



# 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:

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

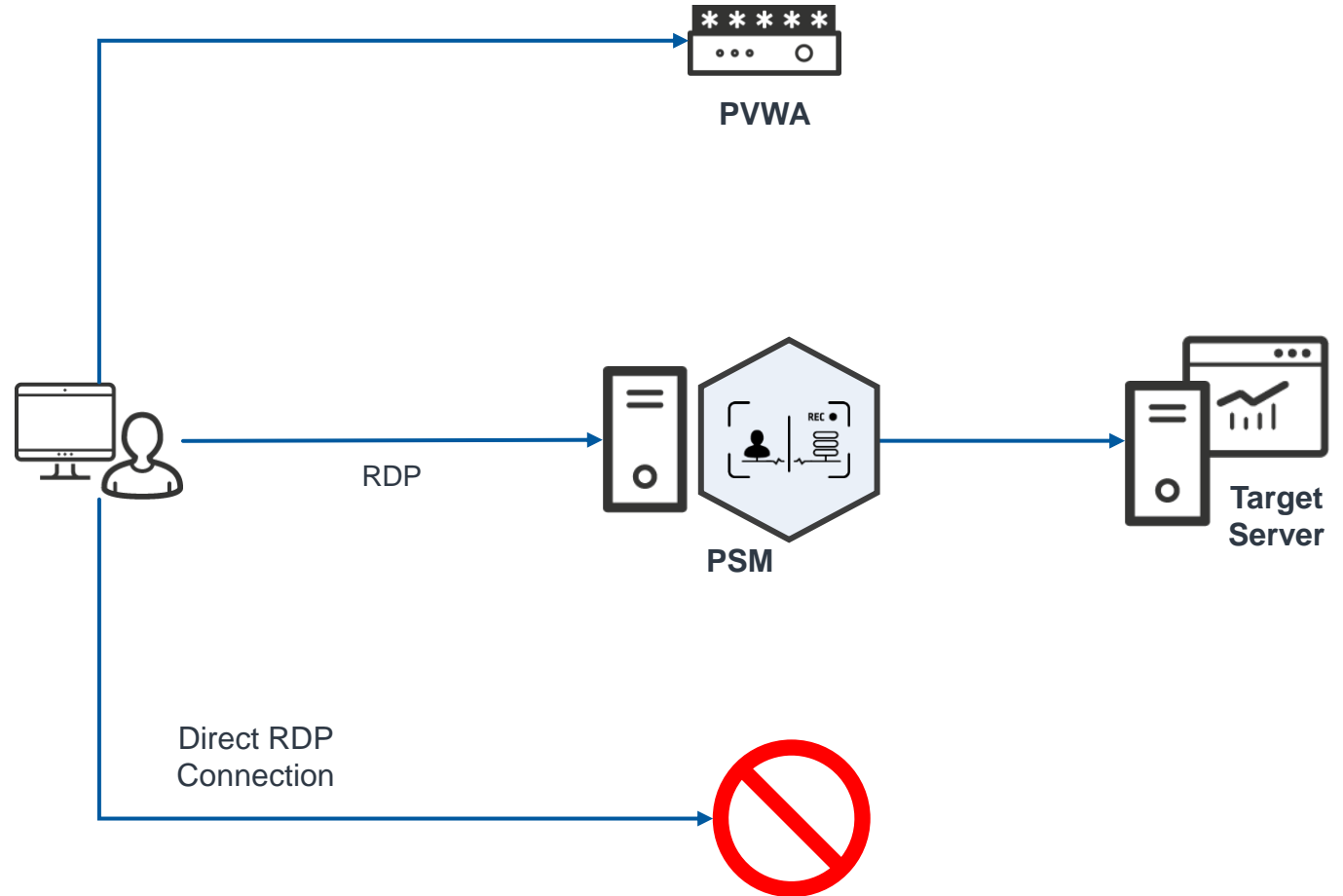
# Privileged Session Manager



# The Privileged Session Manager

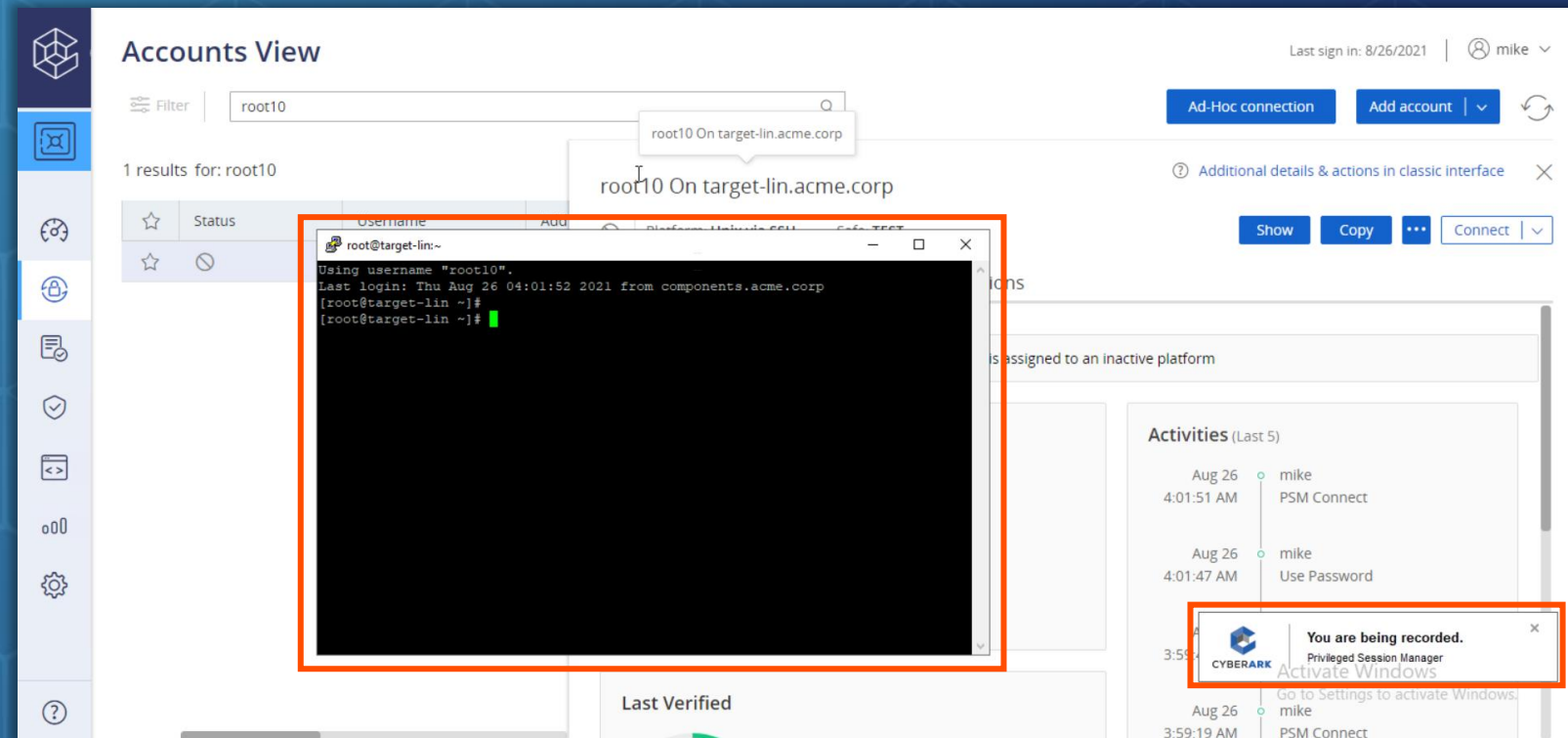
When we talk about **PSM**, the **Privileged Session Manager**, we are usually referring to the **PSM** installed on a Windows server.

