

MOVEIT DMZ ENTERPRISE: MANAGED FILE TRANSFER SERVER

ABSTRACT

MOVEit DMZ Enterprise is designed to be the world's most secure and compliant file transfer server. This powerful solution is optimized for mission-critical encrypted transfer and storage of files and data with global vendors and partners.

The MOVEit DMZ Enterprise 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 exceed their security and compliance expectations, improve global collaboration, focus on file transfer governance, and enhance existing business processes.

In addition to the on-premise version of MOVEit DMZ Enterprise, we also offer a hosted services version. MOVEit DMZ Hosted Services delivers all the functionality of MOVEit DMZ Enterprise, yet with all the benefits you'd expect from a hosted service subscription.

This document provides an overview of MOVEit DMZ Enterprise's basic and optional capabilities and licensing.

SECURITY. MOVEit DMZ Enterprise is designed to operate securely on an Internet-exposed, security-hardened, Windows server on a demilitarized zone (DMZ) network segment protected by one or more firewalls. MOVEit DMZ Enterprise 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 Enterprise 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 Enterprise, its users, and data does not depend on the security of the underlying OS.

COMPATIBILITY. MOVEit DMZ Enterprise multi-protocol support means that employees, customers, and partners can quickly, easily, and safely exchange files of any size or type via MOVEit DMZ Enterprise using regular Web browsers, secure FTP SSL (FTPS/TLS), and SSH2 (SFTP/ SCP2) clients, plus all AS2 and AS3 clients.

EXTERNAL AUTHENTICATION. While MOVEit DMZ Enterprise 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 Enterprise user profiles are all supported under this option, as is SSO (single sign-on) via CA SiteMinder Web Access Manager and with US Department of Defense CAC (Common Access Cards).

TIERED ARCHITECTURE DEPLOYMENTS. Distributed architecture enables the deployment of multiple DMZ nodes in the form of a web farm. Administrators can deploy MOVEit DMZ Enterprise on one server, the encrypted data store on a second server, and the configuration database on a third server. This flexible architecture extends the performance, availability, and security of MOVEit DMZ Enterprise solutions.

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

INTEGRATES WITH SQL SERVER DATABASE. Administrators have the option to either use the embedded MOVEit database or integrate with Microsoft SQL Server or Microsoft SQL Server Express for both user authentication and server system configurations such as access controls, user permissions, and password policies.

ON-PREMISES 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

ON- PREMISES BASIC LICENSE CAPABILITIES

- HTTPS and FTPS/TLS (SSL) (FTPS IMPLICIT, TLS-P, TLS-C, Passive)
- SFTP/SCP2 (SSH2) transfer support
- FTPS server-side NAT support
- AS2 and AS3 file and MDN transfer server (requires use of MOVEit Central with Central AS option enabled)
- FTP 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
- Microsoft SQL Server and MySQL support
- 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
- Tiered architecture deployments

HOST SPECIFICATIONS

- Runs as service on Windows Server 2008 (32-bit and 64-bit) and 2003 (32-bit and 64-bit)
- Supported under VMware ESX and Microsoft Hyper-V

END-USER LANGUAGES. Enables end-users to view and use the MOVEit DMZ Enterprise Web interface and the Secure Messaging interface in English, French, Spanish, or German.

COMPLIANCE. MOVEit DMZ Enterprise enables licensees to achieve and demonstrate compliance with their corporate, contractual, industry, and regulatory privacy and security requirements, including FISMA, GLBA, HIPAA, MA 201 CMR 17, 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 run against the database (as can customized reports), and data sets can be extracted for use by third-party billing and reporting applications.

VALUE. The MOVEit DMZ Enterprise 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 Enterprise basic license affordable, the following built-in capabilities are offered as separately licensed and priced options that can be added at any time:

AD HOC TRANSFER MODULE. The Ad Hoc Transfer module enables secure person-to-person file sharing using the convenience of a Web browser or Microsoft Outlook. Authorized MOVEit DMZ Enterprise users can send files to anyone in the world with an email address – quickly, easily, and securely.

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

MULTIPLE ORGANIZATIONS MODULE. The MOVEit DMZ Enterprise 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 Enterprise software running on a single host can support two or more agencies, divisions or subsidiaries.

END-USER LANGUAGE MODULE. Enables end-users to view and use the MOVEit DMZ Enterprise Web interface and the Secure Messaging interface in English, French, Spanish, or German.

HIGH AVAILABILITY MODULE. MOVEit DMZ Enterprise has a flexible architecture that can ensure 24/7 uninterrupted service through its out-of-the-box high-availability, auto-failover configuration. MOVEit DMZ Enterprise can also be configured with third party applications for load balancing and clustering to ensure smooth deployment of multiple MOVEit DMZ Enterprise Servers in your web farm.

