IPSWITCH File Transfer

MOVEIT CENTRAL: SECURE MANAGED FILE TRANSFER ENTERPRISE CLIENT SOFTWARE

The MOVEit Central software is a powerful standalone secure MFT client that IT staff use to easily automate, manage and audit the transfer of files between internal, local DMZ-based, and remote computers — including MOVEit DMZ servers. This document provides an overview of Central's basic and optional capabilities and licensing.

TRANSFER AUTOMATION. Central uses easily clicked-together tasks to manage the automated transfer and processing of files without scripting or programming. Tasks define the files to be moved, where they are, where they are to be sent to, the authentication and transfer methods to be used, and what processing (if any) is to be done. Each task can move one or more files (regardless of size or format) between multiple systems using combinations of different methods and processes. Tasks can also synchronize/replicate files and/or folders between separate systems, automatically.

SCHEDULING AND ADMINISTRATION. Tasks are run on a scheduled, event-driven or on-demand basis, and multiple tasks can be run simultaneously. IT Staff use the bundled Central Admin console to remotely configure, monitor and control tasks. Tasks can also be controlled by third-party schedulers and other programs via Central's optional API.

MULTI-PROTOCOL SUPPORT. Central can move files using a multitude of popular, non-proprietary transfer standards. These enable Central to transfer files between file, email and Web servers, mid-range and mainframe hosts, and FTP, secure FTPS (SSL), SFTP (SSH2), and MOVEit DMZ servers. An option enables transfers using AS1, AS2, and AS3.

PROCESSING. Tasks can process files using built-in Central functions (Zip/Unzip, rename, string search/replace, running third-party command-line utilities, and more). Central can also start VBS scripts to run programs with COM interfaces and script interpreters such as Perl. An OpenPGP option provides file encryption/decryption and key management.

BASIC LICENSE TERMS

- Unlimited tasks, unlimited transfers, and unlimited processes permitted
- Can be run on 1 production system and on 1 non-production system (physical or virtual, and without limit on the number or type of CPUs)
- Central Admin can be run on an unlimited number of systems

BASIC LICENSE CAPABILITIES

- HTTPS and FTPS (SSL) transfers (FTPS IMPLICIT, TLS-P, TLS-C, Passive)
- SFTP and SCP2 (SSH2) transfers
- HTTP and FTP (non-secure) transfers
- Copy to local and network file systems
- SMTP/POP3 support for sending and receiving email and file attachments
- File/folder synchronization/replication
- FIPS 140-2 validated cryptography
- AES and S/MIME file encryption
- MD5 and SHA1 file integrity checking
- SSL server certificate validation
- HTTPS client certificates support
- STPS client key authentication
- FTPS client certificates support
- FTPS client-side NAT support
- Automatic transfer resume and retry
- Commercial MySQL database
- Real-time transfer statistics
- Built-in reporting capabilities
- Tamper-evident audit logs
- Remote administrative control with Free MOVEit Central Admin console
- Anti-Virus real-time integration with McAfee, Symantec and Trend Micro
- RFC 959, 1122, 1123, 1579, 2228, 4217 as well as IETF Work Group “SSH File Transfer Protocol” and “SSH Public Key File” compliant
- NIST SP 800-88 data erasure compliant

HOST SPECIFICATIONS

- Central runs as a service on Windows Server 2008, Vista Business Edition, and Server 2003
- Central admin runs on Windows Server 2008, Vista Business Edition, Server 2003, and XP Professional
- Supported under EMC VMware ESX and Microsoft Virtual Server

AUDIT TRAIL. Transfer/processing actions/errors are logged to Central's commercial, tamper-evident, ODBC compliant database for use by Central Admin for real-time status and history reports, and by third-party billing/reporting programs.

SECURITY. Administrative access requires authorization and authentication, and can be made over an SSL encrypted link. Config and permissions data and scripts are AES encrypted.

To keep the Central Basic license as affordable as possible, the following built-in capabilities are offered as separately priced options (so you only pay for what you actually need).

AS1 AS2 AS3 OPTION. The "Applicability Statement" protocols define methods to securely exchange structured data over the Internet, and are used globally by retailers, distributors, manufacturers and others. Central includes the commercially licensed ability to send and receive files via email servers using AS1, via AS2-capable servers using AS2 (requires MOVEit DMZ to receive files and MDNs) and via FTP or FTPS servers (including MOVEit DMZ servers) using AS3. This option enables unlimited AS1, AS2 and AS3 transfers.

