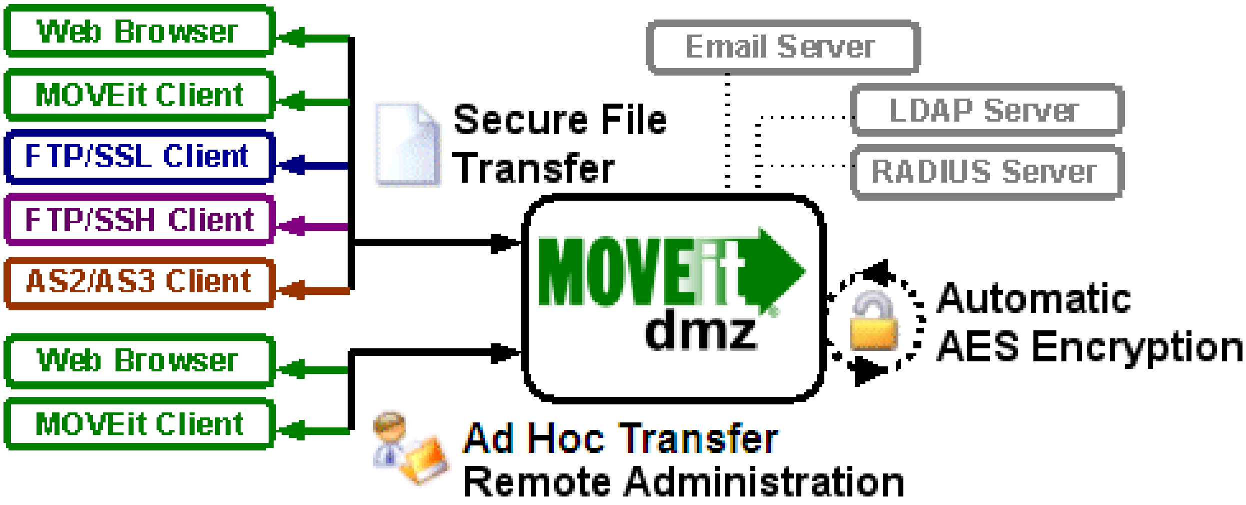
MOVEit® DMZ Manual

v7.5

Contents

Introduction

MOVEit® DMZ Enterprise is a secure file transfer server. It is a vital component of the MOVEit® family of secure file processing, storage, and transfer products developed by Ipswitch, Inc.. These products provide comprehensive, integrated, standards-based solutions for secure handling of sensitive information, including financial files, medical records, legal documents, and personal data.



MOVEit DMZ safely and securely collects, stores, manages, and distributes sensitive information between your organization and external entities. Web browsers and no cost/low cost secure FTP clients can quickly, easily, and securely exchange files with MOVEit DMZ over encrypted connections using the HTTP over SSL (https), FTP over SSL (ftps) and FTP over SSH (sftp) protocols. And all files received by MOVEit DMZ are securely stored using FIPS 140-2 validated AES encryption, the U.S. Federal and Canadian government encryption standard.

In addition, a web interface offers easy online administration and monitoring of MOVEit DMZ activities while a programmable interface (via MOVEit DMZ API Windows and MOVEit DMZ API Java) makes MOVEit DMZ accessible to custom applications.

MOVEit DMZ includes an optional MOVEit Wizard plug-in that works with Internet Explorer, Firefox and Mozilla to help web-based users to quickly upload and download large and/or multiple files and folder trees to and from MOVEit DMZ.

Encryption capabilities throughout the MOVEit product line are provided by MOVEit Crypto. The AES encryption in MOVEit Crypto has been FIPS 197 validated. The entire cryptographic module has been FIPS 140-2 validated after rigorous examination by cryptographic specialists in the United States' National Institute of Standards and Technology (NIST) and Canada's Communications Security Establishment (CSE).

MOVEit DMZ also has an approved Certificate of Networthiness (CoN) from the United States Army. This certification involves a review of how MOVEit DMZ meets Army requirements for network security, integration, interoperability, and ease of management and support.

