



SECRETS MANAGER

SM (AAM) INTEGRATION - TECHNICAL DOCUMENTATION

Devolutions

<https://devolutions.net>

Remote Desktop Manager

2023.3

November 1st, 2023

PARTNER SOLUTION OVERVIEW

Remote Desktop Manager (RDM) is a solution designed to store and securely share details of connections, credentials, VPNs, and more. RDM integrates with 160+ technologies/protocols to become the single pane of glass that IT personnel use to perform maintenance tasks, monitor asset health, and, most importantly, control access to remote devices securely.

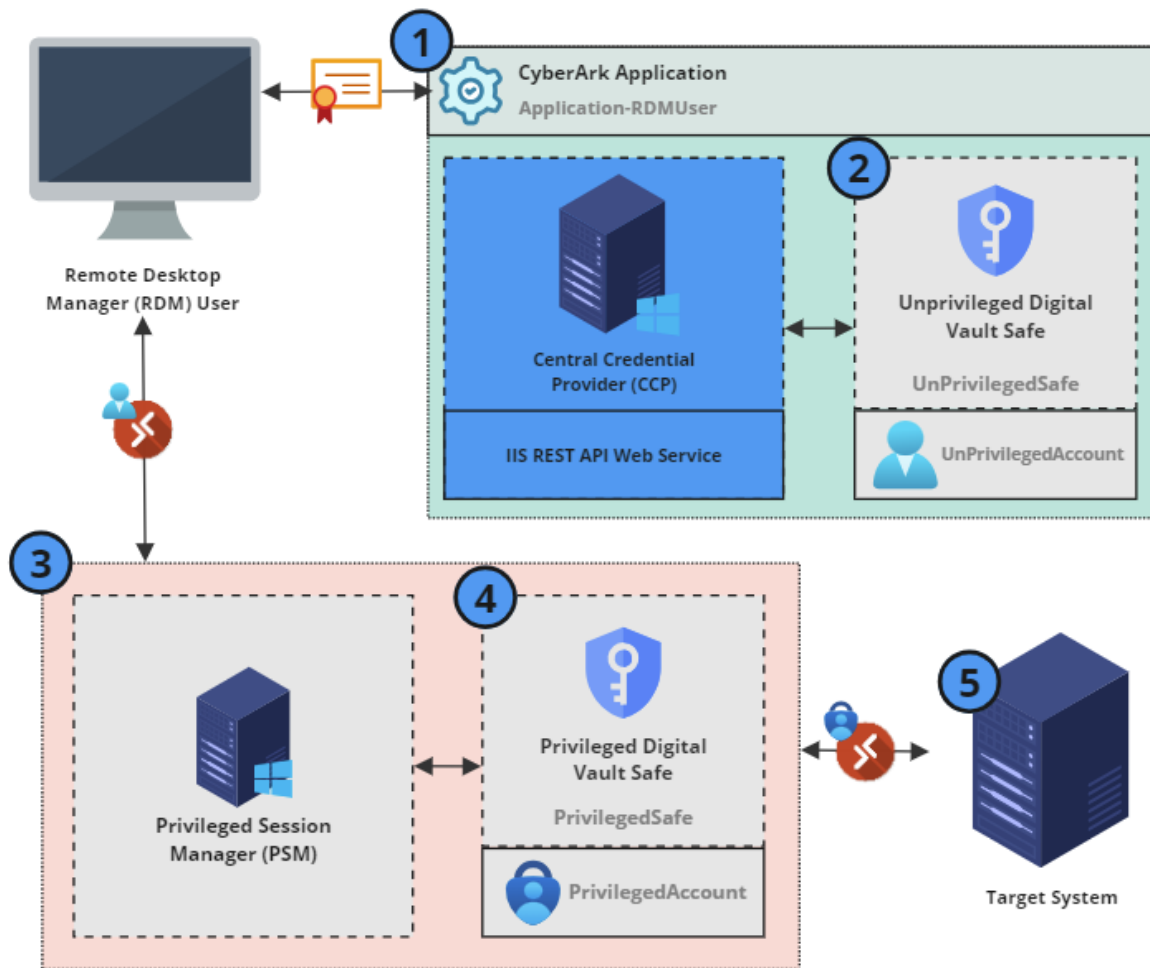
KEY BENEFITS

With its asset-centric workflow, Remote Desktop Manager allows an IT technician to search for an asset and launch a connection (with optional VPN pre-connection). RDM best practices dictate using linked credentials, which the IT technician is unaware of and cannot view. Robust RBAC (role-based access control) offers flexible permissions with extensive activity logging and change versioning.

