How to use One Time Password (OTP)

Devolutions

WE PULLED ANOTHER RABBIT OUT OF A HAT TO SIMPLIFY YOUR LIFE!

Remote Desktop Manager has done it again, we pulled another rabbit out of a hat to simplify your life! RDM has added **One Time Password (OTP)** to our long list of supported credential entries. You can now get all the benefit of the OTP without all the hassle that could come with managing multiple 2FA to authenticate yourself on different websites.

What is OTP?

An OTP (One Time Password) is an automatically generated numeric or alphanumeric string of characters that authenticates a user. The password is only valid for a single login session or transaction.

Benefits of OTP

There are several important benefits of using an OTP, including:
An OTP isn't a static password, so it's not vulnerable to replay attacks. As such, if a hacker steals an OTP that has been previously used to log into a service, it won't work again.
A second major advantage is that a user who uses the same password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker.

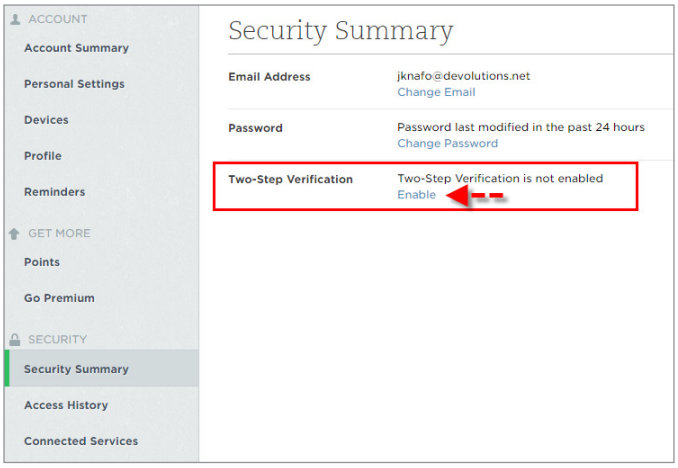
OTP in Remote Desktop Manager

OTP is a new credential entry type that integrates with the 2FA functionality, but first it must be enabled on the corresponding app. RDM will act as an intermediary and call the OTP provider to get the OTP code from any compatible source, then will allow you to copy/paste it where needed. This follows our strategy of RDM being your single pane of glass that integrates hundreds of technologies and hides a lot of the complexity.

Here's a list of some popular apps that support OTP :

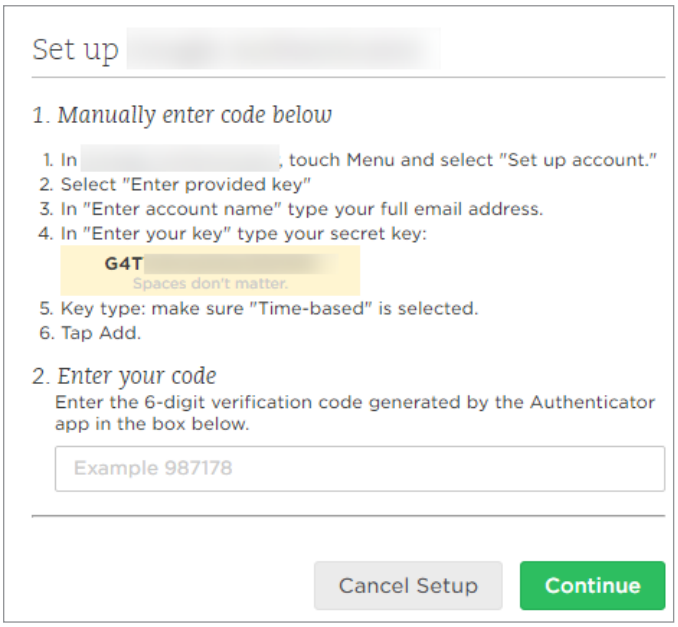
- AeroFS
- Box
- Dropbox
- Evernote
- Google Drive
- iCloud
- OneDrive
- Synology
- Tresorit
- Zetta.net

1. In the application of your choice (we have chosen Evernote for our example), start by finding the 2 Factor Authentication feature and click **Enable**.



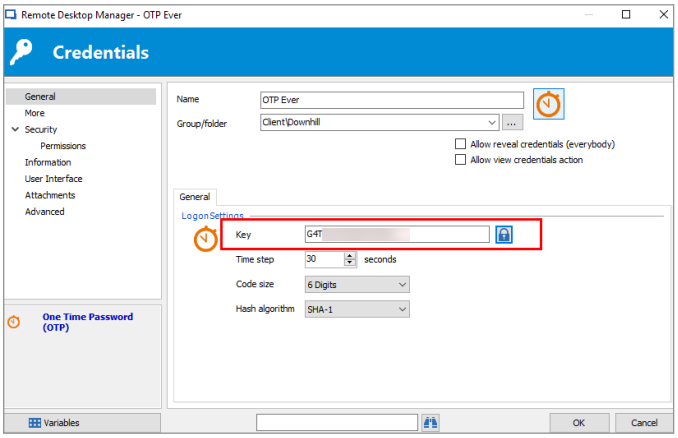
2. Choose to receive your security key via an application (not via text message).

