

MOVEIT DMZ: REPORTING CAPABILITIES

MOVEit DMZ comes with over 90 pre-defined reports, plus the ability to create an unlimited number of custom reports, all of which can be run against the data that MOVEit DMZ automatically logs to its secure, built-in database. This document provides details on the pre-defined file transfer, secure message, user status, user maintenance, security events, storage and performance reports, on its custom reporting, and also on its automated report scheduling and retrieval capabilities.

FILE TRANSFER ACTIVITY REPORTS

These reports summarize secure file transfer activity based on entries stored in the logs. Each of these reports breaks out organizations and uploads/downloads separately.

- Totals: to Date, or by Month, Week, or Day.
- Per User: Totals to Date, or by Month, Week, or Day.
- Per Group: Totals to Date, or by Month, Week, or Day.
- Per IP Address: Totals to Date, or by Month, Week, or Day.
- Per Interface: Totals to Date, or by Month, Week, or Day.

Each of these file transfer activity reports support the following options:

- Size Units (“K,” “M,” or “G”; used to express file sizes.)¹
- Start Date (e.g., “2004-10-01” or “” (none); if provided, log entries earlier than this date will be ignored). Note: Macros can be used.²
- End Date (e.g., “2004-10-31” or “” (none); if provided, log entries later than this date will be ignored). Note: Macros can be used.²

¹ Generation of file size data in these reports requires MOVEit DMZ v.3.3 or later.

² Examples of macros include [yyyy]-[mm-3]-[dd] and [yyyy]-[mm]-15.

SECURE MESSAGE ACTIVITY REPORTS

With the optional Secure Messaging module for MOVEit DMZ Enterprise, reports summarize secure message activity based on entries stored in the logs. Each of these reports breaks out organizations and posts/reads separately.

- Totals: to Date, or by Month, Week, or Day.
- Per User: Totals to Date, or by Month, Week, or Day.
- Per Group: Totals to Date, or by Month, Week, or Day.

Each of these secure message activity reports support the following options.

- SizeUnits (“K,” “M,” or “G”; used to express file sizes.)³
- StartDate (e.g., “2004-10-01” or “” (none); if provided, log entries earlier than this date will be ignored).
- EndDate (e.g., “2004-10-31” or “” (none); if provided, log entries later than this date will be ignored).

³ Generation of message size data in reports requires MOVEit DMZ v.3.3 or later.

USER STATUS REPORTS

These reports list users (and groups), their current status, and their permissions.

- Active Users
- Inactive Users
- Password About To Expire
- Group Summary
- Group Membership
- User List for Auditors
- Default Home Folder Permissions
- Folder Permissions
- Secure Message Address Books
- Quota: Any, Defined, or New or Above.

It is recommended that all of the following reports be run during a security audit.

- Group Summary
- Group Membership
- User List for Auditors
- Default Home Folder Permissions
- Folder Permissions
- Secure Message Address Books

SECURITY EVENT REPORTS

The following reports each highlight suspicious sign on attempts performed against MOVEit DMZ and should be run during a security audit.

- **Suspicious Usernames:** Many Attempts, or Different IP addresses.
- **Suspicious IP Addresses:** Many Attempts, or Different Usernames.
- **Locked-Out IP Addresses:** Current, or Historical.
- **Locked-Out Usernames:** Current, or Historical.

Each of these security event reports support the following options.

- **IPThreshold** (minimum number of different IP addresses required to be “many different IP addresses” - default=5).
- **UsernameThreshold** (minimum number of different usernames required to be “many different IP addresses” - default=5).
- **AttemptThreshold** (minimum number of attempts required to be “many attempts” - default=10).
- **StartDate** (e.g., “2004-10-01” or “” (none); if provided, log entries earlier than this date will be ignored).
- **EndDate** (e.g., “2004-10-31” or “” (none); if provided, log entries later than this date will be ignored).

STORAGE REPORTS

These reports display how many files, messages, and archived log files are currently stored on MOVEit DMZ, and how much disk space they currently consume.

- **Storage:** by Total, by Folder or User.
- **Storage:** by Folder including Subfolders.

Each of these storage reports supports the following options.

- **SizeUnits** (“K,” “M”, or “G”; used to express file sizes).

