



CyberArk Webservices SDK Integration

Devolutions Remote Desktop Manager Integration Guide

Devolutions

<http://devolutions.net>

Remote Desktop Manager

2019.2.18

August 25th, 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.

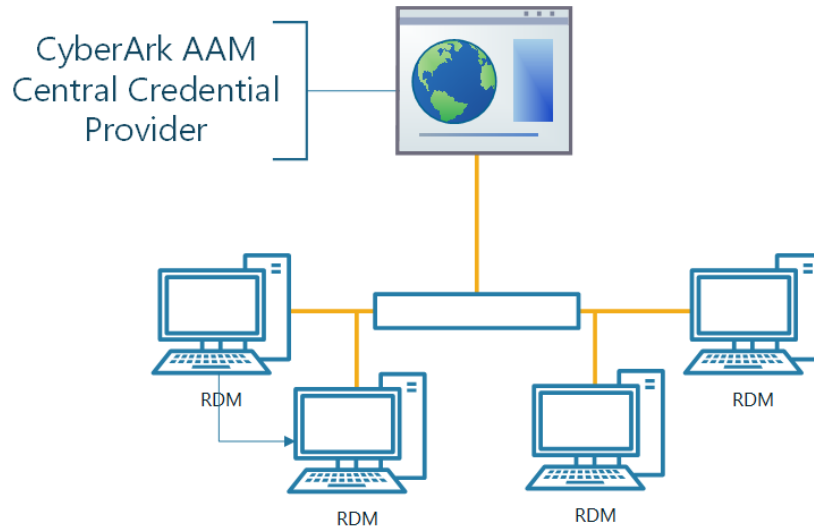
KEY BENEFITS

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 does not 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 Credential Management space and supporting CyberArk provides tremendous value to both CyberArk's and Devolutions' customer base.

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 Central Credential Provider. 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 Credential Entry is stored in RDM. It contains the details of what is ultimately a query against the CCP. The passwords are never cached by RDM. Since one of its key features is the possibility of launching many technologies (Remote Access, VPNs, Web Portals) and performing the authentication **without** user interaction, most users would not even be aware of the origin of the credentials. They would launch an RDP or SSH session, and the credentials will be obtained *Just in Time* and submitted automatically.

One key aspect of our integration is that the user can in fact be prompted to select from a list of accounts that match the keywords specified in the entry. There is also some level of flexibility in specifying which of the Vault's fields to use for domain matching. Indeed, some customers have their own preference and do not always use the *Address* field.

Our **Dynamic link model** allows the user to pick from **ANY** account he has access to to establish the connection.

This current implementation of this integration is only in our Windows Edition. Also note that an RDM license SITE or higher is required for the CyberArk integrations to be available.

DEVOLUTIONS RDM INSTALLATION

Refer to <https://help.remotedesktopmanager.com> for detailed instructions on Remote Desktop Manager's installation.

SPECIFYING THE CREDENTIALS USED TO ACCESS THE VAULT

Although RDM offers multiple ways to store and share credentials, some of these options become undesirable when using a Vault such as CyberArk. In a coming release, the full capability of the AAM will be used to essentially go Password Less. In the current release, you have two supported models.

1. Each user has unique credentials for the PVWA
 - a. They know their credentials: Instruct each user to use *My Accounts Settings (File -> My Account Settings -> CyberArk)* to fill their credentials once.
 - b. The admin manages the user credentials: The admin creates the CyberArk entry himself but uses RDM's role base access control (RBAC) to only allow this specific user to access it.
2. Users have shared account: The admin creates the CyberArk entry and uses RDM's RBAC to grant permissions as required.

Note that the credentials used to access the PVWA must be typed the same way as the user account appears in the vault user list.

INTEGRATION CONFIGURATION – Static account link

In this scenario, you will indicate a specific keyword to search within the safe that accessible to the user.

For using the integration, in RDM, create a new entry of the **CyberArk** type.