Remote Desktop Manager helps workers maintain and regain productivity and, by 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 entries and associated information in multiple back-ends (known as Data Sources), such as on-premise RDBMS, cloud services, simple files, etc. To ease the deployment of the CyberArk solution, RDM uses CyberArk's Central Credential Provider (CCP) and CyberArk PSM. A single application server is sufficient for current customers, but the CyberArk integration can support multiple servers.



An RDM passwordless CyberArk entry, or SM (AAM) certificate credentials, directly queries the CyberArk CCP REST API for an unprivileged account. The RDM CyberArk integration never knows or caches any CyberArk passwords in any scenario.

A key feature of RDM is the ability to launch many different technologies (Remote Access, VPNs, Web Portals) and perform the authentication without user interaction. With CyberArk, the credentials are obtained just-in-time (JIT) without users knowing their origin.

SM (AAM) INSTALLATION

Aside from having the certificates' serial numbers added to the CyberArk Application, as defined in the CyberArk PVWA, there are no special steps for installation. Refer to the Central Credential Provider implementation guide for CyberArk Central Credential Provider installation.

SM (AAM) CONFIGURATION

CREATING THE CYBERARK APPLICATION

Before RDM may open a connection, a CyberArk Application, added via the CyberArk PVWA dashboard (as shown below), must be defined to allow an external client (RDM) to query the CCP REST API. As a best practice, limiting external client access is recommended by defining a single application per user, using certificate authentication via serial number, and including IP address restrictions (a specific IP or CIDR).

1. Log in to **PVWA** as a user with the “**Manage Users**” permission, navigate to **Applications**, and click the **Add Application** button.

The screenshot shows the 'Add Application' dialog box. It has a title bar with a close button. The form includes the following fields and options:

- Name:** A text input field containing 'AAM_banderson'.
- Description:** A large text area.
- Business owner:** A section with a blue header containing:
 - First Name:** 'Product'
 - Last Name:** 'Manager'
 - Email:** 'product@devolutions.net'
 - Phone:** An empty text input field.
- Location:** A dropdown menu showing a backslash character.
- Access Permitted:** A checkbox followed by 'From:' and 'To:' dropdown menus.
- Expiration Date:** A checkbox followed by a date picker.
- Disabled:** A checkbox.
- Buttons:** 'Add' and 'Cancel' buttons at the bottom right.

2. Enter the following and click the **Add** button.
 - a. Specify the Application's (client) unique name (APPID) in the **Name** input.
 - b. In the **Description** input, specify a short application description, if desired.
 - c. In the **Business Owner** section, specify contact information about the application's Business owner.
 - d. Finally, specify the **Location** in the Digital Vault Safe hierarchy. If a **Location** is not selected, the application will be added in the exact location of the user who is creating the application (here, the location is the root).

3. Once added, the application is opened and displayed on the **Application Details** page.

The screenshot shows the 'Application Details' page for 'AAM_banderson'. On the left is a sidebar with navigation icons. The main content area has a header with 'Back', 'Edit', and 'Delete' buttons. Below the header, application details are listed: ApplicationId: AAM_banderson, Description: (empty), Business Owner: Product Manager, Business Owner's Phone: (empty), Business Owner's Email: product@devolutions.net, Location: \, Access Permitted: None, Expiration Date: None, and Disabled: No. To the right is a tabbed interface with 'Authentication' and 'Allowed Machines' tabs. The 'Authentication' tab is active, showing an 'Add' button and a table with columns 'Value' and 'Extended Info'. The table is currently empty. At the bottom of the table, it says 'No authentications to display' and 'Allow extended authentication restrictions. This requires Provider/s upgrade for this application.'

4. Under the **Authentication** tab, add the **Certificate Serial Numbers** of the RDM user's private certificate key.

This screenshot is similar to the previous one, but the 'Add' button in the 'Authentication' tab is clicked, and a dropdown menu is open. The dropdown menu contains four options: 'OS user', 'Path', 'Hash', and 'Certificate Serial Number'. The 'Certificate Serial Number' option is highlighted with a blue background. The rest of the page content remains the same.

PROVISIONING ACCOUNTS AND SETTING PERMISSIONS FOR APPLICATION ACCESS

To ensure that RDM never knows privileged account credentials, Devolution recommends the following best practices for CyberArk and RDM.

1. The RDM CyberArk Application accesses CyberArk PSM via an account stored within a CyberArk Digital Vault Safe designated for unprivileged accounts only.
2. Once connected to the PSM, the unprivileged account accesses the target endpoint via an account stored within a separate CyberArk Digital Vault Safe designated for privileged accounts only.

