Devolutions

WHY I DECIDED TO MOVE MY COMPANY FROM A SINGLE SEAT LICENSE TO DEVOLUTIONS SERVER BY BRENT QUICK

I have been working as an IT consultant for the past 18 years, and during that time, I have connected to thousands of servers.

I have also come across many instances of users "securing" their passwords under their keyboards on a sticky note. Yes, we IT professionals always get a little smirk on our faces when this happens. **But, are we really doing a much better job securing "the keys to the kingdom" that we need to be effective administrators?**

Over the years, I have seen administrators carrying notepads around with entries scribbled in it, passwords scratched out and new ones scribbled in, SharePoint sites containing Excel workbooks or Word documents (which one hopes are up to date), and KeePass and Password Safe database files with shared passwords – **and yet no way to sync changes**. The only positive that I can think of in using these methods – assuming the data is current -- is that when something needs to be fixed, an administrator can quickly log in and fix the issue.

The Challenges

However, the negatives quickly add up, and I would argue they are far riskier and more concerning than users storing passwords on sticky notes. For instance, what happens if an administrator loses their notepad? Who might find it and what could they do with it? **Using Word or Excel also raises major concerns, such as not having the latest copy of the document**. And the situation is even worse if two administrators are editing different parts of the same document – because neither will have the most accurate version, and yet will be sharing it with other administrators.

Our team has also encountered scenarios where an administrator makes changes without documenting them, because he or she is leaving the company. Nothing is like the face of a frustrated administrator who has been locked out of the domain admin account, because of excessive failed login attempts! In light of these risks and drawbacks, there must be a better way to manage and, more importantly, secure all that information.

While all of these issues are major concerns, in my company, the biggest problem has always been **the inability to grant and manage specific rights for various systems, and for our different user types**. This is a common dilemma for consulting firms. While I have worked with large companies that had great systems for managing and restricting access to credentials, the consulting companies I have worked for had 5 to 10 consultants, and on any given day, one or all of us would need to connect to one client's various systems.

And then Remote Desktop Manager happened...

In 2013, I received a free copy of Remote Desktop Manager (RDM) when I was a vExpert, and have been using it ever since. Previously, I used another product, but the company was bought and even if they weren't enhancing their product, the licensing was enhanced from an annual support renewal to an annual subscription.

It took some time to move all of my connections and credentials to RDM, but since doing so, I have never looked back. **RDM does everything that the other product did, and much more**. I changed jobs to a Hyper-V shop and had to drop my vExpert status, and when my RDM annual support and version upgrade renewal came due, I submitted a request to my employer to cover the cost.

That led to several long conversations with my boss about RDM, how it worked, how we could use it, what concerns needed to be addressed, and how it could improve our

day-to-day processes. Our company has a strong "run it ourselves" attitude, so the cloud solution was not an option. **We therefore decided to choose Devolutions Server to get more control, and establish an audit trail.**

The magic of Devolutions Server

I am assuming that most of you already know about and love RDM, and so there is no need for me to go into details on its capabilities and advantages. However, for those of you who are unfamiliar with **Devolutions Server** used in conjunction with RDM Enterprise in a team environment, here are some of the most valuable benefits:

- Assign different and granular access levels and optionally manage them via integration to **Active Directory**.
- **Audit trace** of the connection usage and password access allowing for monitoring the activity and capturing changes.
- **Offline mode** using encrypted local repositories with options like limited life, being read-only, or read/write that update the server using smart synchronization.
- Ability to connect to a server without revealing any credentials to the technician and can force **2-factor authentication** to launch the application.
- Rollback any unwanted or incorrect changes, and the true savior of us all, **recover deleted entries**.

To compare the **different features** for **RDM Free, RDM Enterprise, Devolutions Server** (which we are using) and **Devolutions Cloud**, please follow this link: http://remotedesktopmanager.com/