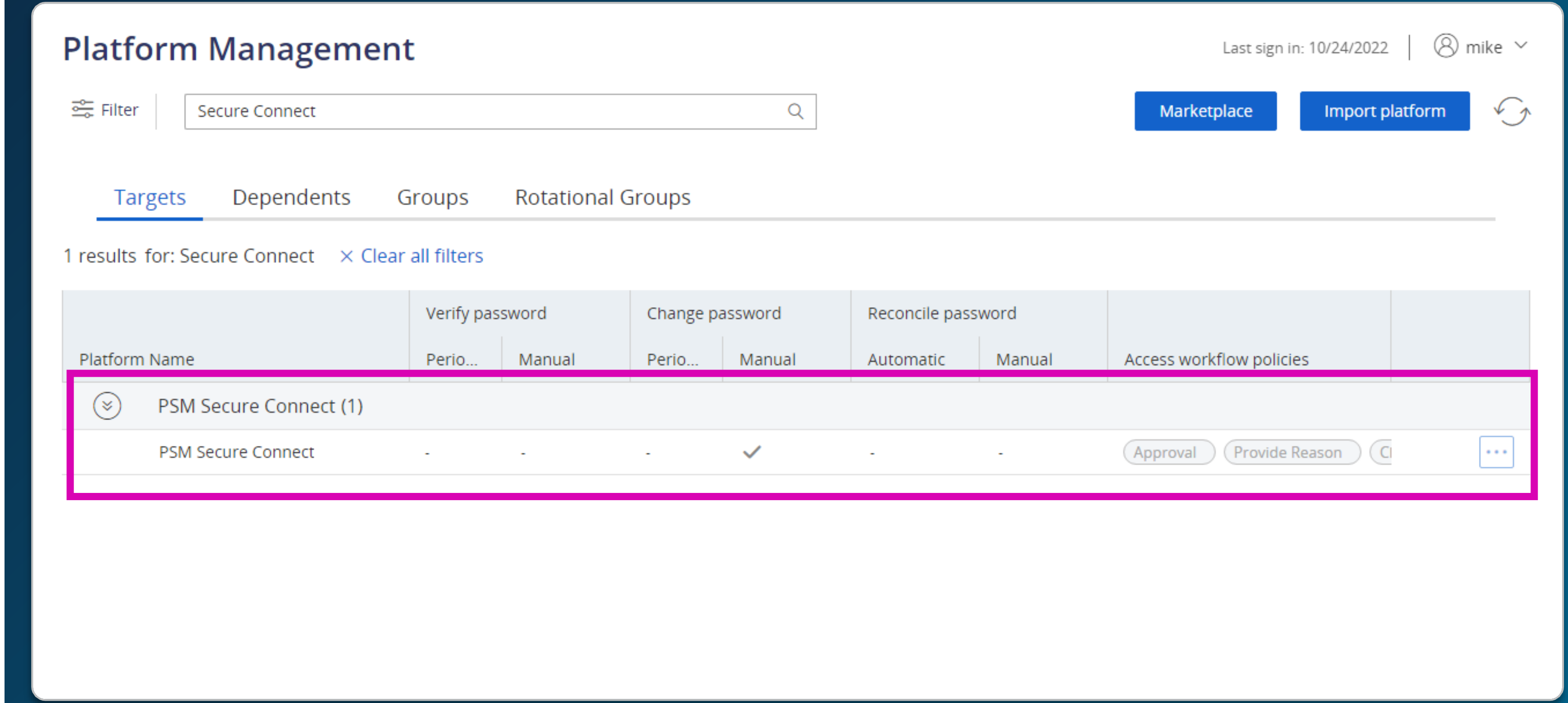
33 results for: All accounts

Additional details & actions in classic interface

☆	Status	Username	Address	Platform ID	Safe ↑	Acce		
☆	⚡	cybrreconcile	acme.corp	WINDOMADM15	CyberArk-Service-Acc...	-	Connect	···
☆	⚡	cybrscan	acme.corp	WINDOMADM15	CyberArk-Service-Acc...	-	Connect	···
☆	⚡	root01	10.0.0.20	LINKEYS90	Lin-Fin-US	-	Connect	···
☆	⚡	app-account01	10.0.0.20	LINSSH30	Lin-Fin-US	-	Connect	···
☆	⚡	logon01	10.0.0.20	LINSSH30	Lin-Fin-US	-	Connect	···

Enable Ad-hoc Connections

- The **PSM Secure Connect** Platform must be activated
- Privileged session monitoring and isolation must be enabled for the **PSM Secure Connect** platform. This can be done either globally or via an exception to the Master policy.



