Bloomberg FIX Configuration Guidelines

Connectivity

Port

All new sessions and compliant existing sessions use the following port:

8228

IP Addresses

The range for valid Bloomberg FIX target IPs for sessions which comply with the updated standards is shown below. The actual IP assigned to a session is based on several criteria including product and workflow. Firewall adjustments may need to be made.

Internet: 69.191.230.0 – 69.191.230.127 = CIDR: (69.191.230.0/25)
69.191.198.0 – 69.191.198.127 = CIDR: (69.191.198.0/25)

Dedicated (Leased): 160.43.172.0 – 160.43.172.127 = CIDR: (160.43.172.0/25)

Session Disablement

1) Configurations for sessions that have not been "Active" in 3 months (95 days) will be deactivated

IP Whitelisting and Deletion

1) The potential source(s) of all inbound sessions must be "whitelisted" to permit access
2) The potential target(s) of all outbound sessions must be "whitelisted" to permit access
3) Session IPs that have not been "Active" in 6 months (188 days) will be deleted from the whitelist; this will be enforced beginning 4/3/2017)

What constitutes an "Active" Session or IP

Bloomberg requires that clients, or their providers, maintain an "Active" status for all FIX Session-related connectivity. This is achieved by successfully connecting each FIX session from each relevant IP address in order to remain active in our registry. This requirement applies to all sessions and IP addresses, including those that may be associated with disaster recovery (DR) or "backups." A successful connection consists of a FIX logon message and the associated confirming heartbeat. Application messages aren't required.

Authentication / Encryption

Basic Requirements

1) TLS Mutual Authentication is required for all internet connections (requires the use of certificates)
2) TLS Mutual Authentication is required for all dedicated/private network connections (requires the use of certificates)
3) TLS version levels, ciphers, and hashing algorithms conform to established standards (SSL not supported)

Cypher Strength / Encryption Standard

The following encryption standards are allowed. They are listed in order of strength from top and it is advised that the strongest possible be used. Note: The "Minimum" standard expires on 1/31/2018.

Preferred: (In order of preference)

Descriptor	Expiration Date (Bloomberg)	Auth Algo	Key Exchange	Cypher Mode	TLS Level	Symmetric Encryption Algorithm	Hash
TLS_ECDHE_RSA_AES_256_GCM_SHA384	12/31/2019	RSA	ECDHE	GCM	1.2	AES 256-Bit	SHA-384
TLS_ECDHE_RSA_AES_256_CBC_SHA384	12/31/2019	RSA	ECDHE	CBC	1.2	AES 256-Bit	SHA-384
TLS_ECDHE_RSA_AES_128_CBC_SHA256	12/31/2019	RSA	ECDHE	CBC	1.2	AES 128-Bit	SHA-256
TLS_RSA_WITH_AES_256_CBC_SHA	12/31/2019	RSA	RSA	CBC	1.2	AES 256-Bit	SHA-1
TLS_RSA_WITH_AES_128_CBC_SHA	12/31/2019	RSA	RSA	CBC	1.2	AES 128-Bit	SHA-1

Minimum: (In order of preference)

Descriptor	Expiration Date (Bloomberg)	Auth Algo	Key Exchange	Cypher Mode	TLS Level	Symmetric Encryption Algorithm	Hash
TLS_RSA_WITH_AES_256_CBC_SHA	1/31/2018	RSA	RSA	CBC	1.0	AES 256-Bit	SHA-1
TLS_RSA_WITH_AES_128_CBC_SHA	1/31/2018	RSA	RSA	CBC	1.0	AES 128-Bit	SHA-1