OPENPGP ENCRYPTION OPTION. OpenPGP is the Internet standard specification for the PGP encryption algorithms and data formats — enabling full encryption/decryption and key interoperability between OpenPGP compliant programs. Central offers a commercially licensed, tightly integrated OpenPGP software module. It provides key management and enables Central tasks to automatically encrypt/decrypt files and to log the relevant details as part of a transfer. This option allows unlimited encryption/decryption and keys.

API INTERFACE OPTION. In addition to the comprehensive task scheduling capabilities provided under the Basic license, this option allows third-party applications (such as job and workflow schedulers) to create and control tasks via Central's built-in API. Applications can use the API to dynamically create and start tasks, to define and select file source and destination systems, paths and files, and to receive task status data. This option provides unlimited use of the API, as well as unlimited use and the right to re-distribute the MOVEit Central API Java and Windows clients.

AUTOMATED FAILOVER OPTION. Since its release in 2001, Central has gained a well earned a reputation for reliability, but as a "business critical" enterprise application it also has the built-in ability to provide automatic, unattended failover to a co-located or remotely located hot standby copy of itself. When deployed for failover, the primary Central continuously updates the secondary so that it can automatically take over should the primary fail. Implementing this option requires two identical Central licenses (the second copy of which is offered at half price because it is rarely used for production).

The diagram on the next page shows the network locations, transfer protocols and their firewall port requirements, and the client/server

AS1 AS2 AS3 TRANSFER OPTION

- AS1 (SMTP/POP3) transfers
- AS2 (HTTP/HTTPS) transfers
- AS3 (FTP/FTPS) transfers
- S/MIME data encryption
- Digital Signature authentication
- Message Disposition Notification (MDN) for data integrity checking
- RFC 3335 and RFC 4130 compliant
- EDIINT Working Group Internet "FTP Transport for Secure Peer-to-Peer Business Data Interchange Over the Internet" draft compliant
- Uses integrated code commercially licensed from /n Software.
- Certified as "eBusinessReadyTM" for AS2 by Drummond Group, Inc.

OPENPGP ENCRYPTION OPTION

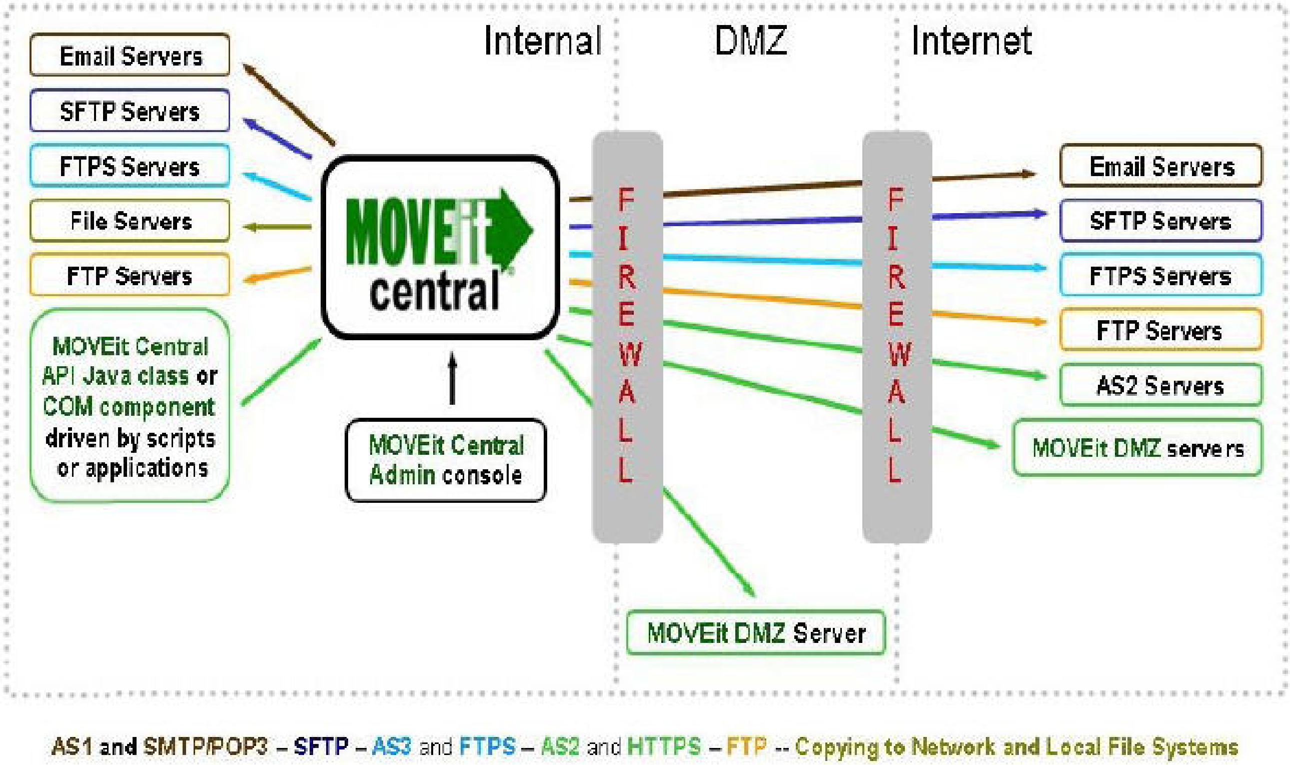
- Automatic file encrypt, encrypt and sign, and decrypt during transfers
- Creates, imports public/private keys
- Exports ASCII-Armored, Binary keys
- Unlimited file encryption decryption
- Unlimited encryption keys
- All encrypt/decrypt details logged
- Fully interoperable with all third-party
- OpenPGP products, including PGP
- Uses integrated, commercially licensed
- OpenPGP software from Veridis