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



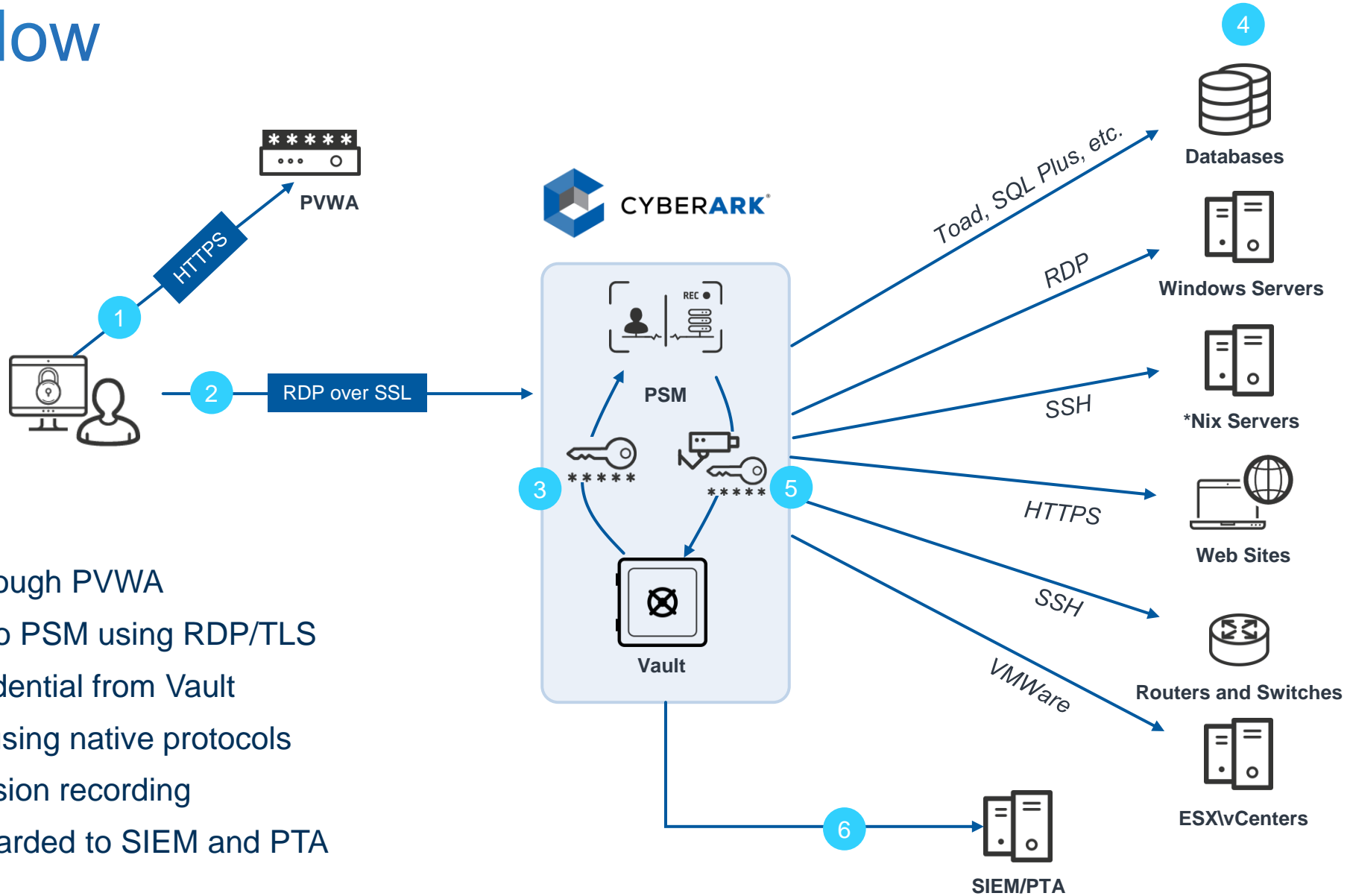
# The Privileged Session Manager

- 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





# PSM Flow




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





# Enable PSM: Master Policy





POLICIES


Master Policy


Policy by Platform


Access Control (Safes)




















Policies > Master Policy

Master Policy

▼ Privileged Access Workflows

Policy Rule	Value	Exceptions
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	-

8/26/2021 | mike

review

roduction to Policy Management

Master Policy allows you to easily define a corporate level policy that reflects the business goals and guidelines for managing privileged accounts and sessions across your entire organization.

Using policy exceptions, 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.

Activate Windows  
Go to Settings to activate Windows.

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



# Enable PSM: Platform

Platform Management

Filter

Search for target account platforms

Targets

Dependents

Groups

Rotational Groups

42 results

Platform Name	Verify password	Periodic	Manual	Periodic	Manual	Automatic	Manual	Access workflow policies	PSM Server		
Windows (9)											
*NIX (4)											
LIN KEYS 90	7 days	✓	90 days	✓	-	✓	Approval	Provide Reason	Check in/out	OTP	PSM Server on COMPONENTS
LIN SSH 30	7 days	✓	30 days	✓	-	✓	Approval	Provide Reason	Check in/out	OTP	PSM Server on COMPONENTS
Unix via SSH	-	✓	-	✓	-	✓	Approval	Provide Reason	Check in/out	OTP	PSM Server on COMPONENTS
Unix via SSH Keys	-	✓	-	✓	-	✓	Approval	Provide Reason	Check in/out	OTP	PSM Server on COMPONENTS

Apply

OK

Cancel

LIN SSH 30

Search...