Platform Management

Last sign in: 10/24/2022 | mike

Filter | Secure Connect

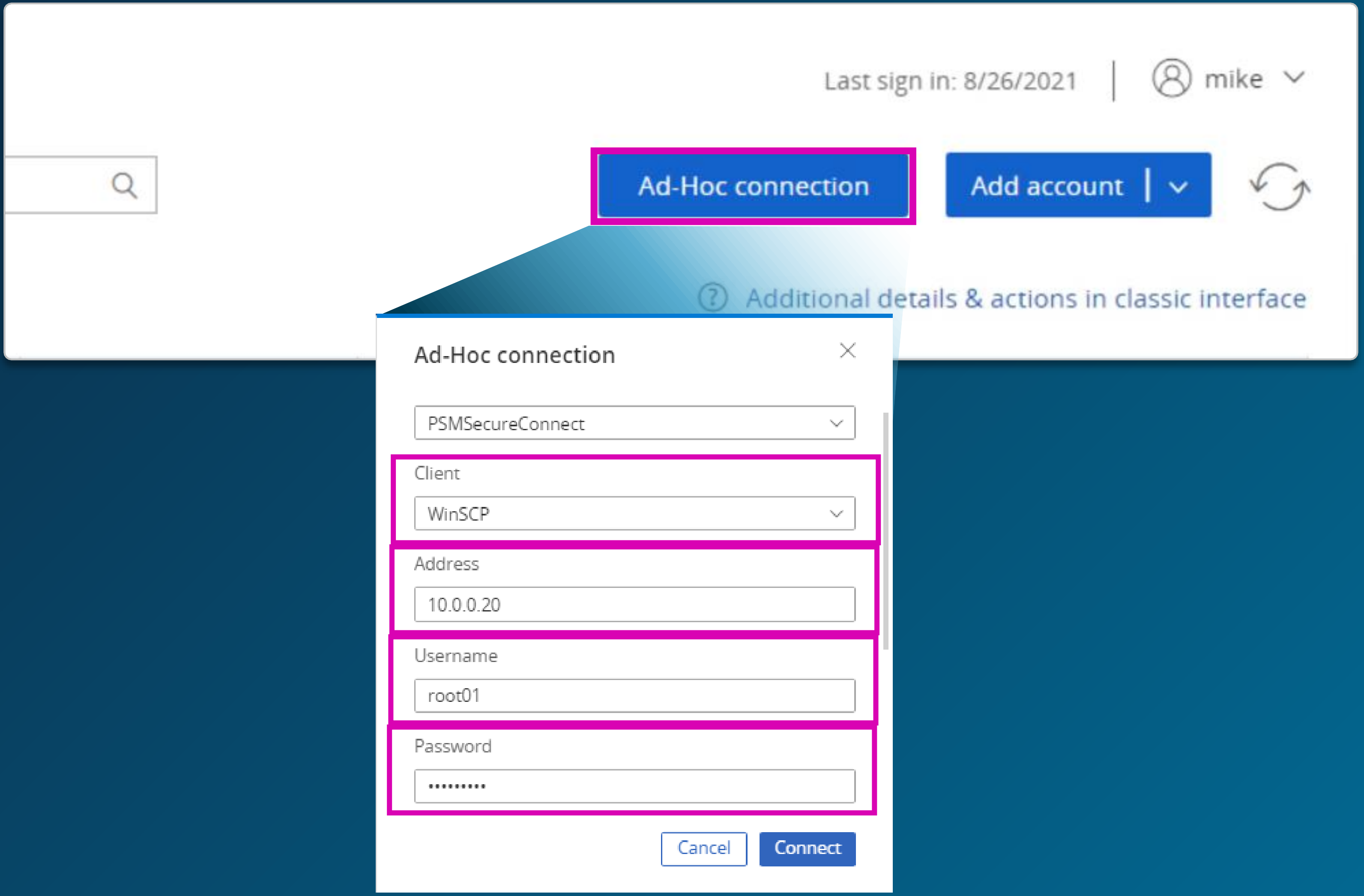
1 results for: Secure Connect × Clear all filters

	Verify password		Change password		Reconcile password			
Platform Name	Perio...	Manual	Perio...	Manual	Automatic	Manual	Access workflow policies	
PSM Secure Connect (1)								
PSM Secure Connect	-	-	-	✓	-	-	Approval Provide Reason C	⋯

Launch Ad-hoc Connection

Users will need to specify all the account details when they connect:

- The **Client** they want to use on the PSM
- Target system **Address**
- Username
- Password, etc.