API INTERFACE OPTION

- Start synchronization and transfer tasks
- Passes parameters (file and folder masks, and destination file names)
- Dynamic per task selection of sources/destinations, paths, and files/folders
- Exports task status data in XML, CSV, and HTML formats
- Java class and its command-line client require Sun Java v.1.4.2 or higher
- COM component and its command-line client runs on Windows Vista Business
- Edition, 2003, XP, 2000 and NT 4.0

AUTOMATIC FAILOVER OPTION

- Unattended automatic failover to a second, hot-standby copy of Central
- Continuously updates failover Central with settings, state information and statistics from the production Central.
- No use of Windows Clustering Services


Internal
DMZ
Internet
Email Servers
SFTP Servers
FTPS Servers
File Servers
FTP Servers
MOVEit Central API Java class or COM component driven by scripts or applications
MOVEit central
MOVEit Central Admin console
FIREWALL
FIREWALL
MOVEit DMZ Server
Email Servers
SFTP Servers
FTPS Servers
FTP Servers
AS2 Servers
MOVEit DMZ servers
AS1 and SMTP/POP3 – SFTP – AS3 and FTPS – AS2 and HTTPS – FTP -- Copying to Network and Local File Systems

interactions of MOVEit Central and the wide variety of local and remote servers, including MOVEit DMZ servers, that it can automatically pull files from, process them as necessary, and push files to on a scheduled, event-driven or ad hoc basis. MOVEit Central provides enterprises with the "anywhere to anywhere" managed file transfer capabilities they need to exchange large volumes of files, with minimal operational staff time and system resources, in the following common transfer situations.

INTERNAL TO INTERNAL. Between backend hosts, including mainframe and mid-range systems as well as application, archive, email, file and internal Web servers.

INTERNAL TO DMZ. Between backend hosts and the local MOVEit DMZ server, as well as to other DMZ resident systems.

INTERNAL TO REMOTE. Between backend hosts and remote FTP, secure FTP, and MOVEit DMZ servers at field offices and customer or partner locations.

Whether deployed on a standalone basis or together with a MOVEit DMZ server, MOVEit Central is a cost-effective, quickly deployable, operationally flexible and consistently reliable solution for businesses and government agencies that need to exchange files with their subsidiaries, customers and partners.

To receive additional information about MOVEit Central, or to request a licensing and pricing proposal and/or a free, live online Web demonstration or onsite evaluation, please contact Ipswitch directly.

IPSWITCH
File Transfer
Simple. Secure. Managed.

Ipswitch
10 Maguire Road • Lexington, MA 02421
MOVEit: (608) 824 3600 • moveitinfo@ipswitch.com