Physical Specifications

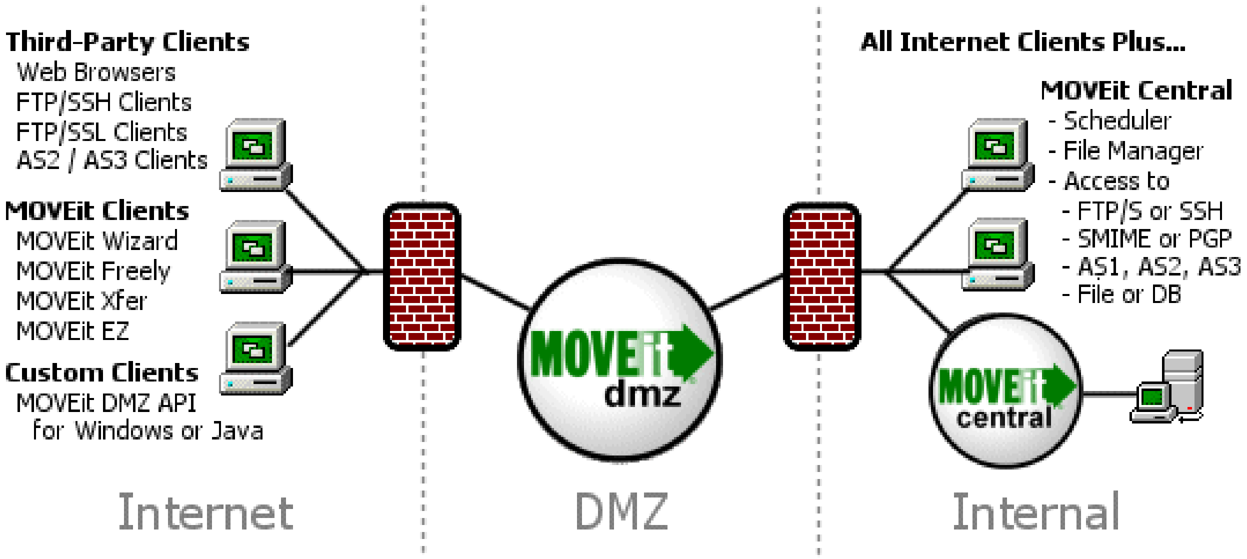
The MOVEit DMZ software itself resides on a Microsoft Windows Server platform hardened against threats from the Internet and trusted networks. Organizations that need to support very large volumes of file transfers and/or many users may require additional hardware, but for many organizations the minimum recommended specifications of a MOVEit DMZ should suffice:

- 2 GHz Pentium-compatible CPU
- 80 GB SATA or SAS Hard Drive
- 1 GB RAM
- 100/1000 Mb TCP/IP-capable ethernet interface

The latest production recommendations can be found in the online Support Knowledge Base.

Network Specifications

In a typical network topology MOVEit DMZ is best located on a secured "DMZ" segment accessible to both internal and external users."DMZ" is short for DeMilitarized Zone - a network "no man's land" where both internal and internet hosts are allowed to connect. By default, connections originating from a DMZ network segment are not to be trusted and are usually not allowed unless there is a compelling case to allow a particular service through.



Web and secure FTP clients can upload and download files to MOVEit DMZ from internal and external networks. For security reasons, MOVEit DMZ is NOT permitted to establish connections with or push files to systems on either your internal network or on an external network. (If a "proxy push" or "proxy store-and-forward" solution is desired, MOVEit Central can be used with MOVEit DMZ to fill this role.)

MOVEit DMZ's Security Advantages Over Other "Secure FTP" Solutions

There are three "areas" where files are at risk when transferred between an external network (such as the Internet) and your internal network:

- When transferred over the INTERNET to a system in your DMZ.
- When temporarily stored on a system in your DMZ.
- When transferred from the system in your DMZ to a system on your internal network.

Most secure Web and FTP file transfer products reside on a system in a DMZ and use industry-standard SSL or SSH to provide secure transfers between the INTERNET and DMZ. (MOVEit DMZ does as well.) Unfortunately, that is as far as most products go; they fail to secure files stored on the DMZ (at risk if the DMZ box gets hacked) and fail to secure files being transfered between DMZ and MY ORG (at risk if a hacker sets up a sniffer inside the DMZ).

