Which multi-factor authentication (MFA) options does Parallels Secure Workspace support?

- Parallels Secure Workspace

Resolution

The **multi-factor authentication** can be configured per Workspace domain.

There are a couple of options available under **System Settings > Configure > User Connector: Multi-Factor Authentication**.

- **Workspace OTP: counter-based**
  This allows users to authenticate with the Google Authenticator App. Mind that other authenticator apps have limited support nowadays for counter-based OTP. Even Google's app suffers from a bug in recent versions.
- **Workspace OTP: time-based**
  For customers who don't use federated authentication to integrate with an external Identity Provider (IdP), this is the most commonly used option.
- **RADIUS**
  There is limited support to integrate with RADIUS.
- **Duo Security**
  This allows integration with the third-party solution Duo Security.

However, a lot of customers also set up a **federated authentication** using **SAML** or **OpenID**.

For example, the most common scenario seen in this case is users integrating with their **Microsoft Entra ID (Azure AD)** environment. This way, users log on using their Microsoft account to the Workspace. In this situation, it's possible to set up different multi-factor requirements on Azure.
