Built-in multi-factor authentication (MFA): which authenticator apps are compatible?

- Parallels Secure Workspace

Resolution

Any authenticator app that supports counter-based authentication (also called HOTP) or time-based authentication (also called TOTP) should work with the built-in multi-factor authentication.

For most use cases, it's highly recommended to **use time-based authentication**, as this is generally more secure and the token can be generated from different devices.

- **Android**: Authy, Google Authenticator, Microsoft Authenticator, Sophos Authenticator, ...
- **iOS**: Authy, Google Authenticator, Microsoft Authenticator, Sophos Authenticator, ...
- **Linux:** Authy
- **Windows Phone:** Microsoft Authenticator
- **Windows:** Authy (requires one-time phone verification, can be done by SMS)

Most authenticators require a phone number in some way. If the user does not have a mobile device available to use for MFA, they could also use a browser extension such as Authenticator.cc . When setting up MFA with this extension, you can either use its **Scan QR** feature or you can use the text **code (secret key)** on the MFA set-up screen (when the user logs in).

Note that it is worth evaluating different authenticator apps as there may be specific limitations or advantages. Some useful criteria for such an exercise are:

- Back-up.
- Synchronization.
- Multi-platform / operating system.
- Device type (smartphone, tablet, pc, ...).
- Does it require linking a phone number?
- Support for HOTP (counter-based) and/or TOTP (time-based) methods.
