PRIVILEGE SESSION MANAGER

PSM INTEGRATION - TECHNICAL DOCUMENTATION

Devolutions

http://devolutions.net

Remote Desktop Manager

2019.1

August 1st, 2020

PARTNER SOLUTION OVERVIEW

Remote Desktop Manager (RDM) is a solution designed to store and securely share details of connections, credentials, VPNs, etc. It integrates with 160+ technologies/protocols and becomes the single pane of glass that IT personnel uses to perform maintenance tasks, monitor system health, but most importantly, control access to remote devices in a secure fashion.

KEY BENEFITS

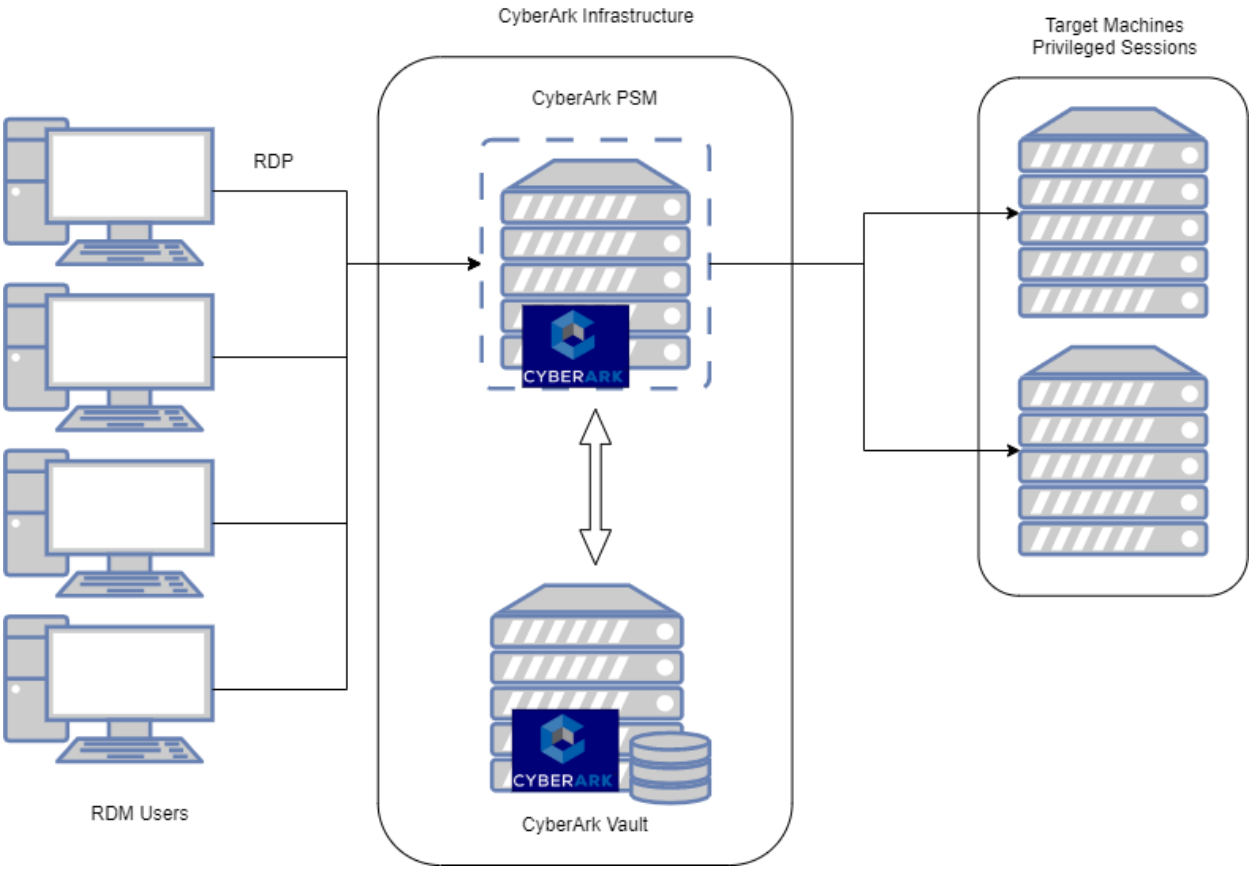
Remote Desktop Manager enables a workflow where the IT technician simply searches for a system that needs to be worked on, then launches a connection towards it. If needed, a VPN client is launched automatically and finally the chosen protocol is launched. Most of the times the credentials are provided automatically, but what is key is that the end user doesn't even need to be made aware of the credentials and, as such, they are not exposed. A strong security system is in place to grant permissions in a flexible fashion, there is also extensive logging of user activity and full versioning of all changes.

