SSH Ciphers Upgrade Meeting

Bank of America

Go Paperless! Please do not print this document.

Receiving this document electronically reduces greenhouse gas emissions (GHG).
Each page not printed avoids 15 grams of CO_2.

Agenda

Bank of America
Merrill Lynch

- Scope of the Change
- Actions Needed
- Technical Support
- Testing Approach
- Accept a Host Key (Example)
- Researching Support Ciphers/MACs
- Appendix (URLs)

SSH Cipher Upgrade

Bank of America
Merrill Lynch

Scope:

Bank of America is strengthening its secure connections by changing the SSH Host Key and removing obsolete Ciphers and MACs**.**

Not in Scope:

You are not required to migrate to a different URL.

Background:

SSH (Secure Shell) is a protocol (based on: RFC 4251-RFC 4256 standards) used to transfer files across a secure channel between two computers. It is very flexible and has been implemented hundreds of times on most modern computer platforms. The flexibility has resulted in ever growing list of encryption Ciphers and MAC (algorithms) added to promote ease in connections between two completely different computers.

Actions Needed

Bank of America
Merrill Lynch

- Accept a new SSH host key (2048 bits)
  - Clients simply accept a new key when connecting to B2Bi.
- Three encrypting ciphers: aes256-ctr; aes192-ctr; aes128-ctr.
  - If clients already have these ciphers in their data transmission software; no further action needed.
- One MAC algorithm is supported: hmac-sha2-256.
  - Same action as for ciphers.

Support

Bank of America
Merrill Lynch

Please provide your User-ID when contacting support:

Hotline: 855-515-6600 Option 2
DTS.Service.Desk@bankofamerica.com

Testing

Bank of America
Merrill Lynch

Each client can “test” their SSH Connectivity by simply doing a “sign-in” to a strong URL.

For testing purposes, there is a strong URL on each system:

- **b2b32.bankofamerica.com**
- **elink-sftp-p2.bankofamerica.com**

Action: Doing a sign-in, checks the SSH Host Key and performs the Cipher/MAC negotiation.

Result: On the command line, you should reach the prompt line. In a GUI, the client will display the default directory.

Accepting a SSH Host Key

Bank of America
Merrill Lynch

SFTP Client (Putty)

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.

The server's rsa2 key fingerprint is:

ssh-rsa 2048 2e:1d:7a:fc:d5:c4:da:d5:

if you trust this host, enter "y" to add the key to cache and carry on connecting. If you want to carry on connecting just once, without adding the key to the cache, enter "n".

If you do not trust this host, press Return to abandon connection.

Store key in cache? (y/n)

login as:

Enter password:

Remote working directory is /

psftp>

Researching Ciphers and MACs

Bank of America Merrill Lynch

In this example, the WinSCP (v5.13.1 released March 28, 2018) client software includes many ciphers and MACs. The latest version WinSCP 5.15.3 was released July 21, 2019.

WinSCP supports the following ciphers, MAC algorithms, and Hostkey types with SSH:

Ciphers: 3des-cbc, 3des-ctr, des-cbc, des-cbc@ssh.com, **aes128-ctr, aes192-ctr, aes256-ctr**, aes128-cbc, aes192-cbc, aes256-cbc, rijndael-cbc@lysator.liu.se, arcfour128, arcfour256, blowfish-cbc, blowfish-ctr, chacha20-poly1305@openssh.com

Message authentication codes (MACs): hmac-md5, hmac-sha1, hmac-sha1-96, **hmac-sha2-256**, hmac-md5-etm@openssh.com, hmac-sha1-etm@openssh.com, hmac-sha1-96-etm@openssh.com, hmac-sha2-256-etm@openssh.com

Bank of America Merrill Lynch

URLs

Environment	URL	Primary IP	Secondary IP
UAT	b2b02u.bankofamerica.com elink-ftps8-uat.bankofamerica.com	171.162.109.30	171.162.108.30
UAT	elink-sftp-u.bankofamerica.com	171.162.109.32	171.162.108.32
Production	b2b22.bankofamerica.com elink-ftps8.bankofamerica.com	171.162.110.17	171.162.111.17
Production	elink-sshftp.bankofamerica.com	171.161.160.130	171.159.64.130
Production	b2b32.bankofamerica.com	171.162.110.18	171.162.111.18

URLs

Bank of America Merrill Lynch

URLs

Environment	URL	Primary IP	Secondary IP
UAT	ftpsqa.b2b.ml.com b2b02u.bankofamerica.com	171.162.109.30	171.162.108.30
Production	ftps.b2b.ml.com	171.162.110.117	171.162.108.117
Production	elink-sftp-p2.bankofamerica.com	171.162.110.118	171.162.108.118

FAQ

Bank of America Merrill Lynch

- Must we migrate to the strong URL? **No, it was provided to assist your testing. If you do migrate to a current strong URL then you are "ready" and no further actions are required.**
- Can we keep all of the ciphers and MACs in our software? **Yes, you can continue to use the other Ciphers and MACs so long as you have at least one of our Ciphers and MAC.**
- Is it sufficient to have a strong Cipher and a weak MAC? **No, you must have at least one strong Cipher and the same strong MAC (hmac-sha2-256).**
- Can we send a file? **Maybe. Any files sent to the production URLs are handled as-is by our downstream production systems. So, you can only send a proper production file. You should coordinate these files directly with your business contact.**