Ad-Hoc connection

PSMSecureConnect

Client: WinSCP

Address: 10.0.0.20

Username: root01

Password: •••••••••

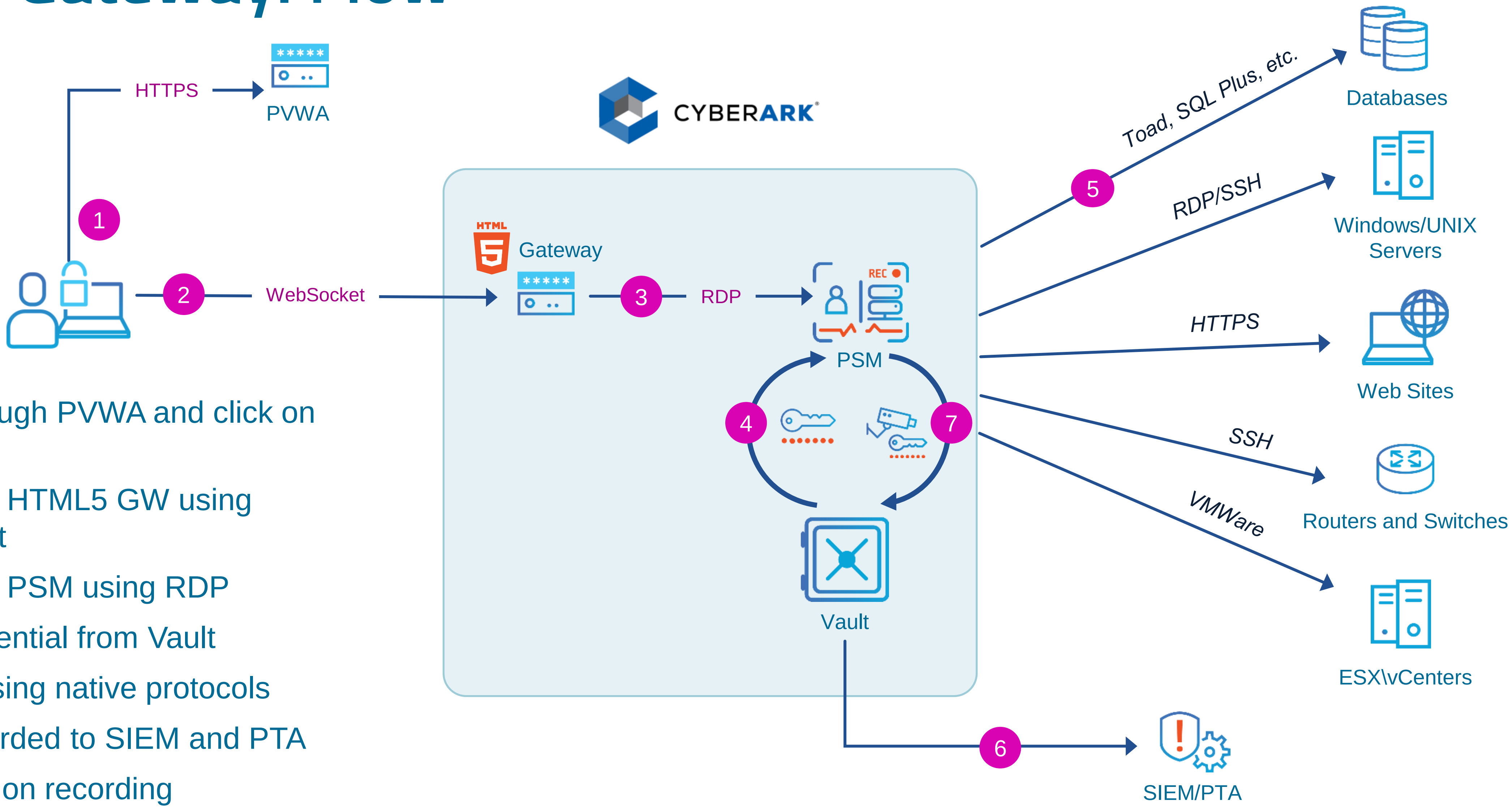
HTML5 Gateway

HTML5 Gateway: Overview

- Many organizations block RDP client connections from end-users' machines for security reasons or regulatory requirements.
- RDP is a Microsoft protocol, so in order to use it in Linux, Unix, or MAC environments, users must install a 3rd-party client in order to connect to the PSM.
- The HTML5 Gateway tunnels the session between the end user and the PSM proxy machine using a secure WebSocket protocol (port 443). This solution eliminates the need to open an RDP connection from the end user's machine. Instead, the end user only requires a web browser to establish a connection to a remote machine through PSM.
- Secure access through HTML5 requires integrating an HTML5 gateway on a Linux server (can be co-hosted with PSM for SSH). The Gateway is based on Apache Guacamole.

Apache Guacamole

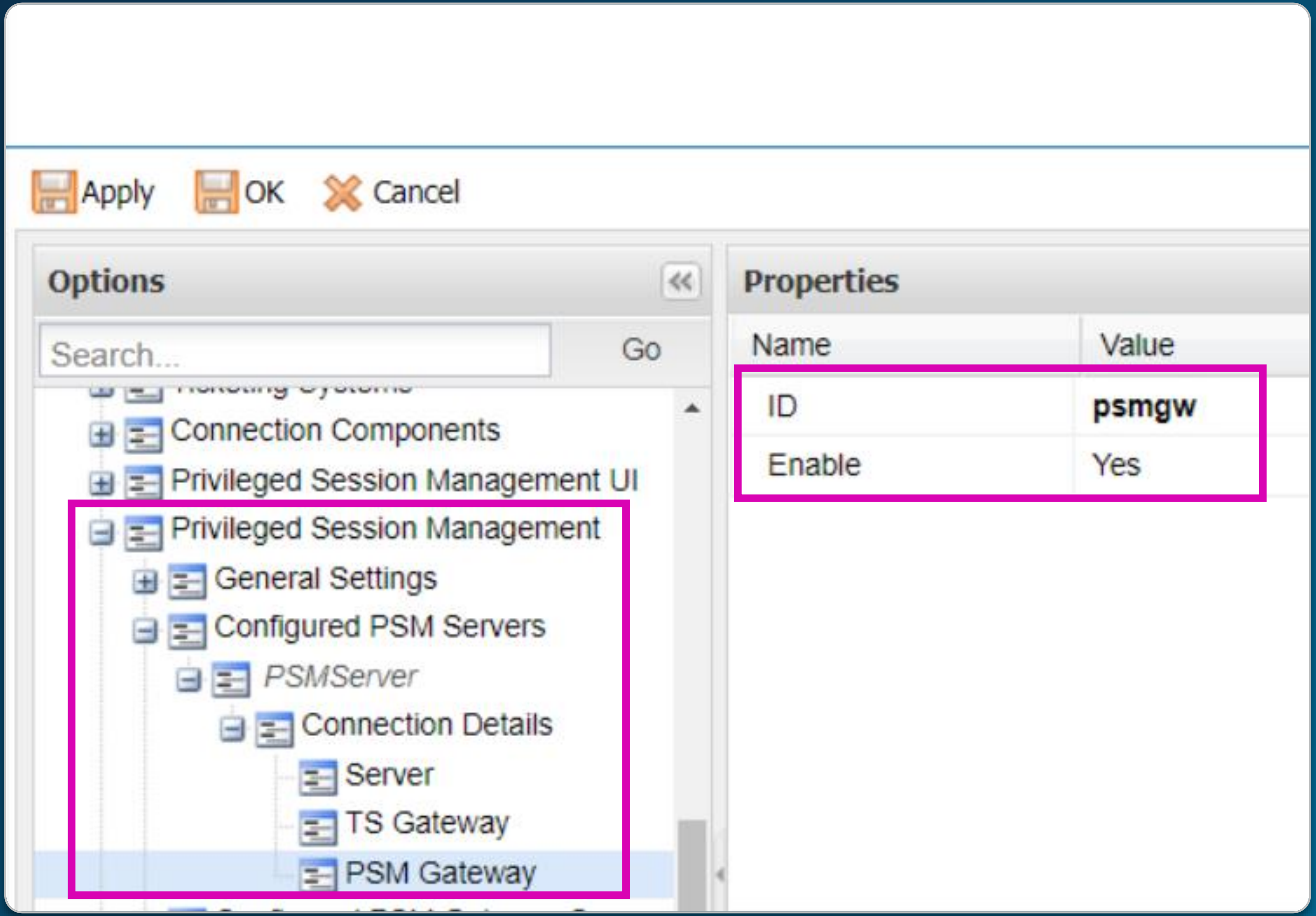
HTML5 Gateway: Flow



1. Logon through PVWA and click on Connect
2. Connect to HTML5 GW using WebSocket
3. Connect to PSM using RDP
4. Fetch credential from Vault
5. Connect using native protocols
6. Logs forwarded to SIEM and PTA
7. Store session recording