Remote Desktop Manager integrates with multiple solutions in the Remote Session space and supporting CyberArk provides tremendous value to both CyberArk's and Devolutions' customer base.

Following that thought, Remote Desktop Manager can connect to a PSM Server in order to connect a privilege session as endpoint.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

Devolutions customers can elect to store their information in multiple back-ends: on premise RDBMS, cloud services, simple files, etc. The storage system used by our application is therefore omitted from this diagram. To ease deployment of the solution, the strategy has been to use CyberArk's Privilege Session Manager. For the current customers in the pipeline, a single application server will be sufficient, but the integration would support multiple servers if need be.



The definition of what is called a CyberArk PSM Server / Connection is stored in RDM. It contains the details of what us ultimately a call to the PSM Server using an Alternate Shell. No information regarding Privileged account credentials are cached by RDM. This also implies that the user's credentials to connect to CyberArk must be LDAP, and both the connection to CyberArk Vault (PVWA) and the PSM server use and are the same.

In no case RDM will use the service account defined for PVWA to authenticate on the PSM Server.

This implementation can support most

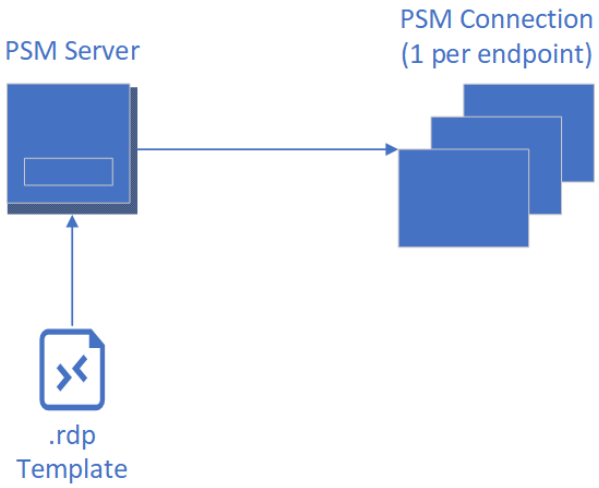
PSM INSTALLATION

Refer to PSM Manual Installation for CyberArk Privileged Session Manager Installation

Since our integration cannot use the PSM Windows Account to login the PSM Server, CyberArk Users must be LDAP integrated and granted the permission to logon the PSM Server. The Endpoint Privileged Account is then used to logon the endpoint.
This also means that the LDAP Account used on the PSM Server connection must be granted sufficient permissions to access the privileged account to connect to the endpoint.

PSM CONFIGURATION

Essentially, RDM generates a PSM connection that conforms to Privileged Single Sign-on (as per https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.1/en/Content/PASIMP/PSSO-ConfigureRDPStart.htm), but does this in a more intuitive fashion when considering not only the privileged accounts, but also the endpoints that you want to reach.



In RDM's endpoint centric design, we have elected to create two session types

- CyberArk PSM Server
- CyberArk PSM Connection

The CyberArk PSM Server is a specialized entry that represents a single PSM server or a PSM Gateway. Since the initial connection can only use an RDP connection, rather then replicate the hundreds of settings that exist for that type, we've simplified the workflow by using a RDM template that allows you the full flexibility of the RDP protocol. The PSM Server type is always simple, from common scenarios in a secure environment, to advanced network topologies where an RDS Gateway and/or a VPN connection are in play.

As for the PSM Connection entry, it is linked to a PSM Server, but holds only the information used to launch to the endpoint: Host, Privileged Account, PSM Component. It can really be corroborated to the PSM command line used for the alternate shell.

IMPACT ON CYBERARK PSM OR OTHER COMPONENTS

This will not prevent CyberArk to record a session or monitor any action on the endpoint or the server

DEVOLUTIONS RDM INSTALLATION & INTEGRATION CONFIGURATION

Prerequisites

Create an RDP template that will reflect your requirements for reaching the PSM Server. For most of the audience, it will most likely be a plain RDP template.

If you must use an RDS Gateway, a VPN, adapt network routes, etc. this would be where you would apply these settings. Please refer to https://help.remotedesktopmanager.com/commands_creatingtemplates.html for full details on the templates.

Since you need one template per PSM Server, it makes sense to name the template in a manner that clearly indicates the server, in our sample V-WINDPSM1

A note on credentials

The PSM ecosystem identifies the user by an exact match in its user list. Your LDAP directory matching may be configured to create the user simply with the **SAMAccountName**, or with the full **UPN**. The user account used for the connecting to the PSM Server must be typed **exactly** as you see in the vault user list. As far as locating the privileged account used to connect to the endpoint, the CyberArk documentation is a better source of information on the topic.

