Highmark SFTP Communication Standards

SFTP SPECIFICATIONS FOR THE SECURE TRANSPORT SYSTEM

MARCH 2024

EDI Operations 1-800-992-0246

Highmark SFTP Communication Standards

The Secure Transport system utilized by Highmark is maintained on a Secure FTP (SFTP) server. It utilizes 128-bit HTTPS encryption to safeguard data. The system provides an Internet- accessible SFTP service over an encrypted data session, allowing entities that exchange data with Highmark to do so using a simple SFTP process in an encrypted and private manner. The system is a mature file transfer system that was designed to provide you with enterprise-grade security, reliability, scalability, and performance.

Highmark offers the following Internet file transfer options to its data sharing entities:

HTTPS Encryption, or SFTP Using SSH Encryption:

The above solutions can be accessed via standard file transmission clients that can transmit using HTTPS or SCP/SFTP and provide for user ID and password authentication.

Standard SCP or SFTP Clients:

Highmark also has the ability to accept files via a Secure Copy Protocol (SCP) or SFTP client. These are clients that are provided with most Unix systems, and available for free for Windows systems. These clients use the encryption and communications provided by SSH (Secure Shell) software. Each external entity that wishes to use this type of client will be responsible for obtaining and implementing this software from a source with which they feel comfortable.

Software Requirements

As with any SFTP connection, entities will need a third-party transfer application in order to transfer files using the Secure Transport system. The following two options are available with Highmark:

- A standard SFTP or SCP client.
- Any state of the art browser that supports strong encryption (128 bit) and is set to allow cookies for session tracking purposes.

SFTP: Configuration

Entities will need to configure their third-party transfer application or browser to access the following server URL: **mft.hmhs.com**. These credentials must be supplied to gain access to the Secure Transport system. SFTP clients should be configured to utilize port 22 for SFTP over SSH.

Additional Capabilities Offering Increased Security:

PGP encryption: If desired, the Secure Transport system can support PGP encryption. Please note that the transmission of the files must still be done via HTTPS or scp/sftp. In this case, we must provide the Highmark public PGP encryption key to be used to encrypt the file before it is put to the Highmark Secure FTP server and saved with a file extension of .pgp. If a file is received with a file extension of ".pgp," the service will automatically PGP decrypt the file. The Secure Transport system also supports file reception of zipped and compressed files, and virus scans all files that are placed on the Highmark server for protection of internal and external systems.

Entities should contact Highmark EDI Operations at 800-992-0246 to obtain a public PGP encryption key directly from Highmark.

Firewall Considerations:

Both HTTPS and SSH are implemented by Highmark using the standard port numbers of 443 (HTTPS) and 22 (SSH). Entities must configure their network and firewalls to allow the system exchanging files to communicate with Highmark via one of these two standard methods. Below are the IP addresses that should be opened for traffic. To prevent potential disruption, connections must be made to the hostname and will resolve to one of our internal servers. The IP addresses are provided for firewall rule configuration only.

Protocol	Port	Hostname/URL	IP Address
Web Browser – HTTPS	443	PROD: https://mft.hmhs.com	157.154.4.135
	443	TEST: https://mft-test.hmhs.com	157.154.6.96
SFTP Client - SSH	22	PROD: mft.hmhs.com	157.154.4.135
	22	TEST: mft-test.hmhs.com	157.154.6.96

External Access NOT Supported:

Highmark does **NOT** support the use of the FTP transport protocol. The standard ftp transport protocol does not provide any encryption of session (login and password) or data transmission, and therefore, jeopardizes the integrity of the data on our system.

Highmark does **NOT** support the use of the FTPS transport protocol. Although this software provides encryption of session and data, our firewall will not permit this data to pass over the standard port number. Its use of non-standard ports requires complex firewall rules to be implemented by both parties engaged in the transfer.

Highmark does **NOT** support SSH with key authentication. Our system requires user ID and password authentication. SSH key authentication is not supported.

To help safeguard our company's confidential information, the Managed File Transfer team continually evaluates and enhances our security protocols for our Secure File Transfer Protocol (SFTP) system, Secure Transport (ST).

Entities will be required to comply with the latest technology and encryption standards. Questions may be directed to EDI Operations at 1-800-992-0246.

SSH - SFTP Client Requirements

Public Key / Host Key algorithms
rsa-sha2-256
rsa-sha2-512

ecdsa-sha2-nistp521*

*Our server will support one of the above types, rsa OR ecdsa. Individual configuration is needed to support for edcsa host keys.

Ciphers
aes128-ctr
aes192-ctr
aes256-ctr
aes128-gcm@openssh.com
aes256-gcm@openssh.com

Key Exchange Algorithms (KEX)
diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha256
diffie-hellman-group15-sha512
diffie-hellman-group16-sha512
diffie-hellman-group17-sha512
diffie-hellman-group18-sha512
rsa2048-sha256
ecdh-sha2-nistp384
ecdh-sha2-nistp521*
* This currently only exists in Test only

Message Authentication Code (MAC)
hmac-sha2-256
hmac-sha2-512

HTTPS – Browser Requirements

SSL Protocols
TLSv1.2
TLSv1.3

Cipher Suites
TLS_AES_256_GCM_SHA384
TLS_AES_128_GCM_SHA256
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_CCM_SHA256
TLS_AES_128_CCM_8_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256