APPLICATION ACCESS MANAGER

AAM INTEGRATION - TECHNICAL DOCUMENTATION

Devolutions

http://devolutions.net

Remote Desktop Manager

2020.2

June 2nd, 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.

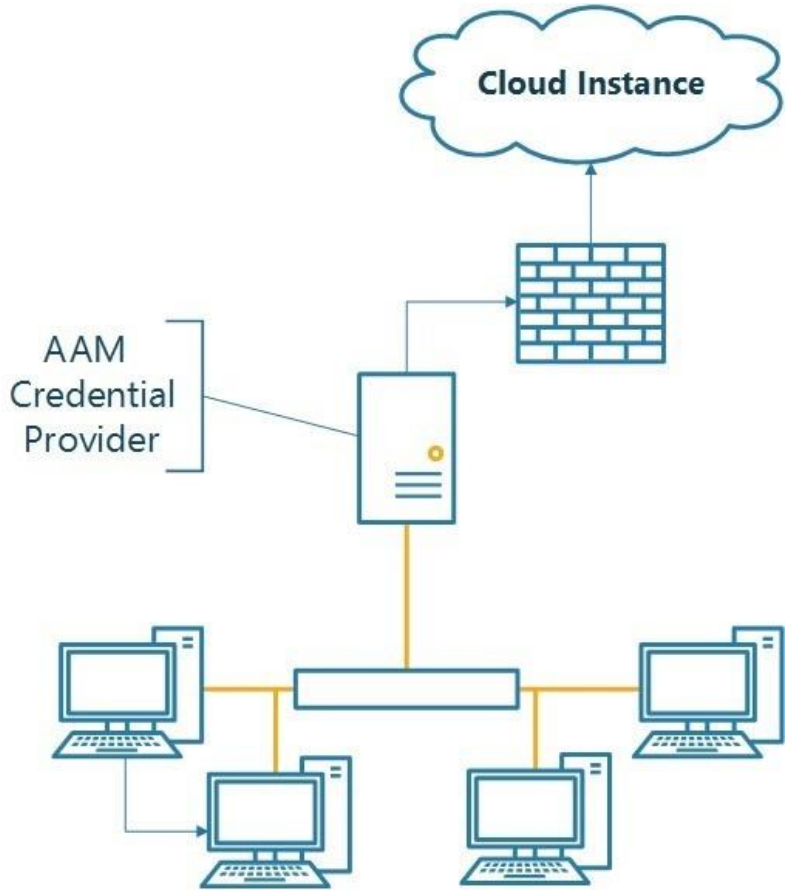
KEY BENEFITS

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 AAM. The passwords are never cached by RDM and supports Certificate Authentication (Serial Number, provided by AAM). 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 a RDP or SSH session, and the credentials will be obtained Just In Time and submitted automatically.

This current implementation of this integration is only in our Windows Edition.

AAM INSTALLATION

Refer to “Central Credential Provider Implementation Guide” for CyberArk Credential Provider installation.

Aside from having the certificates serial numbers added to the application on CCP, There are no special steps for installation because of our integration, the default procedure can be followed to the letter.