In our tests, we have also hit an issue when the user's device was not on the same domain as the PSM Server. By default, RDP connections enforce Network Level Authentication (NLA) and this prevents authentication from working. The regretful aspect of this is that Windows simply states that the credentials are wrong. The fix is simply to disable NLA in the RDP template used for the PSM Server.

August 2020 update for RDM 2020.2.18

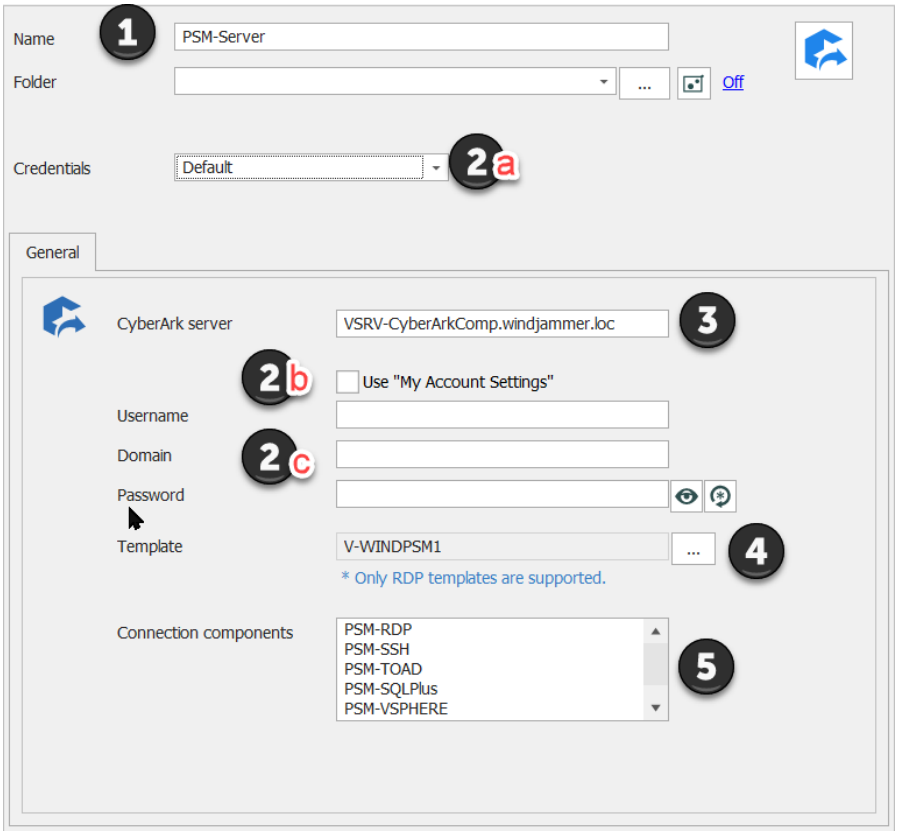
Although RDM offers multiple ways to store and share credentials, some of these options become undesirable when using a Vault such a CyberArk. With the greatly improved AAM integration that was released in RDM 2020.2.18, RDM can be transformed to be **Password Less**, going as far as enabling a RDM policy to prevent any passwords from being saved.

This new AAM integration in fact uses a Client Authentication Certificate to access the CCP, which then returns a privileged user which can be used to launch PSM connection, connect to the PVWA, etc.

Depending on your organization's security posture, using this new pattern could be a huge step forward in controlling privileged access by any user.

Configuration of the CyberArk PSM Server entry

The CyberArk PSM Server entry type will be the PSM Host.