Enable HTML5 Gateway

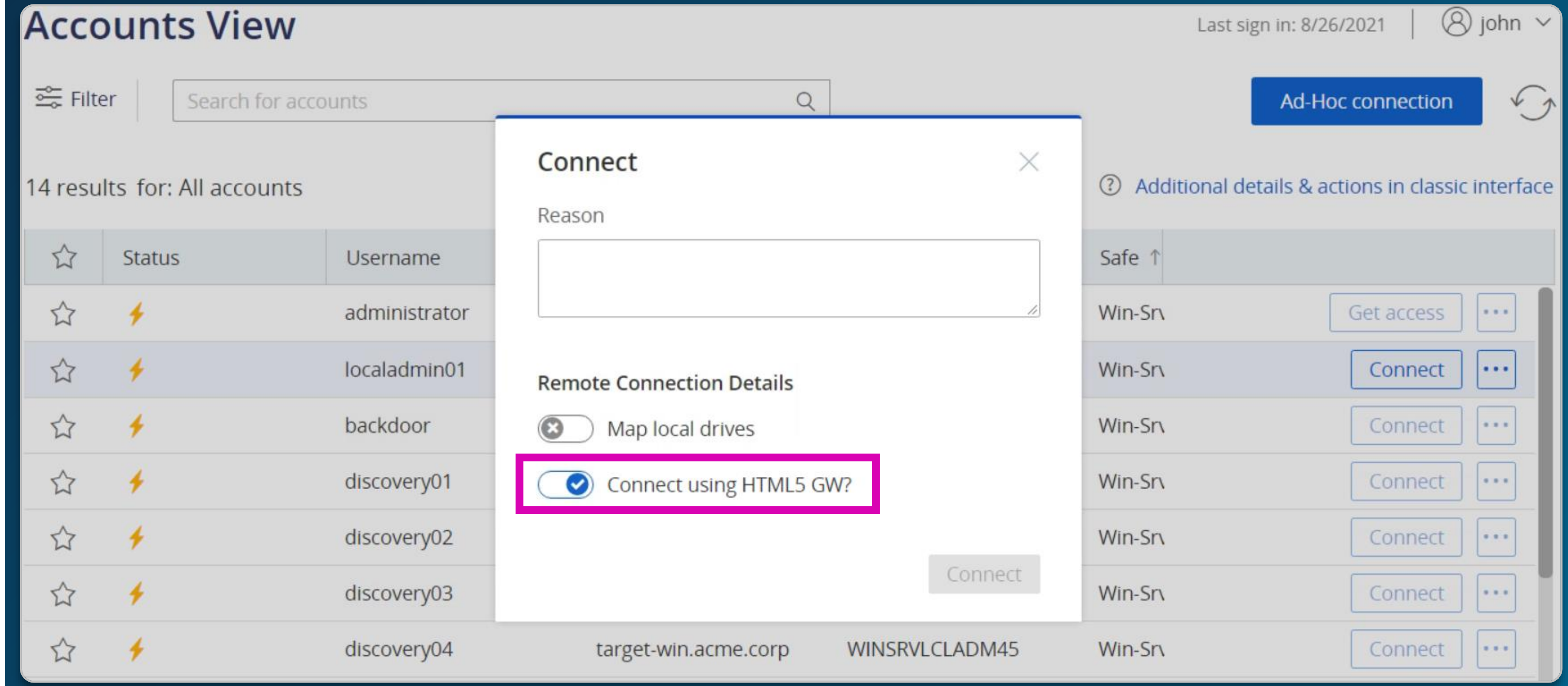
The **HTML5 GW** is enabled at the system level for each **PSM** server



Name	Value
ID	psmgw
Enable	Yes

Use HDML5-based or RDP-file Connection Method

- Users can be given the option to connect either an HTML5-based or RDP-file connection method when connecting to the remote server
- This setting is applied at the **Connection Component** level



Accounts View

Last sign in: 8/26/2021 | john

Filter | Search for accounts | Ad-Hoc connection

14 results for: All accounts

Additional details & actions in classic interface

☆	Status	Username			Safe		
☆	⚡	administrator			Win-Srv	Get access	···
☆	⚡	localadmin01			Win-Srv	Connect	···
☆	⚡	backdoor			Win-Srv	Connect	···
☆	⚡	discovery01			Win-Srv	Connect	···
☆	⚡	discovery02			Win-Srv	Connect	···
☆	⚡	discovery03			Win-Srv	Connect	···
☆	⚡	discovery04	target-win.acme.corp	WINSRVLCLADM45	Win-Srv	Connect	···

Connect

Reason

Remote Connection Details

○ Map local drives

● Connect using HTML5 GW?

