



MOVEIT: SECURE, GUARANTEED FILE DELIVERY

BY JONATHAN LAMPE, GCIA, GSNA

White Paper

MOVEIT: SECURE, GUARANTEED FILE DELIVERY

W H I T E P A P E R

The MOVEit line of secure managed file transfer software products by Ipswitch File Transfer consists of two flagship products, the MOVEit Central super-client and the MOVEit DMZ server. Each uses public standards and widely adopted protocols to provide secure, end-to-end encrypted transfer and storage of sensitive data in file, message, and Web form posting formats.

MOVEit Central typically resides on an internal trusted network and is used by IT staff to automate the pulling, processing and pushing of files between internal hosts, local DMZ-based servers (including MOVEit DMZ), and remotely located file transfer systems. As its name implies, MOVEit DMZ typically resides in a DMZ and is used as a secure file transfer portal through which files can be exchanged by local and remote users and automated secure file transfer clients.

Rounding out the product line are several specialized clients designed for exchanging files with MOVEit DMZ servers, including the free MOVEit Freely and MOVEit Xfer command-line clients, the MOVEit EZ automated desktop client, and the free MOVEit Wizard Web browser plugins. This paper defines Guaranteed Delivery and explains how the MOVEit products provide it.

DEFINITIONS

It is commonly accepted that secure file transfer solutions must have all of the following capabilities in order to provide guaranteed file delivery (aka Guaranteed Delivery).

Transfer Retry – Used to automatically retry a transfer that has failed to start (also used when Transfer Resume fails to work with an interrupted transfer).

Transfer Resume – Used to automatically resume an interrupted transfer, (starting where the transfer was halted rather than starting from the beginning).

Non-Repudiation – The ability to prove who sent a file, who received it, and that the file sent and the file received are exactly the same.

In order to provide file Non-Repudiation, secure transfer solutions must include each of the following security functions.

- Authentication – To prove the identity of the sender and recipient(s).

MOVEIT: SECURE, GUARANTEED FILE DELIVERY

- Integrity Checking – To prove the file has not been changed while being uploaded to, stored on, or downloaded from the secure transfer server.
- Audit Trail – To preserve the authentication and integrity checking results.

In addition, secure file transfer solutions must also provide the following in order to guarantee that unauthorized persons cannot read the contents of the files being transferred.

- Transfer Encryption – To safeguard files while they are in transit (i.e., when uploaded to/downloaded from a secure file transfer server).
- Storage Encryption – To safeguard files while they are at rest (i.e., when stored on a publicly accessible secure file transfer server).

Details on how MOVEit DMZ server and the MOVEit clients provide secure, guaranteed file delivery is presented on the following pages.

TRANSFER RETRY

Server-Side. MOVEit DMZ server supports automatic retry features (including the ability to overwrite existing files), but “retry” is itself a client-oriented feature. Note: The MOVEit DMZ API clients each have capabilities that allow them to retry transfers.

Client-Side. All of the MOVEit clients are able to retry transfers.

Automated Clients. MOVEit Central automatically retries failed transfers to any of its remote hosts or to the local file system. The MOVEit Central API clients each have capabilities that allow them to retry transfers. The MOVEit EZ HTTPS Windows desktop client automatically retries failed transfers to its local file system and to MOVEit DMZ.

Command-Line Clients. The free MOVEit Freely FTP/FTPS Windows client and the free MOVEit Xfer HTTPS Java and Windows clients can be instructed with a short script to automatically retry a failed transfer.

Web Browser Plugins. The MOVEit Wizard ActiveX and Java plugins each have capabilities that allow them to prompt users to retry transfers.

TRANSFER RESUME

Server-Side. MOVEit DMZ supports automatic transfer resume on its HTTPS and FTPS interfaces.

Client-Side.

MOVEIT: SECURE, GUARANTEED FILE DELIVERY

W H I T E P A P E R

Automated Clients. MOVEit Central and its API clients will automatically resume interrupted transfers to the MOVEit DMZ HTTPS interface, as will the MOVEit EZ Windows desktop client. MOVEit Central will also automatically resume file transfers when using the MOVEit DMZ FTPS interface.

Command-Line Clients. The MOVEit Freely Windows client and MOVEit Xfer HTTPS Java and Windows clients can be instructed with a short script to automatically resume an interrupted transfer with the MOVEit DMZ FTPS and HTTPS interfaces, respectively.

Web Browser Plugins. The MOVEit Wizard ActiveX and Java plugins will all automatically resume interrupted file transfers when connecting via the MOVEit DMZ HTTPS interface, once the end-user has re-established the connection.