Go

Target Account Platform

UI & Workflows

Properties

Linked Accounts

Properties

Name	Value
ID	PSMServer
SubnetPolicy	No
SessionRecorderSafe	PSMRecordings
SessionRecorderSafeRetention	180
MaxSessionDuration	-1
ShowRecordedSessionNotification	Yes

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



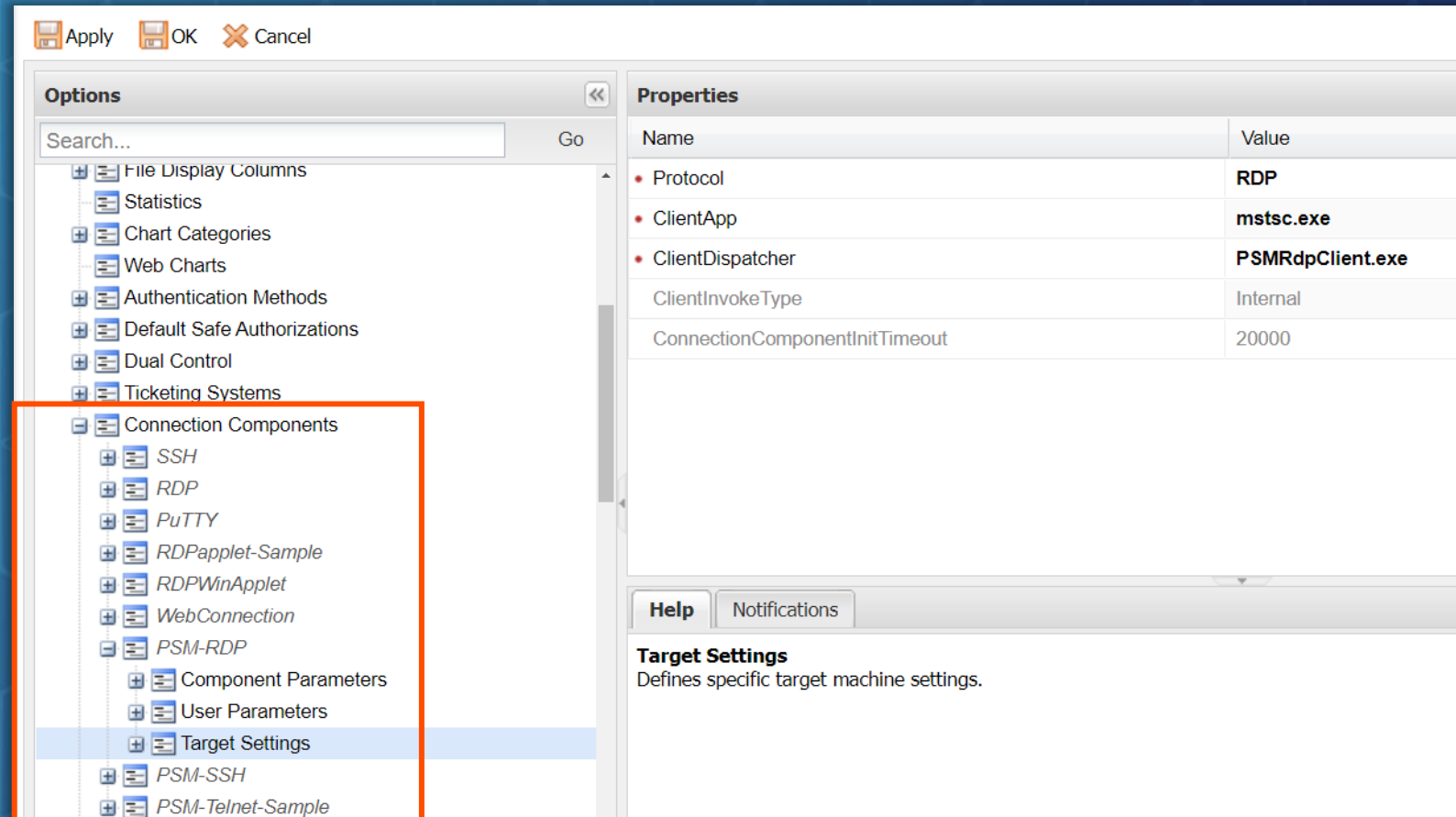
# PSM Connection Components





# Connection Components/ Connectors

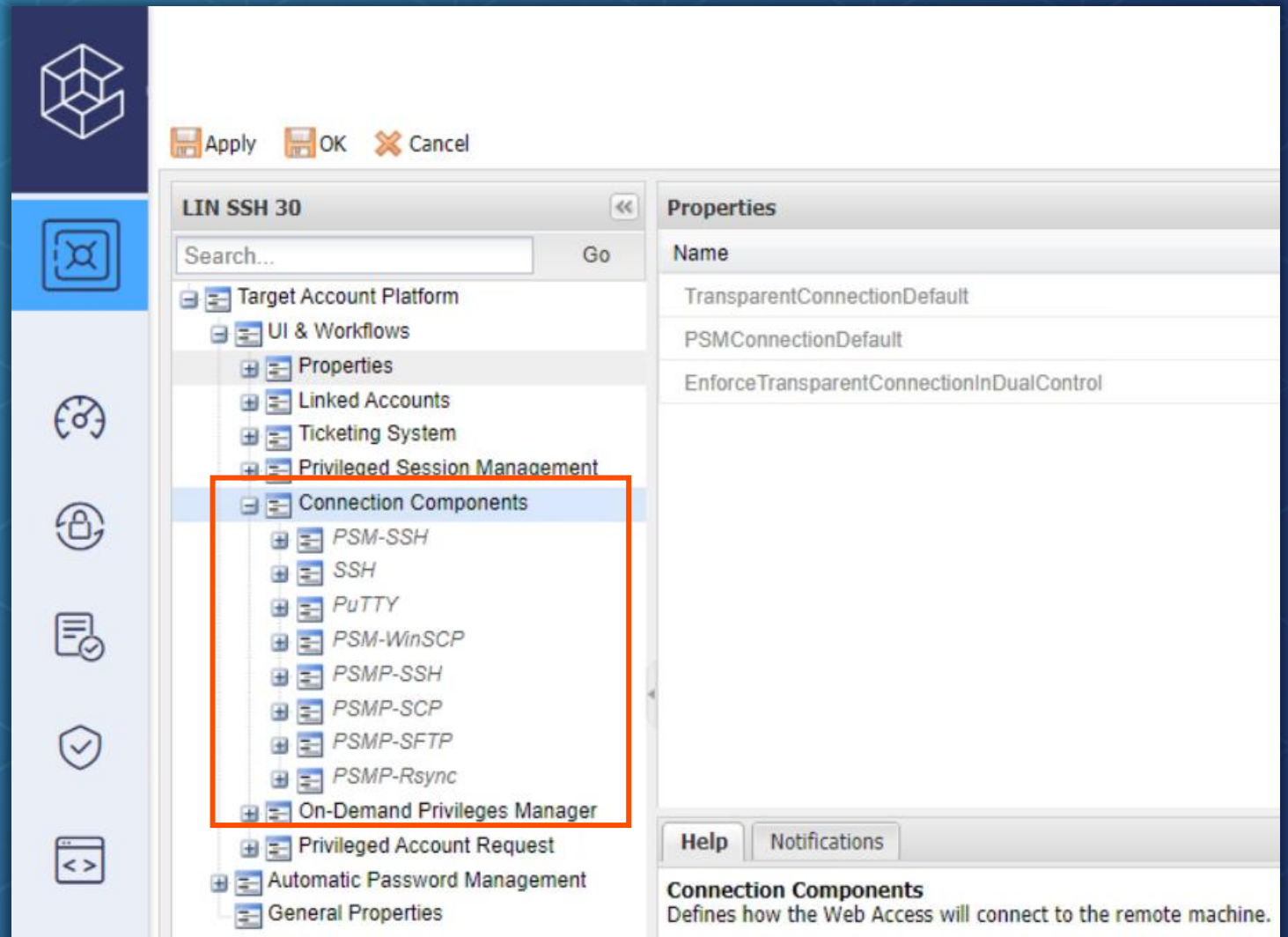
- There are many connection components available out of the box
- Additional connection components can be found in the **CyberArk Marketplace**
- Organizations can also build and add custom connection components to the **PAM** solution