Connect

PSM for Windows

PSM for Windows: Overview

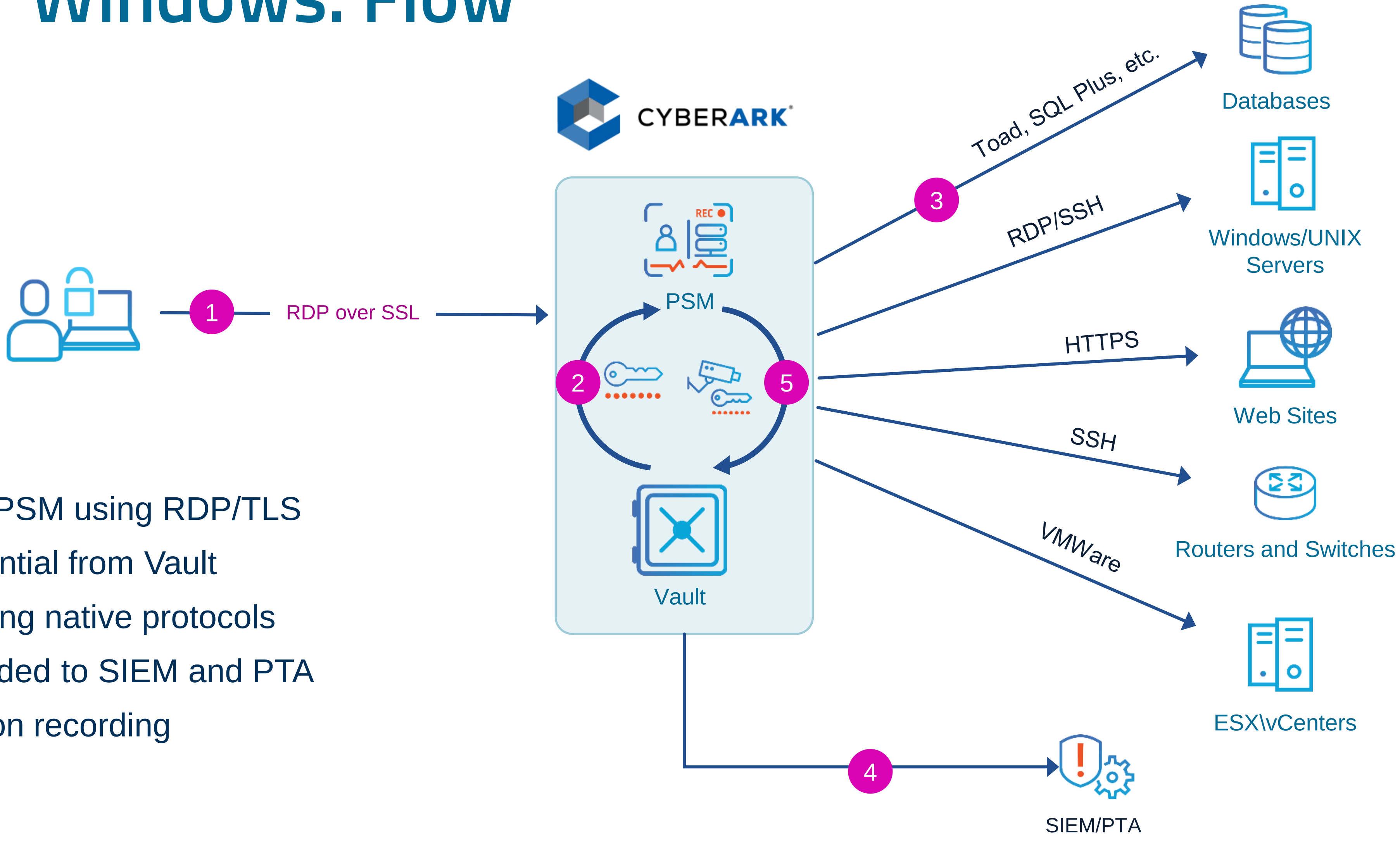
- Users connect directly from their desktops with an RDP-compliant client to the PSM, which then connects to the target host using the protocol appropriate to that host: SSH, RDP, etc.

- There is no need to go through the PVWA.

- Users can launch the RDP client and sign in into CyberArk using single- or multi-factor authentication (for example, LDAP with RADIUS).
  - The RDP client application must include the ability to configure run “Start Program” for the RDP connections.
  - Connections can be made from Unix / Linux / Mac / Windows end user machines.

- PSM continues to provide complete isolation of the target systems, ensuring that privileged credentials never reach users or their devices.

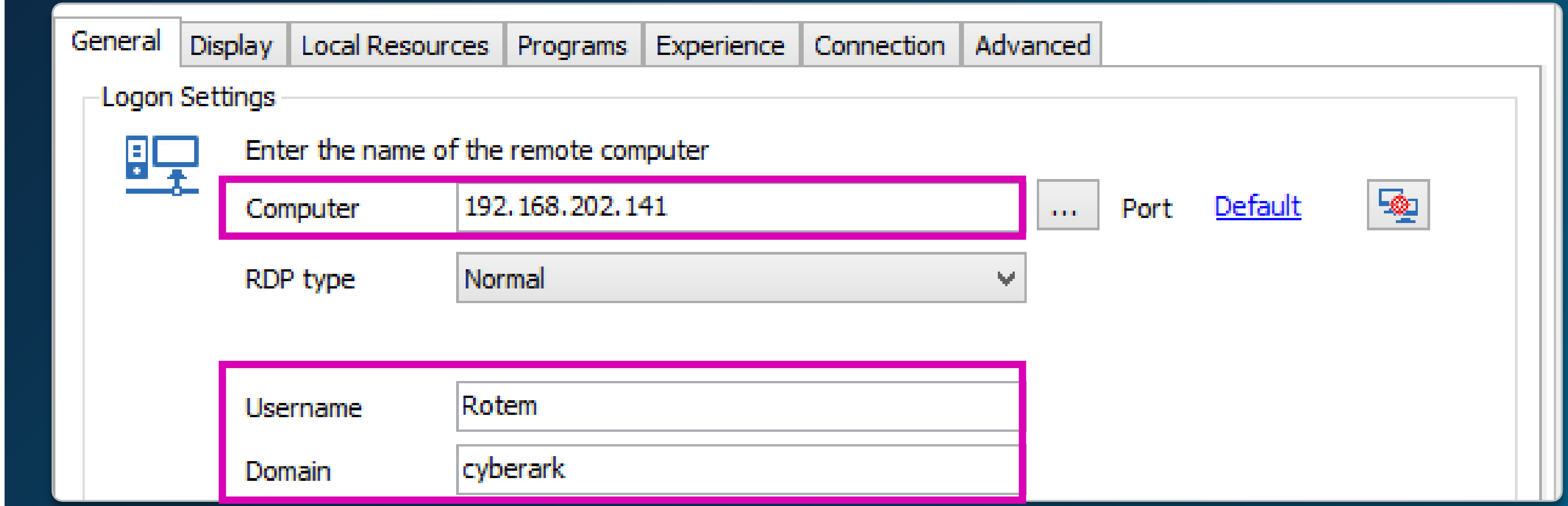
PSM for Windows: Flow



1. Connect to PSM using RDP/TLS
2. Fetch credential from Vault
3. Connect using native protocols
4. Logs forwarded to SIEM and PTA
5. Store session recording

