Remote Desktop Manager + PAM

USE CASE

How Remote Desktop Manager Integrates with Your Existing Privileged Access Management Solution.

Create a Powerful and Versatile Privileged Session Management System Using Account Brokering.

Devolutions

Who Is This Use Case For?

An organization has an existing **privileged access management (PAM)** solution. They do not want to replace their solution but instead want to know how it can be enhanced by integrating it with **Remote Desktop Manager (RDM)**.

The Problem

Privileged access management solutions help secure, control, manage, and monitor privileged access to critical assets. The goal is to provide IT teams with the right balance between keeping the organization's critical assets secure while allowing end-users to be productive.

However, many privileged access management solutions require that SysAdmins use multiple **remote access technologies (RAT)** in order to access a wide range of privileged accounts. This makes it increasingly difficult to use privileged passwords without revealing sensitive information to end-users. It also adds a major administrative burden for SysAdmins, who must spend an excessive amount of time responding to access-related requests from end-users.

The Solution

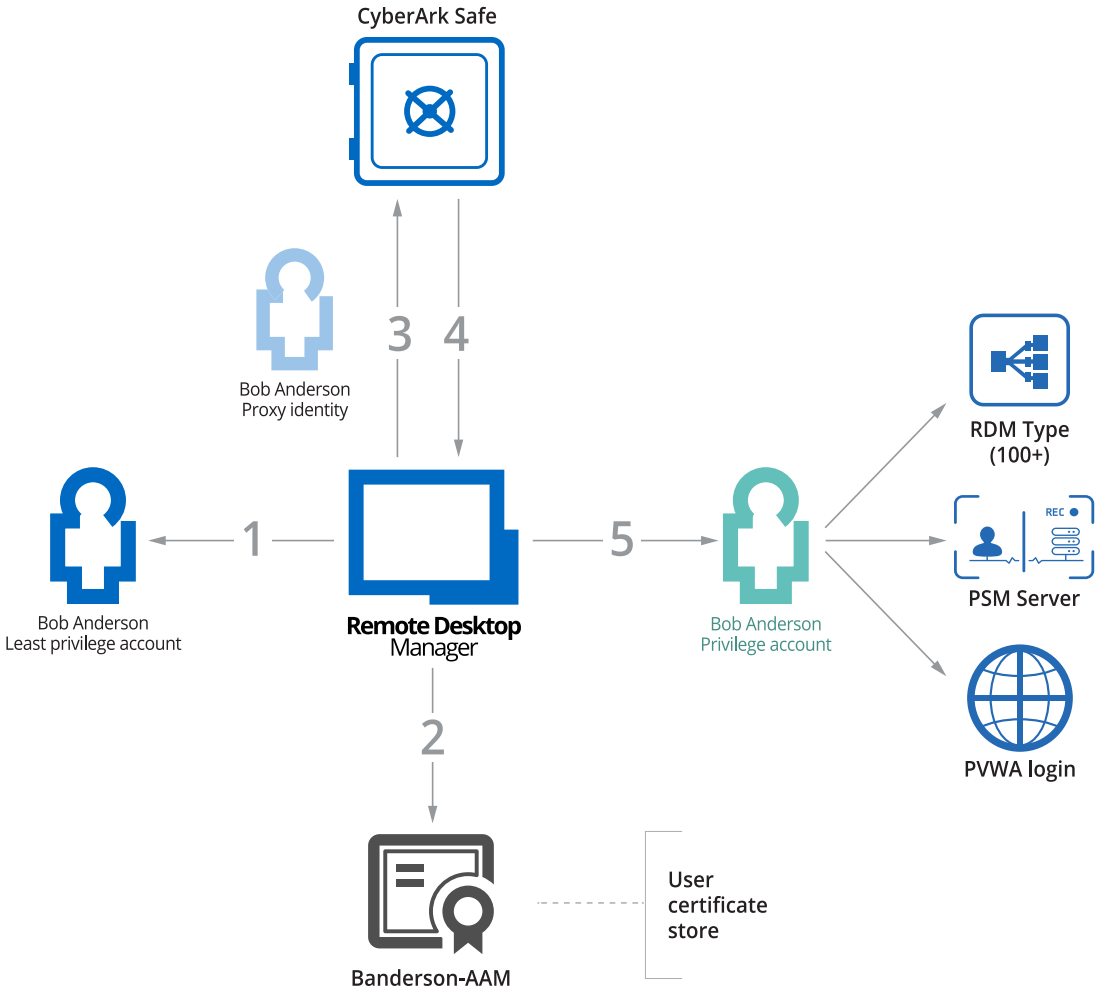
Devolutions is proud to collaborate and partner with leaders in the PAM industry including BeyondTrust, Centrify, CyberArk, ManageEngine, and Thycotic. Integrating these (and other) highly trusted PAM solutions with Remote Desktop Manager creates an effective, efficient and secure **Privileged Session Management (PSM)** system.

