Password Policy Complexity

Devolutions

HOW TO MAKE SURE YOUR PASSWORDS MEET SECURITY REQUIREMENT IN REMOTE DESKTOP MANAGER

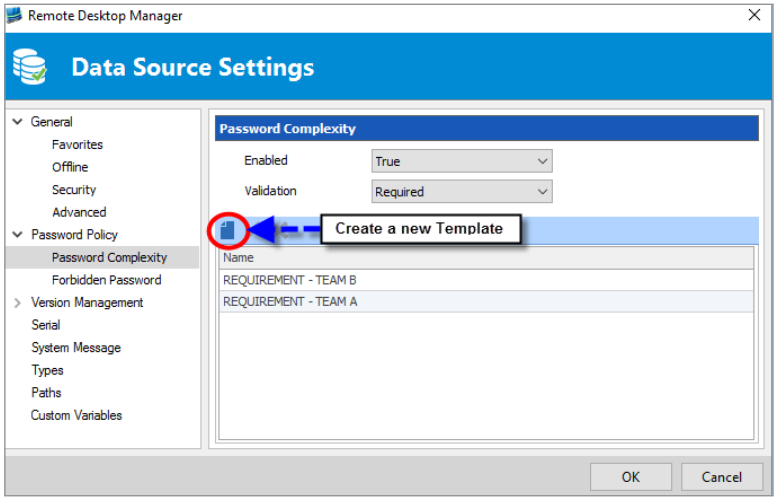
Here at Devolutions, we like to have fun – seriously, you should see our game room! We also have a few team members who can be described as "professional pranksters". So yeah, there's never a dull moment around here.

BUT...there's one thing we never joke about, and that's security! It's our top priority, which is why we've designed **Remote Desktop Manager with a built-in password complexity feature.**

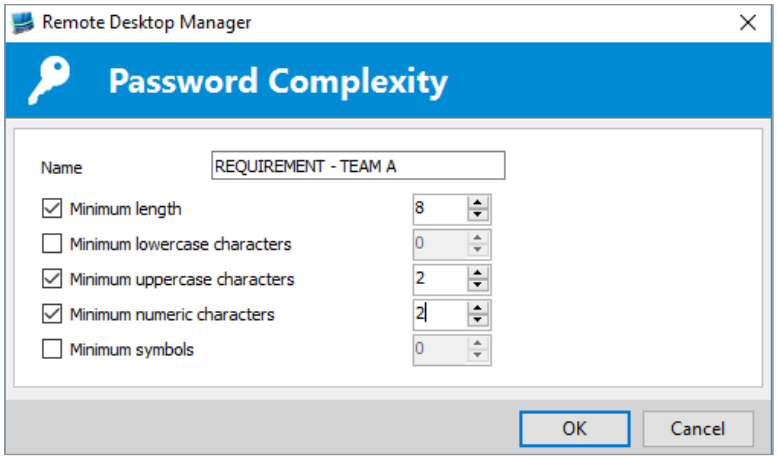
Here's the scoop: we all know that some users don't know the first thing about password security. Their version of a strong password is "123456" or "password", which is hardly secure! (still the top 2 used passwords out there according to Password Random) That's where RDM's password complexity policy feature comes to the rescue!

This feature lets you ensure that all passwords meet pre-determined complexity requirements, so that your valuable systems and devices can't be hacked by a gifted 5-year old. Here's how to set things up:

In **Administration – Data Source Settings – Password Complexity**, click the **New Template** button to create your Password Complexity template. Just a little side note, you could also select **Forbidden Password** and create a blacklist of forbidden password, banning 123456 forever!