3. When you receive the key, copy it to your clipboard.



4. Go into Remote Desktop Manager and create a new One Time Password (OTP) credential entry.

5. In the Key field, enter the security key that you copied in Step 3 (if there are any spaces in the key, make sure to remove them).

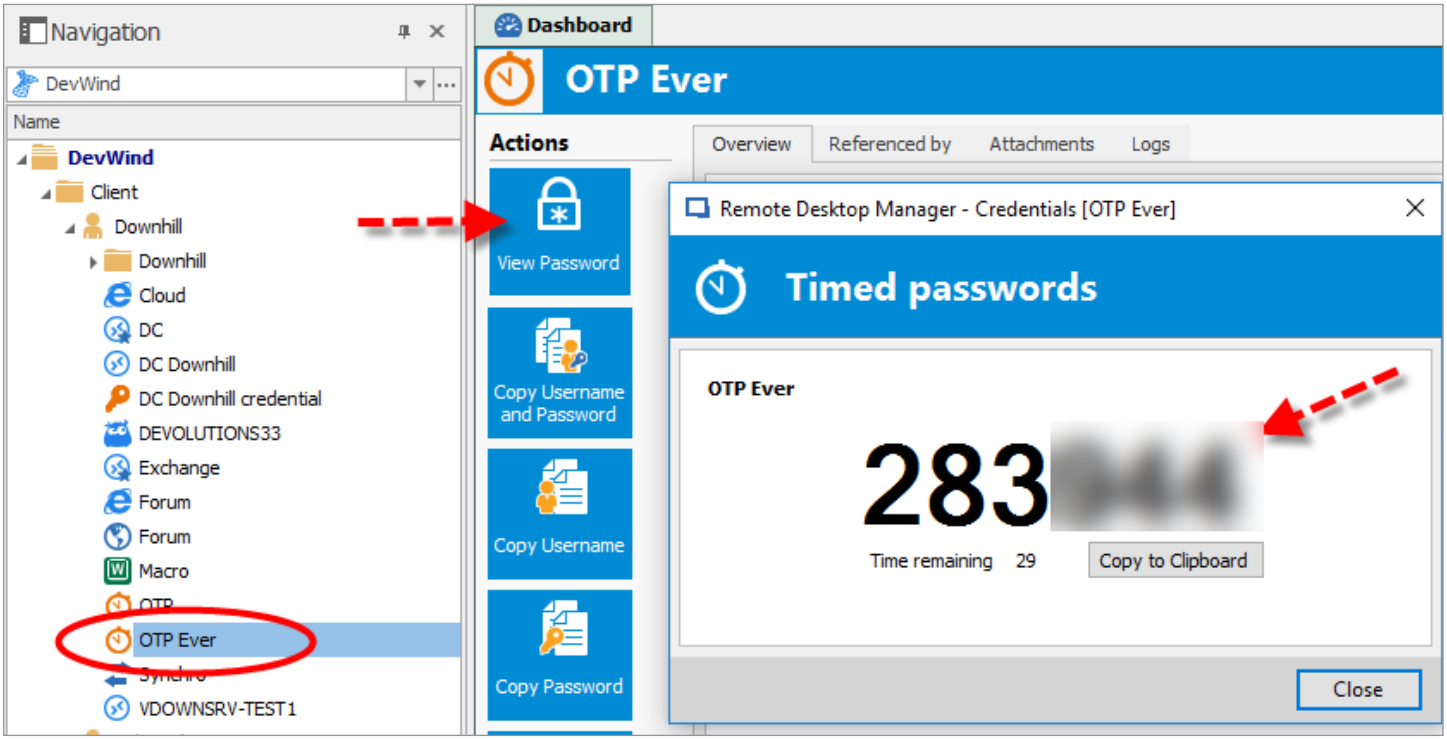


Now you're ready to generate a 6-digit code that will complete the OTP setup:

6. Close your entry.

7. From the navigation pane, select your entry and click **View Password.** The current OTP will be displayed.

8. Copy the 6-digit code into the app.



Now that 2FA and OTP are enabled, every time you log onto the app you'll be asked to enter an OTP. RDM will automatically get this for you when you select your OTP entry, and click **View Password**.

And that's it! It only takes a minute to setup, and you'll be more secure from intruders trying to steal your information. 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.

https://www.youtube.com/watch?v=vCo_y-qSLy8