How It Works

Remote Desktop Manager is designed to store and securely share connection details, credentials, VPNs, and other sensitive data. It integrates with more than 160 technologies and protocols to function as a single pane of glass that IT professionals use to perform maintenance tasks, monitor system health, and control access to remote devices in a secure manner. Privileged passwords are secured and managed through the existing privileged access management solution, while remote connections are accessed and launched from Remote Desktop Manager **using account brokering**.

Account brokering inserts credentials on the back end (by integrating with the privileged account management solution), which means that **end-users never see credentials in the first place**. However, they can still access the necessary accounts to complete their day-to-day work. Not only is this much more secure, but it is highly efficient as well. End users get their work done, and SysAdmins do not have to deal with numerous access-related requests. In addition, all actions performed in Remote Desktop Manager can be logged and reported for auditing and compliance purposes.

Below is an example diagram demonstrating how Remote Desktop Manager integrates with CyberArk's PAM Solution



STEP 1: The end-user attempts to access a privileged remote connection through RDM.

STEP 2: RDM confirms that the end user's certificate is valid.

STEP 3: RDM connects to CyberArk and requests the necessary credentials.

STEP 4: CyberArk accepts the request and sends the credentials to RDM.

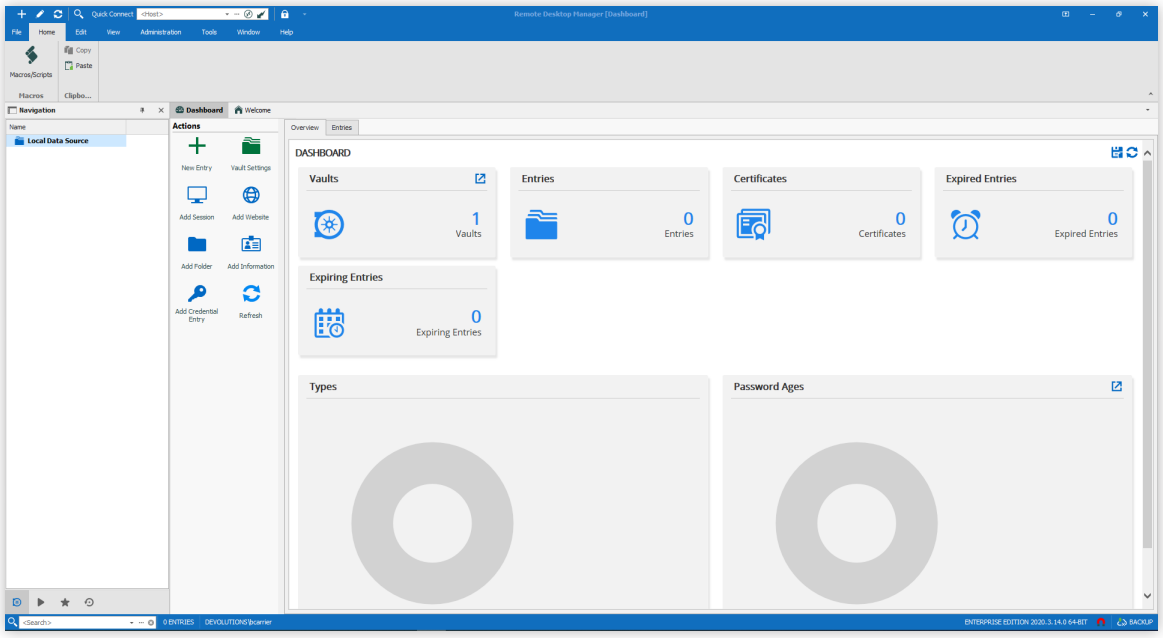
STEP 5: The credentials are used to grant the end-user access, so they can complete their work-related task.

At **no point in this process** does the end-user see the credentials!