MOVEit DMZ secures all three areas by using SSL/SSH-encrypted transfers for ALL transfers and by using FIPS 140-2 validated AES encryption to secure files on disk.

In addition, only MOVEit DMZ offers complete end-to-end file integrity over FTP. In other words, files transferred with secure FTP or web clients which support file integrity checks through the MOVEit system can be proven to be 100% identical to their source files through the use of SHA-1 cryptographic hashes. (When combined with authentication, complete file integrity provides non-repudiation.)

Accessing MOVEit DMZ

"Client" access to MOVEit DMZ is available through several interfaces, including HTTPS, FTP over SSL, and FTP over SSH.

The built-in web interface provides access to anyone with a desktop web browser (see the complete list of supported browsers). Authorized administrators may configure the MOVEit DMZ server from authorized locations while customers and partners use a simpler portal to move files in and out of the MOVEit DMZ system.

Also available through the web interface, the optional MOVEit Upload/Download Wizard provides for faster and more reliable file transfers using the web than are normally available through "stock HTTP". The MOVEit Wizard is also the only browser-based client that supports file integrity checking.

A secure FTP interface is also available on the MOVEit DMZ server for people or programs with secure FTP clients. The MOVEit family offers two free, scriptable command-line clients, MOVEit Freely (FTP) and MOVEit Xfer (HTTPS) both of which support file integrity checking. Ipswitch also offers WS_FTP Professional, a Windows file transfer client with a robust feature set, which also supports file integrity checking. Many third-party companies manufacture secure FTP clients for desktops and servers which will also interface with MOVEit DMZ's secure FTP over SSL and FTP over SSH servers.

For IT departments who desire more control over the MOVEit DMZ environment than the FTP protocol can provide, the MOVEit DMZ API products provide easy access to and control of MOVEit DMZ via a COM object (for Windows) or Java classes (for *nix, Windows, IBM, etc.). MOVEit DMZ API also supports file transfers with full integrity checking and ships with several command-line utilities for administrators who would rather script than program.

If desktop-to-server automation or the ability to access MOVEit DMZ as a local folder is desired, consider using MOVEit EZ. MOVEit EZ is a "tray icon application" which synchronizes content between a user's desktop and MOVEit DMZ and schedules transfers.

When coupled with MOVEit Central and the appropriate licensing, MOVEit DMZ supports AS2 and AS3 file transfer. (MOVEit DMZ can be used as a standalone AS3 server, but without MOVEit Central it has no way of encrypting or decrypting specific messages.)

More information about these clients and the dozens of third-party clients which can also be used to securely exchange files with MOVEit DMZ can be found in the "Client Support" document.

Ad Hoc Transfer

The Ad Hoc Transfer Module, which requires a separate license, provides a secure way to do person-to-person file transfers. Registered MOVEit DMZ users can use a browser or an Outlook plug-in to send files and/or a message (which is called a 'package') to an email address. Composing a MOVEit package that includes files is like composing an email with attachments.

However, there are differences. File attachments sent as part of a package are uploaded to a MOVEit DMZ server. A 'new package notification' email will be sent to the recipients, to inform them that a package is waiting for them. Recipients can click on the web link in this notification, sign on to MOVEit DMZ, and view the package, where they can download the files.

If enabled, a recipient can also reply to a package and send additional attachments, which will also be uploaded to the file transfer server. The organization administrator can set options that determine who can send and receive packages, enforce user- and package-level quotas, and control package expiration and download limits.

Large files and multiple attachments can be sent quickly and securely, avoiding the limitations of a mail server.