# 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



# 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

The screenshot displays the 'Platform Management' interface. At the top, there's a search bar for 'target account platforms' and buttons for 'Marketplace' and 'Import platform'. Below this, a tabbed interface shows 'Targets', 'Dependents', 'Groups', and 'Rotational Groups'. A table lists 42 results with columns for 'Platform Name', 'Verify password', 'Change password', 'Reconcile password', and 'Access workflow poli...'. A context menu is open over the table, showing options: 'Edit', 'Manage PSM connectors', 'Duplicate', 'Delete', 'Deactivate', and 'Export'. The 'Manage PSM connectors' dialog box is prominently displayed in the foreground. It features a search bar, a 'Show only selected connectors (7)' toggle, and a grid of connector packages: PSM-WinSCP, PSMP-SCP, PSMP-SSH, PSM-SSH, PSMP-Rsync, PSMP-SFTP, and SSH. At the bottom of the dialog, it says 'Find more connectors in the CyberArk Marketplace' and has 'Cancel' and 'Save' buttons.

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...
Windows (9)	Perio... Manual	Perio... Manual	Automatic Manual	

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](#)

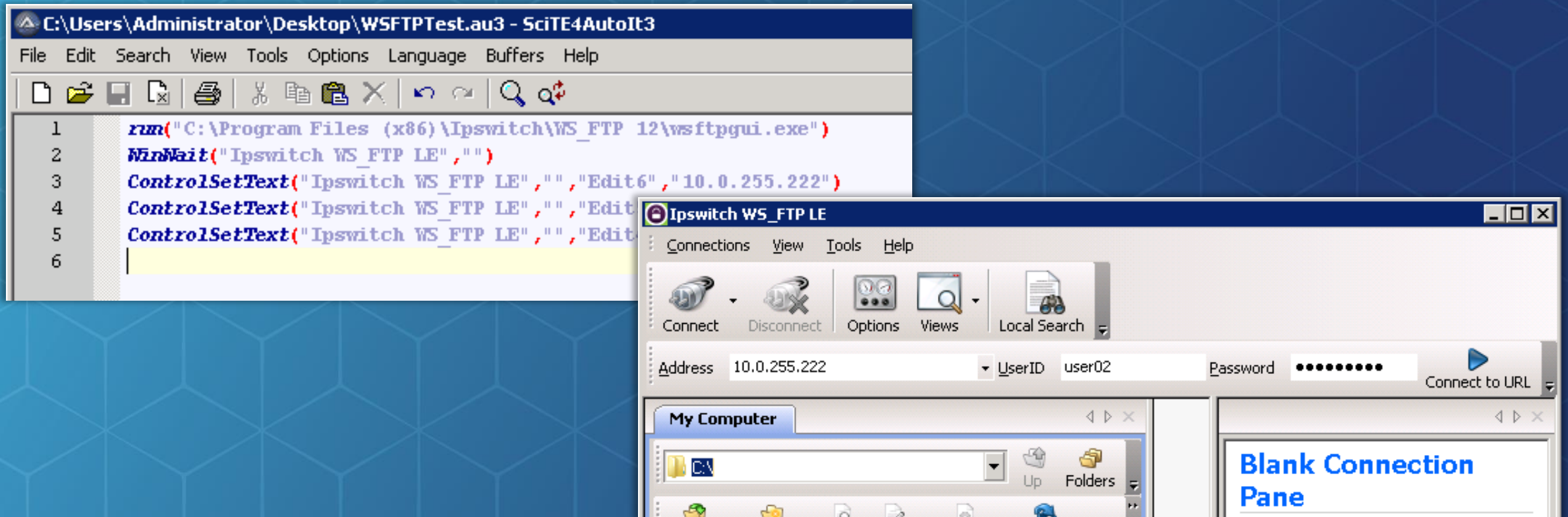
Cancel Save





# Universal Connector

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



# 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

Filter | Search for accounts

**Ad-Hoc connection** Add account

33 results for: All accounts

Additional details & actions in classic interface

☆	Status	Username	Address	Platform ID	Safe ↑	Access	
☆	⚡	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.

The screenshot displays the CyberArk Platform Management interface. The left sidebar shows the navigation menu with 'Platform Management' selected. The main content area is titled 'Administration > Platform Management' and 'Platform Management'. It features a table of 'Target Account Platforms' and 'Service Account Platforms'. The 'PSM Secure Connect' platform is highlighted with a red box, showing its status as 'Active'. The right sidebar shows the 'Platform Preview' for 'PSM Secure Connect', with fields for NAME, DESCRIPTION, and STATUS (Active).

Name	Device Type	Status
Business Website	Website	Active
CyberArk PTA	Application	Active
Generic Web App	Website	Active
LIN KEYS 90	Operating System	Active
LIN SSH 30	Operating System	Active
OPA DBA 30	Database	Active
<b>PSM Secure Connect</b>	<b>PSM Secure Connect</b>	<b>Active</b>
WIN DOM ADMIN 10	Operating System	Active



# 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.

The screenshot shows the CyberArk interface. At the top right, it says "Last sign in: 8/26/2021" and "mike". Below this, there is a search bar and a button labeled "Ad-Hoc connection" which is highlighted with a red box. To the right of this button is another button labeled "Add account" with a dropdown arrow. Below the "Ad-Hoc connection" button, there is a link that says "? Additional details & actions in classic interface". A callout box points to the "Ad-Hoc connection" dialog, which contains the following fields:

- Client: PSMSecureConnect (dropdown)
- Client: WinSCP (dropdown)
- Address: 10.0.0.20 (text input)
- Username: root01 (text input)
- Password: (masked text input)

At the bottom of the dialog are "Cancel" and "Connect" buttons.

