TLS Configuration

CipherSpecs and SNI

QMgr CipherSpec ordering in qmgr

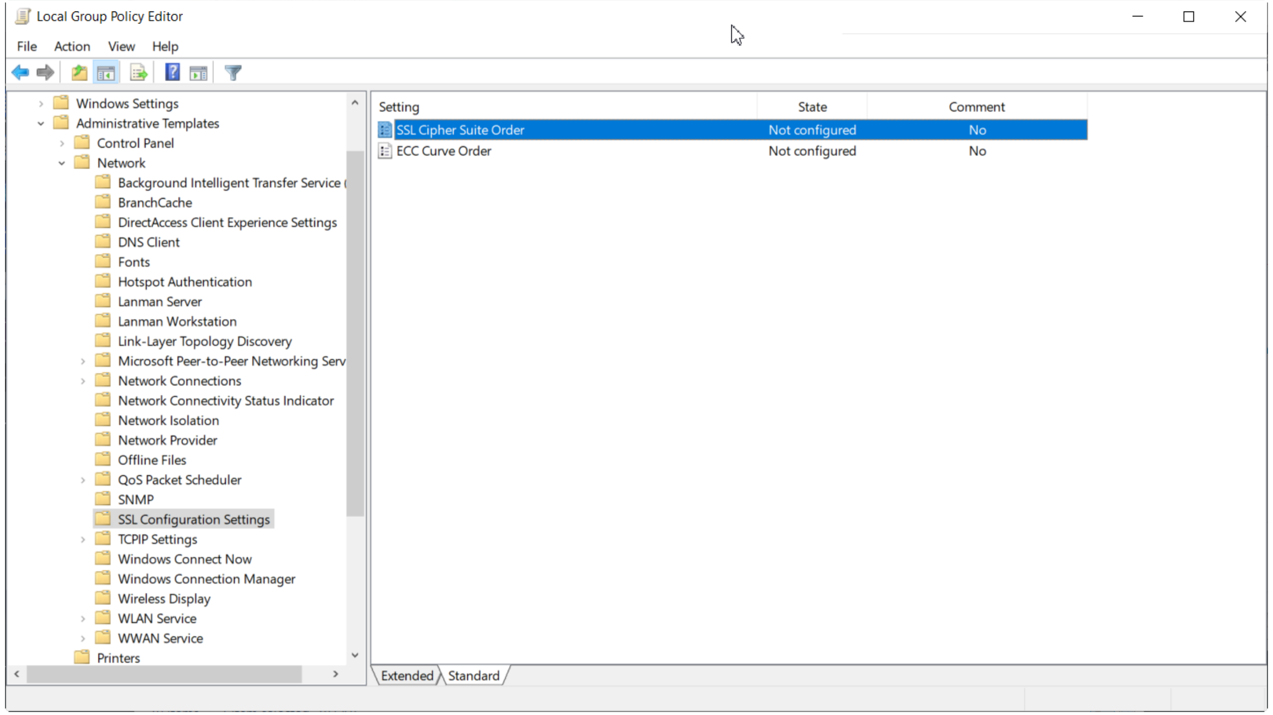
- https://www.ibm.com/docs/en/ibm-mq/9.2?topic=cipherspecs-cipherspec-order-in-tls-handshake
  - Lists the ordering used in 9.2 and previously
  - Shows how to change the ordering and allowed lists
- Tool to test connections is at https://testssl.sh/

