IPSWITCH File Transfer

MOVEIT DMZ: SECURE MANAGED FILE TRANSFER ENTERPRISE SERVER SOFTWARE

The MOVEit DMZ server supports quick, easy and secure end-to-end encrypted transfer and storage of confidential information over the Internet — in file, message and Web posting formats — enabling companies and governments to achieve and demonstrate compliance with their contractual, industry and regulatory privacy and security standards. This document provides an overview of MOVEit DMZ's basic and optional capabilities, and licensing and technical details.

SECURITY. MOVEit DMZ is designed to operate securely on an Internet-exposed, security-hardened, Wwindows server on a de-militarized zone (DMZ) network segment protected by one or more firewalls. MOVEit DMZ can be safely accessed from the Internet and the local trusted network, without opening firewall ports from the DMZ into the local network. MOVEit DMZ protects itself and the data it receives using its own built-in: FIPS 140-2 validated cryptography, 256-bit AES encrypted storage, and authentication and access controls. This means that the security of MOVEit DMZ, its users and data does not depend on the security of the underlying OS.

COMPATIBILITY. MOVEit DMZ multi-protocol support means that employees, customers and partners can quickly, easily and safely exchange files of any size or type via MOVEit DMZ using regular Wweb browsers, secure FTPp SSLI (FTPpS/TLIS) and SSH2 (SFTP/ SCP2) clients, plus all AS2 and AS3 clients.

FLEXIBILITY. MOVEit DMZ Aadministrators have the ability to manage users with aging, profiles and cloning capabilities, to organize them into groups run by group administrators, and have MOVEit DMZ send email notices when files arrive.

COMPLIANCE. MOVEit DMZ enables licensees to achieve and demonstrate compliance with their corporate, contractual, industry and regulatory privacy and security requirements, including FISMA, GLBA, HIPAA, PCI DSS, PIPEDA and SOX. All transfer and processing actions and errors are logged to MOVEit's commercially licensed, tamper-evident database. Over 90 pre-defined, built-in reports can be

BASIC LICENSE TERMS

- Unlimited users and file transfers
- 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)
- Unlimited use of MOVEit Wizard and MOVEit Xfer secure transfer clients

BASIC LICENSE CAPABIILITIES

- HTTPS and FTPS/TLS (SSL) (FTPS IMPLICIT, TLS-P, TLS-C, Passive)
- SFTP/SCP2 (SSH2) transfer support
- FTPS server-side NAT support
- AS2 file and MDN transfer server (requires use of MOVEit Central with Central AS option enabled)
- AS3 file and MDN transfer server
- FTP (non-secure) transfer support
- SMTP for file and message arrival and administrative event notifications
- FIPS 140-2 validated cryptography
- AES 256-bit encrypted storage of files, messages and other data
- Integrated permissions system
- MD5 and SHA1 integrity checking for Non-Repudiation
- Transfer resume and retry support for Guaranteed Delivery
- User groups and group administrators.
- User profiles, cloning and aging
- Authentication using up to 3 factors: FTPS and HTTPS client certificates, SFTP SSH public keys (fingerprints), passwords, and IP addresses
- FFIEC authentication rules compliant
- Tamper-evident audit logs
- Pre-defined and customizable reports.
- Remote secure administrative access using regular Web browsers
- RFC 959, 1122, 1123, 1579, 2228, 4217 as well as IETF Work Group "Securing FTP with TLS" compliant
- NIST SP 800-88 data erasure compliant

HOST SPECIFICATIONS

- Runs as service on Windows Server 2008 and 2003
- Supported under VMware ESX and Microsoft Virtual Server

run against the database (as can customized reports), and data sets can be extracted for use by third-party billing and reporting apps.

VALUE. The MOVEit DMZ basic license permits the software to be run on one production and one non-production system, with unlimited users and transfers. The license also includes unlimited use of the MOVEit Wizard and MOVEit Xfer clients.

To help keep the MOVEit DMZ Basic license affordable, the following built-in capabilities are offered as separately licensed and priced options that can be added at any time.

EXTERNAL OPTION. While MOVEit DMZ has its own secure database to authenticate users against, this option enables it to also authenticate against one or more external user databases (such as active Directory) using any combination of the LDAP, Secure LDAP or RADIUS Server protocols. LDAP user and group replication, user expiration, and custom mapping of LDAP user records to MOVEit DMZ user profiles are all supported under this option, as is SSO (single sign-on) via CA SiteMinder Web Access Manger and with US Dept. of Defense CAC (Common Access Cards).

SECURE MESSAGING OPTION. Authorized MOVEit DMZ users can employ this option to create messages (with or without attached files), send them to other authorized users of that MOVEit DMZ, and retrieve and reply to messages they get. This is not secure email; it is a separate, parallel, end-to-end encrypted solution that uses regular Web browsers as clients, requires authorization and authentication, and is used when messages (and attached files) contain sensitive information. This option allows unlimited sending/receiving of messages.

API INTERFACE OPTION. Pprovides third-party programs (including Web applications) with programmatic access to MOVEit DMZ transfer, storage and user database services, and to its user, folder, permissions and reporting functions. This option includes unlimited use of the MOVEit DMZ API Java class, COM component, and command-line interfaces.

MULTIPLE ORGANIZATIONS OPTION. The MOVEit DMZ basic license includes a single organization, but the software is able to support specific numbers of additional "orgs" — each with its own unique URL, users, administrators, permissions, logs, files, folders, branding and encrypted storage. This means a single copy of MOVEit DMZ software running on a single host can support two or more agencies, divisions or subsidiaries.

END-USER LANGUAGE OPTIONS. Enables end-users to view and use the MOVEit DMZ Web interface in French or Spanish.

EXTERNAL AUTHENTICATION OPTION

- Supports multiple databases, protocols
- LDAP and Secure LDAP protocols to Active Directory (AD), eDirectory, iPlanet, and Tivoli user databases
- LDAP user and group replication
- LDAP custom mapping of users records to MOVEit DMZ user profiles
- RADIUS Server protocol to Border Manager and Internet Authentication Services (IAS) user databases
- RADIUS to ODBC compliant databases
- LDAP and RADIUS configuration testing
- CA SiteMinder SSO support
- US DoD CAC card SSO support

SECURE MESSAGING OPTION

- Firefox, Internet Explorer, Mozilla, Netscape, Opera and Safari supported
- HTTPS secure message transmission
- SSL encrypted transfer and AES encrypted storage of messages, files
- Message drafts and templates
- Spellchecking dictionaries
- Detailed, tamper-evident audit trail

API INTERFACE OPTION

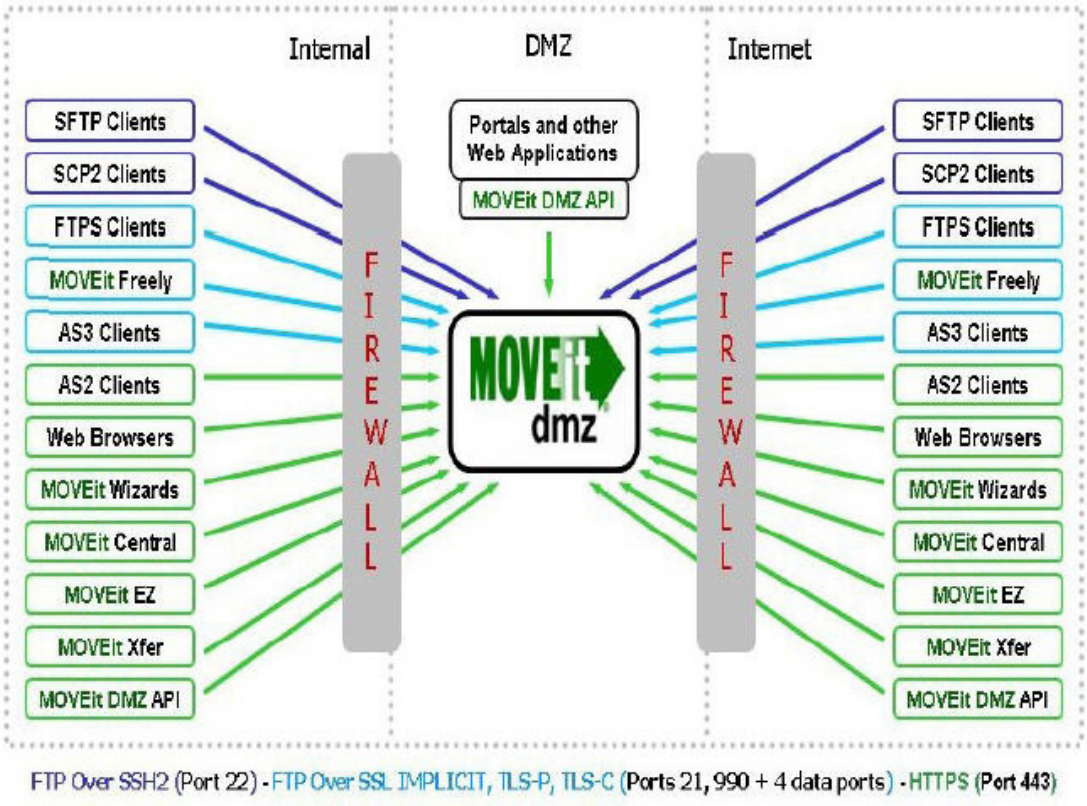
- Create, transfer, store and delete files and secure messages
- Create, manage and delete folders, users and permissions
- Run pre-defied reports, create and run custom reports, and retrieve them
- Use MOVEit DMZ user database and secure file and message storage
- API Java class and command-line client require Sun Java v.1.4.2 or higher
- API COM component and command-line client runs on Windows Vista Business Edition, 2003, XP, 2000 and NT 4.0

HIGH AVAILABILITY OPTION

- Unattended automated failover between two co-located production MOVEit DMZ
- Scalability over two (or more) systems
- Continuous updating of settings, stats, and state information
- Requires two identical DMZ licenses, hardware or software load balancing, and a NAS in order to implement
- No use of Windows Clustering Services

HIGH AVAILABILITY OPTION. MOVEit DMZ is highly reliable, but MOVEit DMZ can be deployed on two or more co-located, load balanced production systems to provide scalability and automatic updating and unattended failover between them.

The diagram above shows the network locations and transfer protocols and firewall port requirements of MOVEit DMZ



server and compatible clients. As the arrows indicate, all connections to MOVEit DMZ are initiated by the clients. As a pure server product, MOVEit DMZ is incapable of pushing files into the local trusted network. This means files and messages can be securely exchanged with a MOVEit DMZ server without opening any firewall ports from the DMZ into the local internal network. Opening such ports creates holes in the perimeter defenses, exposing the internal network to Internet based security risks.

The MOVEit DMZ architecture stands in stark contrast to some competing products that use DMZ based secure file transfer gateways (proxy servers) to exchange files between the DMZ and the local network. (For details see the Secure File Transfer Gateways: Danger in the DMZ whitepaper www.IpswitchFT.com).

For those concerned about the security implications of storing even strongly encrypted files in the DMZ, the MOVEit Ccentral secure managed file transfer client can do real-time monitoring of file arrivals on MOVEit DMZ and immediately and automatically pull new files from it into the local trusted network.

To receive additional information about MOVEit DMZ 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