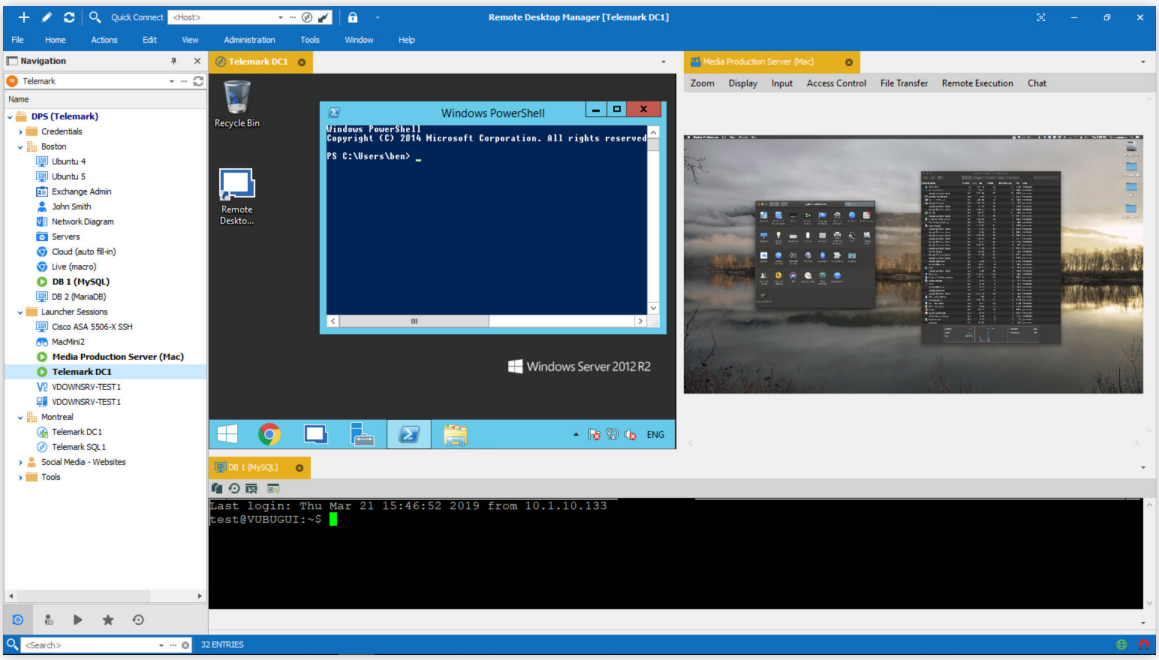
Summary of Benefits

Using **Remote Desktop Manager to enhance an existing Privileged Access Management solution and establish a Privileged Session Management** system delivers the following key benefits:

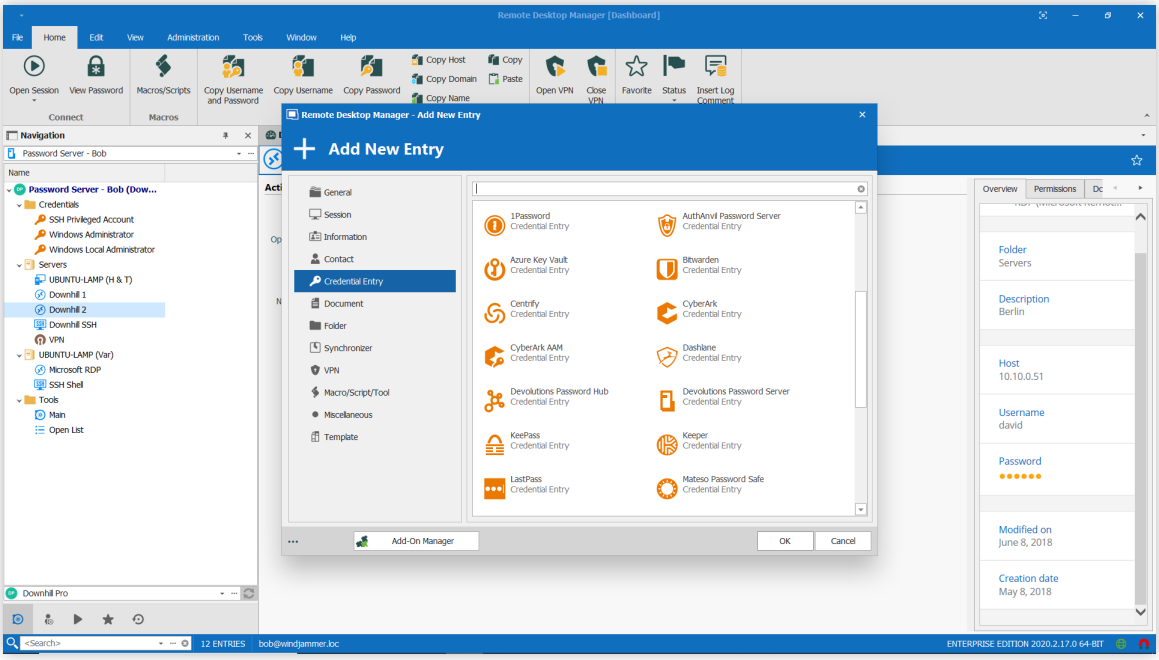
- **Enhance Security:** securely retrieve and inject credentials into remote sessions, without divulging sensitive information to end-users — thus eliminating the need and risk of copying/pasting passwords into remote connections.
- **Maintain Workflow:** seamlessly launch remote connections using current infrastructure, without disrupting workflow.
- **Automate Tasks:** routine tasks can be easily automated, which improves efficiency without compromising security. For example, in a single click, a predefined playlist can launch multiple remote connections using specific credentials from an end user's vault, while passing through a VPN connection using a different privileged account credential.
- **Create Audit Trails:** actions performed in Remote Desktop Manager can be logged and reported on for audit and compliance purposes, in accordance with security policy.