AAM CONFIGURATION

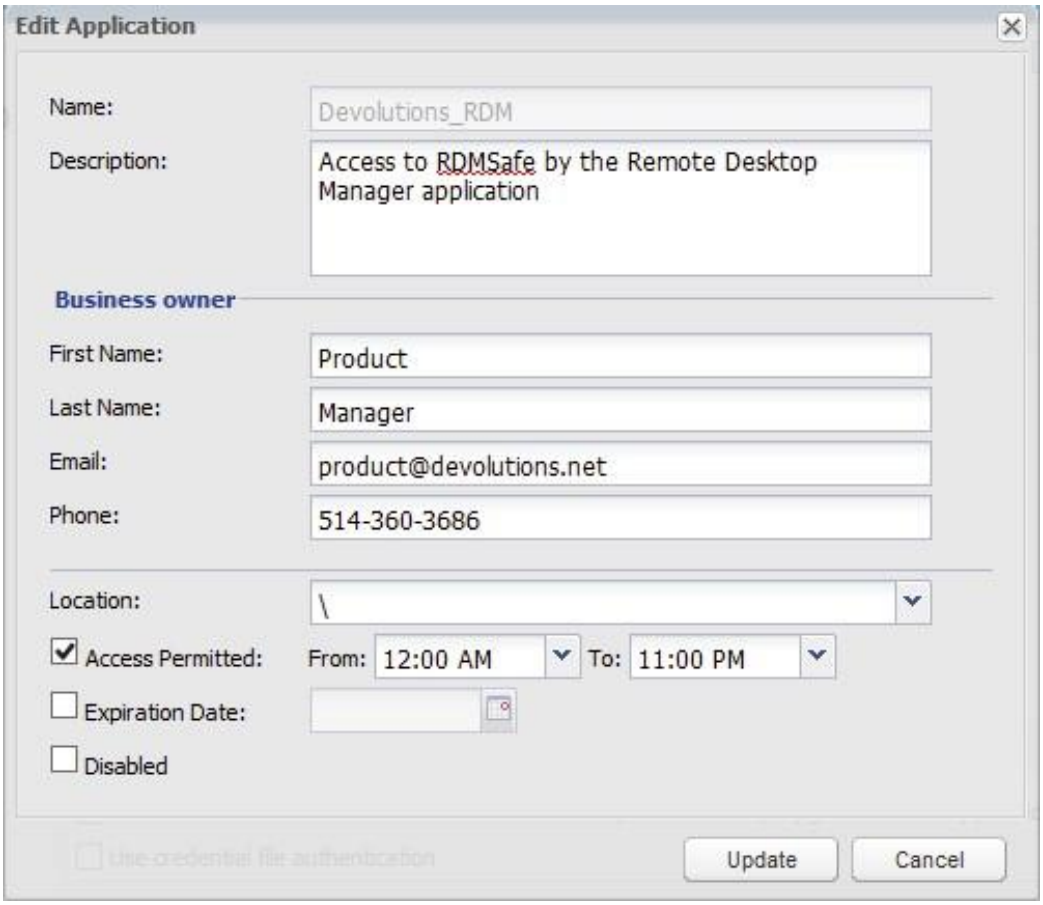
DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

The Application is the entry point for RDM. Since the AAM integration is currently used, care must be taken to add constraints that validate that only the proper Application Server can call the CyberArk services.

To define the Application, here are the instructions to define it manually via CyberArk’s PVWA (Password Vault Web Access) Interface:

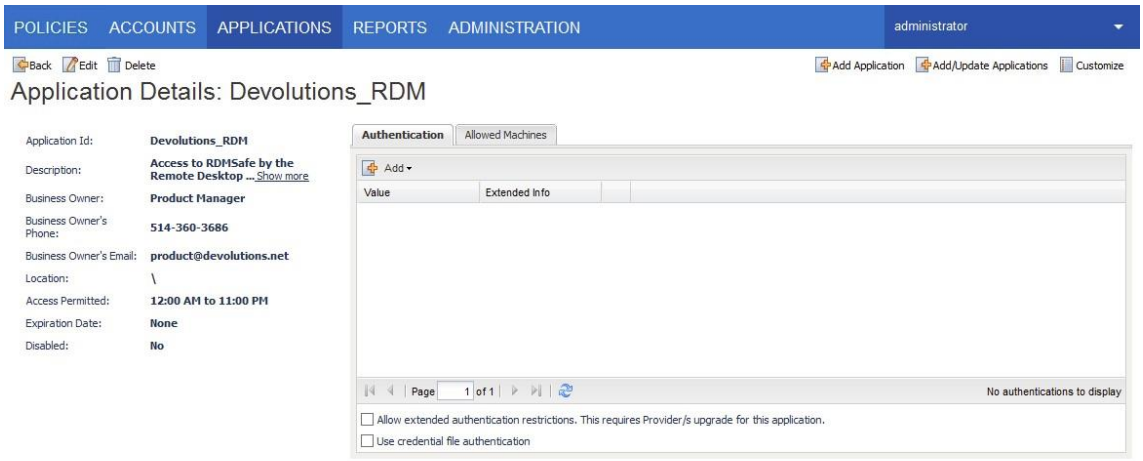
1. Logged in as user allowed to managed applications (it requires Manage Users authorization), in the Applications tab, click **Add Application**; the Add Application page appears.

   The customer can elect to use one or multiple Application ID to meet with his needs of isolating credentials form various segments of his staff. Segmenting the credentials across multiple applications will help in securing the interface at a higher level. For illustration purposes, we will define an application called ***Devolutions_RDM***.