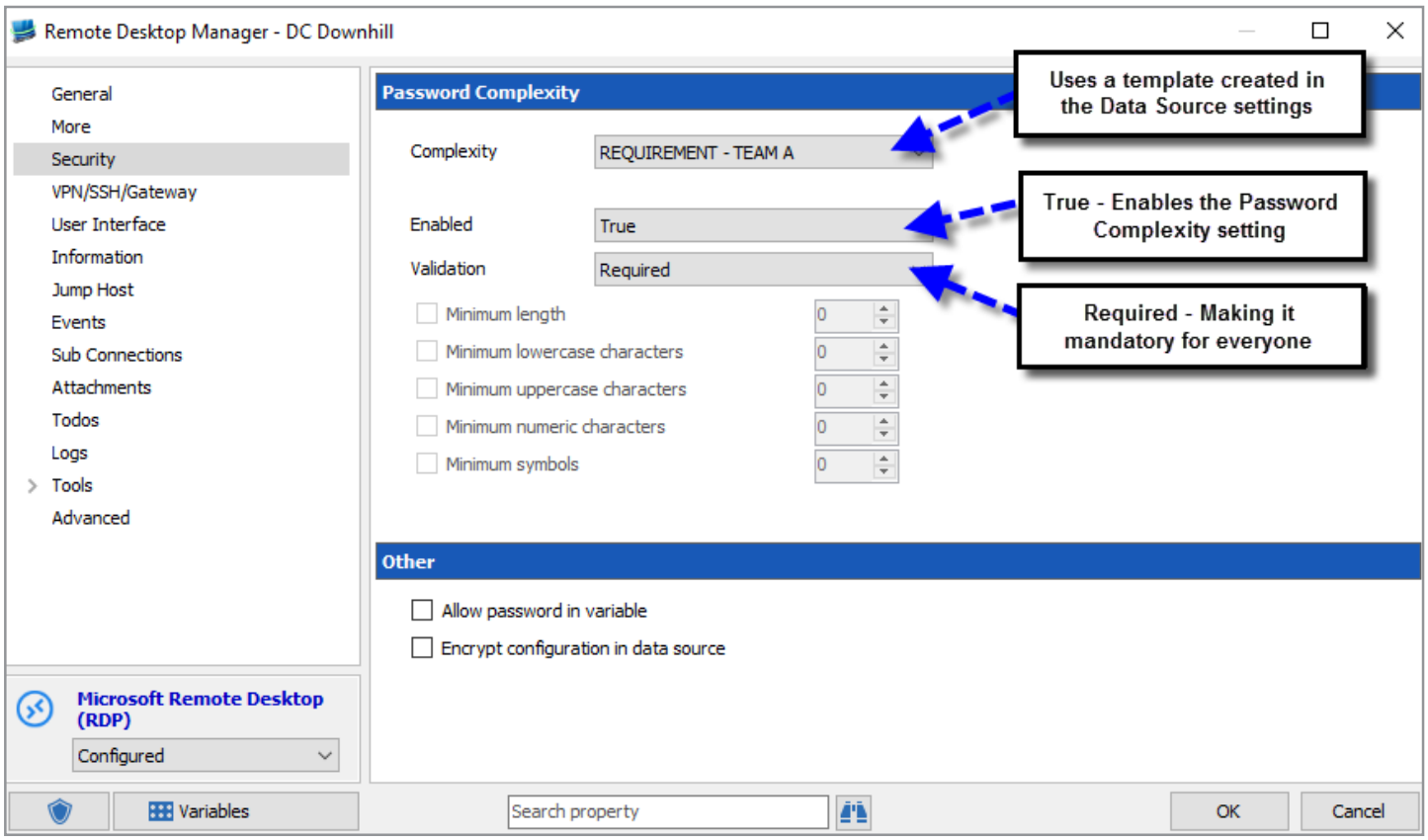
Next, enter a name for your new template and select your specific requirements, including the minimum password length and the minimum number of lowercase characters, uppercase characters, numeric characters and symbols.



From there, edit one of your sessions; on the **Security** side menu, choose **Complexity** and select your template from the dropdown menu.

When the setting is enabled (True) and a user tries to change or create a password, one of the following will happen based on your settings:

- **Required:** the user must meet the pre-set requirements or the password will not be accepted.
- **Warn:** the user will get a warning that their proposed password fails to meet complexity requirements and that they should change it. Users who choose to ignore this warning may do so, only to incur your wrath later on.
- **Inherit:** the password complexity rules will be inherited from the validation rules set on the parent folder (i.e. either "Required" or "Warn" as described above).



And that's it! It's like having your very own Sheldon Cooper to make sure everyone follows the Roommate agreement... and we all know how he is with rules. Bazinga!

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 here.