PERFORMANCE STATISTICS REPORTS

These reports examine the statistics gathered by the MOVEit DMZ SysStat service, which typically captures and writes data to the MOVEit DMZ database twelve times per hour. Note: Use of the SysStat service requires MOVEit DMZ v.3.2 or later.

Several of these reports are always broken down into additional categories. Typical breakdowns include Maximum, Minimum and Average values, and TotalSystem, DMZCore, DMZISAPI, IIS, MySQL, DMZFTP, DMZSSH, DMZScheduler, DMZResiliency, and Central application breakouts. There are some exceptions, as noted below.

- CPU Performance: All, or by Hour, or Day.
- Disk Performance: All, or Hour, or Day. ⁴
- Handles Performance: All, or by Hour, or Day.
- Memory Performance: All, or by Hour, or Day. ⁵
- Processes Performance: All, or by Hour, or Day.
- Threads Performance: All, or by Hour, or Day.
- Sessions Performance: All, or by Hour, or Day. ⁶
- Summary of Performance: All, or by Hour, or Day. ⁷

⁴ Disk reports list space available on the various drives.

⁵ Memory reports list Virtual and (Regular) memory separately.

⁶ Sessions reports list Active and All sessions separately.

⁷ Summary reports provide a summary of total CPU, total Free Disk Space, total Handles, total Processes, total Memory usage, and total Active Sessions.

Each of these performance reports support the following options.

- SizeUnits (“K,” “M”, or “G”; used to express file sizes).
- StartDate (e.g., “2004-10-01” or “” (none); if provided, log entries earlier than this date will be ignored).
- EndDate (e.g., “2004-10-31” or “” (none); if provided, log entries later than this date will be ignored).

USER MAINTENANCE ACTIVITY REPORTS

These reports summarize user maintenance activity based on entries stored in the logs. Each of these reports breakout organizations separately.

- Totals: To Date, or by Month, Week, or Day.
- By Activity: Totals to Date, or by Month, Week, or Day.
- Each of these user maintenance activity reports supports the following options.
- StartDate (e.g., “2004-10-01” or “” (none); if provided, log entries earlier than this date will be ignored).
- EndDate (e.g., “2004-10-31” or “” (none); if provided, log entries later than this date will be ignored).

CUSTOM REPORTS

In addition to all the previously listed pre-defined MOVEit DMZ reports, one can also define, run, and automate “custom” reports. Such reports must include defined fields and tables, and can also optionally include criteria, groupings, order, and limits.

Before running a custom report, MOVEit DMZ will automatically check to make sure the custom query works off of valid tables. In addition, MOVEit DMZ will also insert such additional criteria as may be needed to prevent custom queries from crossing organizational boundaries, and to ensure the final query is a safe, read-only query.

RUNNING AND RETRIEVING REPORTS

Reports can be scheduled to automatically run during the usual nightly run of MOVEit DMZ tasks. Reports can also be executed on an on-demand basis. Buttons and links enable a report to be run immediately and either: downloaded and/or viewed in a Web browser, or run and saved to a MOVEit DMZ folder. Scheduled reports can be run on specific days, which can be defined in a comma-delimited list of days of the weeks (“Tue, Wed, Thu”) and/or days of the month (“1, 15”).

A variety of MOVEit or third-party secure HTTP (HTTPS), secure FTP over SSH (SFTP and SCP2) and secure FTP over SSL (FTPS) clients can be used to download reports from MOVEit DMZ. (See the “MOVEit DMZ Compatible

Clients” document for specific clients, by protocol and OS.)

MOVEit Central tasks can automatically download reports from MOVEit DMZ and: copy them to the local file system or to shared network folders; transfer them using FTP or FTPS, SFTP or HTTPS; attach them to email messages and send them via SMTP. The same task can also optionally encrypt the reports using the MOVEit Central S/MIME object or OpenPGP option.

Third-party applications can dynamically create new custom reports as well as start and retrieve the output of pre-defined and existing custom MOVEit DMZ reports. This can be done by using a locally-installed copy of the MOVEit DMZ API Java class or the MOVEit DMZ API Windows COM component to remotely access the reporting functions via the optional MOVEit DMZ API interface.

To learn more, please visit www.lpswitchFT.com.

