APPLICATION ACCESS MANAGER

AAM INTEGRATION - TECHNICAL DOCUMENTATION

Devolutions

http://devolutions.net

Remote Desktop Manager

2020.2.12

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.

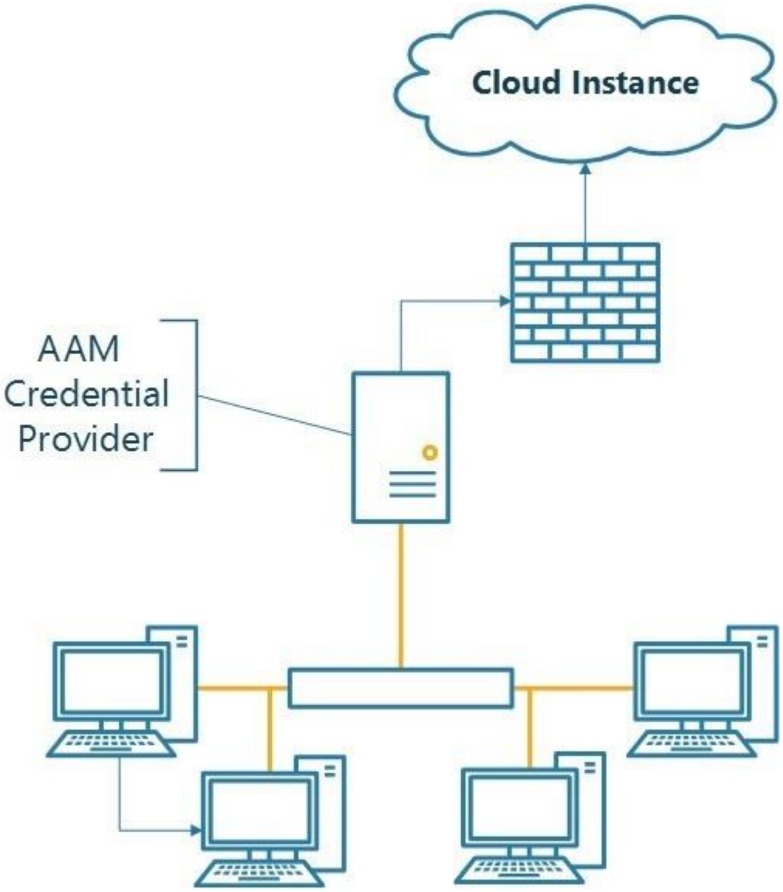
KEY BENEFITS

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 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

