

## How to Integrate Your Password Management Software into Remote Desktop Manager



## INTEGRATION IS FAST AND SIMPLE

Recently we hosted a Password Managers Webinar on integrating the most popular Password Managers with Remote Desktop Manager, you can find the recorded video on our <u>Youtube channel</u>. In this webinar, we showcased how easy it was to implement that integration. For most password managers, integration is fast and simple. Here are the steps: **1.** Create a new credential entry. **2.** Select your password manager from the list. **3.** Connect your password management account to Remote Desktop Manager. **4.** Use that entry from other sessions, or even better for a whole folder. (Spoiler alert! Next week blog will explain everything about inherited credentials.)

And that's it! You're all done, and can sit back, relax, and enjoy some hilarious <u>Sysadminotaur comics</u>.

However, for the most popular tool in our community, namely Keepass, integration involves a few more steps. Here are the steps to follow:

1. Create a new credential entry. 2. Select KeePass.

3. You'll notice that a plug-in is required; you can either click Install Plug-in, or you can click: Tools –
Extensions Manager – Others – KeePass Plugin. (Note: a KeePass Professional Edition (AKA 2.x) is required to proceed with the integration.)

**4**. You'll see that there are multiple options in the **Credential Selection** tab; if you choose the Default Method, you can select a specific KeePass credential from your list, which will create a hard link to the credential stored in your KeePass database.

Another option is to select **Always prompt with list**. With this option, once your KeePass credential is linked to a session in RDM, you'll notice a blue link that will grant you direct access to your KeePass credential list every time you connect, thus creating a bridge between RDM and KeePass. You will then simply have to select the proper credential for your session.



🍰 Remote Desktop Manager				- [		
🔎 Credential	s					
General More Security Information User Interface Attachments Advanced	Group/folder		New reveal credentials (everybody)			
		fault Method uid	)	Validate	:	
A KeePass	N	me Filtering Method ame Default ase sensitivity Default	only one ma If there is n	es are allowed. If there is e match, it will be chosen. : is many, you will be ed to choose one during on.		
		ys prompt with list view credentials action				
🕥 🎛 Variables	S	earch property	4°h	ОК	Cance	

General	Name	Exchange				$\bigcirc$
More						60
Security	Group/folder	Group/folder Client\Downhill		×	👪 <u>Off</u>	
VPN/SSH/Gateway	Display Embedded (		tabbed) V Primary	monitor ~		
User Interface						
Information	Security group	<none></none>	✓ □ AI	ow reveal credentials (ev	erybody)	
Jump Host	Credentials	Credential re	epository V KeePas	,	~	
Events			Select f	rom list 🚤 🕳 🕳 🕳		
Sub Connections						
Attachments			rces Programs Experience	Connection Advanced		
Todos	Logon Setting					
Logs		nter the name o	of the remote computer			
Tools		omputer	Exchange		Port Default	-
ControlUp		DP type	Normal	~		
Intel® AMT	×	or type	Normal	*		
Is Online (Ping/Port scan)						
Remote Desktop Commander	U	sername				
Remote Management		omain				
Remote Tools			Open console (Admin mode			
Spiceworks				-)		
Wake on LAN			Always ask for credentials			
Advanced						
		Store passwor	rd on the local computer			
			Save Password	Clear Passwo	rd	
Microsoft Remote Desktop (RDP)		Store passwor	rd in the database	Password		0 /8

And that's it! So easy that even Peter Griffin could do it! For more help on how to integrate other password management software into Remote Desktop Manager (like LastPass or 1Password), please take a look at our <u>Online help</u>!

As always, please let us know your thoughts by using the comment feature of the blog. You can also visit our forums to get help and submit feature requests, you can find them <u>here</u>.