# HTML5 Gateway





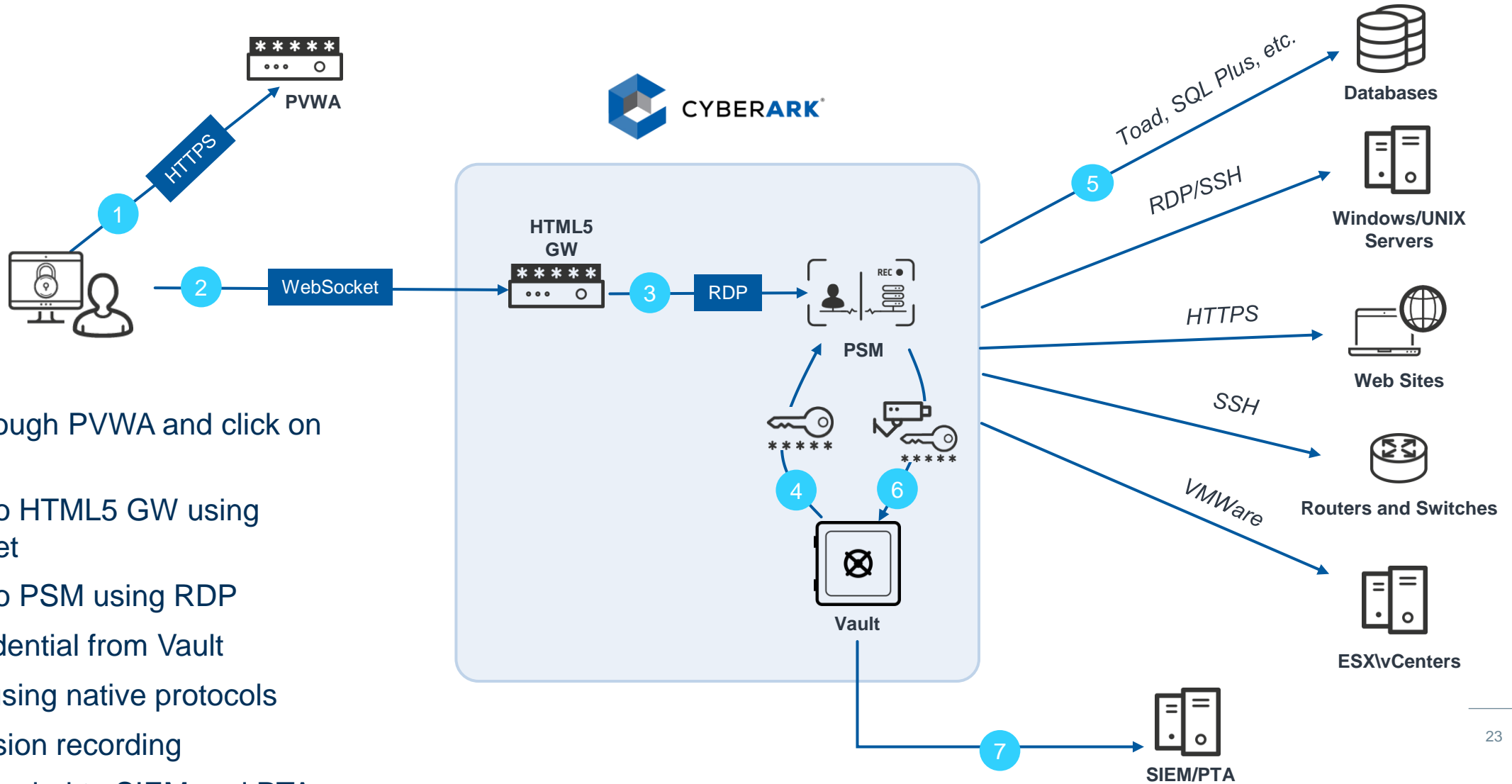
# HTML5 Gateway: Overview

- ▶ Many organizations simply 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.



