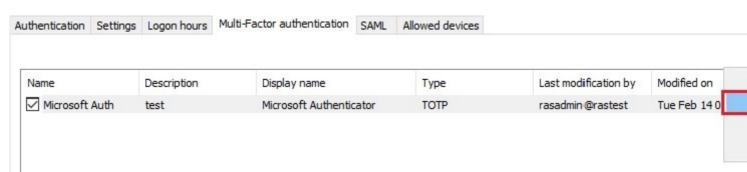


<u>Time-based One-Time Password (TOTP) Tolerance for Google and Microsoft Authenticator</u>

- Parallels Remote Application Server 19.1
- Parallels Remote Application Server 18.3

It is now possible to increase the one-time password validity. The new option called "**TOTP Tolerance**" is located at RAS Console > **Connection > Multi-factor authentication** tab:

Note: The option **TOTP Tolerance** can be set in the RAS console starting from v18. Starting from v19.2, **TOTP Tolerance** can be set to Microsoft Authenticator.



|| Parallels

Display name: Google Authenticator

2/14/2023

O Do not allow Authentication

User enrollment

Status: Enabled

Allow

O Allow until

Date:

When using Time-based One-time Password (TOTP) providers, it is required to have both Connection Brokers and client devices' time synchronized with a global NTP Server (e.g. time.google.com).

Time;

Adding TOTP tolerance increases the one-time password validity which might have security implications.

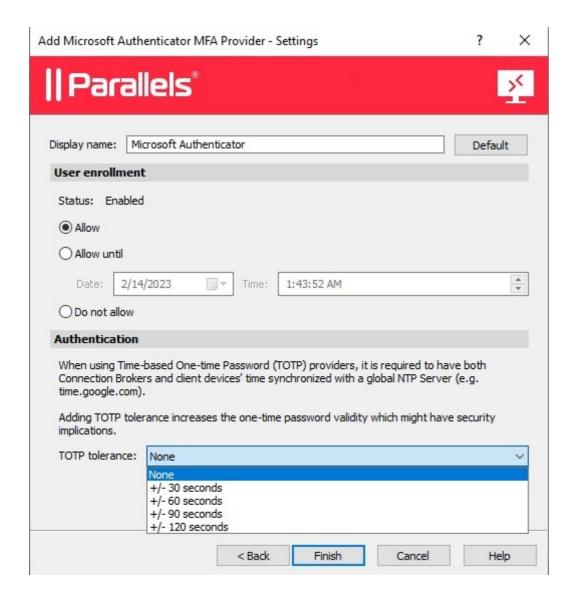
TOTP tolerance:

None

None

+/- 30 seconds
+/- 60 seconds
+/- 90 seconds
+/- 120 seconds





Note: Google authenticator is set to default display name when it is configured from RAS Management portal.

© 2024 Parallels International GmbH. All rights reserved. Parallels, the Parallels logo and Parallels Desktop are registered trademarks of Parallels International GmbH. All other product and company names and logos are the trademarks or registered trademarks of their respective owners.