AD HOC TRANSFER MODULE

- Person-to-person file sharing via browser or Outlook
- Secure way to quickly share files with other people, both internal and external to an organization
- No file size limit
- Recipients can send files back to the sender
- Ability to send multiple files and folders of files
- Automatic provisioning for non-company recipients
- Archival of entire package, both messages and files
- Enforce administrator defined policies and rules for sending files to other people
- Provides complete visibility into all file sharing activities
- Removes the file attachment burden from the email server

EXTERNAL AUTHENTICATION MODULE

- 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

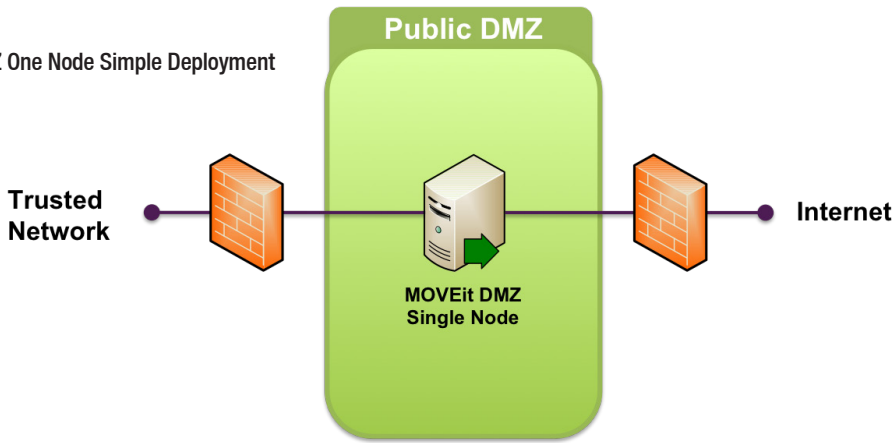
API INTERFACE MODULE

- 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, XP, 2000, 2003, 2008

HIGH AVAILABILITY MODULE

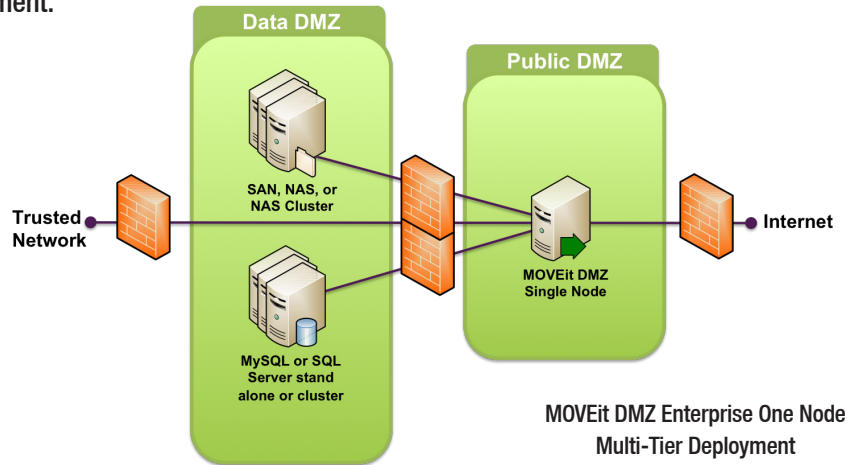
- Unattended automated failover between two co-located production MOVEit DMZ
- Scalability over two (or more) systems
- Continuous updating of settings, stats, and state information
- Requires two identical DMZ licenses, hardware or software load balancing, and a NAS in order to implement

