[NEW] Use Case: How Organizations Can Use Devolutions Server to Improve Security When Authenticating Remote Desktop Manager Users

REMOTE DESKTOP MANAGER IS A SECURE SOLUTION THAT AUTHENTICATES EACH USER

Remote Desktop Manager is a secure solution that authenticates each user. This prevents unauthorized logins, and it also enables comprehensive auditing.

One of the methods that Remote Desktop Manager supports user authentication is an SQL Database login. This is fast and convenient. However, it also presents a potential security vulnerability since it allows end-users to connect directly to the database using a readily available tool like Excel or SQL Server Management Studio. In some organizations, this may be undesirable or unacceptable for compliance.

This security vulnerability — which is not rooted in Remote Desktop Manager, but is due to the external connection with the SQL database — can be eliminated by using Devolutions Server. This is our **full-featured, shared account and password management solution that offers built-in privileged access components created to meet the ever-expanding security requirements of all organizations, including SMBs.**

In our new case study, **you will discover how Remote Desktop Manager + Devolutions Server:**

- **Increases security** by eliminating the possibility that end users can access the database during Remote Desktop Manager authentication.
- **Ensures compliance** by meeting requisite InfoSec rules and regulations.
- **Improves user management** by giving Sysadmins more control and oversight over staff turnover and access removal.

Click here to instantly download the Use Case [PDF].

Click here for a full list of Use Cases that are also available for download.