RDP Client Settings

- PSM IP
- Vault user
- Activate Start Program
- Program path:
  - Privileged Account name
  - Target address
  - Connection Component



Logon Settings

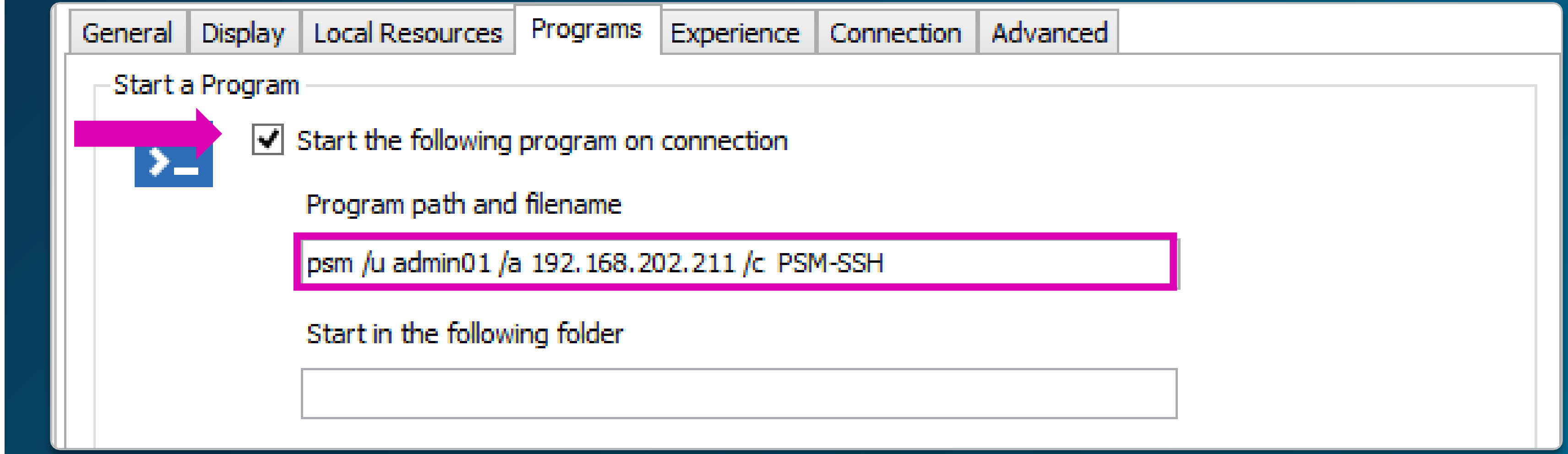
Enter the name of the remote computer

Computer: 192.168.202.141

RDP type: Normal

Username: Rotem

Domain: cyberark



Start a Program

☑ Start the following program on connection

Program path and filename

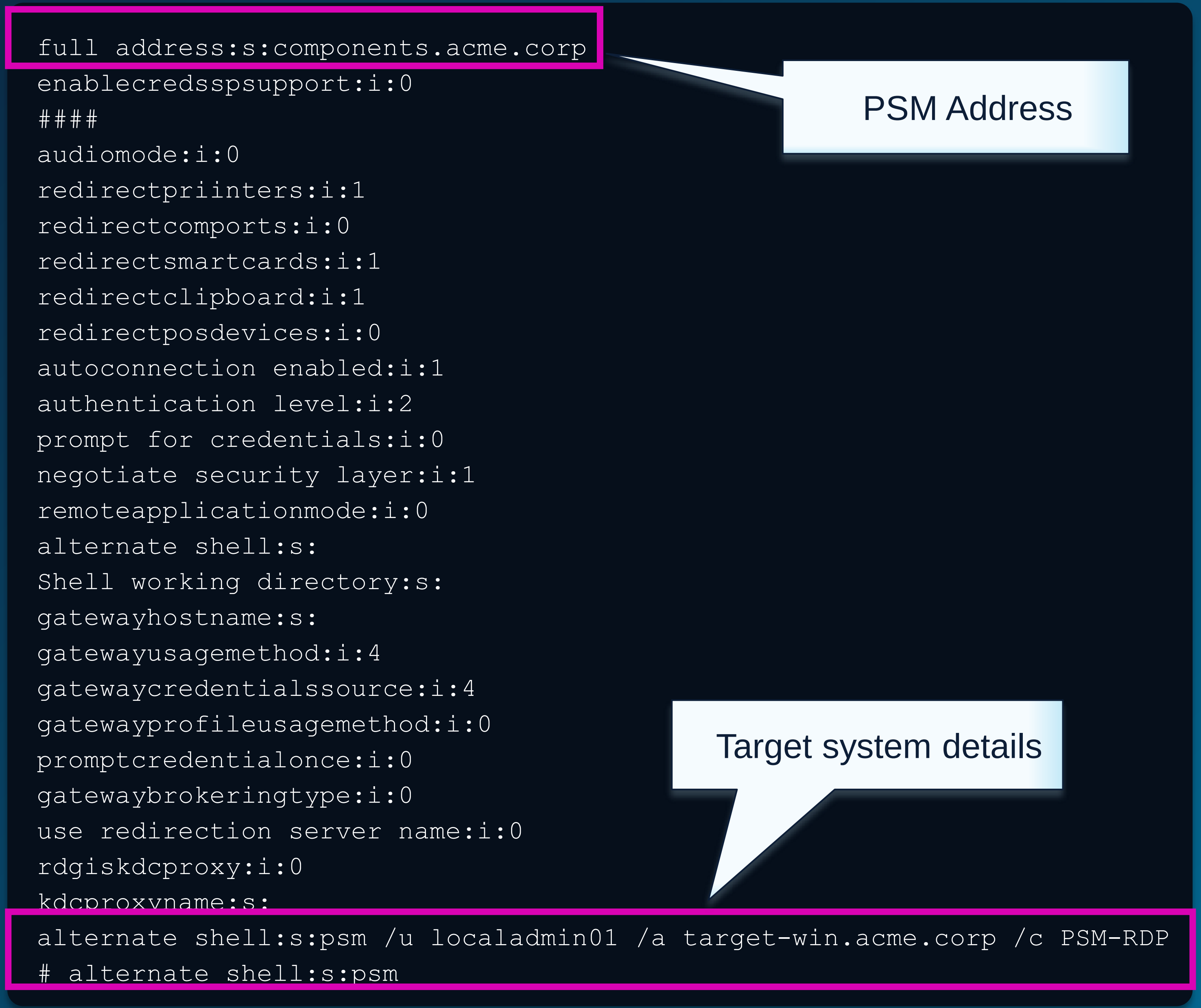
```
psm /u admin01 /a 192.168.202.211 /c  PSM-SSH
```

