SSL accepted versions and cipher strength in Parallels Remote Application Server

- Parallels Remote Application Server

Information

Parallels Remote Application Server provides ability to enforce and use specific versions of SSL, as well as allowing custom configuration of cipher strength.

This article explains how to configure the cipher strength when a Gateway SSL or Direct SSL connection from a Remote Application Server Client is established against a Secure Client Gateway.

The configuration is available in **Secure Gateway** Properties and may be found under the SSL/TLS tab:

The following accepted SSL versions are available:

- TLS v1.2 Only (Strong)
- TLS v1.1 - TLS v1.2
- TLS v1 - TLS v1.2
- SSL v3 - TLS v1.2
- SSL v2 - TLS v1.2 (Weak)

These options allow an administrator to choose the preferred version and protect against vulnerabilities discovered in older versions of SSL.

In addition, it is possible to configure cipher strength. All the available options are based on OpenSSL standards, documented here.

As mentioned in the OpenSSL documentation, the cipher strength options provided within the Remote Application Server are as follows:

- **Low:** low encryption cipher suites, currently those that use 64 or 56-bit encryption algorithms but exclude export cipher suites.
- **Medium:** medium encryption cipher suites, currently some of those that use 128-bit encryption.
- **High:** high encryption cipher suites, currently those with key lengths larger than 128 bits, and some cipher suites with 128-bit keys.

An additional configurable part is inputting a custom cipher string:

A cipher string can be constructed by linking different cipher parameters from the list available here.

For example, the following cipher: **!SSLv2:ALL:!DH:!ADH:!EDH:!MD5:!EXPORT:@SPEED** has the following parameters defined:

- !SSLv2: Do not use SSL version 2
- ALL: Use all SSL ciphers in the default SSL stack
- !DH: Do not use DH ciphers
- !ADH: Do not use ADH ciphers
- !EDH: Do not use EDH ciphers
- !MD5: Do not use MD5 ciphers
- !EXPORT: Do not use EXPORT grade (weak) ciphers
- @SPEED: Order the cipher preference by speed

Documentation on ciphers and their possible configurations is available here:

https://www.openssl.org/docs/apps/ciphers.html

Detailed information about Cipher Suites is available in this article.

It is possible to check the current cipher strength for all gateways quickly in the **Information** pane > **Site Information** tab: