Authentication in Parallels Secure Workspace

- Parallels Secure Workspace

Resolution

Parallels Secure Workspace has several layers of **authentication**, which are briefly summarized below.

LDAP / LDAPS

In all possible setups, an LDAP server is required.

The most basic implementation is by relying on **LDAP** servers, which are for most customers their **Active Directory Domain Controllers**.
This becomes more secure when these servers have an SSL/TLS certificate and when the Parallels Secure Workspace appliance is set to communicate with those servers in an encrypted way. This more secure implementation is referred to as **LDAPS**.

There is no exhaustive list of LDAP servers that can be used. Microsoft Active Directory domain controllers are actively supported. But for example, JumpCloud is known to work as well.

Multi-Factor Authentication (MFA)

This makes authentication more secure by adding at least one other way to authenticate the user.
For instance, besides their password, the users must **additionally** be able to provide a second way to prove their identity. This is typically a six-digit code, generated by an authenticator app.

Parallels Secure Workspace also offers two **built-in** mechanisms: **counter-based** and **time-based authentication**. When relying on the built-in MFA options, time-based is recommended.

There are also external mechanisms which are supported:

- RADIUS (Note: CHAP v2 is not supported).
- Duo Security

Federated Authentication

As soon as this federated authentication is enabled, Parallels Secure Workspace no longer handles the authentication of the user. Instead, it is handled by an external **Identity Provider (IdP).**
Support for **SAML** and **OpenID** has been implemented.

As the external IdP doesn't expose the passwords and the Microsoft Remote Desktop Protocol (RDP) doesn't support ticket/token based logins, this means users still need to enter their **password** in Awingu in order to be able to connect to application servers.

This first phase is called **pre-authentication.**

So in a second phase, the **credential-based** (username/password) authentication towards back-end systems (remote app, VDI, storage, ...) is replaced by a **user certificate-based** login mechanism to enable **Single Sign-On (SSO)**.