Important Notice
Fixed Income Clearing Corporation - MBSD

MBS #:	MBS1326-24
Date:	April 19, 2024
To:	Mortgage-Backed Securities Participants and Members
Category:	Connectivity Security Requirements and Standards
From:	DTCC Chief Information Security Officer and President, Clearing and Securities Services
Attention:	Technology Risk Officers and Managers, Technical Connectivity Managers
Subject:	FICC MBSD Secure Connections

Amidst the increasing cyberattacks in the financial services industry, DTCC upholds its role to protect the global financial markets, which includes safeguarding the security, integrity, and confidentiality of our data and our systems. As a result, DTCC enforces the connectivity and data encryption requirements and standards for IBM MQ, Connect:Direct, previously known as Network Data Mover (NDM), Secure File Transfer Protocol (sFTP), and File Transfer Protocol (FTP) protocols to ensure that only sufficiently secured connections are allowed access to DTCC systems.

Important Dates

Compliance to DTCC security standards is mandatory by December 31, 2024. Any connections that are non-compliant will be subject to disconnection.

Action required:

Participants and members with non-compliant connections must take one or more of the actions below to avoid **connectivity disruption.** Please review the Security Requirements and contact our dedicated connectivity team immediately at sccp@dtcc.com with the following information to review, plan, and implement changes required to ensure compliance and avoid discontinuation of service:

- IBM MQ – provide channel name
- FTP/SFTP – provide IP address
- NDM – provide node name or IP address

Security Requirements and Remediation

IBM MQ

To comply with DTCC's security requirement clients will need to perform:

1. Configuration of TLS (Transport Layer Security) Certificate
    a. Ensure that the intermediate and root signing certificates are from the DTCC approved Certificate Authorities (DTCC's CA List) found on the Learning Center. Self-signed and private-signed certificates are not allowed.
    b. Ensure that the certificate has a signing algorithm of SHA256 or above. SHA1 certificates are not allowed.
    c. Ensure that the chosen intermediate signing certificate's serial number matches what is on DTCC's CA list. Some certificates have common CN= values but different serial numbers.
2. Configuration of Cipher Spec.
    a. Cipher Specs must be compatible with TLS 1.2 protocol. Supported values are indicated below and can also be found on IBM's website. It is recommended to use AES values of 256 instead of 128.
        - *TLS_RSA_WITH_AES_256_GCM_SHA384*
        - *ECDHE_RSA_AES_256_GCM_SHA384*
        - *TLS_RSA_WITH_AES_256_CBC_SHA256*
        - *ECDHE_ECDSA_AES_256_CBC_SHA384*
        - *ECDHE_RSA_AES_256_CBC_SHA384*
        - *TLS_RSA_WITH_AES_128_GCM_SHA256*
        - *ECDHE_RSA_AES_128_GCM_SHA256*
        - *TLS_RSA_WITH_AES_128_CBC_SHA256*
        - *ECDHE_ECDSA_AES_128_CBC_SHA256*
        - *ECDHE_RSA_AES_128_CBC_SHA256*

Changes detailed above are synchronous changes, (i.e., requires DTCC and the client to make the changes at the same time), clients are required to schedule the upgrade with the DTCC Connectivity team to ensure the upgrade can be performed seamlessly. Inbound and outbound tests within the MQ application is required to confirm that changes have been correctly applied on both ends. MQ related changes need at least 2 weeks advance notice.

Connect:Direct, previously known as Network Data Mover (NDM)

1. NDM must have Secure+ installed.
2. Configuration of TLS Certificate
    a. Ensure that the intermediate and root signing certificates are from the DTCC approved Certificate Authorities (DTCC's CA List) available on the DTCC Learning Center. Self-

signed and private-signed certificates are not allowed.

b. Ensure that the certificate has a signing algorithm of SHA256 or above. SHA1 certificates are not allowed.

c. Ensure that the chosen intermediate signing certificate's serial number matches what is on DTCC's CA list. Some certificates have common CN= values but different serial numbers.

3. Configuration of Cipher Spec.

    a. Cipher Specs must be compatible with TLS 1.2 protocol. Supported values are indicated below and can also be found on IBM's website. It is recommended that clients use AES values of 256 instead of 128.

        - *TLS_ECDHE_ECDSA_W_AES_256_GCM_SHA384*
        - *TLS_ECDHE_ECDSA_W_AES_256_CBC_SHA384*
        - *TLS_ECDHE_RSA_WIT_AES_256_GCM_SHA384*
        - *TLS_ECDHE_RSA_WIT_AES_256_CBC_SHA384*
        - *TLS_RSA_WITH_AES_256_GCM_SHA384*
        - *TLS_RSA_WITH_AES_256_CBC_SHA256*
        - *TLS_ECDHE_ECDSA_W_AES_128_GCM_SHA256*
        - *TLS_ECDHE_ECDSA_W_AES_128_CBC_SHA256*
        - *TLS_ECDHE_RSA_WIT_AES_128_GCM_SHA256*
        - *TLS_ECDHE_RSA_WIT_AES_128_CBC_SHA256*
        - *TLS_RSA_WITH_AES_128_GCM_SHA256*
        - *TLS_RSA_WITH_AES_128_CBC_SHA256*

Changes above are synchronous changes, i.e., requires DTCC and the client to make the changes at the same time, clients are required to schedule the upgrade with the DTCC Connectivity team over a weekend to ensure the upgrade can be performed seamlessly. Inbound and outbound tests within the NDM application is required to confirm that changes have been correctly applied on both ends. NDM related changes need at least 2 weeks advance notice.

SFTP

The following key exchange algorithms, ciphers, and MACs must be used:

Key Exchange Algorithms:

ecdh-sha2-nistp521
ecdh-sha2-nistp384
ecdh-sha2-nistp256
diffie-hellman-group18-sha512
diffie-hellman-group16-sha512
diffie-hellman-group14-sha256

Ciphers
aes256-ctr
aes256-cbc
aes192-ctr
aes192-cbc

MACs
hmac-sha2-512
hmac-sha2-256

This is a client-side change only, which means that DTCC servers have been upgraded to accept the more secure encryption key exchange algorithms, ciphers, and MACs listed below. Clients are recommended to contact DTCC Connectivity, sccp@dtcc.com, to confirm that the upgrade has been performed so validation can be performed.

FTP

Unencrypted FTP will not be supported and must be converted to SFTP connectivity method set up.

Clients on this setup will need to get in touch with DTCC's Client Connectivity Services team to perform a migration to a compliant protocol.

Migration to a compliant protocol can take up to 3 months due to new network and protocol configurations required. Clients are advised to reach out as soon as possible to ensure that your Production connectivity is not impacted.