AUDITING AND REPORTING MODULE (ARM) FOR EFT™

KEY RESULTS

- **Custom design reports** to show only the data that you care about
- **Preconfigured reports** of commonly requested reports
- **XML-based templates** make it easy to design, import, and export reports
- **Connect to SQL Server or Oracle relational database** to query report data

The Enhanced File Transfer™ (EFT™) Auditing and Reporting Module (ARM) captures all of the transactions passing through the EFT platform. When you want to run a report, EFT connects to the database, retrieves audited data based on your criteria, and then generates and displays the report. You can then export the report in XML, HTML, or PDF format to save or share.

QUICKLY FIND AND SOLVE FILE TRANSFER ISSUES

ARM records the events between the server and client, then enables you to effectively search and present that information any way you want, for billing, statistical analysis, troubleshooting, and non-repudiation. ARM captures significantly more data points than standard "flat-file" logging. Data is stored in real time in a relational database, which you can then query from within EFT, or query directly from your own reporting system.

SEE WHO CHANGED WHAT IN EFT

Administrators often need to know when and what changes were made to EFT and who made them. The Admin Actions report displays all EFT administrator activity for a specified range. EFT logs the following changes made to EFT to the ARM database:

- The date the action occurred
- The affected feature or Function.
- The type of Action (created, added, removed, modified, enabled, disabled, started, and stopped).
- The Affected Area (Server, Site, Settings Template, User Account, Event Rule, Command, Group, VFS, Report).
- The name of the affected object, Affected Name (Server Name, Site Name, Settings Template Name, User or Admin Account Name, Event Rule Name, Command Name, Group Name, Folder Name, Report Name).
- The name of the administrator that made the change, Change Originator.

USE BUILT-IN OR CUSTOM REPORT TEMPLATES

ARM comes with everything you need to run reports of EFT data, including more than 40 preconfigured reports, and a wizard-based custom report designer. The preconfigured reports have been carefully defined based on extensive interviews and research into the most important reporting needs, such as troubleshooting, nonrepudiation, billing, and trending.

You can use the preconfigured reports as is, edit the preconfigured reports, or create your own custom reports from scratch. The report designer uses familiar controls that you can use to build or edit reports quickly and easily. You can save your customized report definition templates as XML files to reuse or share.
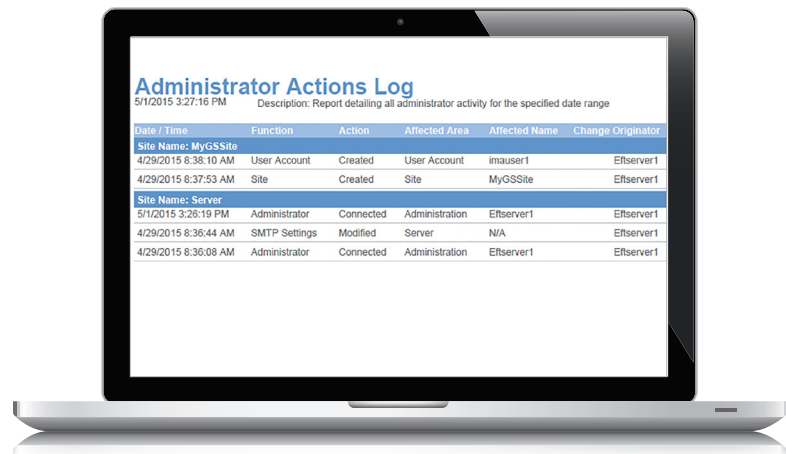
EFT

GLOBALSCAPE

The preconfigured reports fall into the following categories:

- **Billing**: If you need to bill your customers for file transfer services and need to supply accurate reports to customers and for your own invoicing purposes, these reports allow you to query and produce reports based on multiple criteria such as a specific client, a group of clients or all clients, a particular date range, and a specific file or all files transferred for that user.

- **Non-repudiation**: If you need to audit transactions throughout their life cycle and determine whether a particular Event occurred and when it occurred, these reports allow you to search for all activity for a specific user for a specific date or to locate a transaction within a date range for auditing purposes, and allow you to show conclusively whether something happened, when it happened, and who was responsible for making it happen.

- **Statistics:** Gathering statistical data allows you to take preventive measures (such as scale to meet increasing demand), to establish trends, create general usage reports for stakeholders, and to query and analyze trends and server usage (peak usage times, most active customers, etc.).

- **Technical troubleshooting:** Granular auditing of all socket, protocol, authentication, and transaction information allows the administrator to quickly locate and solve problem scenarios.

Administrator Actions Log
5/1/2015 3:27:16 PM   Description: Report detailing all administrator activity for the specified date range

Date / Time	Function	Action	Affected Area	Affected Name	Change Originator
Site Name: MyGSSite					
4/29/2015 8:38:10 AM	User Account	Created	User Account	imauser1	Eftserver1
4/29/2015 8:37:53 AM	Site	Created	Site	MyGSSite	Eftserver1
Site Name: Server					
5/1/2015 3:26:19 PM	Administrator	Connected	Administration	Eftserver1	Eftserver1
4/29/2015 8:36:44 AM	SMTP Settings	Modified	Server	N/A	Eftserver1
4/29/2015 8:36:08 AM	Administrator	Connected	Administration	Eftserver1	Eftserver1