

MOVEIT DMZ: SECURE MESSAGING OPTION

The combination of secure messaging and secure file transfer capabilities in MOVEit® DMZ server is designed to help organizations improve collaboration and productivity for their employees, partners, and customers by providing a quick, easy, and secure way to safely exchange sensitive information via the Web — without using your email system to send either the messages or any attached files. This document offers an overview of the MOVEit DMZ Secure Messaging option and how it works.

Authorized users can securely exchange messages (with or without files attached) by logging into MOVEit DMZ using a regular Firefox, Internet Explorer, Mozilla, Netscape, Opera, or Safari browser (no Java, ActiveX or plugins required). Such connections are protected by 128-bit SSL encryption.

To send a message, users authenticate to MOVEit DMZ, click on the “Messages” link and then:

- Select recipients from their dropdown address book of users and groups.
- Enter a Subject line, type or “cut & paste” in a message and spell check it.
- Upload a file or files to go with the message, if desired.
- Save the message (and any attached files) as a draft or template.
- Choose to receive email notification when the message is received.
- Send the message and any attached files with a single click.

When sent, MOVEit DMZ starts an audit trail, securely stores the message and any attached files, (automatically safeguarding them with strong, built-in, FIPS 140-2 certified 256-bit AES encryption) and sends the recipients an arrival notification email via SMTP (this is its only use of regular email).

To retrieve a message, recipients open the arrival notification email and click on the URL in it. This points their browser to the MOVEit DMZ login page and automatically sets up an encrypted link. After authenticating themselves, recipients are shown the message and can then:

- Read the message, and download and delete the attached file(s).
- Reply to the sender and/or to others who received the message.
- Forward the message to other users or groups in their address book.
- Print, copy and paste, delete the message, or check its audit trail.

MOVEit DMZ secure messaging is especially well-suited for safely exchanging and storing financial, medical, consumer, human resource, legal, and trade secret information where the

contents of both the message and attached files are confidential and need to be safeguarded in transit and at rest. Secure messaging also complements existing email systems by providing a user-friendly alternative for transmitting file attachments. This helps organizations to maintain network security by letting them restrict email attachments to protect themselves against worms, trojans, and other malware.

Developers, scripts, and third-party applications can use the MOVEit DMZ API Java class or Windows COM component (each of which has an FTP command-line interface) to automatically exchange messages and files with a MOVEit DMZ server via its optional API interface. This can provide secure, automated delivery of messages with attached invoices, credit or medical reports, etc., with automatic email notification to senders and recipients, and a centralized end-to-end audit trail.

Please contact Ipswitch directly for additional information on MOVEit DMZ Secure Messaging. Or you can learn more by visiting www.IpswitchFT.com.



Ipswitch

10 Maguire Road • Lexington, MA 02421

MOVEit: (608) 824 3600 • moveitinfo@ipswitch.com