Remote Desktop Manager Security Upgrade: Application Lock

Devolutions

WE DECIDED TO TACKLE REMOTE DESKTOP MANAGER'S APPLICATION LOCK FEATURE

Hello, fellow Remote Desktop Manager users! This is Mathieu Morissette from the Security Team here at Devolutions. I've finally climbed out of our secret underground bunker located at an undisclosed location in North America, so that I could share some important news concerning a few upgrades in the latest release of Remote Desktop Manager (versions 2019.2.5 and higher).

First, let me say that as a member of the Security Team, we are always working hard to meet the latest compliance standards and enhance the overall security of our products. Recently, we decided to tackle Remote Desktop Manager's application lock feature in order to pave the way for some future functionality (more on this later), and also to simplify the way your data can be secured.

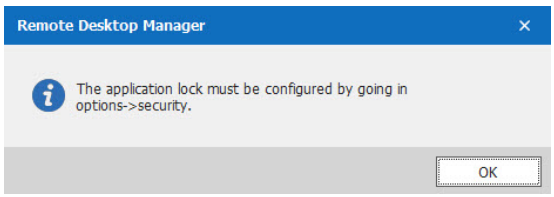
Application Security

In case you aren't familiar with Remote Desktop Manager's application lock feature, this is a security measure that places the product in a locked state. It can be triggered manually or due to a specific event. Once enabled, users are forced to re-authenticate themselves when re-opening the application.

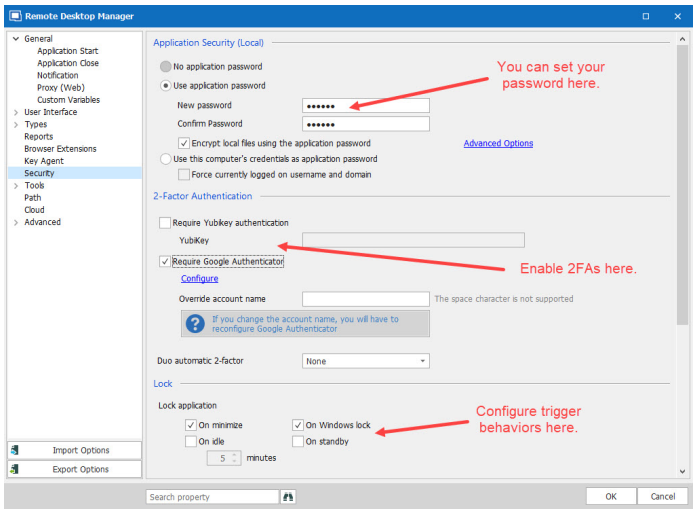
Currently in Remote Desktop Manager, it is possible to lock the application from the File menu, or to put a lock on each data source. However, with the growing number of users who are accessing multiple data sources, we've discovered that in some cases this could cause issues within the application. Furthermore, depending on how things have been configured and enforced, it could also lead to gaps in security. To address both of these risks — while enhancing overall security — we have made two significant upgrades that are described below.

Upgrade #1: Consolidating Application Lock

The first upgrade is that we consolidated the application lock feature, so that it can only be configured from one location. This eliminates the possibility (and the confusion) of configuring the application lock in two places, or not having the same settings across multiple configurations. Starting with Remote Desktop Manager 2019.2.5, if you try to manually lock the application without first configuring it, you will receive this pop-up alert:



From here, you can simply configure the application lock by going to ***File - Options - Security*** and inserting your application password/2FA in the respective fields (see screenshot below).



Once your preferred options are set, you can trigger the application lock manually, or based on a specific event. This will prevent you from running into any conflicts regarding your data source's individual settings.