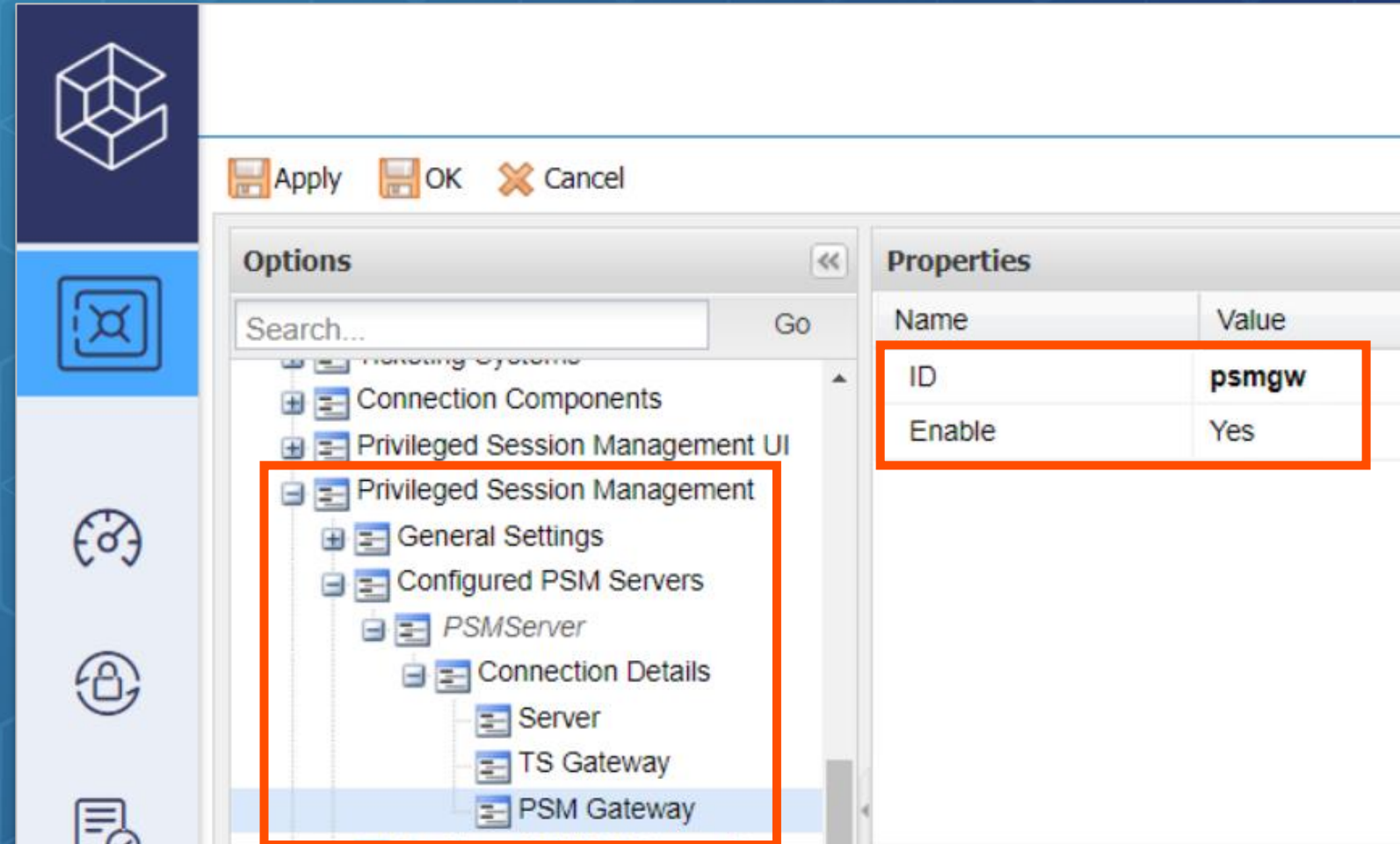


# HTML5 Gateway: Flow



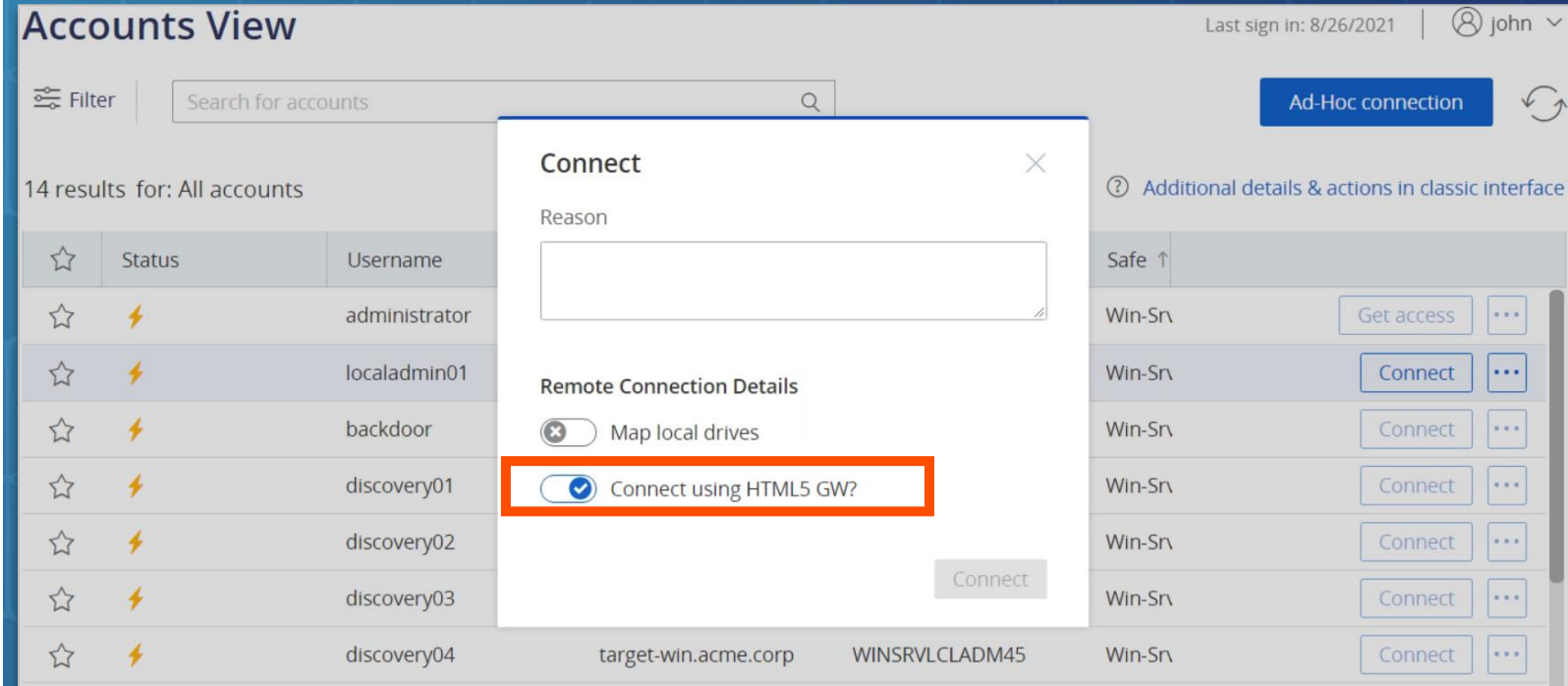
# Enable HTML5 Gateway

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



# Use HTML5-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

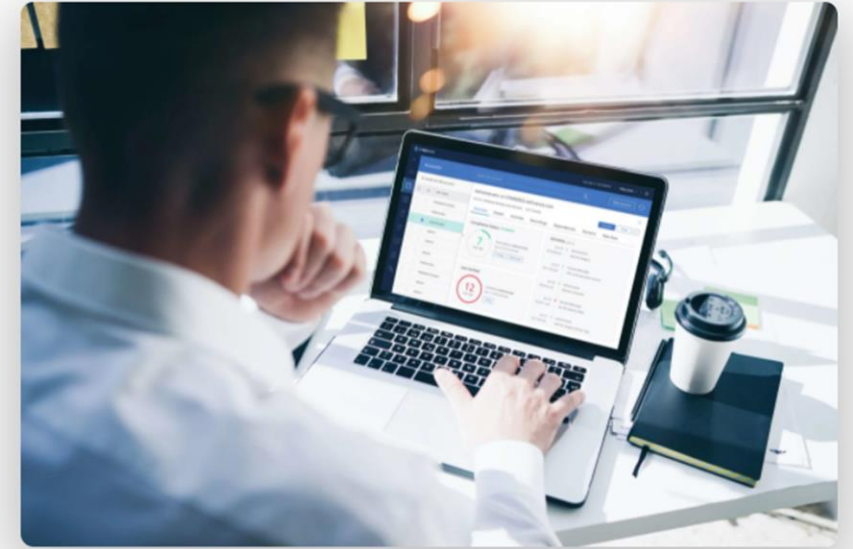


# PSM for Windows



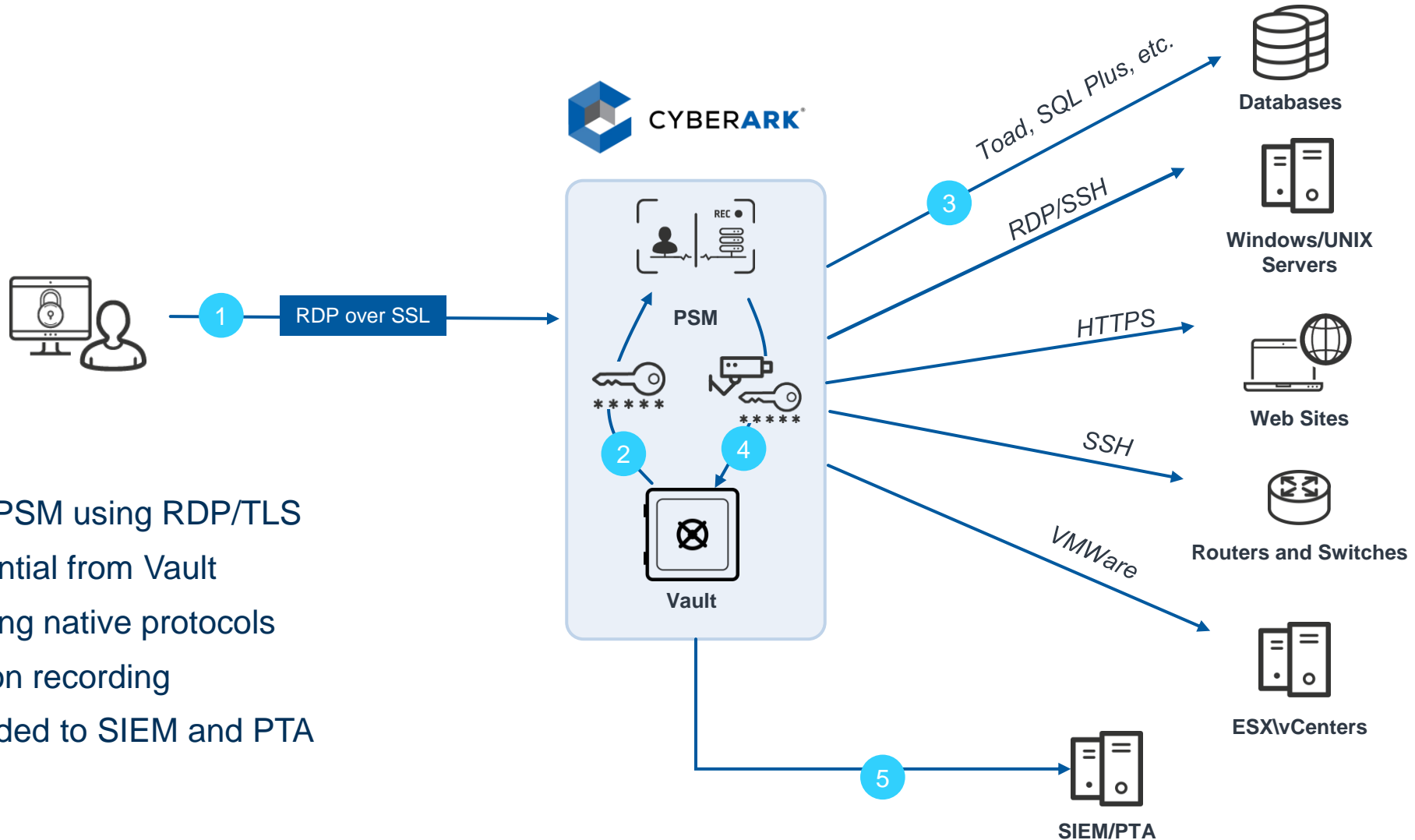