MOVEit Central

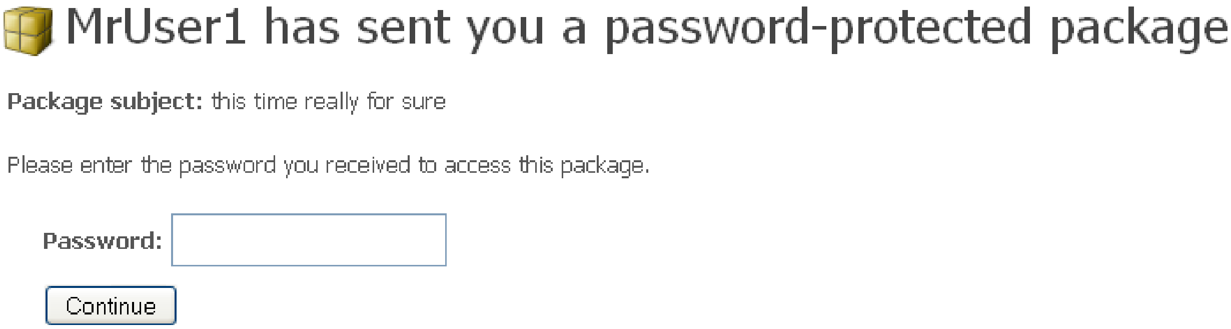
If more than ten scheduled file transfers, immediate movement of files to/from backend servers from MOVEit DMZ, or connectivity to other servers is desired, MOVEit Central is the best tool to use.

MOVEit Central can support thousands of file transfer tasks and is used in production to securely move hundreds of thousands of files a day at major data centers. MOVEit Central instantly knows when a file has arrived on MOVEit DMZ or a Windows file system and can immediately begin transferring that file to its final destination. MOVEit Central supports the most popular secure protocols used across industries, including FTP, SSH, FTP over SSL, SMIME, PGP, email and AS1/AS2/AS3.

In short, when paired with MOVEit DMZ, MOVEit Central completes a secure transfer system which can securely receive, record and send files to/from to almost anyone supporting a secure transfer protocol.

Guest User - Password Prompt

The Password prompt page is the first page you will see from the MOVEit DMZ site, after clicking (or copying into your browser) the link provided in the new package notification email.



MrUser1 has sent you a password-protected package

Package subject: this time really for sure

Please enter the password you received to access this package.

Password:

Enter the Password that was sent to you in either the package notification email, or via a separate notification email, then click **Continue**

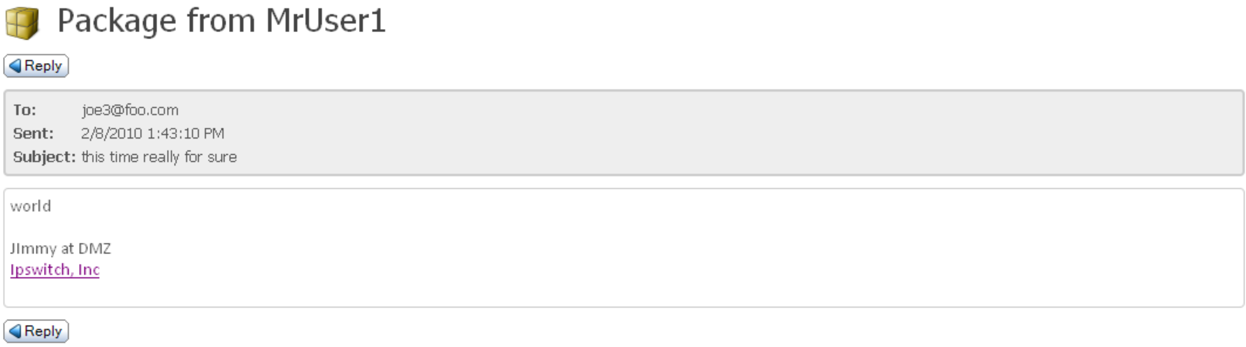
When you press the Continue button, your password is transmitted securely (via HTTPS) to MOVEit DMZ. If your password fails, you will see an error message. If you attempt to enter the password too many times in a short period of time you may get locked out of the system altogether.

If your password succeeds you will see the 'Package from [sender]' page.

Guest User - Viewing Packages

If you received a **new package notification**, click (or copy into your browser) the link provided in the email. The link will take you directly to the package referenced (after signing on with the password sent to you).

A package can contain a message and/or attached files.