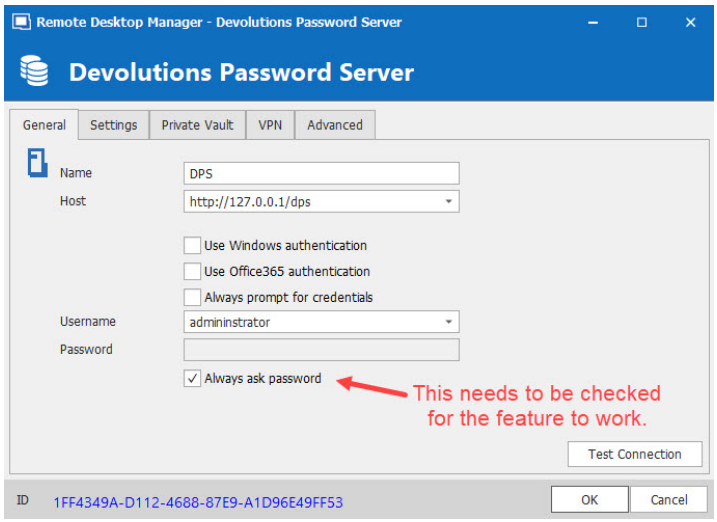
On a side note, this upgrade also allows us to expand some security features in upcoming releases, such as adding Devolutions Authenticator as a 2FA option (you're welcome!).

Upgrade #2: Disconnecting Data Source

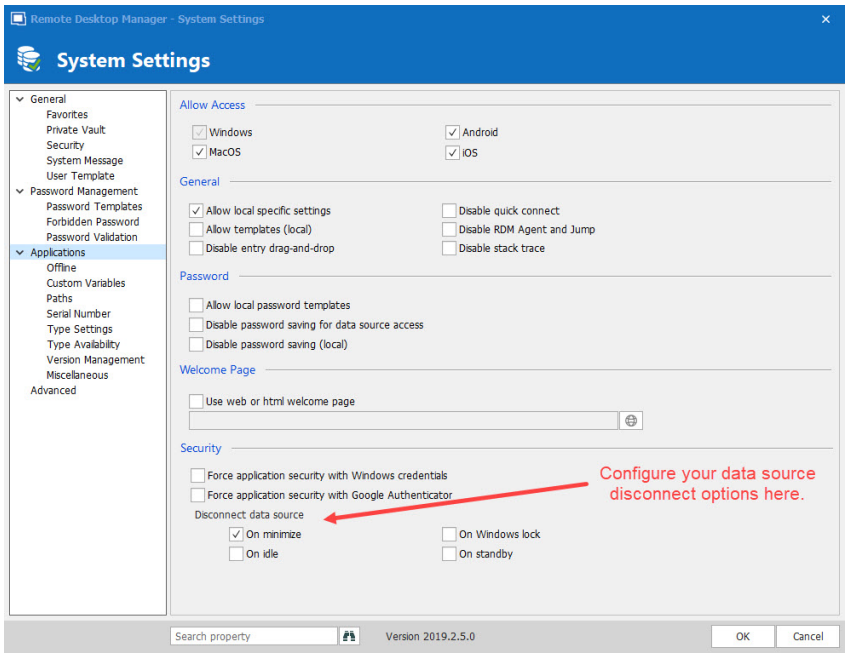
The second upgrade is the result of consolidating the application lock in one location (as described above). We have reconfigured the lock feature that was specific to data sources and renamed it data source disconnect. Now you can set individual disconnect settings for each data source without worrying about potential conflicts with the application lock feature.

For your convenience, the disconnect data source feature offers similar options to the application lock feature. If an event is triggered, it will disconnect the data source and force users to re-authenticate when they attempt to re-connect. As such, you can keep Remote Desktop Manager running, while removing access to a specific data source.

Please note: this feature will only work if ***Always ask password*** is checked in your data source configuration (see screenshot below).



You can access the disconnect data source feature by going to ***Administration - System Settings - Applications***.



In Conclusion

As mentioned earlier, our team is always working hard to make Remote Desktop Manager the most secure way to manage all your remote connections, while also giving you an efficient and intuitive experience. After all, who needs more confusion in this ever-evolving world of IT? These upgrades are also part of our focus on introducing more granular controls, which give you even more power and choice over how you implement security protocols.

If you have any questions, comments, or suggestions, our team would love to hear from you. Yes, even in our super-secure bunker, we are allowed to communicate with the outside world!