Note: The AS2 and AS3 protocols do not include support for automated file transfer resume.

Note: The SSH2 protocol does not include support for automated file transfer resume. Some vendors have created non-standard resume capabilities for their SFTP products. MOVEit DMZ server and the MOVEit clients do not support non-standard resume capabilities.

AUTHENTICATION

Server-Side. Authentication is a server-side function, using data that the client presents. MOVEit DMZ does not permit “anonymous” file transfers: all users must authenticate to login. MOVEit DMZ can authenticate users against one or any combination of the following sources.

- Internal – MOVEit DMZ’s own secure, built-in user database¹, and/or
- External – Any user database accessible via the LDAP, Secure LDAP or RADIUS Server protocols (including Microsoft Active Directory or IAS, Novell Border Manager or eDirectory Sun iPlanet, Tivoli Access Manager, and ODBC-compliant databases). MOVEit DMZ also supports single sign on (SSO) via a CA eTrust SiteMinder server.

MOVEit DMZ administrators can permit or require users (on a per user basis) to authenticate using a valid username and one, two or three authentication factors that are listed below.

FTPS Factors. MOVEit DMZ can require a valid username and any of the following one, two or three factor combinations when clients attempt to authenticate to its FTPS (SSL) interface.

- Password
- Client Certificate

MOVEIT: SECURE, GUARANTEED FILE DELIVERY

W H I T E P A P E R

- Password and IP address
- Client Certificate and IP address
- Client Certificate and Password
- Client Certificate and Password and IP address

SFTP Factors. MOVEit DMZ can require a valid username and any of the following one, two or three factor

- Combinations when clients attempt to authenticate to its SFTP (SSH) interface.
- Password
- SSH Key (aka “fingerprint”)
- Password and IP Address
- SSH Key and IP Address
- SSH Key and Password
- SSH Key and Password and IP address

HTTPS Factors. MOVEit DMZ can require a valid username and any of the following one, two or there factor combinations when clients attempt to authenticate to its HTTPS (SSL) interface.

- Password
- Password and IP Address
- Client Certificate and IP address
- Client Certificate and Password
- Client Certificate and Password and IP address

AS2/AS3 Factors. As per these protocols, a digital signature is required when an AS2 or AS3 client attempts to authenticate to the MOVEit DMZ HTTPS or FTPS interfaces, respectively.

¹Since 2003 MOVEit DMZ has included a built-in FIPS 140-2 validated cryptographic module that it uses to securely encrypt all the passwords it stores in its built-in commercially licensed user database.

MOVEIT: SECURE, GUARANTEED FILE DELIVERY

W H I T E P A P E R

Client-Side. At minimum, all MOVEit clients can present username/password data to the server. Below are details on the additional factors that each specific MOVEit clients can present.

Automated Clients. MOVEit Central and its API clients, and the MOVEit EZ client, can authenticate to MOVEit DMZ using SSL client certificates. In addition, MOVEit Central can authenticate to third-party FTP and FTPS servers using SSL client certificates, and to third-party SFTP servers using SSH keys. MOVEit Central can also authenticate to MOVEit DMZ and third-party AS2 and AS3 servers using digital signatures.

Command-Line Clients. The MOVEit Freely Windows client and MOVEit Xfer HTTPS Java and Windows clients can authenticate to MOVEit DMZ using SSL client certificates.

Web Browser Plugins. The MOVEit Wizard ActiveX and Java plugins can authenticate to MOVEit DMZ using SSL client certificates.

INTEGRITY CHECKING

Server-Side. MOVEit DMZ uses the cryptographically valid SHA-1 hash capability in its FIPS 140-2 validated cryptographic module to automatically ensure the integrity of the files it stores in its 256-bit AES encrypted file system. The same SHA-1 capability is used to ensure the integrity of files uploaded to/downloaded from MOVEit DMZ by any of the MOVEit clients. MOVEit DMZ records the success or failure of these checks as part of its' permanent audit trail.

Note: Cyclic redundancy checking (also known as CRC, CRC-32 or XCRC) is cryptographically inadequate for doing integrity checking because it produces errors and is easily subverted. This means it cannot be used for Non-Repudiation, a security 'best practice' that is required by FISMA, GLBA, HIPAA, PCI DSS and SOX – and an essential element for Guaranteed Delivery. For these reasons, MOVEit DMZ does not support cyclic redundancy checking.

Client-Side. All MOVEit clients support automatic SHA-1 integrity checks with MOVEit DMZ.

