TLS issue with recent OS for older SMP Gateway software versions

SMP Gateway automation platforms running versions 6.1R7 and older may have a SSL/TLS secure connexion issue with recent versions of Windows 10, Windows 11, Windows Server 2016 and Windows Server 2019 operating systems (OS), where RC4 cipher suites are disabled by default.

Contents

Quebec City
1990 5th Street
Suite 220
Levis, Quebec
Canada G6W 5M6
Phone: +1.418.830.5800
Toll free: +1.877.834-0009
Fax: +1.514.227.5256

Montreal
1155 Boulevard Robert-Bourassa
Suite 1215
Montreal, Quebec
Canada H3B 3A7
Phone: +1.514.845.6195
Toll free: +1.877.834-0009
Fax: +1.514.227.5256

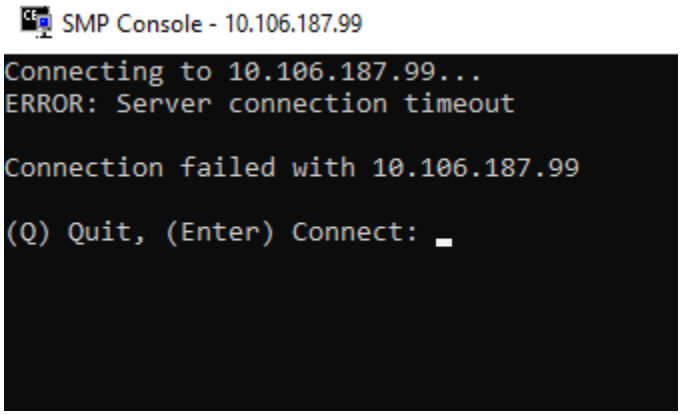
www.Eaton.com/smartgrid

Template: EAS-SA QF-MKT01 Rev.05
2022/09/15

Powering Business Worldwide

The problem

The symptom of the problem occurs with a communication timeout with the SMP Gateway automation platform. The same issue does not happen for an SMP Gateway running a more recent software version.

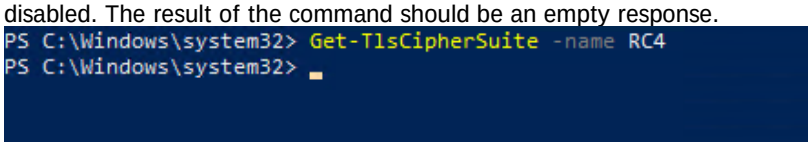


The solution

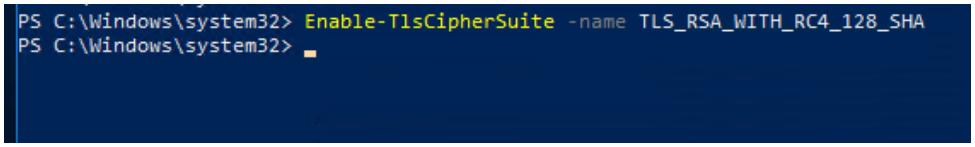
The solution to this problem is to enable the TLS_RSA_WITH_RC4_128_SHA cipher suite (also called RC4 cypher suite in this document) on the Windows platform used on the computer.

To do so:

1. Launch the Windows PowerShell in command-line mode, with administrator rights.
2. Enter the command: `Get-TlsCipherSuite -name RC4` to verify that RC4 cipher suite is disabled. The result of the command should be an empty response.