Start in the following folder

Preconfigured RDP Files

You can also configure individual RDP files to connect through the **PSM**

- It is possible to configure connections with or without providing the target system details



```
full address:s:components.acme.corp
enablecredsspsupport:i:0
####
audiomode:i:0
redirectpriinters:i:1
redirectcomports:i:0
redirectsmartcards:i:1
redirectclipboard:i:1
redirectposdevices:i:0
autoconnection enabled:i:1
authentication level:i:2
prompt for credentials:i:0
negotiate security layer:i:1
remoteapplicationmode:i:0
alternate shell:s:
Shell working directory:s:
gatewayhostname:s:
gatewayusagemethod:i:4
gatewaycredentialssource:i:4
gatewayprofileusagemethod:i:0
promptcredentialonce:i:0
gatewaybrokeringtype:i:0
use redirection server name:i:0
rdgiskdcproxy:i:0
kdcproxyname:s:
alternate shell:s:psm /u localadmin01 /a target-win.acme.corp /c PSM-RDP
# alternate shell:s:psm
```

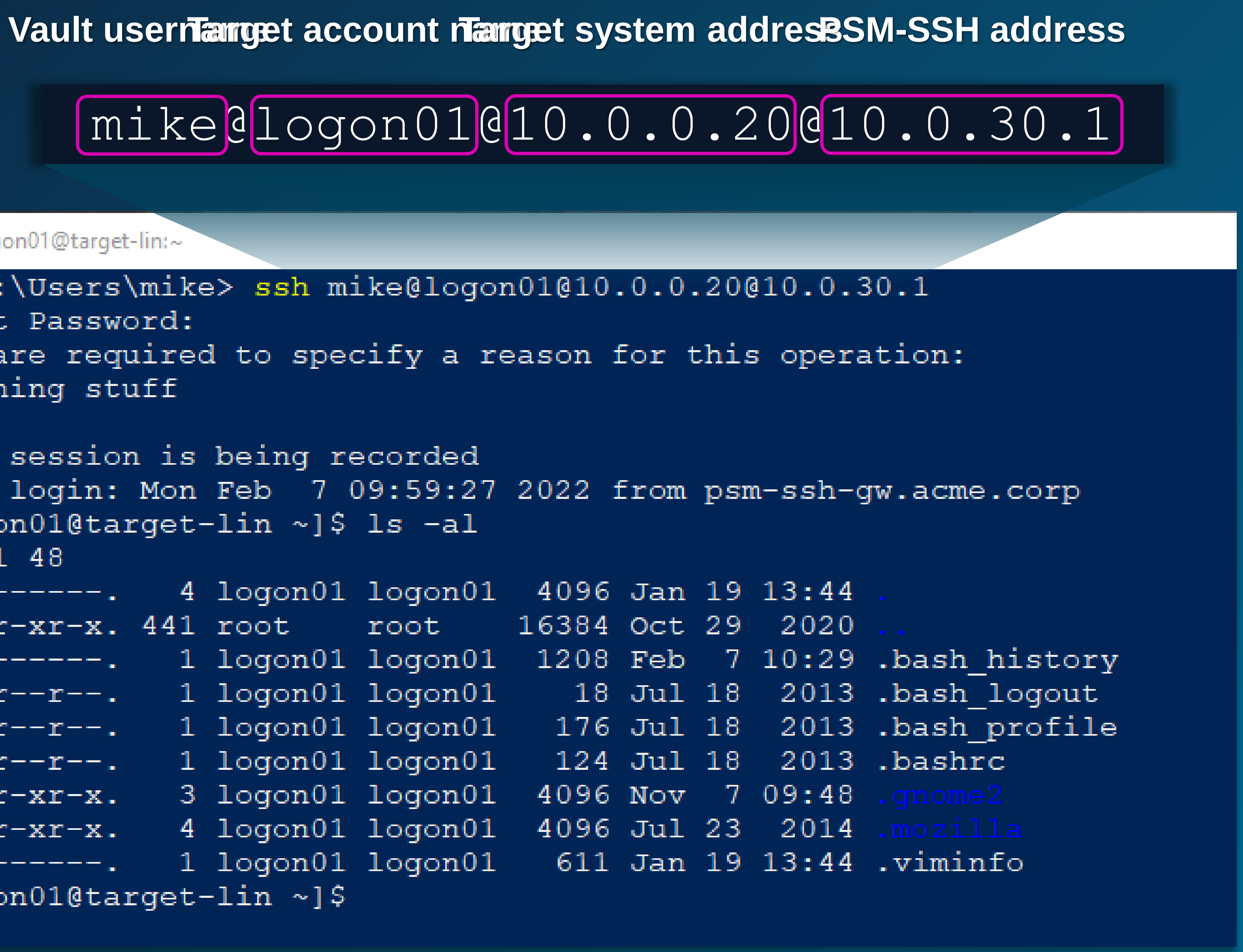
PSM for SSH

PSM for SSH: Overview

- The average enterprise manages hundreds of Unix servers and network devices
- Systems are usually critical, but access to them is uncontrolled
- Network and Unix teams are reluctant to change their existing workflows and tool sets
- PSM for SSH (previously PSM SSH Proxy or PSMP) is designed to provide a native Unix/Linux user experience when connecting to any SSH target system