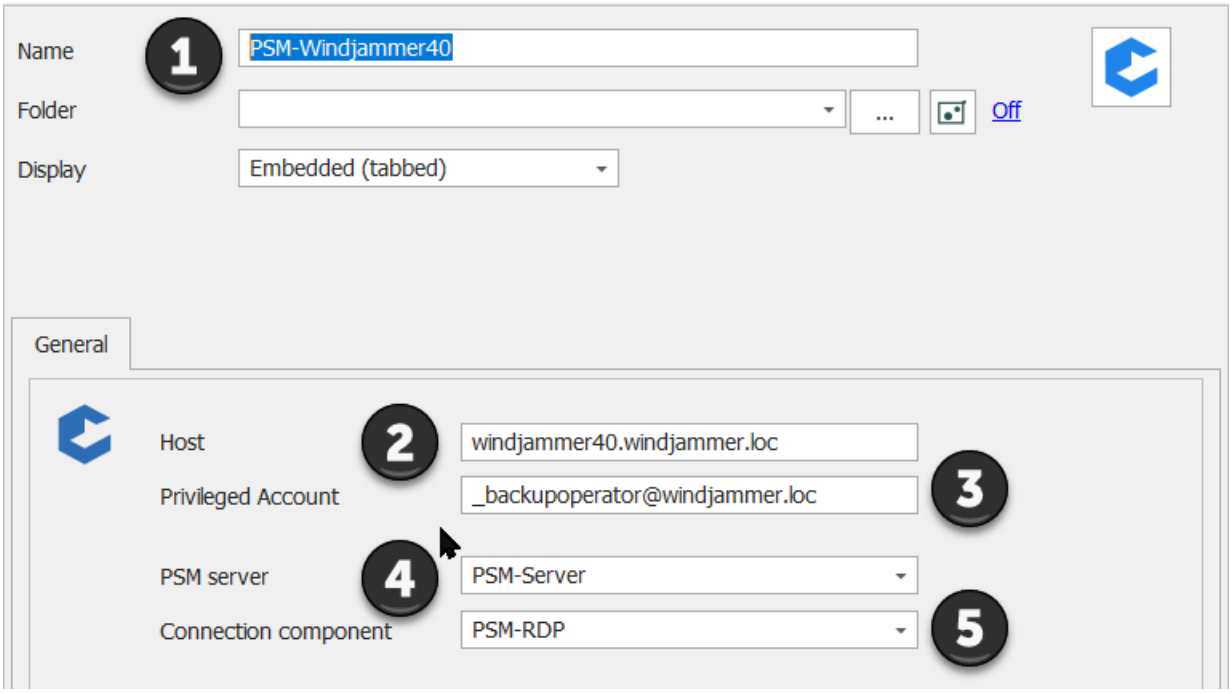


1. Name of the Entry (Label)
2. Username / Domain / Password for the PSM Initial Connection and CyberArk Vault.
    a. With RDM 2020.2.18 and up, an AAM entry can be used for the greatest security
    b. *My Accounts Settings* refer to RDM: File -> My Account Settings -> CyberArk PSM Server. This case is when the user has a personal account to access the PSM/PVWA.
    c. use a shared account. Note that entry level security in RDM will not allow users to learn these credentials. You can create multiple entries and use RDM's Role Based Access Control to limit permissions.
3. PSM Host Server address (IP or Hostname)
4. Template… An RDM template as described above in the prerequisites section.
5. Connection components: this list are the default components available to a default installation of a PSM. Please adapt to removed unwanted ones, as well to reflect name changes in your environment. This list is available in the PSM Connection entry when you have linked it to a PSM Server entry.

Configuration of the CyberArk PSM Connection entry

The CyberArk PSM Connection entry is the connection to the target endpoint

The PSM Connection will be using the PSM Server created above.



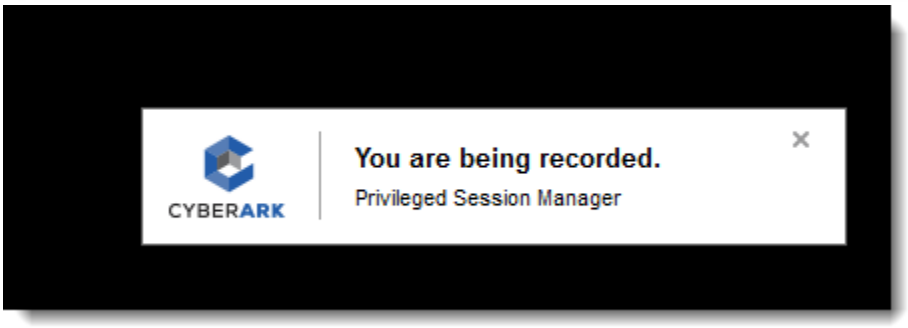
1. Name of the Entry (Label)
2. Hostname or IP address of the endpoint
3. Privileged Account to use (**Username** field in CyberArk PVWA)
4. PSM Server: dropdown that lists all PSM Server entries in RDM. Select the entry created above
5. Connection Component is the type of connection / protocol to open. It shows only the components as present in the PSM Server entry.

Launching the session

The session (CyberArk PSM Connection) can then be launched from RDM.

Some or all the following images should be seen depending on your PSM ecosystem.


CYBERARK
Please wait for the Local Session Manager


CYBERARK
You are being recorded.
Privileged Session Manager

PARTNER CONTACT INFORMATION

Business Contact	Name	Maurice Côté
	Email	mcote@devolutions.net
	Tel	514-360-3686
Technical Contact	Name	Maurice Côté
	Email	mcote@devolutions.net
	Tel	514-360-3686
Support Contact	Name	Support Team
	Email	ticket@devolutions.net
	Tel	844-463-0419