# SQL Server with Integrated Security – That's So 2015...

Devolutions

## OUR MOST POPULAR AUTHENTICATION MODEL AGAINST SQL SERVER IS THE INTEGRATED SECURITY MODE.

During the early stages of Remove Desktop Manager's development, focus was set on click-next-to-continue deployment and ease of use. We can all agree that the IT field has changed drastically these past few years, and the security landscape has gone from nice rolling hills to a precipitous Norwegian fjord.

Our most popular authentication model against SQL Server (incidentally our most widely-used data source...) has always been the Integrated security mode. This means that your current Windows session authentication token is used to validate your identity against the SQL Instance. This is extremely easy, and it just works. The downside is that you can connect directly to the database, with readily available simple tools that expose all of the database content – tools that most of us have access to, like Microsoft Excel!

You may ask why this is not desirable since you surely know that Remote Desktop Manager stores passwords using AES 256-bit encryption. Well, you need to realize that most modern regulations focus on malicious users gaining access through poor user password management habits. Or they focus on an internal rogue administrator that steals the content of the database while erasing all traces of their actions. The simple fact that you can see some of the database content is deemed an unacceptable risk, as it opens the door to targeted attacks.

In order to offer a safe alternative, we've implemented a Custom login model, preventing the end user from knowing which account was used to connect to the database. This is now the recommended login mode for those in our community who don't need to meet stringent security regulations. For those that need to comply with prevalent compliance regimes (HIPAA, PCI-DSS, GDPR, PIPEDA, etc.), the only choice is to use Devolutions Password Server as the backend. This unavoidably results in us being challenged because some members of our community, as well as potential customers, interpret this as an up-selling tactic. I have a few email conversations with many common counter arguments, but it all boils down to one simple fact: you cannot rely on encryption performed by a locally installed application because cracking that encryption is simply a matter of time! Devolutions Password Server protects that data at rest, in transit, but most importantly, it ensures that sensitive operations are carried out on a service tier with which users cannot interfere.

We obviously allow you to use whichever product you see fit, but if you ask us how to become compliant, it's honestly the only answer we can provide. To summarize:

- Switch from using integrated security to using custom logins. This will prevent your users from directly accessing the database.
- Switch to Devolutions Password Server (or any of our PAM partners, like CyberArk or BeyondTrust), in order to totally isolate the end user from not only sensitive data, but also the encryption algorithms.