Package from MrUser1

To: joe3@foo.com
Sent: 2/8/2010 1:43:10 PM
Subject: this time really for sure

world

Jimmy at DMZ
Ipswitch, Inc

The sender is shown in the title. The sent date and time, and subject, are shown in the package header section. Below that, the message body is shown, followed by a list of attachments, if there are any. A Download button is provided for each file attachment.

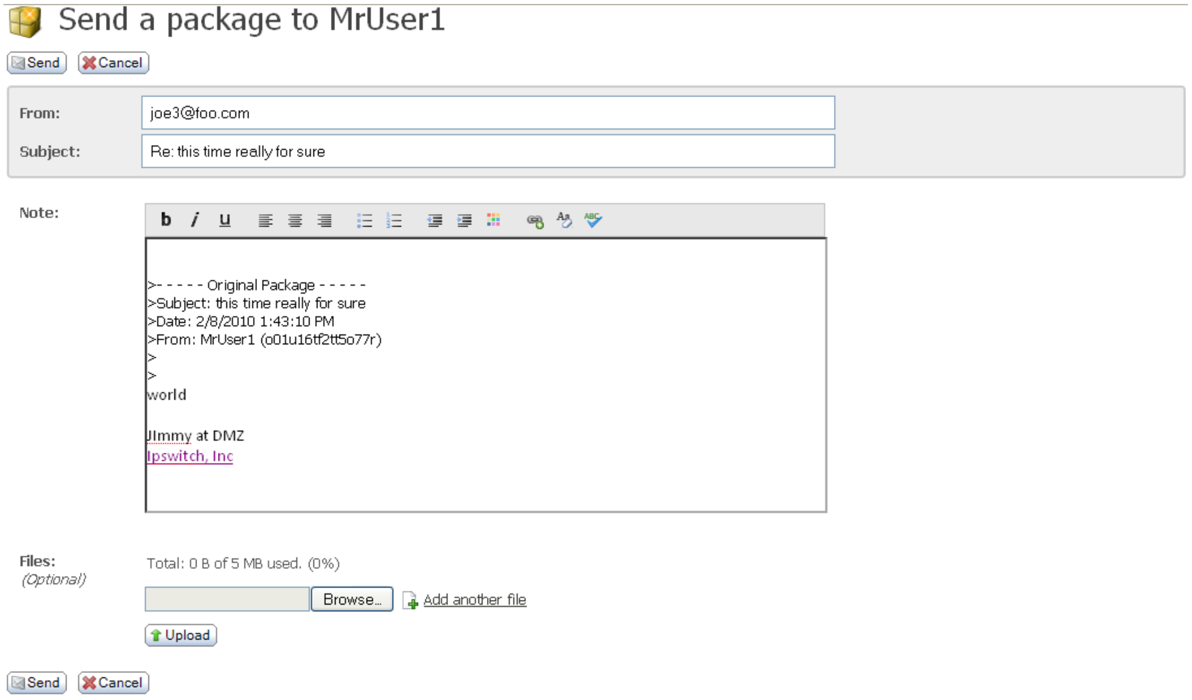
The actions you can take on this page are:

- **Download** - Downloads the file to your computer.
- **Reply** - Start composing a new package to the sender of the current package. The note from the current package will be retained and each line marked with the ">" character.

Guest User - Sending Packages

You can reply to a package and send files to the sender. This works like sending an email with attachments. As such, it is a familiar process, and uses a form similar to a compose email form.

1. While viewing a package, click **Reply**. The Package compose page opens.



Send a package to MrUser1

From: joe3@foo.com

Subject: Re: this time really for sure

Note:

>- - - - - Original Package - - - - -
>Subject: this time really for sure
>Date: 2/8/2010 1:43:10 PM
>From: MrUser1 (o01u16tf2tt5o77r)
>
>
world

JImmy at DMZ
Ipswitch, Inc

Files: *(Optional)*

Total: 0 B of 5 MB used. (0%)

2. Review the information, and optionally, enter your own Note.

   The title at the top of the compose page shows the intended recipient (the original sender). The **From** field shows your email address. The **Subject** field shows the original subject preceded by "Re:".