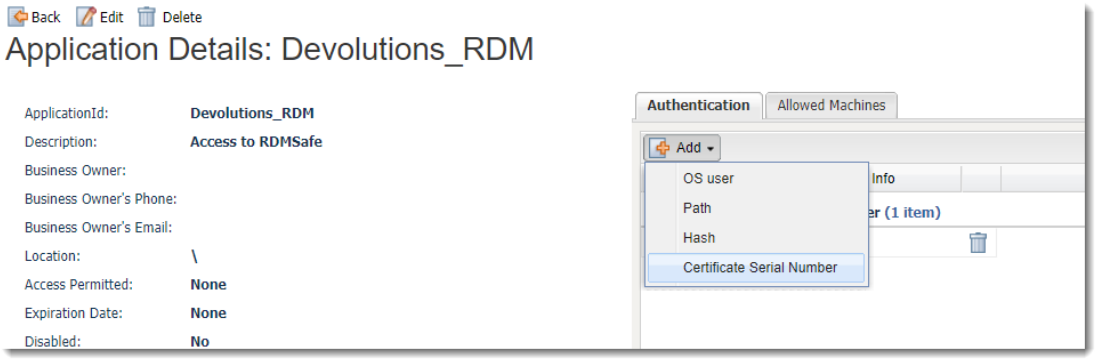
2. Specify the following information:
    - In the Name edit box, specify the unique name (ID) of the application.
      PARTNER: APP ID = ***Devolutions_RDM***
    - In the Description, specify a short description of the application that will help you identify it.
    - In the Business owner section, specify contact information about the application's Business owner.
    - In the lowest section, specify the Location of the application in the Vault hierarchy. If a Location is not selected, the application will be added in the same Location as the user who is creating this application.

3. Click **Add**; the application is added and is displayed in the Application Details page.



4. Specify the IP address of the Application Server in the Allowed Machines tab.

5. Add the Certificate Serial Numbers of the allowed entities



6. Refer to CyberArk's documentation on adding a certificate to the Application Server to further secure not only the communication, but also to positively identify the server itself.

PROVISIONING ACCOUNTS AND SETTING PERMISSIONS FOR APPLICATION ACCESS

For the application to perform its functionality or tasks, the application must have access to particular existing accounts, or new accounts to be provisioned in CyberArk Vault (Step 1). Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application (Step 2).

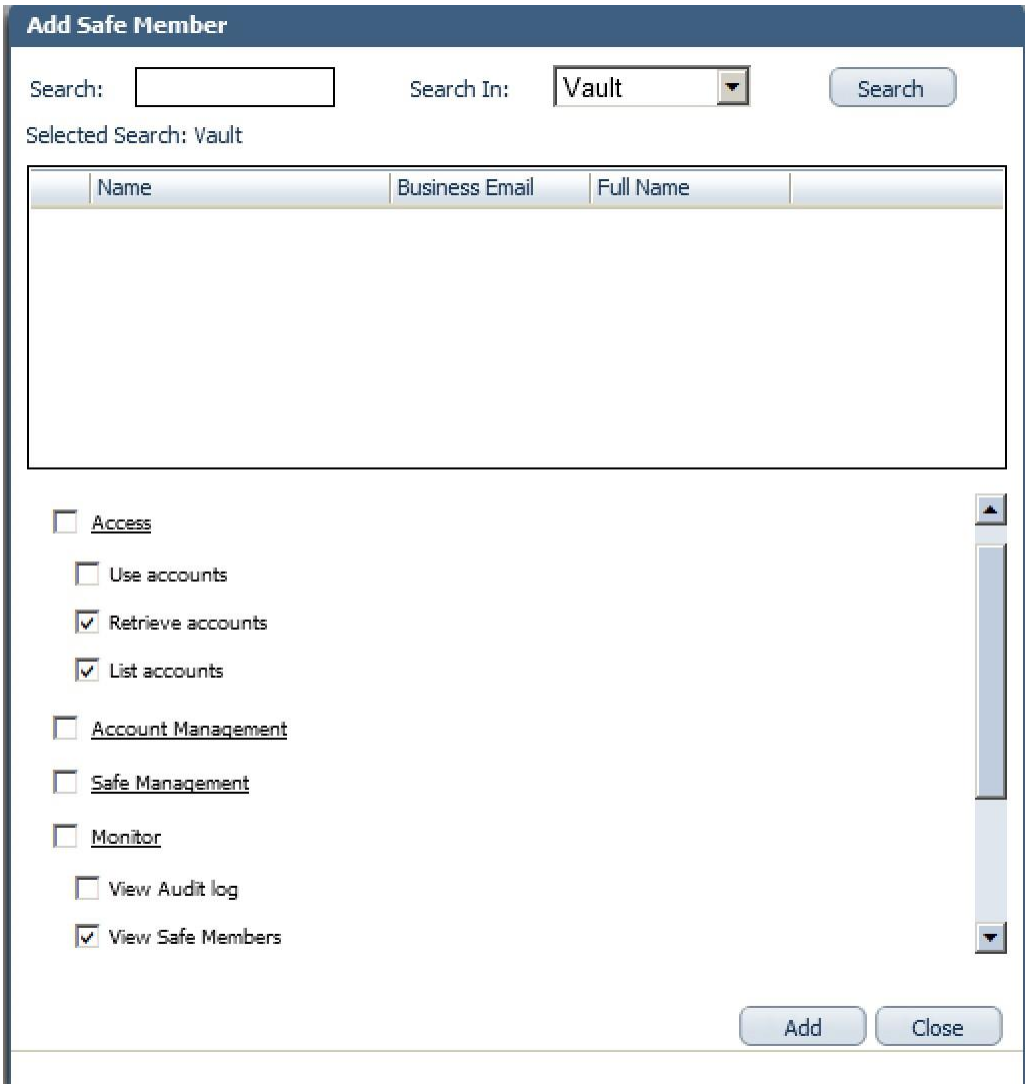
1. In the Password Safe, provision the privileged accounts that will be required by the application. You can do this in either of the following ways:
   - **Manually** – Add accounts manually one at a time, and specify all the account details.
   - **Automatically** – Add multiple accounts automatically using the Password Upload feature.

For this step, you require the **Add accounts** authorization in the Password Safe.

For more information about adding and managing privileged accounts, refer to **the Privileged Account Security Implementation Guide.**

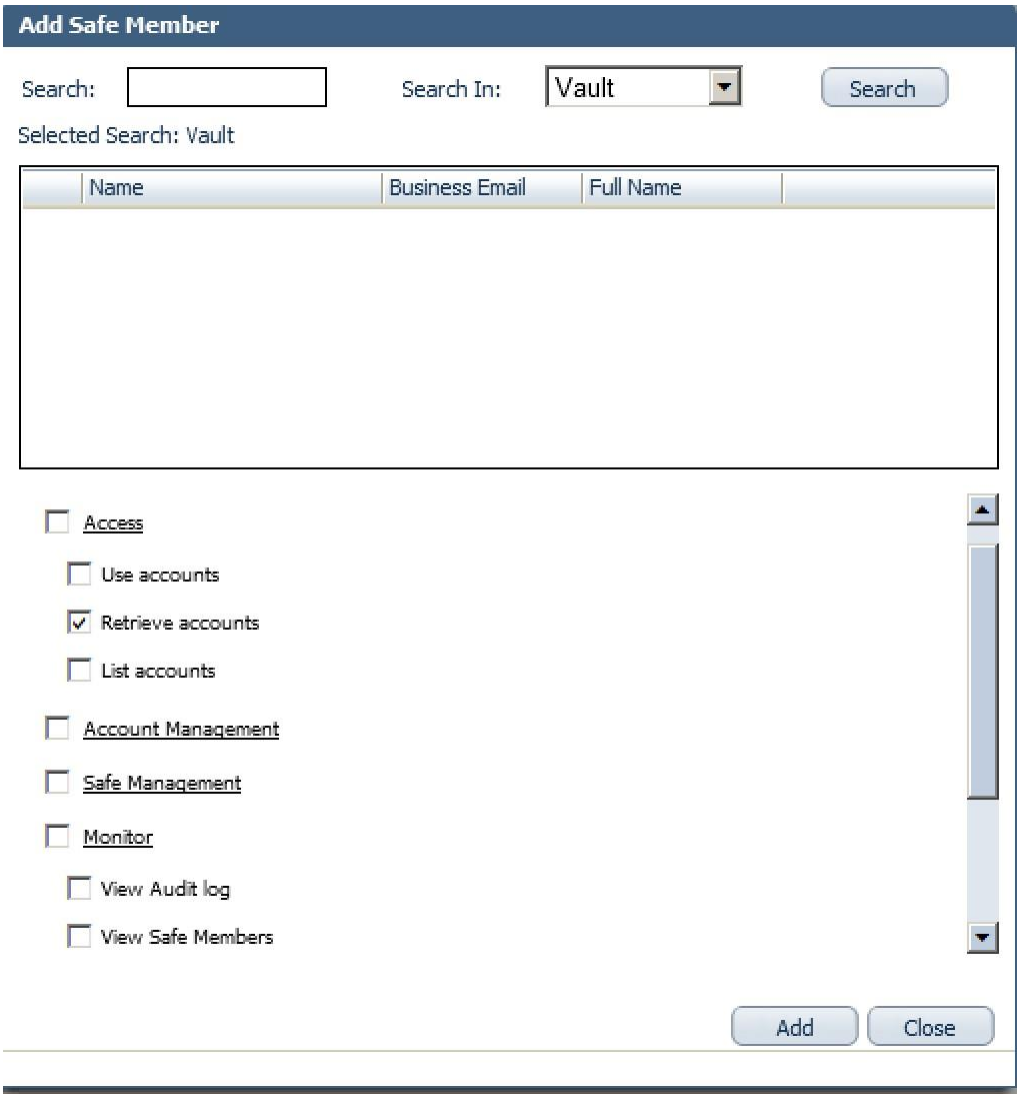
2. Add the Credential Provider and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.
    i. Add the Provider user as a Safe Member with the following authorizations:
        - List accounts
        - Retrieve accounts
        - View Safe Members