PSM for SSH
Client Settings

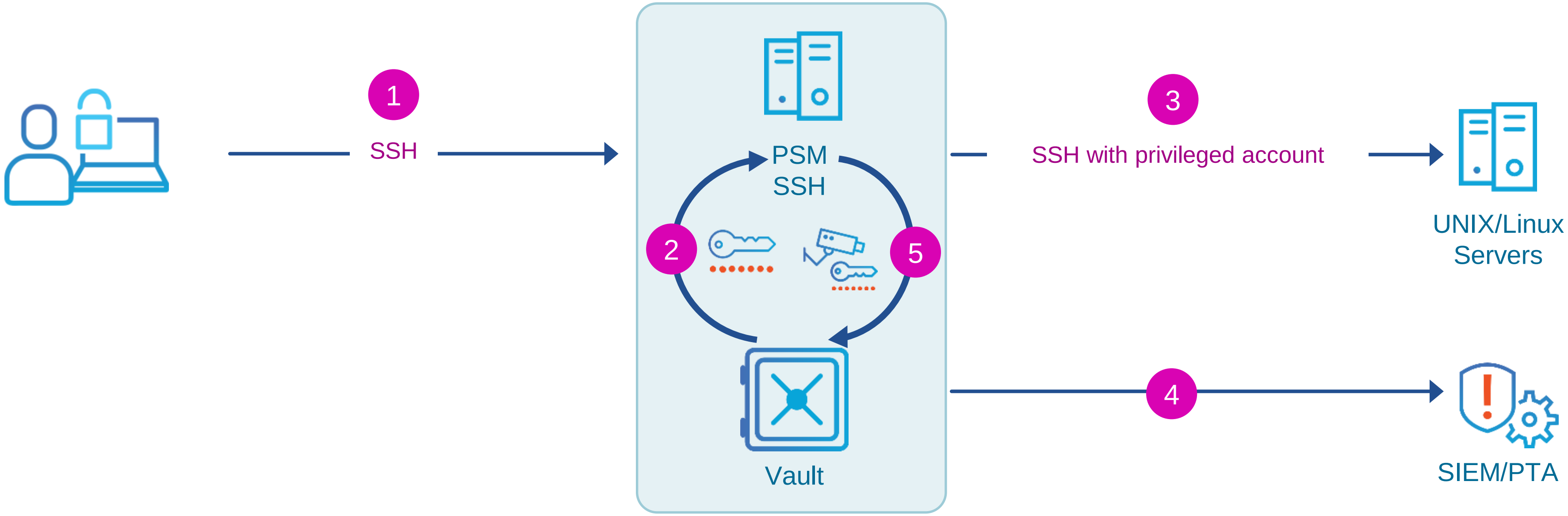
- The connection settings for **PSM for SSH** resemble those of **PSM for Windows**.
- Connections are not launched via the **PVWA**, but through a special connection string.



```
PS C:\Users\mike> ssh mike@logon01@10.0.0.20@10.0.30.1
Vault Password:
You are required to specify a reason for this operation:
training stuff

This session is being recorded
Last login: Mon Feb  7 09:59:27 2022 from psm-ssh-gw.acme.corp
[logon01@target-lin ~]$ ls -al
total 48
drwx------.   4 logon01 logon01  4096 Jan 19 13:44 .
drwxr-xr-x. 441 root    root    16384 Oct 29  2020 ..
-rw-------.   1 logon01 logon01  1208 Feb  7 10:29 .bash_history
-rw-r--r--.   1 logon01 logon01    18 Jul 18  2013 .bash_logout
-rw-r--r--.   1 logon01 logon01   176 Jul 18  2013 .bash_profile
-rw-r--r--.   1 logon01 logon01   124 Jul 18  2013 .bashrc
drwxr-xr-x.   3 logon01 logon01  4096 Nov  7 09:48 .gnome2
drwxr-xr-x.   4 logon01 logon01  4096 Jul 23  2014 .mozilla
-rw-------.   1 logon01 logon01   611 Jan 19 13:44 .viminfo
[logon01@target-lin ~]$
```

PSM for SSH: Flow



1. User opens SSH session to the PSM server
2. PSM retrieves privileged account password from the vault
3. Open SSH session to the target using the privileged account
4. Logs forwarded to SIEM and PTA
5. Store SSH session audit

Summary

Summary

In this session we covered the main PSM features, as well as how to enable and use:

- Privileged Session Manager (PSM)
  - PSM Connection Components
  - PSM Ad-Hoc Connections
  - PSM via HTML5 Gateway
  - PSM for Windows
- PSM for SSH

Additional Resources

HTML5 Based Remote Access

https://training.cyberark.com/elearning/html5-based-remote-access

Note: You must be logged into the CyberArk training portal to access this material

You may now complete the following exercises:

Privileged Session Management – Part 1

- Remove Privileged Access Workflows Exceptions
- Disabling the PSM Globally

- Privileged Session Manager
  - Adding Exceptions
  - Connect with a Linux Account
  - Connect with an Oracle Account
  - Connect via HTML5 Gateway
  - Connect using PSM Ad-Hoc Connection
- Privileged Session Manager for Windows
  - Connect using RDP file without providing the target system details
  - Connect using RDP file with the target system details
- Privileged Session Manager for SSH

CYBERARK®