   The **Note** field shows the note from the original package, with each line marked with the ">" character. You can add a note for the original sender.

   If you are using a modern browser, depending on organization settings, you may see a rich text editor where you can type your note. In this editor, buttons above the editing box let you change the font, size, style, alignment, indentation, and even color of the text you enter. You can also enter links and lists.

   Users of modern browsers may also have a Check Spelling button available, which will check the spelling of both the package subject and the note. Misspelled words will be highlighted and you may use your left mouse button to select appropriate replacements.

3. Add files. To add a file attachment to your package, click the Browse button. You can select a file by using the browser's file selection interface, then click **Upload**.

You can add multiple files to the package. Click 'Add another file' to display another file entry field.

4. When you are done composing your reply and uploading any attachments, click **Send** to send the package.

   A 'package notification' email will be sent to the original sender, to inform them that a reply package is waiting for them.

General Information - Security

The following security features are functions of the MOVEit DMZ software and exist in addition to the hardening of the operating system and associated application services.

Transport Encryption

During transport MOVEit DMZ uses SSL or SSH to encrypt communications. The minimum strength of the encryption used during web transport (e.g., 128-bit) is configurable within the MOVEit DMZ interface.

This value is configurable by organization. To configure this value for any particular organization, sign on as a SysAdmin, view the organization for which this value should be set, and click the "Change Req" link to set the value. NOTE: If you set the minimum encryption value of the "System" organization (#0), you will be given the chance to apply your setting to ALL organizations in the system.

Storage Encryption

MOVEit DMZ stores all files on disk using FIPS 140-2 validated 256-bit AES (http://csrc.nist.gov/encryption/aes), the new (US) federal standard for encryption. MOVEit Crypto, the encryption engine on which MOVEit DMZ relies, is only the tenth product to have been vetted, validated and certified by the United States and Canadian governments for cryptographic fitness under the rigorous FIPS 140-2 guidelines.

MOVEit DMZ also overwrites just-deleted files with random bytes to prevent even encrypted files from lingering on a physical disk after users thought them to have been destroyed.

Precautions Taken During Transport-Storage Exchange

If files received by MOVEit DMZ were simply copied to a large cleartext memory buffer, trojan programs could potentially "sniff" sensitive files out of these spaces.

Instead MOVEitDMZ spools pieces of files received into much smaller buffers, encrypts them and writes them to disk almost immediately. Spooling files in this manner reduces overall exposure in two ways: 1) reduces amount of information exposed and 2) reduces time information is exposed. (This technique also yields some important performance gains.)

(A frequently asked question regarding this issue is "why not just store the file using SSL or SSH" - a short answer to this question is: SSL or SSH uses temporary keys which are renegotiated each time a client establishes a new connection, and we need "more permanent" keys for storage.)

Integrity Checking

When certain file transfer clients are used with a MOVEit DMZ server, the integrity of transferred files will be confirmed. All MOVEit secure FTP, API and web-based clients (including the upload/download Wizard) support integrity checking. Other FTP clients can also take advantage of integrity checks; see "FTP - Interoperability - Integrity Check How-To" for more information.

To perform an integrity check, both the client and the server obtain a cryptographic hash of the transferred file as part of the last step of the transfer. If the values agree, both sides "know" that the file transferred is completely identical to the original. The results of any integrity check are not only displayed to the user of the file transfer client but stored for ready access on the MOVEit DMZ server.

Immediate Transfer off Server

When used with MOVEit Central, MOVEit DMZ supports "event-driven" transfers which allow files to begin spooling to internal servers as soon as they land on an Internet-facing MOVEit DMZ server. This prevents even encrypted files from remaining on the server for longer than absolutely necessary.

Transfer Resume

MOVEit DMZ supports file transfer resume on both its HTTPS and FTPS interfaces. In addition to being useful during transfers of multi-gigabyte file, this feature is also a secure feature in the sense that it makes large file transfers less susceptible to denial-of-service attacks.

Folder Quotas

Enforceable folder size quotas can be set on various folders to prevent system storage from being exhausted.

User Quotas

Enforceable user size quotas can be set on various users to prevent them from exhausting system storage.

