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.

Note: The QR code option is only available on desktop versions of Parallels Client (Windows, Mac or Linux) version 17. In Parallels Clients on mobile platforms, HTML5 and Parallels Clients of old versions (16, 16.5 or others), only 26 alphanumeric code is available.

3. Once your device is paired, enter the 6-digit one-time password (OTP) code from Google Authenticator into Parallels Client and log in.

How do I reset my account?

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.**