Automated Clients. MOVEit Central and its API COM component and Java class, and the MOVEit EZ client all support SHA-1 integrity checks with the MOVEit DMZ HTTPS interface. Central does automatic SHA-1 integrity checks when using the MOVEit DMZ FTPS interface. Central runs AS2 and AS3 integrity checks with Message Disposition Notifications (MDNs).

Command-Line Clients. The free MOVEit Xfer HTTPS Java and Windows clients both support SHA-1 integrity checks with the MOVEit DMZ HTTPS interface. The MOVEit Freely client does automatic SHA-1 integrity checks when using the MOVEit DMZ FTPS interface.

MOVEIT: SECURE, GUARANTEED FILE DELIVERY

W H I T E P A P E R

Web Browser Plugins. The MOVEit Wizard ActiveX and Java plugins all support SHA-1 integrity checks when using the MOVEit DMZ HTTPS interface.

Note: The SSH2 protocol does integrity checks using Message Authentication Code (MAC). This method does not always detect missing packets at the end of a transmission, which makes it inadequate for purposes of file Non-Repudiation and Guaranteed Delivery. For these reasons, MOVEit clients do not support integrity checking when using SFTP.

INTEGRITY CHECKING

Server-Side. MOVEit DMZ uses the cryptographically valid SHA-1 hash capability in its FIPS 140-2 validated cryptographic module to automatically ensure the integrity of the files it stores in its 256-bit AES encrypted file system. The same SHA-1 capability is used to ensure the integrity of files uploaded to/downloaded from MOVEit DMZ by any of the MOVEit clients. MOVEit DMZ records the success or failure of these checks as part of its' permanent audit trail.

Note: Cyclic redundancy checking (also known as CRC, CRC-32 or XCRC) is cryptographically inadequate for doing integrity checking because it produces errors and is easily subverted. This means it cannot be used for Non-Repudiation, a security 'best practice' that is required by FISMA, GLBA, HIPAA, PCI DSS and SOX – and an essential element for Guaranteed Delivery. For these reasons, MOVEit DMZ does not support cyclic redundancy checking.

Client-Side. All MOVEit clients support automatic SHA-1 integrity checks with MOVEit DMZ.

Automated Clients. MOVEit Central and its API COM component and Java class, and the MOVEit EZ client all support SHA-1 integrity checks with the MOVEit DMZ HTTPS interface. Central does automatic SHA-1 integrity checks when using the MOVEit DMZ FTPS interface. Central runs AS2 and AS3 integrity checks with Message Disposition Notifications (MDNs).

Command-Line Clients. The free MOVEit Xfer HTTPS Java and Windows clients both support SHA-1 integrity checks with the MOVEit DMZ HTTPS interface. The MOVEit Freely client does automatic SHA-1 integrity checks when using the MOVEit DMZ FTPS interface.

Web Browser Plugins. The MOVEit Wizard ActiveX and Java plugins all support SHA-1 integrity checks when using the MOVEit DMZ HTTPS interface.

Note: The SSH2 protocol does integrity checks using Message Authentication Code (MAC). This method does not always detect missing packets at the end of a transmission, which makes it inadequate for purposes of file Non-

MOVEIT: SECURE, GUARANTEED FILE DELIVERY

W H I T E P A P E R

Repudiation and Guaranteed Delivery. For these reasons, MOVEit clients do not support integrity checking when using SFTP.

AUDIT TRAIL

Server-Side. MOVEit DMZ automatically records detailed information on each and every user and file (as well as secure message and Web form post) that it handles, plus all relevant administrative actions. This information includes all of the relevant file sender and recipient authentication data, as well as all the file integrity checking, transfer, and storage details necessary in order to document Guaranteed Delivery.

This audit trail is securely stored in MOVEit DMZ's commercially licensed ODBC database. Access to this information is via Web browser over an encrypted link, and requires authorization and authentication. To further guard against tampering, MOVEit DMZ includes a cryptographic "hash chain" that can be used to prove whether the records have or have not been altered.

MOVEit DMZ also features extensive real-time and historic reporting capabilities. These enable easy access to, and analysis of, the information it stores. In addition, the data can be easily extracted and exported (in CSV, XML, and fixed width formats) for use by third party reporting and billing/tracking applications.

Client-Side. Each MOVEit client automatically records information on the connections and the file transfers that it makes. This data includes the results of the integrity checking that every MOVEit client does on each file it uploads to and downloads from MOVEit DMZ server. MOVEit clients automatically send these results to MOVEit DMZ for comparison with the results of the integrity checks that MOVEit DMZ does on the same files.