Delegation of Authority

Individual end-user members of a group can be designated as Group Admins. These users then are able to administrate the users, folder permissions and address books in their group, subject to various parameters set by organization administrators.

Administrative Alerts

Email notifications are sent to administrators when users are locked out, when the internal consistency checker notices something amiss with the database, etc.

One-Way Workflows

MOVEit DMZ can be configured to never allow users to download what they have just uploaded into the system. This configuration alone can prevent users from misusing MOVEit DMZ as a repository of personal or restricted materials. (Another common way to handle this scenario is through the use of IP restrictions.)

Password Aging

Users can be forced to change their passwords periodically with MOVEit DMZ's password aging features. Users will also be warned (via email) several days in advance of actual expiration, and notified again when their password expires.

Password History

MOVEit DMZ can be configured to remember a certain number of passwords and prevent users from reusing those passwords.

Password Strength Requirements

Various password complexity requirements can be set on MOVEit DMZ, including number/letter, dictionary word and length requirements.

Account Lockout

If someone attempts to sign on to a valid account with an incorrect password too many times, their account can be locked out and administrators will be notified via email.

IP Lockout

A very real concern of administrators of any authenticated resource which supports account lockouts is that someone will get a list of valid usernames and lock all of them out. To mitigate this risk, MOVEit DMZ offers a feature which will prevent a machine with a specific IP address from making any further requests of the system if MOVEit DMZ sees too many bad signon attempts. Administrators will also be notified via email when this occurs.

Restricted IP/Hostname Access

Specific users or classes of users can be restricted to certain ranges of IP addresses and/or hostnames.

Detailed, Tamper-Evident Audit Logging

MOVEit DMZ logs not only signon and signoff events, but permission changes, new user additions and other actions which directly affect the security of the system. Realtime views of this audit trail as well as detailed query tools are available on the Logs and Report pages. All log entries are cryptographically chained together in a way that makes any tampering (add, delete, change) of audit logs evident.

Remote Authentication

MOVEit DMZ's RADIUS and LDAP clients support any standard RADIUS and LDAP servers, including Microsoft's Internet Authentication Server, Novell's BorderManager, Microsoft Active Directory, Novell eDirectory, Sun iPlanet and IBM Tivoli Access Manager (SecureWay).

Obscured Product and Version Identity

MOVEit DMZ does not reveal its product name to unauthorized users via the SSH and FTP interfaces and can be configured to hide this information from web users as well. Version numbers are also only available to authorized users. Obscuring this information prevents hackers from figuring out what they are attacking without doing a fair amount of research.

Client Certificates and Client Keys

All major interfaces of MOVEit DMZ (SFTP, FTPS, HTTPS) support the use of SSL (X.509) client certificates and SSH client keys. SSL client certs and SSH client keys are usually installed on individual machines, but SSL client certificates are also available as hardware tokens.

Multiple Factor Authentication

When used with a username, IP addresses, passwords and client keys/certs offer one-, two- or three-factor authentication.

External Authentication

Organizations worried about storing username-hash combinations on MOVEit DMZ's protected database can use the External Authentication feature and move all non-administrative usernames and passwords to RADIUS or LDAP servers. (Access to the remaining administrative usernames can be locked to specific, internal-only IP addresses.)

Not-In-DMZ Storage Options

There are two ways to store MOVEit DMZ encrypted files in locations that are not in a DMZ. The first is to implement MOVEit DMZ Resiliency and store the data on a remote, logical drive. The second is to deploy MOVEit DMZ on a piece of an existing storage area network (SAN).

Web Browser "Clickable Keyboard" Keystroke Logging Protection

To prevent keystroke logging software and hardware from capturing the keystrokes used to sign on to a MOVEit DMZ using a web browser, a clickable keyboard is provided as an alternate method of data entry. The same keyboard also protects other password fields used throughout the application to protect other users as well.

Cross-Frame Scripting Protection

To help prevent cross-frame scripting attacks against MOVEit DMZ, the web interface will prevent itself from being loaded in a frame or iframe window. This can be overridden using the "contentonly" flag, if the goal is to integrate MOVEit DMZ with an existing portal application using frames. See the URL Crafting doc page for further details.