Name	Username	Address
_backupoperator@windjammer.loc	_backupoperator	windjammer.loc
_financialsmgr@windjammer.loc	_financialsmgr@windjammm...	windjammer.loc

1. Give the entry a meaningful name
2. Specify the URL of the CyberArk Central Credential Provider.
3. Enter the web application name, typically **PasswordVault**
4. The version is for the REST API version to use. V9 is deprecated and should not be used.
5. Specify the authentication mode used to access the vault.
6. As seen above, either use “My Account Settings” or type credentials.
7. Type in the object name as reported in the Vault account details. The ellipsis button allows the user to choose the account using an easy to use form.

Name	Username	Address
_backupoperator@windjammer.loc	_backupoperator	windjammer.loc
_financialsmgr@windjammer.loc	_financialsmgr@windjammm...	windjammer.loc

INTEGRATION CONFIGURATION – Dynamic account link

In this scenario, you will be prompted for which account to get from the vault. This Just-In-Time, but most importantly, this only requires a single CyberArk entry that becomes a bridge to your vault. It's a great time saver and limits administrator's implication drastically.

For using the integration, in RDM, create a new entry of the **CyberArk** type.

The screenshot displays the configuration form for a CyberArk integration. The 'Name' field is set to 'CyberArk Dynamic' (1). The 'Web services URL' is 'https://vsrv-cyberarkcomp.windjammer.loc' (2). The 'Virtual directory' is 'PasswordVault' (3). The 'Version' is 'V10' (4). The 'Authentication mode' is 'LDAP' (5). The 'Use "My Account Settings"' checkbox is checked. The 'Username' field is empty (6). The 'Password' field is empty with an eye icon. The 'Account' field is empty with a dropdown arrow. The 'Always prompt with list' checkbox is checked (7).

1. Give the entry a meaningful name
2. Specify the URL of the CyberArk Central Credential Provider.
3. Enter the web application name, typically **PasswordVault**
4. The version is for the REST API version to use. V9 is deprecated and should not be used.
5. Specify the authentication mode used to access the vault.
6. As seen above, either use "My Account Settings" or type credentials.
7. Check the "Always prompt with list" option

ADVANCED TAB

General Advanced

Domain search method **1** Default

Domain field **2** Default

3 Ask for reason

Ask for ticket number **4**

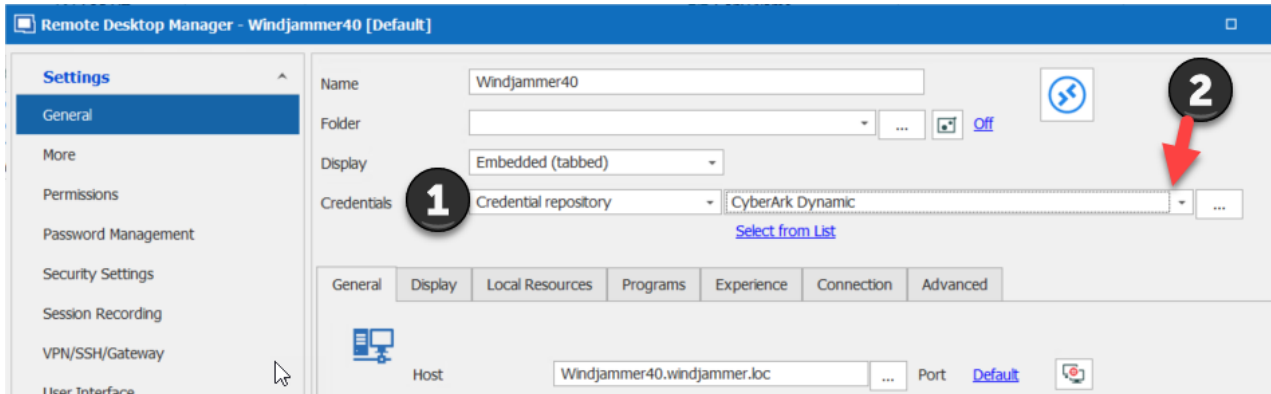
Ticketing system **4**

1. Domain search method: some of our customers store the domain name in various fields. If you intend for RDM to construct the full UPN by concatenating the UserName and a domain field, you must choose "Field"
2. When "Field" is chosen in step 1, you will have to choose between **Address**, **Domain**, **LocalDomain** and even **Custom**. For the latter, an additional field will appear for you to type in the name of the field to use.
3. If the CCP requires a reason, check this box for RDM to display an additional form to allow the user to enter the reason.
4. If the information on a ticket is required, check this box for RDM to display an additional form to allow the user to enter the ticket number. If also required, you can specify the default name of the ticketing system being used.