MOVEit DMZ One Node Simple Deployment

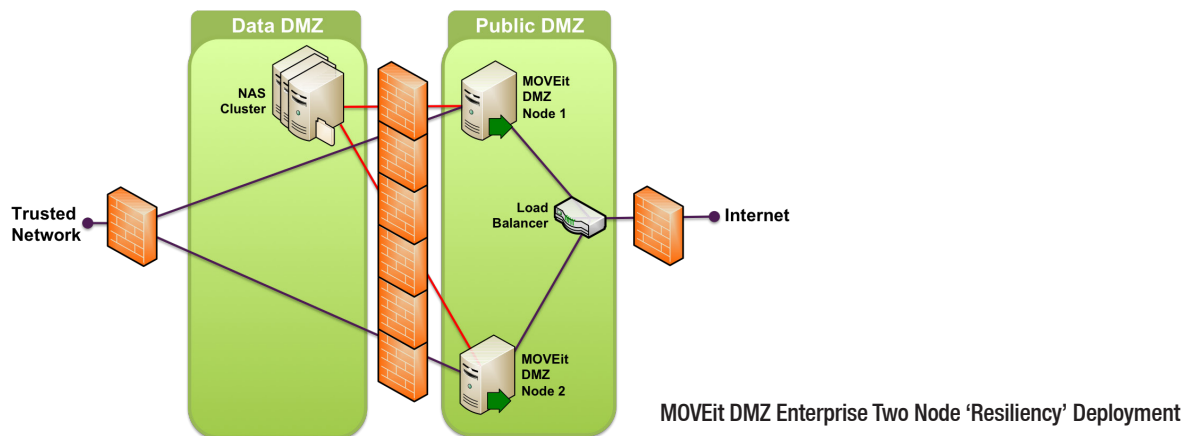


The diagram to the left shows the network locations and transfer protocols and firewall port requirements of MOVEit DMZ Enterprise server and compatible clients. As the arrows indicate, all connections to MOVEit DMZ Enterprise are initiated by the clients. As a pure server product, MOVEit DMZ Enterprise is incapable of pushing files into the local trusted network. This means files and messages can be securely exchanged 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.

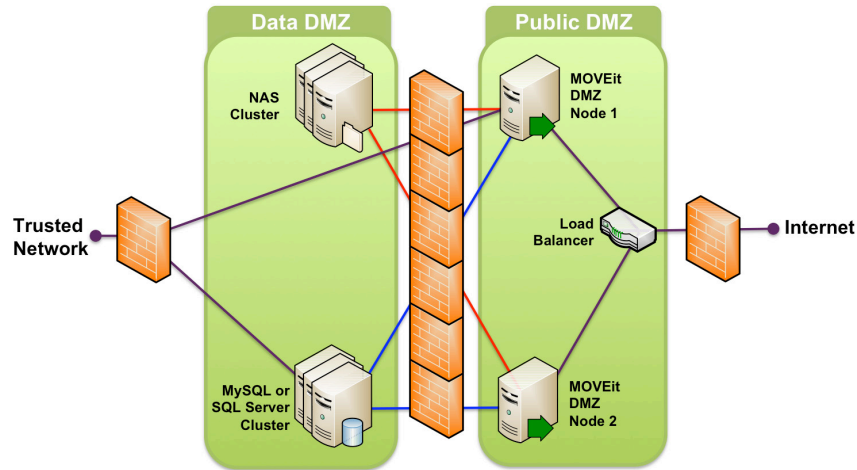
There are two different ways to implement MOVEit DMZ Enterprise on a high availability basis, and both provide scalability, automated failover, and multi-tier deployment for enhanced security. The diagram below illustrates MOVEit DMZ Enterprise's one node multi-tier deployment.



The diagram below shows the MOVEit DMZ Enterprise resiliency method. Under this approach the MOVEit DMZ Enterprise software automatically replicates its configuration and permissions data between the MySQL databases that are built-in to each MOVEit DMZ Enterprise. The MOVEit DMZ Enterprise software also manages the automatic unattended failover between the MOVEit DMZ Enterprise nodes should one of them fail. In addition the software enables the deployment of the MOVEit DMZ Enterprise 256-bit AES encrypted file storage system on a NAS or NAS cluster located on a separate network segment. This latter capability means that all files received by MOVEit DMZ Enterprise can be stored on a non-public, restricted access segment.



The diagram below shows the MOVEit DMZ Enterprise High Availability Web Farms method. Under this approach, MOVEit DMZ Enterprise takes advantage of existing application, database, and network storage server clusters and replication. The MOVEit DMZ Enterprise application resides on two or more Web Farm nodes in the public DMZ segment, with the load balancer handling failover between them. The MOVEit DMZ Enterprise 256-bit AES encrypted file storage system runs on a NAS or NAS cluster, and the MOVEit DMZ Enterprise configuration and permissions data resides in either a MySQL or Microsoft SQL Server cluster, both of which can be located in non-public, restricted access network segments. This approach means only the MOVEit DMZ Enterprise application is exposed in the Internet-facing DMZ segment. The architecture illustrated in the diagram below is used for MOVEit DMZ Hosted Services.



MOVEit DMZ 6.0 Two Node HA Web Farm Deployment

For more information on MOVEit DMZ Enterprise solutions, including pricing or details on how to request a personalized demonstration or onsite evaluation, please visit www.IpswitchFT.com.

ABOUT IPSWITCH FILE TRANSFER

Ipswitch File Transfer is a global technology provider that builds solutions to securely move your valuable data. We enable companies and people to better manage their data interactions when visibility, management and enforcement matter. Our managed file transfer solutions deliver the control necessary to enable governance and compliance for our more than 40 million global users – including the majority of Fortune 1000 enterprises and government agencies. These organizations trust Ipswitch File Transfer solutions to secure, manage, automate and streamline their critical and highly sensitive file transfers and data workflows. Learn more at www.IpswitchFT.com or to contact us at www.IpswitchFT.com/company/contact.aspx, on LinkedIn or Twitter.