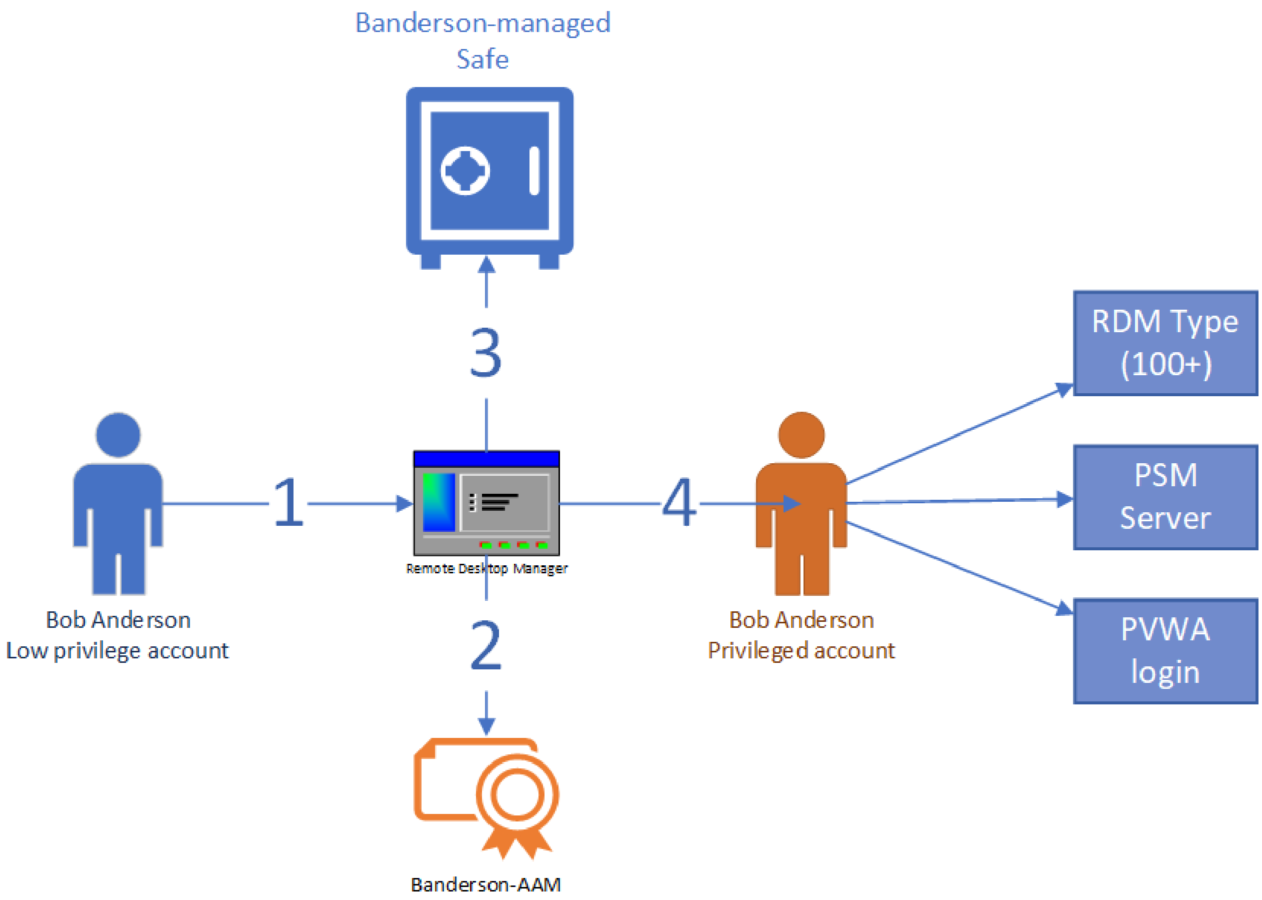
Devolutions customers can elect to store their information in multiple back-ends: on premise RDBMS, cloud services, simple files, etc. The storage system used by our application is therefore omitted from this diagram. To ease deployment of the solution, the strategy has been to use CyberArk's Central 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 using 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 used to connect to the endpoint. They would launch a session using Remote Desktop Manager, and the credentials will be obtained *Just In Time* and brokered automatically.

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

Please note that our current implementation of the AAM integration is for the specific purpose of supporting a "Password less" workflow that gives the vault administrator full control by using client authentication certificates that are managed by the enterprise infrastructure.



The ideal workflow consists of the following:

- The user is authenticated to RDM using a *least privileged* account.
- Within RDM, he launches a connection to any of our supported technology that is adapted to *account brokering*. (step 1).
- RDM obtains the certificate specified in the AAM entry (step 2). This certificate is fully managed by the Enterprise.
- RDM obtains a *Privileged Account* from AAM, typically in a user specific safe. What is key here is that the user does not know his credentials. (step 3)
- The *Privileged Account* is brokered to the desired connection (step 4).

The full power of CyberArk's vaulting is available to manage that Privileged Account: password rotation, time-based limitations, etc.