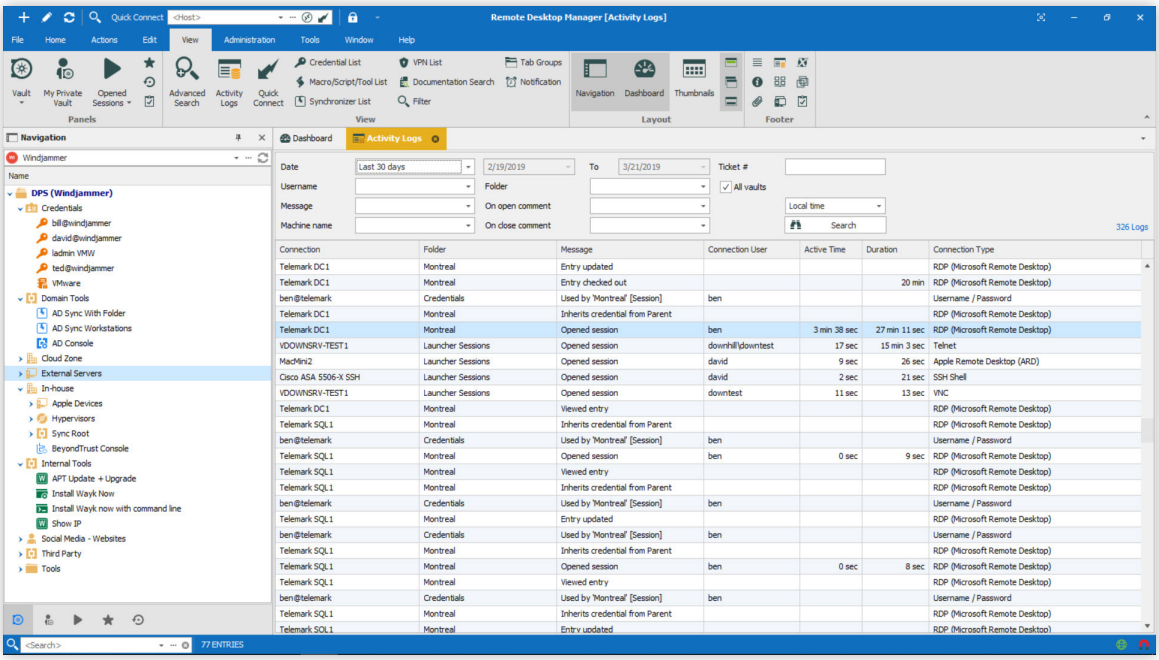
Improve security by injecting your PAM credentials directly into remote sessions.



Increase efficiency by easily launching multiple remote sessions at once using a playlist.



Integrate with a wide variety of popular PAM and Password Management providers.



Provide an audit trail with logs and reports on all activities using PAM credentials.

Next Steps

Integrating Remote Desktop Manager with an existing privileged access management solution creates a powerful and essential privileged session management system — one that enables IT teams to strike a perfect balance between keeping the organization's critical assets secure, while allowing end-users to be productive.

Learn more about how Devolutions can help your organization boost security and productivity.

- **Request a free trial of Remote Desktop Manager –** click here
- **Request a live guided demo of Remote Desktop Manager –** click here
- **Contact us for more information –** click here

DID YOU KNOW... Devolutions was recognized as a 2019 Gartner Peer Insights Customers' Choice for Privileged Access Management. Read the press release.