How to disable particular SSL ciphers

- Parallels Remote Application Server

Information

In case you need to disable a particular SSL cipher, it can be done by adjusting it in RAS Console > Farm > Gateways > right-click on a Gateway > Properties > SSL/TLS > Cipher Strength.

For example, you want to use Medium Cipher Strength, excluding the **TLS_RSA_WITH_3DES_EDE_CBC_SHA** cipher.

Here how it's done:

1. Copy the Medium Cipher string:

   ```
   ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
   ```
2. Add the following after **!EXP:** - **!DES-CBC3-SHA:**
3. End result should be like that:

   ```
   ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:!DES-CBC3-SHA:RC4+RSA:+HIGH:+MEDIUM
   ```

In general, you should get the OpenSSL name of the cipher suite, and insert it into a string with an "!" before the name. OpenSSL name list for cipher suites is available here.