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

For illustrations purposes, Windjammer is a fictitious customer organization which employs Bob Anderson. Multiple entities exist for his use:

- A Least privileged account: ***banderson***, most likely only used to access his computer and low-risk enterprise resources.
- A safe to hold his privileged accounts: ***banderson-managed***
- A privileged Account: ***banderson-p***, stored in the safe above
- A certificate issued by the enterprise certification authority. It replaces password authentication against AAM.
- An application configured to accept the certificate for authentication

Neither the PVWA nor the PSM accept ***banderson*** has a valid account, only ***banderson-p*** has access, most importantly Bob does not know his privileged account credentials.

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

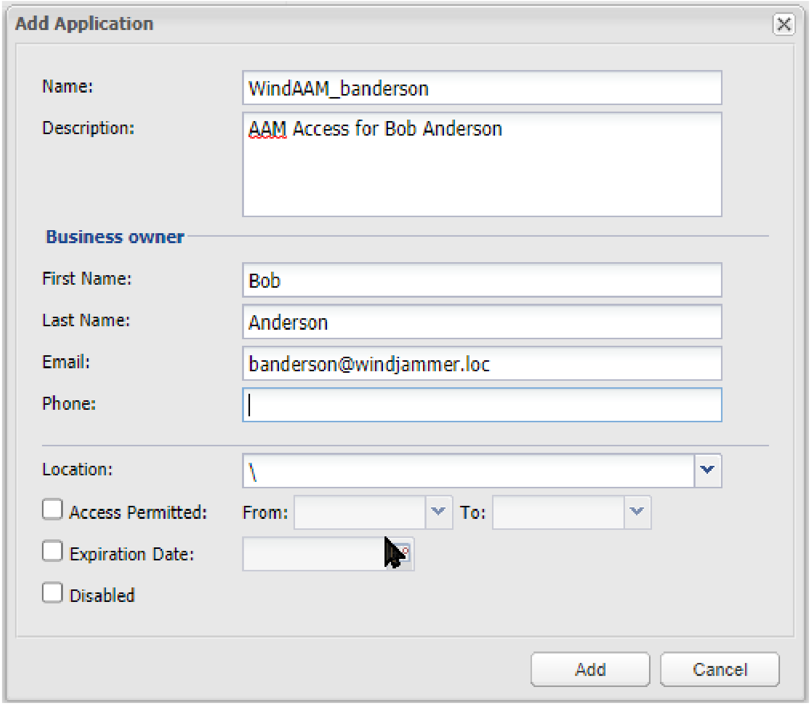
The Application is the entry point for RDM. Since the AAM integration is currently used, care must be taken to add constraints that validate that only the proper Application Server can call the CyberArk services.

Please note that our current implementation of the AAM integration is for the specific purpose of supporting a “Password less” workflow that gives the vault administrator full control by using client authentication certificates that are managed by the enterprise infrastructure.

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 tied a single user called *WindAAM_banderson* (Windjammer's AAM certificate for Bob Anderson's usage)



Add Application

Name: WindAAM_banderson

Description: AAM Access for Bob Anderson

Business owner

First Name: Bob

Last Name: Anderson

Email: banderson@windjammer.loc

Phone:

Location: \

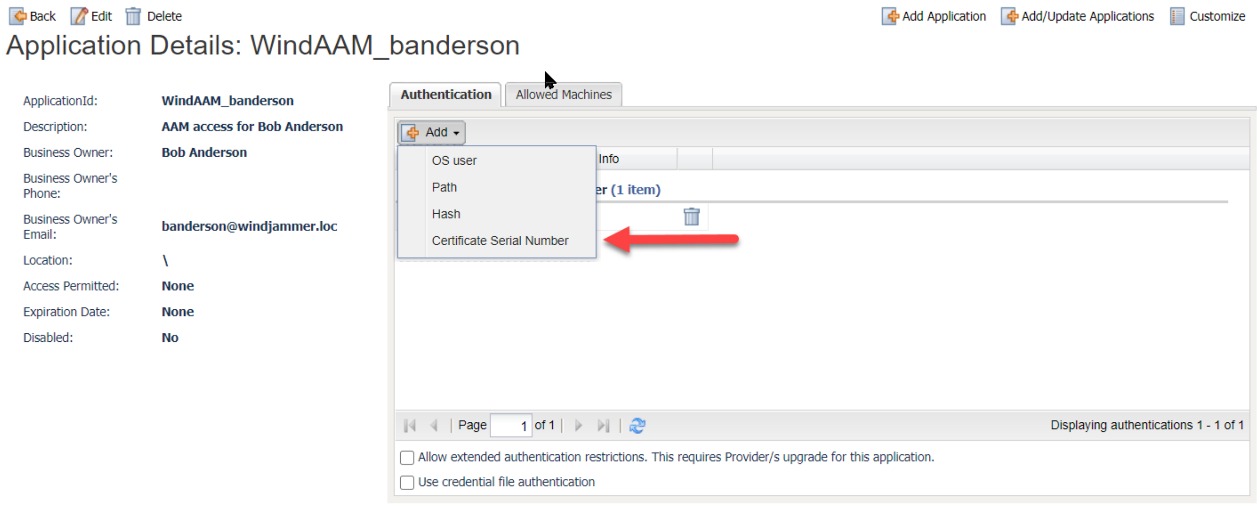
□ Access Permitted: From: To:

□ Expiration Date:

□ Disabled

2. Specify the following information:
   - In the Name edit box, specify the unique name (ID) of the application.
     PARTNER: APP ID = ***WindAAM_banderson***
   - Fill the rest of the fields as required by your organization's policies
3. Click **Add**; the application is added and is displayed in the Application Details page.

4. Add the Certificate Serial Number that is associated to Bob Anderson



Application Details: WindAAM_banderson

ApplicationId:	WindAAM_banderson
Description:	AAM access for Bob Anderson
Business Owner:	Bob Anderson
Business Owner's Phone:	
Business Owner's Email:	banderson@windjammer.loc
Location:	\
Access Permitted:	None
Expiration Date:	None
Disabled:	No

□ Allow extended authentication restrictions. This requires Provider/s upgrade for this application.

□ Use credential file authentication

5. Refer to CyberArk's documentation for all certificate registration steps.

PROVISIONING ACCOUNTS AND SETTING PERMISSIONS FOR APPLICATION ACCESS

For the application to perform its functionality or tasks, the application must have access to 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).

Note	For usage with the PVWA or the PSM, the syntax of the privileged account name must be the same as you see in ***Administration – Users***. Either use the plain ***SamAccountName*** or the full ***UPN*** as required by your systems.

1. In the ***banderson-managed*** safe, provision the privileged accounts as required.

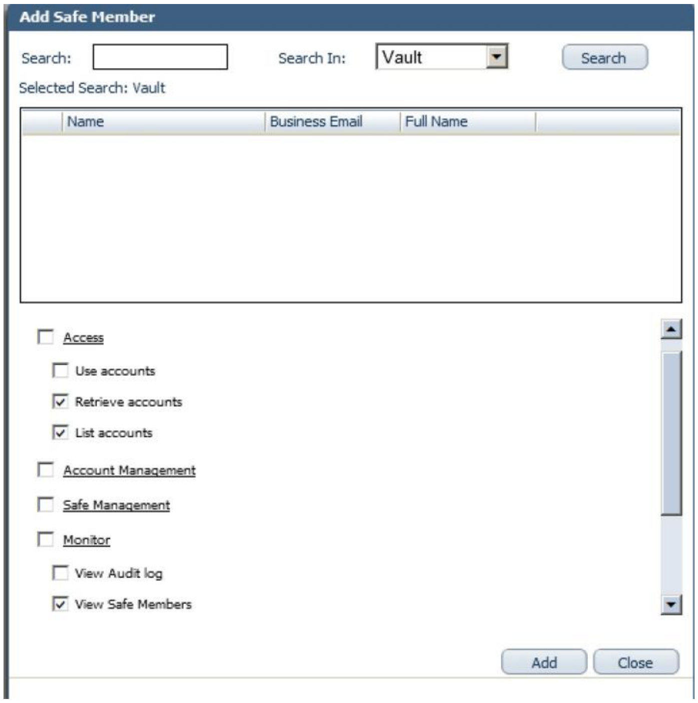
   For more information about adding and managing privileged accounts, refer to **the Privileged Access Security Implementation Guide.**