General Information - Regulations - Privacy/Security/Auditing

This guide answers some questions regarding MOVEit DMZ's expected conformance to HIPAA, FDIC, OCC, G-L-B Act, California SB 1386, Canadian PIPEDA, Payment Card Industry ("PCI"), Sarbanes-Oxley (a.k.a. "SARBOX") and other regulations. Please consult with Ipswitch for the latest information about how MOVEit helps its security-conscious customers achieve their file transfer and storage privacy and security standards as well as relevant contractual, industry and regulatory requirements.

- **"Data at Rest"** - MOVEit DMZ satisfies this requirement by encrypting all files stored on disk with FIPS 140-2 validated 256-bit AES encryption. MOVEit Crypto (the encryption module which powers MOVEit DMZ) is only the tenth product to have been vetted, validated and certified by the United States and Canadian governments for cryptographic fitness under the rigorous FIPS 140-2 guidelines.
- **"Data in Motion"** - MOVEit DMZ satisfies this requirement by using encrypted channels (SSL or SSH) when sending or receiving data.
- **"Tamper-Evident Audit Trail"** - MOVEit DMZ maintains a full audit trail of not only every file transfer but every administrative action as well. All entries are cryptographically chained in a way that makes log tampering (i.e., adding, deleting or changing entries) evident. Scheduled "tamper checks" are run automatically and may also be run manually whenever needed.
- **"Integrity Checking"** - MOVEit DMZ and MOVEit file transfer clients including the Upload/Download Wizard, EZ, Xfer, Freely, Central, API Windows and API Java use cryptographic hashes to verify the integrity of files throughout the transfer chain.
- **"Non-repudiation"** - MOVEit authentication and integrity checking allows people to prove that certain people transmitted and/or received specific files.
- **"Guaranteed Delivery"** - When MOVEit non-repudiation is combined with MOVEit transfer restart and transfer resume features, it satisfies the requirements for a conglomerate concept called "guaranteed delivery".
- **"Obsolete Data Destruction"** - MOVEit DMZ overwrites all deleted files with cryptographic-quality random data to prevent any future access. Specifically, MOVEit DMZ meets the requirements of NIST SP800-88 (data erasure).
- **"Need-To-Know Access Only"** - MOVEit DMZ user/group permissions allow specific access to only those materials users should access.
- **"Good Password Protection"** - MOVEit DMZ requires tough passwords, prevents users from reusing passwords and periodically forces users to change their passwords.
- **"Good Encryption"** - MOVEit DMZ uses SSL to communicate across networks. This "negotiated" protocol can be enforced to connect with 128-bit strength, the maximum currently available. MOVEit DMZ uses MOVEit Crypto's FIPS 140-2 validated 256-bit AES to store data on disk. (This algorithm has been selected by NIST to replace DES, and is faster and more secure than Triple-DES.)
- **"Denial of Service Protection"** - MOVEit DMZ is resilient to DOS attacks caused by resource exhaustion through credential checks or other resources available to anonymous users. ("Nuisance" IP addresses will be locked out.)
- **"Hardening"** - Installation of MOVEit DMZ involves a multi-step (and FULLY documented) hardening procedure which covers the operating system, web service environment, permissions and extraneous applications.
- **"Firewall"** - MOVEit DMZ comes with a detailed firewall configuration guide to minimize confusion on the part of firewall administrators. MOVEit DMZ also supports the use of native IPSec as a

"poor-man's" (packet filtering) firewall as a second line of defense.

- **"Code Escrow"** - The complete source code and build instructions of major (i.e. "3.2") versions of MOVEit DMZ are escrowed with a third-party.
- **"Code Review and Regression Testing"** - All MOVEit DMZ code passes through a code review and change control is maintained with the help of Microsoft's SourceSafe application. Regression testing is performed on each release with an ever-increasing test battery which now includes several thousand tests.
- **"Multiple Factor Authentication"** - When used with a username, IP addresses, passwords and client keys/certs offer one-, two- or three-factor authentication.