# PSM for Windows: Overview

- 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.



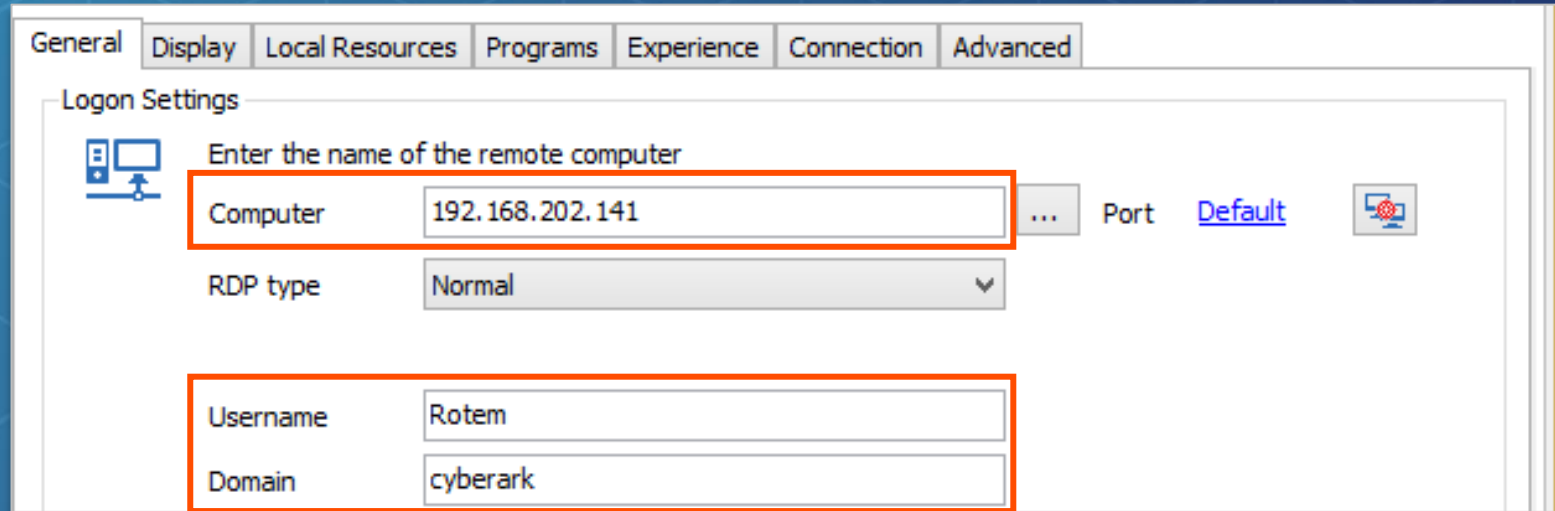
# PSM for Windows: Flow

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



# RDP Client Settings

- PSM IP
- Vault user
- Privileged Account name and address
- Connection Component



General | Display | Local Resources | Programs | Experience | Connection | Advanced

