DXOP Secure FTP Overview

DataExpress enables you to securely transfer business-critical data files to and from your trading partners over an Intranet, the Internet or other TCP/IP networks. Trading partners can send and receive files containing transaction documents, insurance claims, medical records, retail reports, and more.

Easy Setup

- Application is entirely Web-based
- No scripts required, point and click
- Can be administered remotely from anywhere

FTP Server Security

Application security includes authentication via user ID and password. Users are authenticated to DataExpress, not to the operating system. Directory paths are virtual and tied directly to specific transmission definitions. Remote users have no direct access to disk. If desired, restrictions can be placed on authorized activity and access from remote locations. In addition, the FTP server limits the remote user's access to DataExpress job templates according to their user profile. Firewall-type security is generally provided outside of DataExpress using industry standard equipment and technology

SFTP

The DataExpress Open Platform ("DXOP") SFTP components provide a method of secure, reliable and fast file transfer over Secure Shell (SSH2) encrypted channels. Using best-in-class encryption ciphers, DXOP can offer both server-side and client-side SFTP functionality.

By utilizing SFTP server, a company is able to give authorized users with SFTP-enabled clients protected access to its critical data files. With the SFTP client component, a company is able to initiate secure file transfer sessions with its trading partners' SFTP servers. The DXOP SFTP components are designed for enterprise use, containing robust feature sets and scaling to accommodate concurrent sessions. SFTP, a subset of the popular SSH protocol, is a platform independent, secure file transfer protocol. SFTP provides a single connection port for easy firewall navigation, password and public key authentication and strong data encryption, which prevents login, data, and session information from being intercepted and/or modified in transit.

FTP with SSL/TLS

Known as FTPS, FTP over SSL, or FTP-SSL. This protocol utilizes Secure Socket Layer connections that provide host authentication as well as secured channel file transmission. Using the certificate principle of "chain of trust" DXOP offers the option to host servers with SSL/TLS or connect as a client over SSL/TLS.

SECURE FTP FEATURES

- DXOP-INITIATED COLLECTION AND DISTRIBUTION
- REMOTE-INITIATED COLLECTION AND DISTRIBUTION
- SEND OR RECEIVE SCHEDULED OR UNSCHEDULED TRANSMISSIONS
- FILE AND CHANNEL ENCRYPTION AVAILABLE

Transmission Options

DataExpress Initiated Transfers – FTP Client

- Collections – DataExpress operates as the client and receives files
- Distributions – DataExpress operates as the client and sends files

Remote Initiated Transfers – FTP Server

- Collections – DataExpress operates as the server and receives files. The remote client can view a list of “PUT” files that have not yet been confirmed for processing.
- Distributions – DataExpress operates as the server and queues files for the remote client to receive. The remote client initiates the connection and retrieves files. The remote client can view a list of files available for the “GET” command.

DXOP SFTP Benefits Include:

- Enhanced key management – create key pairs, manage keys, import/export keys
- Automated SSH connections - no need to run complex command line sequences to enable SFTP connection
- Public Key support - choose whether connecting clients or trading partners supply
- A public key for dual factor authentication, in addition to standard password authentication
- Enhanced security over open-source SFTP servers - With other SFTP servers, there is the risk of native SSH (interactive command) access. If care is not taken when setting up other SFTP servers, users on machines with the SFTP client installed may be able to use an SSH client to log into the server and execute commands. This is not a problem with DXOP
- The DXOP SFTP server locks the client into DXOP and mitigates risk by only allowing SFTP commands to be executed