This separation of vaults ensures that Remote Desktop Manager never knows the privileged account password, only accessing CyberArk via an unprivileged account through a CyberArk Application. In the CyberArk PVWA, add the following accounts and permissions through a user with "Add Account" privileges.

First, add the previously defined CyberArk Application as a Safe Member to the unprivileged Digital Vault Safe with the "Use Accounts" and "List Accounts" permission only.

Add Safe Member

Search: Search In:

Selected Search: Vault Display 2 result(s)

Name	Business Email	Full Name
AAM_banderson	product@devolut...	Product Manager

☐ Access

- ☒ Use accounts
- ☐ Retrieve accounts
- ☒ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

- ☐ View Audit log
- ☐ View Safe Members

☐ Workflow

Next, add the unprivileged account as a safe member to the privileged Digital Vault Safe with only the Retrieve Accounts permission.

Add Safe Member

Search: Search In:

Selected Search: Vault Display 1 result(s)

Name	Business Email	Full Name
 banderson-p	bob@windjamm...	Boby Anderson

☐ Access

- ☐ Use accounts
- ☒ Retrieve accounts
- ☐ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

- ☐ View Audit log
- ☐ View Safe Members

☐ Workflow

DEVOLUTIONS RDM CYBERARK CONFIGURATION

The RDM CyberArk integration requires an RDM Enterprise license with a CyberArk add-on module license.

Create a new CyberArk AAM entry with a meaningful name. Though the entry may be stored anywhere, Devolution recommends an RDM folder with the same name as the unprivileged vault.

Edit CyberArk AAM - CyberArk - AAM Credential [User Vault]

Common

- General
- Description
- User Interface
- Entry Information

Name: CyberArk - AAM Credential

Folder: CyberArk\WindPrivilegedVaultUsers

General

AAM Server Settings

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

Application name:

☐ Use "My Account Settings"

Application ID:

Certificate mode: Manual

Certificate thumbprint: 8C9007959D7EDE448B38D52DE09A63CB052CF1E2

AAM Entry

Safe name: WindPrivilegedVaultUsers

Folder: Root

Object: banderson-p@windjammer.loc

☐ Prompt for reason

Show All Properties

Variables **Search property** **Update** **Cancel**

Next, fill in the relevant details to complete the RDM CyberArk AAM entry.

- **Application server URL** - Corresponds to the CyberArk Central Credential Provider (CCP) IIS installation.
- **Application name** - If the IIS application name differs from the default **AIMWebService**, enter that here.
- **Application ID (APPID)** - The **Application ID** is treated similarly to a password entry and hidden from view.
- **Certificate Mode** - To locate the stored certificate on the RDM user's system. The **Manual** mode (**Automatic** is available but deprecated) displays a selection screen to locate a specific certificate from the local user's certificate store. Alternatively, the certificate may be set within RDM via **File → My Account Settings → CyberArk AAM** and the "Use My Account settings" option within the CyberArk AAM entry.

Remote Desktop Manager - Certificate

Certificate

Issued To	Issued By	Expiration	Friendly Name	Serial Number	Thumbprint
Bob Anderson	CN=Devolutions HQ Lab C...	8/3/2024 12:41:56 PM	banderson-aam@windjammer.loc Cle...	360000058FF8C2791566EF4FDC00010000...	8C9007959D7EDE448B38D52DE09A63CB052CF1E2

☐ Show invalid certificates

OK **Cancel**

Certificate thumbprint: 8C9007959D7EDE448B38D52DE09A63CB052CF1E2

- **Safe name** - Enter the Digital Vault Safe name from which CyberArk CCP will access the unprivileged account.
- **Folder** - Enter the Digital Vault Safe Folder name, Root, if no sub-folder is defined.
- **Object** - Enter the object name of the CyberArk unprivileged account to use.