Logon Settings

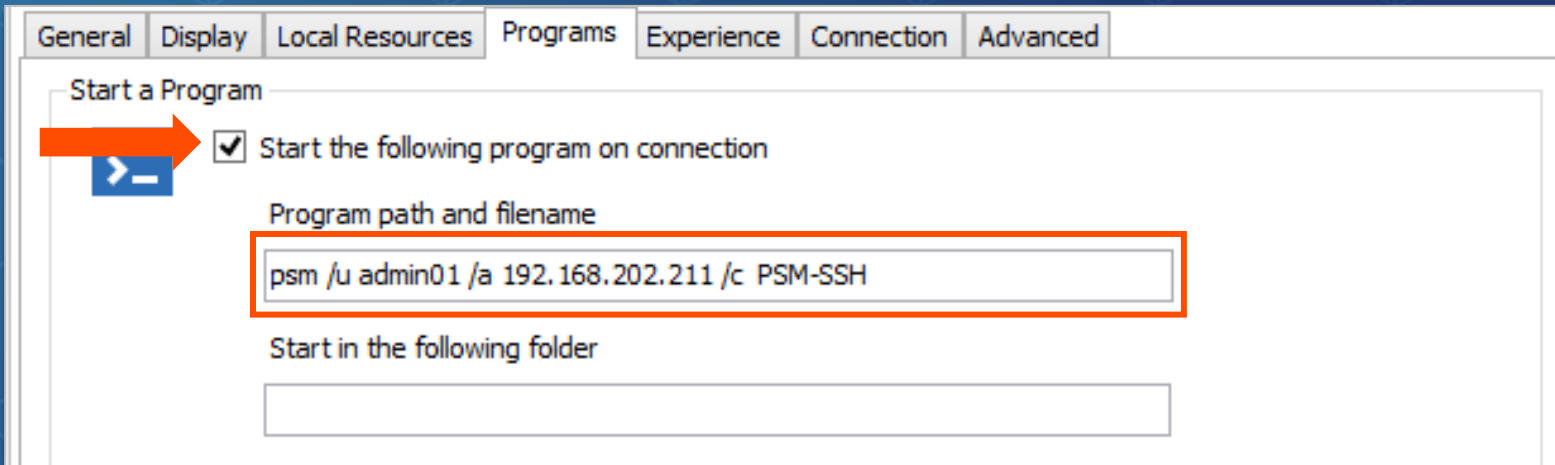
Enter the name of the remote computer

Computer: 192.168.202.141 ... Port: [Default](#)

RDP type: Normal

Username: Rotem

Domain: cyberark



General | Display | Local Resources | Programs | Experience | Connection | Advanced

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
gatewaybrokerintype: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 Address

Target system details

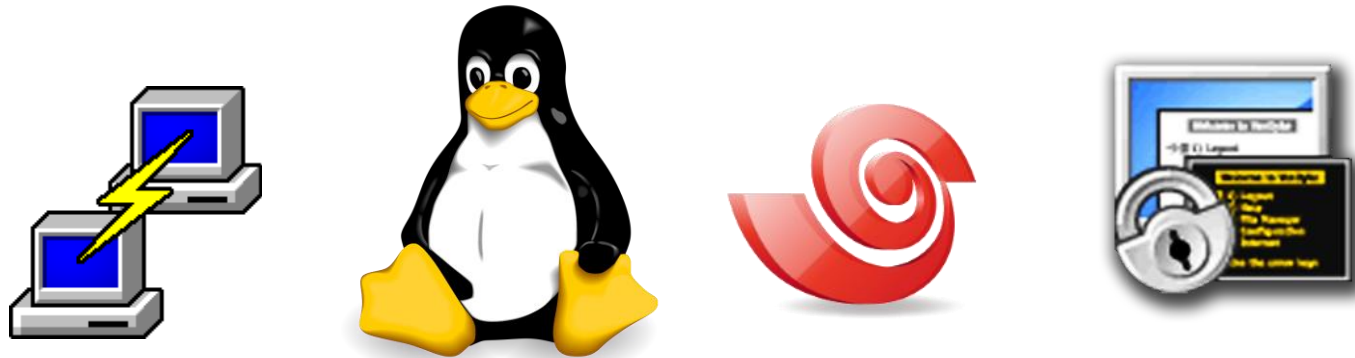


# PSM for SSH



# 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.

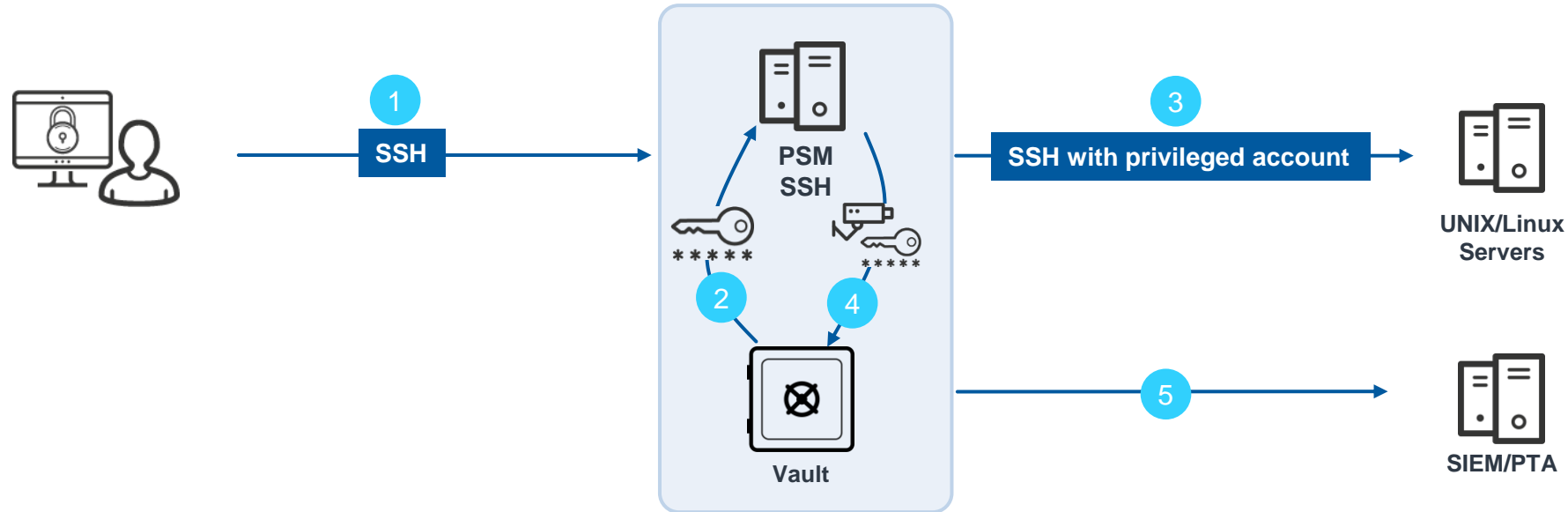
Vault user Target account Target system address PSM-SSH address

mike@logon01@10.0.0.20@10.0.30.1

```
logon01@target-lin:~  
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. Store SSH session audit
5. Logs forwarded to SIEM and PTA





# 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 that 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

