

MOVEit: File Non-Repudiation



This document discusses file non-repudiation as it applies to secure file transfers, and how it is provided by the MOVEit line of secure file transfer server and client products. End-to-end file non-repudiation is the ability to prove who uploaded a specific file, who downloaded it, and that the file uploaded and the file downloaded are identical. It is a security “best practice” and required by Federal Information Security Management Act (FISMA), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and others.

Benefits. The ability to provide end-to-end file non-repudiation is an essential part of any secure file transfer solution because it provides the following benefits.

- Guarantees the integrity of the data being transferred.
- Plays a valuable forensic role if a dispute arises about the file.
- Provides a capability that is required for Guaranteed Delivery.

Server Requirements. Providing end-to-end file non-repudiation requires using a secure file transfer server that can perform all of the following activities.

- Authenticate each user who uploads or downloads a file.
- Check the integrity of each file when uploaded and downloaded.
- Compare the server and client-generated integrity check results.
- Associate and log the authentication and check results.

Client Requirements. The secure file transfer clients used to upload files to the server and download them from it must be able to perform the following activities.

- Check the integrity of each file when uploading or downloading it.
- Transmit the upload and download check results to the server.

Algorithms. The cryptographically valid SHA1 and MD5 algorithms are widely used to do file integrity checking. SHA1 is the stronger of these, and is approved for file integrity checking under US Federal Information Processing Standard FIPS 140-2. The MOVEit DMZ secure file transfer server and the MOVEit Central managed file transfer super-client each have built-in FIPS 140-2 validated cryptographic modules that include the SHA1 and MD5 algorithms, which they use for file integrity checking.

WARNING: Some secure file transfer products still do integrity checking using the outdated cyclical redundancy check algorithm (referred to as CRC, CRC-32 or XCRC). It is not cryptographically valid because it produces errors and is easily subverted. Products that use CRC cannot provide file nonrepudiation or guaranteed file delivery.

MOVEit Non-Repudiation. MOVEit DMZ secure file transfer server provides SHA1 cryptographically valid end-to-end file non-repudiation when exchanging files with MOVEit secure file transfer clients (including free MOVEit Xfer command-line clients), with Internet Explorer, Firefox, Chrome and Safari browsers using free MOVEit Wizard plugins, and with SmartFTP clients by SmartFTP GmbH.

Please contact an Ipswitch File Transfer sales representative for more information about the MOVEit line of managed file transfer software products.

To learn more, please visit:
www.ipswitchFT.com

