

Google Authenticator Support

• Parallels Remote Application Server 19.1

Parallels RAS 19 added support for Google Authenticator, a free and easy Multi-factor authentication (MFA) solution.

How do I configure Parallels RAS to use Google Authenticator?

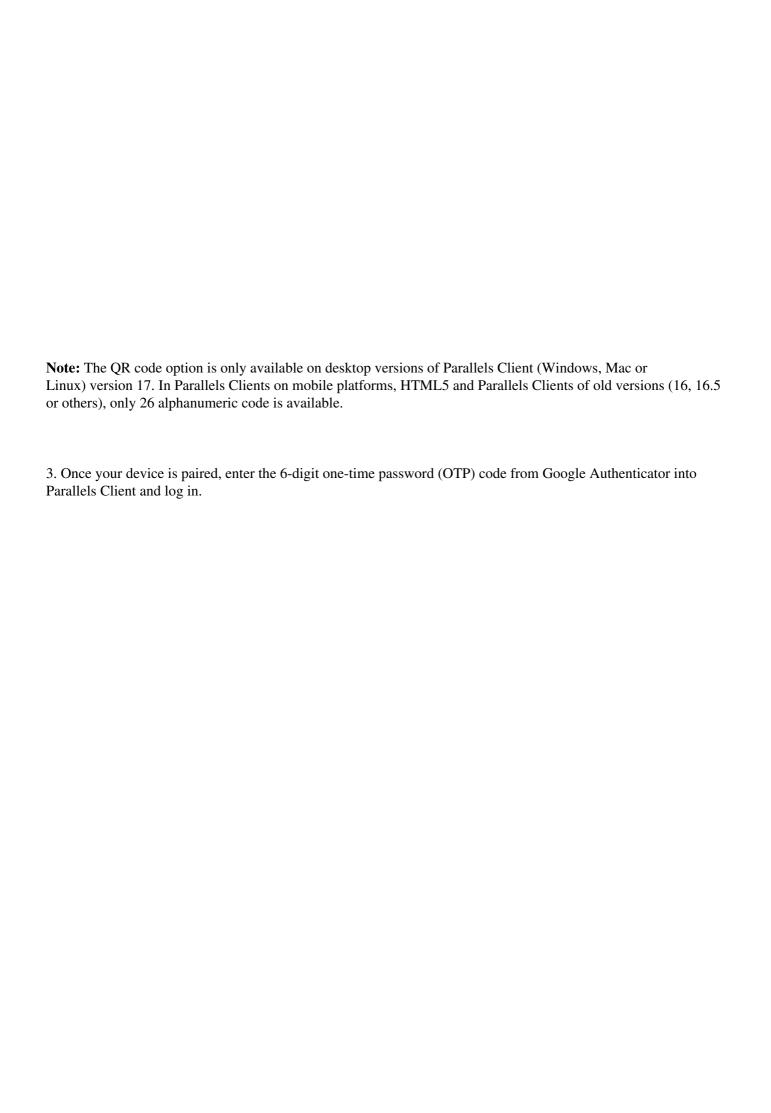
In the Parallels RAS Console:

- 1. Navigate to Connection > Multi Factor Authentication > TOTP > select Google Authenticator as a Provider.
- 2. Select Apply.

Note: When using Google Authenticator it is necessary to have both Connection Broker's and client devices' times synchronized with a **Global NTP** server like time.google.com.

What does an end user need to do in order to authenticate with Parallels RAS and Google Authenticator?

- 1. Install the Google Authenticator application on your mobile device from the Apple App Store, Google Play Market or others.
- 2. Pair your mobile application with RAS Farm and your AD account:
 - Open Parallels Client.
 - Log in using your AD credentials.
 - Enter the 26 alphanumeric code into the Google Authenticator application or scan the QR code.



To use Google Authenticator on a different device, a system administrator needs to reset the user's account, so the end user can run the pairing process again.
It is possible to reset a single account, all accounts or several accounts by importing them from a *.csv file into RAS Console > Connection > Multi Factor Authentication > Settings.

© 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.