        Note: When installing multiple Providers for this integration, it is recommended to create a group for them, and add the group to the Safe once with the above authorization.



ii. Add the application (the APPID) as a Safe Member with the following authorizations:

- Retrieve accounts



iii. If your environment is configured for dual control:

- In PIM-PSM environments (v7.2 and lower), if the Safe is configured to require confirmation from authorized users before passwords can be retrieved, give the Provider user and the application the following permission:
  - Access Safe without Confirmation
- In Privileged Access Security solutions (v8.0 and higher), when working with dual control, the Provider user can always access without confirmation, thus, it is not necessary to set this permission.

iv. If the Safe is configured for object level access, make sure that both the Provider user and the application have access to the password(s) to retrieve.

For more information about configuring Safe Members, refer to the **Privileged Access Security Implementation Guide.**

DEVOLUTIONS RDM REQUIRED SAFE CONFIGURATIONS

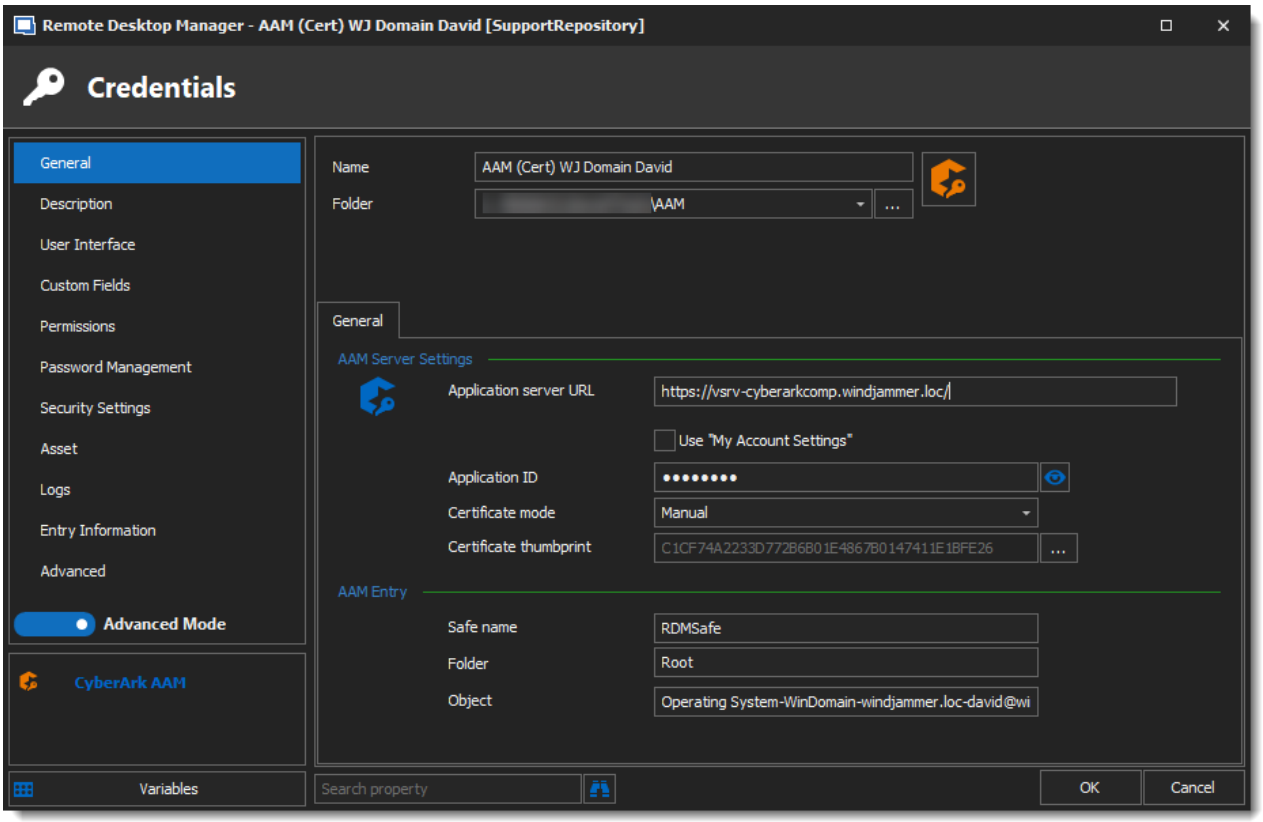
The following safe configurations are required for RDM to work:

1) RDM users require both **Retrieve Password** and **Use Password** authorizations.
2) Safes accessed by RDM cannot have **Object Level Access Control** (**OLAC**) enabled.

DEVOLUTIONS RDM **INSTALLATION & INTEGRATION CONFIGURATION**

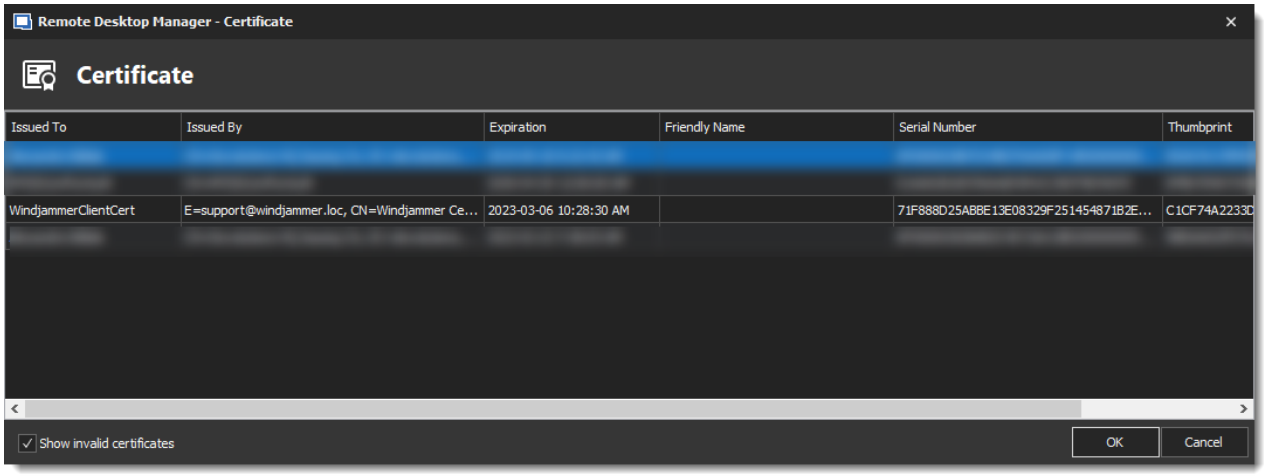
Refer to https://help.remotedesktopmanager.com for detailed instructions on Remote Desktop Manager's installation.

For using the integration, in RDM, create a new entry of the CyberArk AAM type. Note that this type is available only when a Site license or better is registered in the application.



1. Give the entry a meaningful name

2. Store it in a folder that is consistent with your organizations structure. In our example, each CyberArk safe is mapped to a folder named accordingly.
3. Specify the URL of the CyberArk Central Credential Provider.
4. Type in the Application ID. It has been decided to hide this secure this ID just as a password would have been protected.
5. Select Certificate Mode
    a Manual will allow to select a specific certificate from the store



    b Alternatively, to allow customization, those can be set through the “Use My Account settings”
6. Type in the Safe name
7. Type in the Folder name (Root if none)
8. Type in the object name as reported in the PasswordVault account details.

This credential entry can now be linked to by other entries in RDM. Please refer to https://help.remotedesktopmanager.com/credentials.html to see all the possible combinations.

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