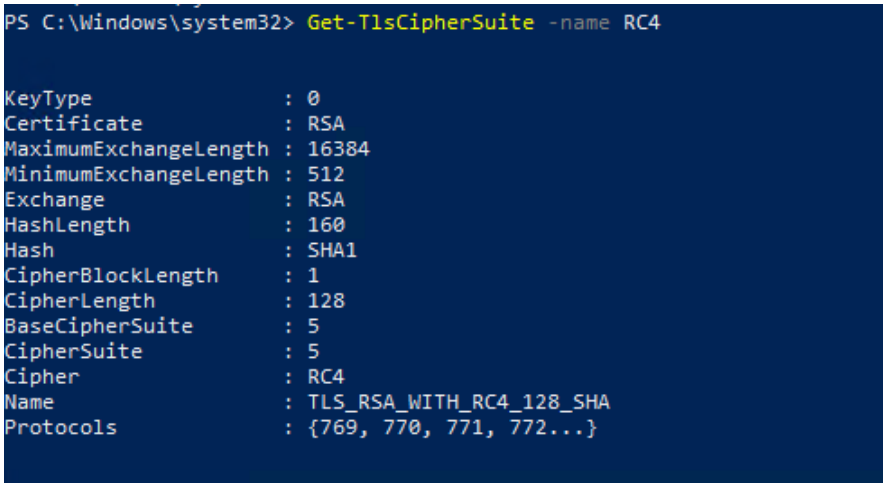


3. Enter the command : `Enable-TlsCipherSuite -name TLS_RSA_WITH_RC4_128_SHA` to enable the RC4 cipher suite. The cipher suite will be added at the lowest priority which ensures that it will be used in the last resort where every other cipher suites are not available at the SSL/TLS server side. The result of the command is an empty response, which is normal.



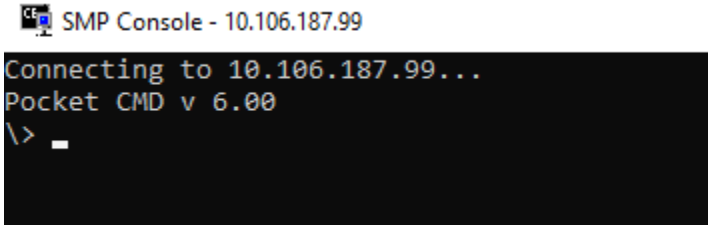
Note: If error 0xD0000022 is returned, it indicates inappropriate authorization level.

4. Enter the command: `Get-TlsCipherSuite -name RC4` to verify that RC4 cipher suite is now enabled. The cipher suite information should be displayed.



5. The command: `Get-TlsCipherSuite` (without arguments) will list all enabled cipher suites; it will confirm that the RC4 cipher suite is at the very end of the priority list. If you don't see it, reboot the computer to finalize the RC4 cipeher suite activation and check again.

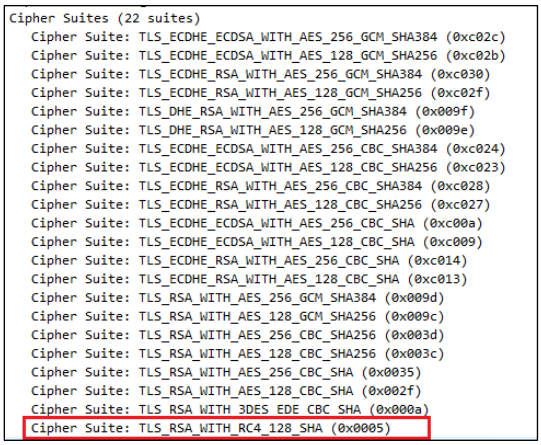
The secured connexion to the SMP Gateway automation platform will now be established without the problem.



The consequences of enabling the RC4 cypher suite

Even if the weaker RC4-based cipher suite is enabled, SSL/TLS connection to more recent servers will always use the stronger cipher suites available, in the priority order configured in the Windows platform; RC4 cypher suite will be used in the last resort.

For instance, the following image shows the partial content of the proposed cipher suites in Windows 10 for a TLS 1.2 connection ("Client Hello" handshake content). The RC4 cipher suite is at the bottom of the list.



Long term solution

Upgrading the SMP Gateway device(s) to a more recent version than 6.1R7 will solve the issue permanently. If you do so, we recommend that you disable the RC4 cipher suite, to return to the Windows default settings.

To do that:

1. Launch the Windows PowerShell in command-line mode, with administrator rights.
2. Enter the command: `Disable-TlsCipherSuite -name TLS_RSA_WITH_RC4_128_SHA` to disable the RC4 cipher suite.
3. Enter the command: `Get-TlsCipherSuite -name RC4` to confirm that the RC4 cypher suite is removed; the list should be empty.

```
PS C:\Windows\system32> Disable-TlsCipherSuite -name TLS_RSA_WITH_RC4_128_SHA
PS C:\Windows\system32> Get-TlsCipherSuite -name RC4
PS C:\Windows\system32>
```

Getting Assistance

If you have any questions regarding the performance, application, testing or repair of this or any other component of the SMP product line, do not hesitate to contact us. Our staff will be happy to assist you.

Technical Support
Eaton's Energy Automation Solutions

Email: eas-support@eaton.com
Phone: +1.877.834-0009 or +1.800.815-2258

Business hours are from 8 a.m. and 5 p.m. CST, Monday to Friday.