Visa Business News

Processing

10 October 2019

Open File Delivery Cipher Changes for FTPS, SSH and Connect:Direct

Global | *Acquirers, Issuers, Processors, Agents*

Visa Network

Overview: To meet Payment Card Industry Security Standards Council (PCI SSC) compliance commitments and maintain the highest standards of system security, Visa will be upgrading the Open File Delivery (OFD) platform to utilize stronger cipher suites, while concurrently decommissioning older and less secure cipher suites effective 30 November 2019. Clients must ensure that their systems are updated to support new requirements in order to successfully connect to the OFD platform once these changes are in effect.

The OFD platform service that Visa provides to clients enables the safe and secure transfer of files between Visa's host systems to client host systems and vice versa. It is the primary file delivery channel used for critical files and reports related to card processing, clearing and settlement exchanged between Visa and all clients.

Mark Your Calendar:

- OFD cipher suites (FTPS, SSH and Connect:Direct) will be decommissioned **(30 November 2019)**

OFD provides the following connectivity options:

- File Transfer Protocol Secure (FTPS)
- Secure Shell 2 (SSH-2)
- Connect:Direct

Changes to all of these options are outlined below, and **will take effect on 30 November 2019**. Clients using these connectivity options in OFD must ensure that their systems are updated to include and use one of the supported ciphers specified in this document.

FTPS Cipher Changes

New FTPS Ciphers Supported Effective Immediately	Current FTPS Ciphers No Longer Supported as of 30 November 2019
• AES128-GCM-SHA256 • AES128-SHA256 • AES256-GCM-SHA384 • AES256-SHA256 • DH-RSA-AES128-GCM-SHA256 • DH-RSA-AES128-SHA256 • DH-RSA-AES256-GCM-SHA384 (continues on next page)	• AES128-SHA • DES-CBC3-SHA • IDEA-CBC-SHA • NULL-MD5 • NULL-SHA • RC4-MD5 • RC4-SHA

• DH-RSA-AES256-SHA256 • ECDH-ECDSA-AES128-GCM-SHA256 • ECDH-ECDSA-AES128-SHA256 • ECDH-ECDSA-AES256-GCM-SHA384 • ECDH-ECDSA-AES256-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDH-RSA-AES128-GCM-SHA256 • ECDH-RSA-AES128-SHA256 • ECDH-RSA-AES256-GCM-SHA384 • ECDH-RSA-AES256-SHA384 • ECDH-RSA-AES256-GCM-SHA384	

SSH-2 Cipher Changes

New SSH-2 Ciphers Supported Effective Immediately	Current SSH-2 Ciphers No Longer Supported as of 30 November 2019
• aes128-cbc: AES with 128-bit key • aes128-ctr: AES in CTR mode with 128-bit key • aes256-cbc: AES (Rijndael) in CBC mode, with 256-bit key • aes256-ctr: AES (Rijndael) in CTR mode, with 256-bit key	• 3des-cbc: three-key 3DES in CBC mode, with 168-bit key (effective 112-bit) • blowfish-cbc: Blowfish in CBC mode, with 128-bit key • twofish128-cbc: Twofish with 128-bit key • twofish-cbc: alias for "twofish256-cbc" (Note: this is being retained for historical reasons) • twofish-ctr: alias for "twofish256-ctr" (Note: this is being retained for historical reasons) • 3des-ctr: three-key 3DES in CTR mode, with 168-bit key (effective 112-bit) • blowfish-ctr: Blowfish in CTR mode, with 256-bit key • cast128-cbc: CAST-128 in CBC mode, with 128-bit key • cast128-ctr: CAST-128 in CTR mode, with 128-bit key • twofish128-ctr: Twofish in CTR mode with 128-bit key • twofish256-cbc: Twofish in CBC mode, with 256-bit key • twofish256-ctr: Twofish in CTR mode, with 256-bit key

Connect:Direct Cipher Changes

New Connect:Direct Ciphers Supported Effective Immediately	Current Connect:Direct Ciphers No Longer Supported as of 30 November 2019
• ECDHE_RSA_WITH_AES_128_GCM_SHA256 • ECDHE_RSA_WITH_AES_128_SHA256 • ECDHE_RSA_WITH_AES_256_GCM_SHA384 • ECDHE_RSA_WITH_AES_256_SHA384 • RSA_WITH_AES_128_GCM_SHA256 • RSA_WITH_AES_128_SHA256 • RSA_WITH_AES_256_GCM_SHA384 • RSA_WITH_AES_256_SHA256 • ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • ECDHE_ECDSA_WITH_AES_256_SHA384 • ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • ECDHE_ECDSA_WITH_AES_128_SHA256	• ECDHE_RSA_WITH_AES_128_CBC_SHA • ECDHE_RSA_WITH_AES_256_CBC_SHA • RSA_WITH_AES_128_SHA • RSA_WITH_AES_256_SHA • ECDHE_ECDSA_WITH_AES_256_CBC_SHA • ECDHE_ECDSA_WITH_AES_128_CBC_SHA

Clients' systems currently utilizing OFD that are not updated to support the above requirements **by 30 November 2019** will not be able to establish connectivity with Visa's OFD platform and will not be able to transmit or receive files and reports. Clients who have made changes to their systems will be able to view their changes in the Visa certification environment, which has already been updated to support the new requirements.

For More Information

Merchants and third party agents should contact their acquirer.