AFTER CREATING THE CYBERARK ENTRY, HOW TO USE

This credential entry that you have created above below will need to be linked to any entry that represents a remote access technology, RDP, SSH, SCP, FTP, iDRAC, iLo, etc. If you also have a PSM Server, this would surely be the most secure option, but for unsupported protocols our integration offers account brokering in a simple fashion.

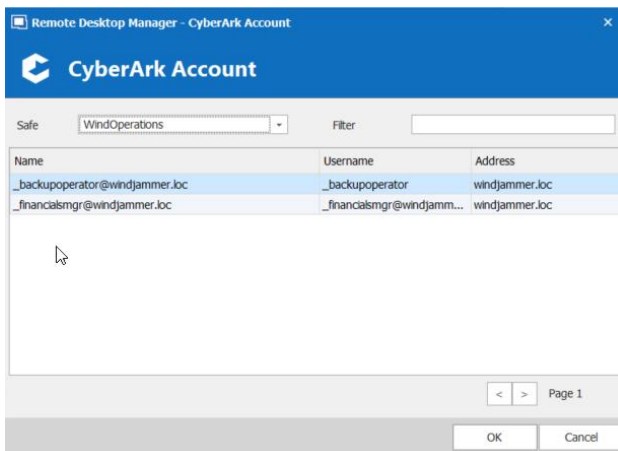
Create an entry for your desired remote access technology, RDP in this case.



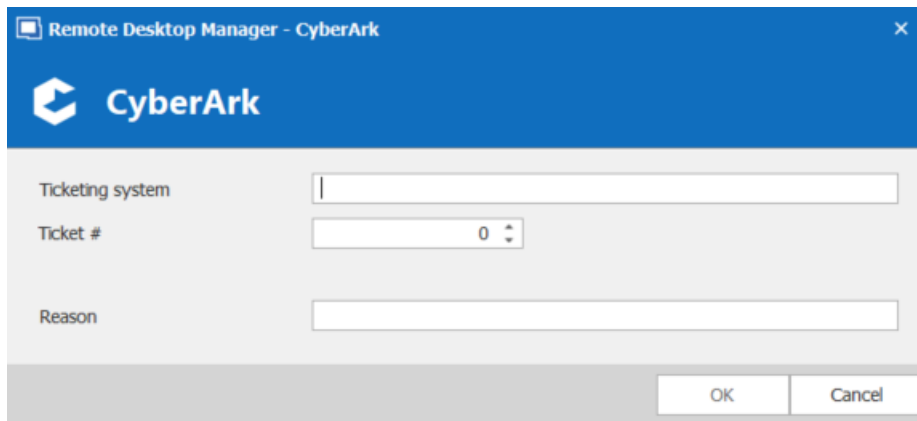
1. In the Credentials dropdown, select “Credential Repository. This is basically a list of all Credential entries that the user has access to.
2. From the list of entries, select the CyberArk entry created above.

Please refer to https://help.remotedesktopmanager.com/settings_general_credentials.htm to see all the possible combinations.

If you have elected for the dynamic model, this form appears for you to select the safe, then the account to use



If you had elected to prompt for a reason, or a ticket number, this second form will appear



The image shows a dialog box titled "Remote Desktop Manager - CyberArk". The dialog has a blue header with the CyberArk logo and name. Below the header, there are three input fields: "Ticketing system" (a text box), "Ticket #" (a spinner box with the value "0"), and "Reason" (a text box). At the bottom right, there are "OK" and "Cancel" buttons.

1. specify or override the name of the ticketing system
2. Enter the ticket number (limited to integer numbers at this time...)
3. Provide the reason if needed

PARTNER CONTACT INFO

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