.Net client CipherSpecs

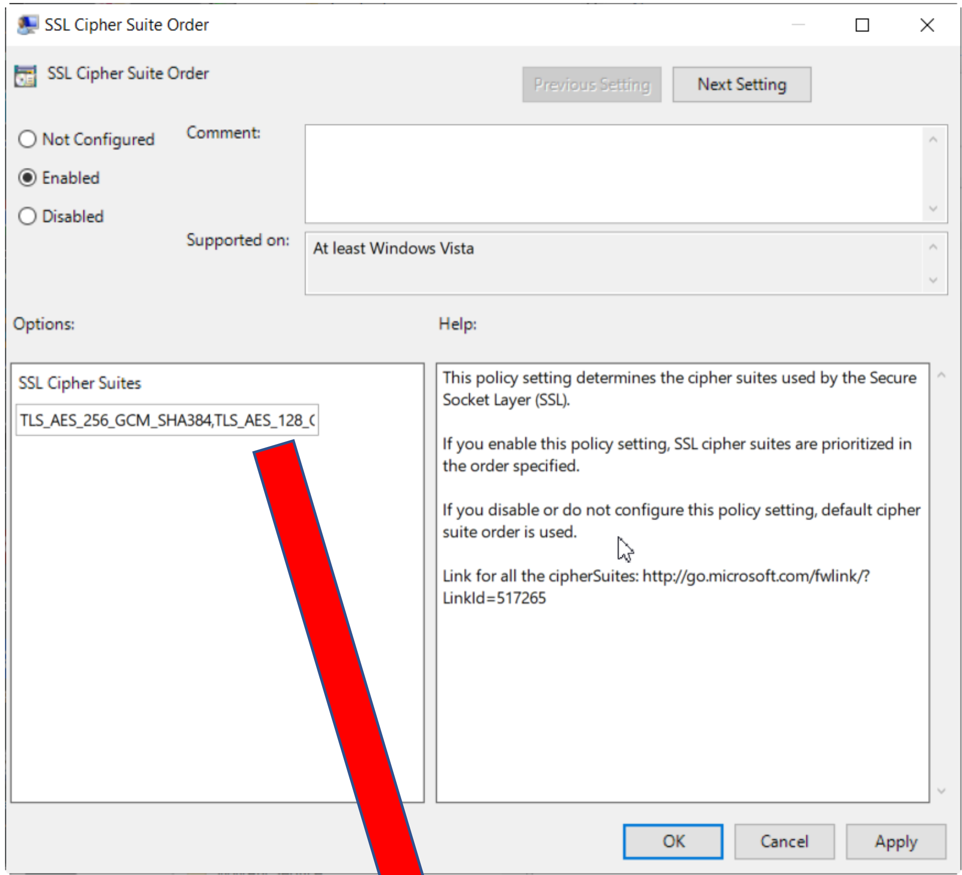
- Mapping MQ CipherSpecs to Windows
  - https://www.ibm.com/docs/en/ibm-mq/9.2?topic=client-cipherspec-mappings-managed-net

- Modifying Windows list
  - https://docs.microsoft.com/en-us/windows-server/security/tls/manage-tls

Windows Group Policy Editor



Setting	State	Comment
SSL Cipher Suite Order	Not configured	No
ECC Curve Order	Not configured	No



○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

SSL Cipher Suites

TLS_AES_256_GCM_SHA384,TLS_AES_128_(

Help:

This policy setting determines the cipher suites used by the Secure Socket Layer (SSL).

If you enable this policy setting, SSL cipher suites are prioritized in the order specified.

If you disable or do not configure this policy setting, default cipher suite order is used.

Link for all the cipherSuites: http://go.microsoft.com/fwlink/?LinkId=517265

Group Policy Editor ➔ Admin Templates ➔ SSL Config Settings ➔ SSL Cipher Suite Order

TLS_AES_256_GCM_SHA384,TLS_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_NULL_SHA256,TLS_RSA_WITH_NULL_SHA,TLS_PSK_WITH_AES_256_GCM_SHA384,TLS_PSK_WITH_AES_128_GCM_SHA256,TLS_PSK_WITH_AES_256_CBC_SHA384,TLS_PSK_WITH_AES_128_CBC_SHA256,TLS_PSK_WITH_NULL_SHA384,TLS_PSK_WITH_NULL_SHA256

Outbound SNI

- Needed for connecting TO an OpenShift environment
- C: mqclient.ini, qm.ini (Dist), TransportSecurity (z/OS) (9.2.1)
  - SSL stanza: OutboundSNI=Hostname
- JMS: default behaviour sets hostname
- .Net: Set property: XMSC_WMQ_OUTBOUND_SNI (9.2.4)
  - Values: XMSC_WMQ_OUTBOUND_SNI_HOSTNAME, XMSC_WMQ_OUTBOUND_SNI_CHANNEL, XMSC_WMQ_OUTBOUND_SNI_ASTERISK