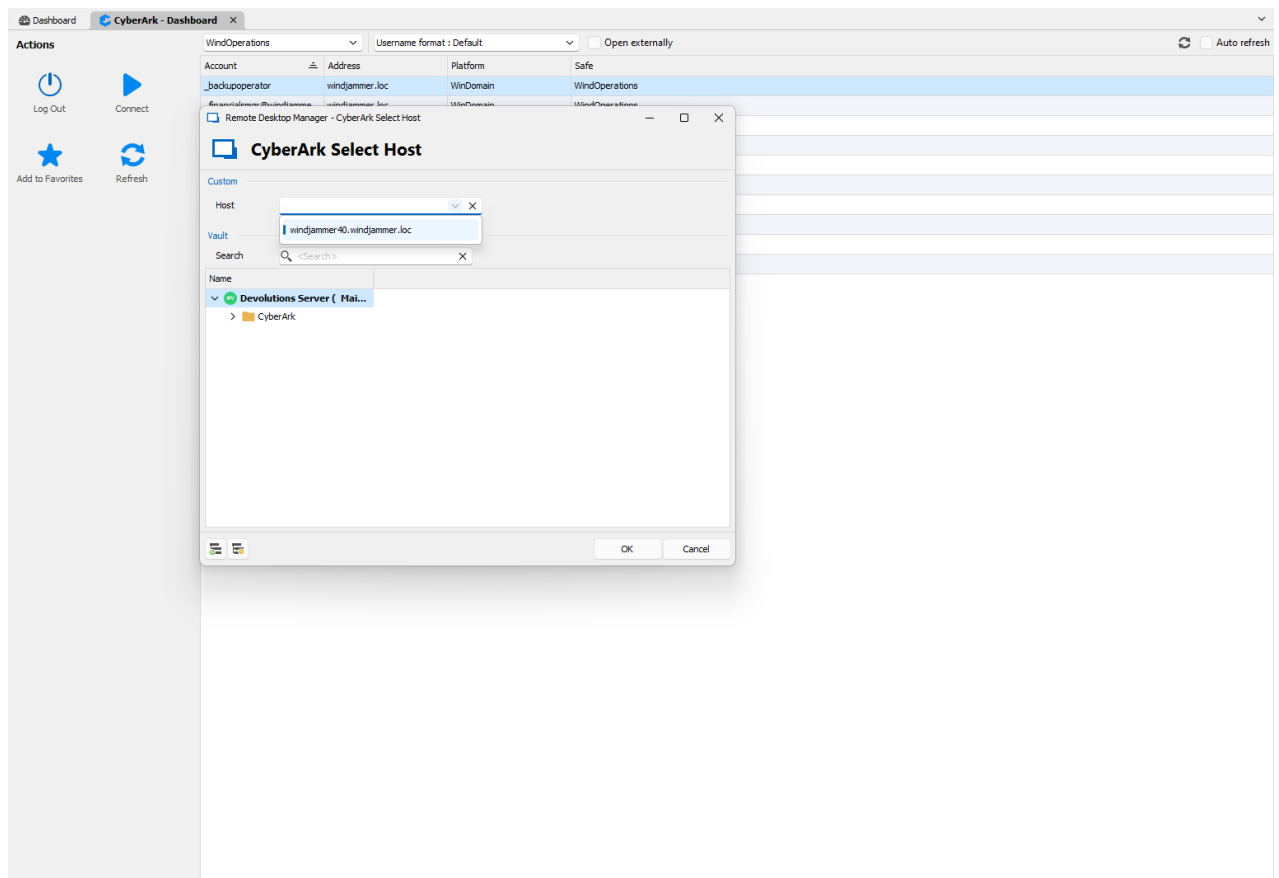
This RDM CyberArk SM (AAM) credential entry can now be linked to other entries within RDM. An example is using RDM CyberArk SM (AAM) credentials with the CyberArk Dashboard entry type in RDM (added as of version 2021.2.13.0).

1. With the newly created RDM CyberArk SM (AAM) credential entry now available, add a **New Entry** in the appropriate location of the type **CyberArk Dashboard**.
2. Enter an appropriate **Name** and populate the **Web services URL** (CyberArk PVWA) and **Virtual directory**, if not the default.

The screenshot shows the 'Edit CyberArk Dashboard' window. The left sidebar has 'Common' and 'Connection' sections. The 'Common' section is expanded, showing 'General', 'Description', 'User Interface', and 'Entry Information'. The 'Connection' section shows 'VPN/Tunnel/Gateway'. The main area has 'General' and 'Advanced' tabs. The 'General' tab is active, showing a list of properties: 'Web services URL' (https://vsrv-cyberarkcomp.windjammer.loc), 'Virtual directory' (empty), 'Version' (Default (V12)), 'Authentication mode' (LDAP), and 'Authentication credentials' (AAM (User vault search) and CyberArk - AAM Credential). At the bottom, there are 'Variables', 'Search property', 'Update', and 'Cancel' buttons.

3. Set the appropriate **Authentication mode** and then the **Authentication credentials** to **AAM (Linked)**, selecting the previously defined CyberArk RDM SM (AAM) credential.

- Once created, the RDM CyberArk Dashboard allows an RDM user to choose the asset to connect to.



PARTNER CONTACT INFO

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