In addition, MOVEit Central automatically records its file processing and administrative actions and details of its transfers to its secure, built-in ODBC accessible database. MOVEit Central Admin (a bundled Windows program) provides access to this data. Access requires authorization and authentication, with the option to require use of an encrypted link. Extensive real-time and historic monitoring and reporting capabilities are built-in to the MOVEit Central Admin program.

MOVEIT: SECURE, GUARANTEED FILE DELIVERY

W H I T E P A P E R

The stored data can also be automatically extracted and exported (in CSV, XML, and fixed width formats) for use by third-party reporting and billing/tracking applications. In addition, third-party programs (including job scheduling and work-flow applications) can use the MOVEit Central API to receive status data in XML, CSV or HTML for the MOVEit Central tasks that they trigger.

TRANSFER ENCRYPTION

Server-Side. MOVEit DMZ provides the following secure file transfer server interfaces. Each supports a widely adopted public standard that enables numerous MOVEit and third-party clients (including Web browsers) to access and exchange files with MOVEit DMZ over an encrypted link.¹

- Secure FTP over SSL (FTPS) including all 3 modes (IMPLICIT, TLS-P, TLS-C) and Passive transfers, which
- MOVEit DMZ can support with as few as 4 open firewall ports. FTPS clients are commonly used on Windows and are native to IBM z/OS mainframes.
- Secure file transfer over HTTP (HTTPS) that supports single port (440) access by Web browsers (including
- Firefox, Internet Explorer, Mozilla, Netscape, Opera, and Safari) as well as by the MOVEit DMZ API Java class and Windows COM component, and by MOVEit Central, MOVEit EZ and the MOVEit Wizard ActiveX and Java plugins.

¹See the MOVEit DMZ Compatible Clients document on the Ipswitch FT website.

- Secure FTP over SSH (SFTP) used by Secure Shell (SSH) and SCP2 clients. These clients use one firewall port (22) and are often used on UNIX/Linux hosts.
- Secure file transfer over AS2 (HTTPS) serving as a file and MDN transfer server (requires use of MOVEit Central v.4.0 or higher with the AS option enabled).
- Secure file transfer over AS3 (FTPS) serving as a file and MDN transfer server (requires use of MOVEit Central v.4.0 or higher with the AS option enabled).

Client-Side. All MOVEit clients support one or more encrypted transfer protocols or methods.

Automated Clients. MOVEit Central and its API COM component and Java class, and the MOVEit EZ client all support SSL-encrypted transfers with MOVEit DMZ HTTPS interface. Central does SSL-encrypted transfers with MOVEit DMZ and third-party AS2 and AS3 servers, and SSL-encrypted transfers with MOVEit DMZ and third-party FTPS servers. In addition, Central can do SSH2-encrypted transfers to MOVEit DMZ and third-party SFTP servers.

MOVEIT: SECURE, GUARANTEED FILE DELIVERY

W H I T E P A P E R

Command-Line Clients. The free MOVEit Xfer HTTPS Java and Windows clients both support SSL-encrypted transfers with the MOVEit DMZ HTTPS interface. The free MOVEit Freely client supports SSL-encrypted transfers with the MOVEit DMZ FTPS interface.

Web Browser Plugins. The MOVEit Wizard ActiveX and Java Web browser plugins can each support SSL-encrypted transfers with the MOVEit DMZ HTTPS interface.

STORAGE ENCRYPTION

Server-Side. Files are vulnerable to unauthorized access when stored on Internet-accessible secure file transfer servers (whether they are located in a DMZ or within a trusted network). For this reason, all files uploaded to a MOVEit DMZ server are securely stored using its built-in, FIPS 140-2 validated, 256-bit AES encryption. File encryption/decryption is done in tiny pieces so the whole file is never exposed, and each file has its own password, which is also encrypted. These safeguards guarantee that hackers cannot read the files stored by a MOVEit DMZ server. It is surprising how many secure file transfer servers lack secure file storage and/or safeguards.

In addition to encrypted storage, MOVEit DMZ has its own built-in permissions system, which is also protected by its FIPS validated cryptography. This combination of MOVEit DMZ's encrypted storage and a secure permissions system means that its settings, as well as all of the files that it handles, are not vulnerable to security flaws in the underlying operating system. This security independence is unique to MOVEit DMZ.

Client-Side. AS1, AS2, AS3, FTPS, HTTPS, SCP, and SFTP clients provide transfer encryption, providing secure links over which files are uploaded to and downloaded from compatible servers, but encrypted file storage is typically a server function. An exception to this is the ability of MOVEit Central to encrypt and decrypt files for storage, automatically, using its commercially licensed OpenPGP and/or S/MIME encryption modules.

For additional information, please contact the Ipswitch File Transfer division or visit www.ipswitchFT.com.