Configuring SSL/TLS for QlikView

Important Warning

Some changes will be done to the underlying Operating System [OS]. Making any changes to the OS could affect it or other applications relying on specific settings. Always make sure to have a full understanding of what ramifications a change could have, and at the very least make sure to have up to date backups of all important data. It is recommended that any changes should first be tested out on a staging environment.

Introduction

There are many SSL/TLS related settings available for the .Net Framework in Windows. Apart from enabling and disabling specific protocol versions, other minor configurations can be done as well. With the new SR16 release, QlikView 11.20 has improved support for TLS, which has previously been introduced in QlikView 12.00 SR1.

There are different ways of configuring the SSL/TLS settings. This document will describe three approaches. They are to be regarded as reference only.

Support matrix

The following matrix shows which releases of QlikView support which SSL/TLS protocols

Release	TLS v1.0	TLS v1.1	TLS v1.2
QlikView 11.20 SR15 or older	🟩	🟥	🟥
QlikView 11.20 SR16 or newer	🟩	🟩	🟩
QlikView 12.00	🟩	🟥	🟥
QlikView 12.00 SR1 or newer	🟩	🟩	🟩
QlikView 12.10 or newer	🟩	🟩	🟩

Legend:

- Green = Supported
- Red = Not Supported

It is also important to note that when changes have been made to the Windows registry, it might be necessary to reboot the server, *sometimes more than once*, to have the settings applied correctly. The need to reboot seems to vary between Windows OS's, thus Qlik recommends that the Windows OS is of as new release as possible.

Configuring SSL/TLS manually

To change which SSL/TLS protocols are enabled, the Windows registry needs to be modified. The following registry paths point towards the different versions:

- `HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0`

- `HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0`
- `HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0`
- `HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1`
- `HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2`

To enable, for example, TLS v1.1, the following changes needs to be done

1. Open the registry editor as administrator on the server
2. Navigate to the registry path for TLS v1.1 per the bullet list above. Create it if it does not already exist.
3. Add a new key named "Server"
4. Navigate into the newly created "Server" key
5. Create a DWORD key named "Enabled"
6. Set the "Enabled" key value to 1

Configuring SSL/TLS using PowerShell

To avoid making mistakes while editing the Windows registry manually, Qlik has provided a PowerShell script to make the necessary changes automatically. The script is for reference only and is not supported. Before using it in any environment it should be reviewed and approved by your IT admin.

To run the script, start a PowerShell as administrator. Since the script is a reference implementation it is not signed. Thus, the environment may need to allow unsigned scripts to be executed. Should this not be an option, the reader will need to either create their own script and sign it per their own internal best practices, or sign the reference script provided by Qlik.

Allowing unsigned scripts to be executed can be accomplished by running the following command in the PowerShell window:

```
set-executionpolicy unrestricted
```

Then navigate to the folder where the script "tls_config.ps1" is stored, and run it.

```
./tls_config.ps1
```

The script will by default set and enable TLS v1.0, v1.1 and v1.2. This can be controlled at execution using flags. Code review the script to see all available flags that can be set.

Run the TLS script with flags for enabling only TLS v1.2 and disable all others:

```
./tls_config.ps1 -ssl3 0 -tls1 0 -tls11 0 -tls12 1
```

Configuring SSL/TLS using other tools

There are GUIs available in Windows to manage the SSL/TLS settings, which can be used for the same results.

There are also 3rd party applications that can be used. One example being "IIS Crypto" from Nartac. Only users experienced in the correct use and implementation of these applications and instructions should attempt to use them.