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

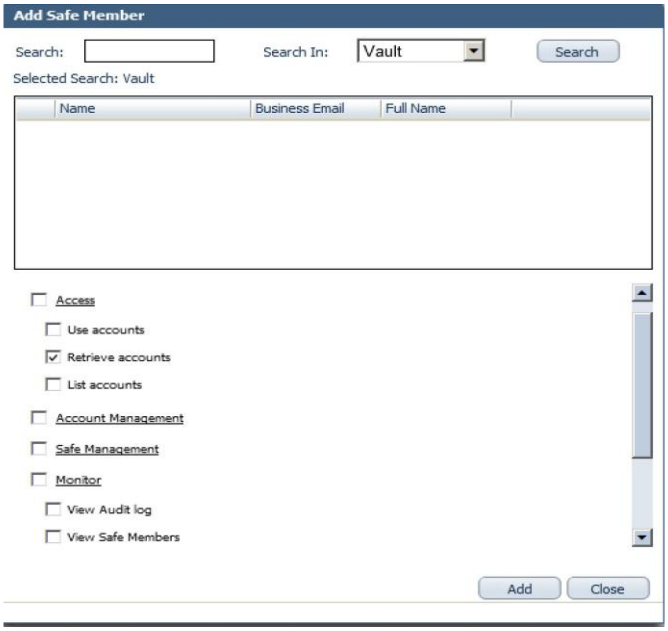
        Note: When installing multiple Providers for this integration, it is recommended to create a group for them, and add the group to the Safe once with the above authorization.



□ Access
□ Use accounts
☑ Retrieve accounts
☑ List accounts
□ Account Management
□ Safe Management
□ Monitor
□ View Audit log
☑ View Safe Members

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

- Retrieve accounts



Search In: Vault

Selected Search: Vault

- □ Access
  - □ Use accounts
  - ☑ Retrieve accounts
  - □ List accounts
- □ Account Management
- □ Safe Management
- □ Monitor
  - □ View Audit log
  - □ View Safe Members

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.**

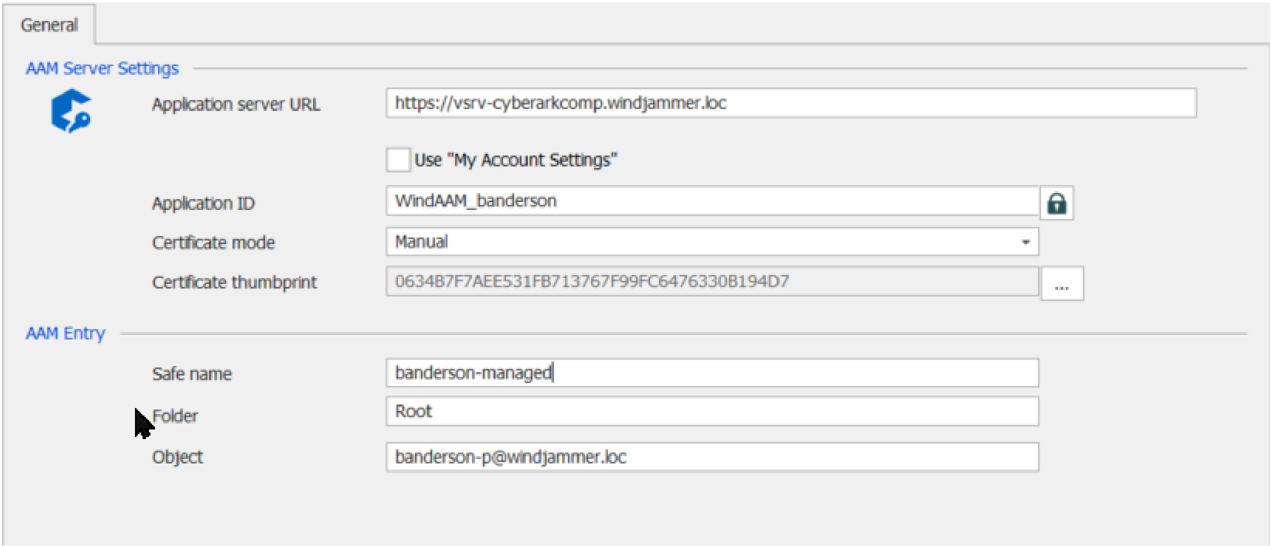
DEVOLUTIONS RDM REQUIRED SAFE CONFIGURATIONS

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**

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



AAM Server Settings

Application server URL: https://vsrv-cyberarkcomp.windjammer.loc

□ Use "My Account Settings"

Application ID: WindAAM_banderson

Certificate mode: Manual

Certificate thumbprint: 0634B7F7AEE531FB713767F99FC6476330B194D7

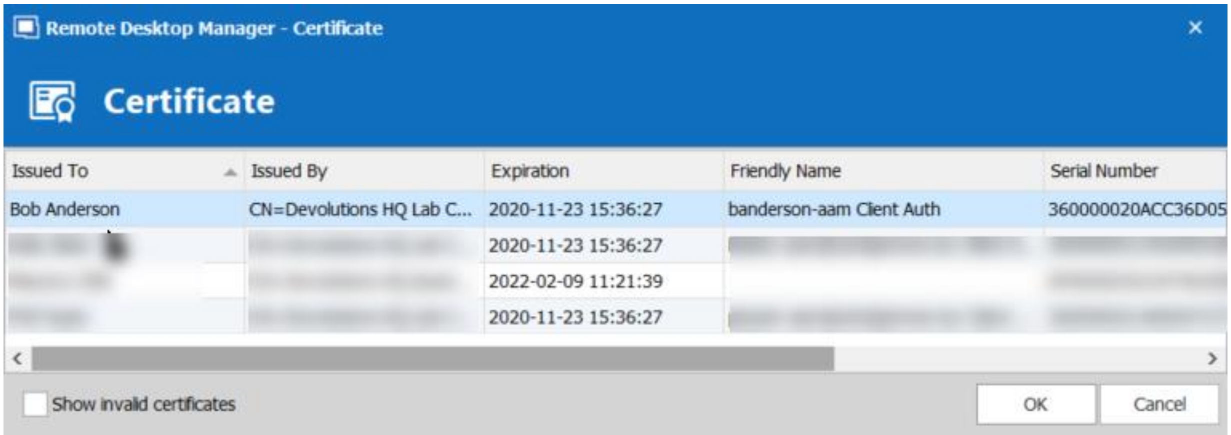
AAM Entry

Safe name: banderson-managed

Folder: Root

Object: banderson-p@windjammer.loc

1. Give the entry a meaningful name
2. Specify the URL of the CyberArk Central Credential Provider.
3. Type in the Application ID.
4. Select Certificate Mode, we recommend the manual mode and intend to remove the Automatic mode in a future release



Issued To	Issued By	Expiration	Friendly Name	Serial Number
Bob Anderson	CN=Devolutions HQ Lab C...	2020-11-23 15:36:27	banderson-aam Client Auth	360000020ACC36D05
[redacted]	[redacted]	2020-11-23 15:36:27	[redacted]	[redacted]
[redacted]	[redacted]	2022-02-09 11:21:39		[redacted]
[redacted]	[redacted]	2020-11-23 15:36:27	[redacted]	[redacted]

□ Show invalid certificates

5. Type in the Safe name
6. Type in the Folder name (Root if none)
7. 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