GlobalSCAPE Enhanced File Transfer Server

Technical Overview of GlobalSCAPE Enhanced File Transfer Server

Published: May, 2007

Abstract

This paper gives IT professionals a technical overview of EFT Server, DMZ Gateway, EFT Web Transfer Client, Audit and Reporting module and Secure Ad Hoc Transfer module. EFT Server and its associated modules leverage cost-effective Internet-based data transfer and encryption technologies to provide secure and reliable file transfers.

Table of Contents

Introduction

The Internet has dramatically changed how organizations share data with business partners, customers and employees. Information that used to be delivered by mail, fax or courier is now transferred online in real time. This increased convenience and speed of delivery does not; however, come without risks: the integrity, confidentiality, auditability, and reliability of data exchange are critical business concerns.

Corporate information managers must protect business assets, ensure that policies and processes meet regulations governing the management of sensitive information, and ensure that the right people have access to the right information at the right time. Global operations, diverse business partners and networks further emphasize the need for common standards to ensure compatibility, scalability and cost-effective integration.

Organizations that use the Internet for data transfer are also faced with a daunting array of security challenges stemming from various regulatory and business requirements for data privacy and confidentiality. Regulatory and privacy requirements include legislation such as the Health Insurance Portability and Accountability Act (HIPAA), California Senate Bill (SB) 1386, and the Gramm-Leach-Bliley Act (GLBA) in the US, and the European Union's Privacy Directive, some of which impose severe penalties for improper disclosure of confidential information. Additionally, industry best-practices and self-imposed business requirements include intellectual property and trade secrets protection and controls regarding disclosure of proprietary information to minimize corporate risk from the devastating consequences of security breaches.

EFT Server meets these needs and more. Thousands of organizations use GlobalSCAPE's secure servers to transfer and manage the enterprise data that drives their business.

Industry Solutions

There are numerous approaches to securing data transactions, ranging from traditional paper-based or closed-network electronic data interchange (EDI) methods to modern secure applications that use the Internet or other IP-based network for secure data delivery. Typical approaches to secure data delivery and their limitations include:

- Paper-based (courier, fax, overnight mail-delivery)
  - Slow delivery
  - No data-on-demand
  - More expensive per MB transferred (under typical scenarios)
- Traditional EDI
  - Expensive (leased lines, VAN charges)
  - Complex new partner setup
  - Too costly for smaller partners
  - Limited or non-existent access for customers
- VPN
  - Protects transport but offers no post-transfer data protection
  - No inherent post-transfer management or automation
  - Not scalable for extranet use
  - Allows login to operating system accounts
  - No industry standard logging of transactions
- Secure E-mail
  - Severe data (attachment) size limitations
  - No post transfer management or automation capabilities
  - Not real-time (depends on recipient checking e-mail)
- Home Grown Solutions
  - Costly to maintain and extend
  - Additional costs for platform coverage
  - Difficult to ensure security

The EFT Solution

Organizations are increasingly moving away from traditional or legacy based data exchange solutions and towards Internet-based technologies due to the many benefits they offer for data transfer and increased security. These benefits include:

- Increased speed of data delivery
- Significant cost savings over legacy transmittal mechanisms
- Increased efficiency of business processes and worker productivity
- Reduced complexity of setup and deployment
- Minimal investment compared to traditional solutions
- Standards compliant transport and data encryption services
- Highly scalable

Analysts have identified a set of business requirement prerequisites that persist across industries that need secure data transfer and management. The solution:

- Reliable, cost-effective, and modular
- Compatible, standards compliant, and works with major global vendors
- Auditable, supports industry standards and detailed logging
- Well documented, includes training, and demonstrates knowledge and skill
- Flexible, contains security measures, access control authentication, and proof of authority mechanisms
- Familiar, encourages rapid adoption by end users, and has a minimal learning curve

The EFT solution meets these requirements and provides:

Flexible client connectivity options

Connect with:

- The EFT Web Transfer Client, a Java-based self-deploying thin client
- CuteFTP Professional Windows or Mac FTP clients
- Any 3rd party clients that adhere to industry standard protocols

Confidentiality and security

- Industry standard FTP and HTTP over:
  - Secure Sockets Layer (SSL)
  - Transport Layer Security (TLS)
  - SSH2 (Secure Shell's SFTP)
- Digital certificates and public key authentication for identity validation
- OpenPGP encryption for files residing on the server
- Multiple mechanisms for registering, authenticating and authorizing users
- User accounts isolated from network user accounts, ODBC-based or network-based authentication (NT/AD/LDAP)
- Advanced protection from Denial of Service (DoS) and flood attacks

Secure DMZ data exchange

- No data stored in the DMZ
- No authentication and directory listings stored in the DMZ
- No inbound holes needed in the firewall
- No synchronization or replication of user database needed in DMZ

Advanced Auditing and Reporting

- Track usage and bill your clients more accurately
- Establish trends, find out who your most active customers are, or when demand is the highest.

- Capture all socket, protocol, authentication, and transfer information then rapidly analyze it to pinpoint problems
- Non-repudiation of receipt

Secure Ad Hoc file transfers

- Send files too large for e-mail attachments
- Pick-up files sent back to your organization
- Admin doesn't need to setup FTP accounts
- Transparently secures files sent
- Provides auditing compliance
- Non-repudiation of receipt

Data transfer reliability and integrity

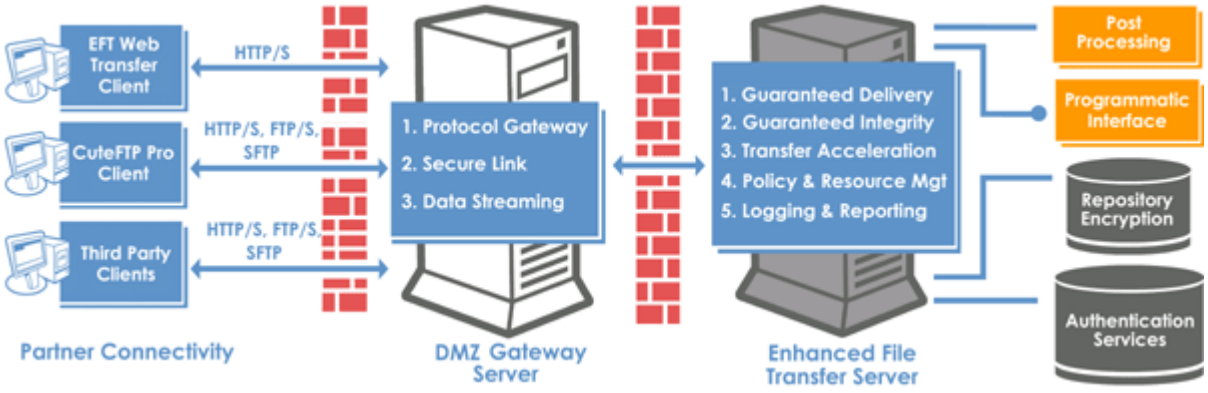
- Manual or automatic checkpoint restart for guaranteed delivery
- Cyclical Redundancy Check (CRC) checksums for data integrity validation
- Scheduled backup and archival for easy data backup and restoration
- Accelerated data transfers using segmented (multi-part) and concurrent delivery

Automated data management

- Event triggers for performing post-delivery actions including:
  - E-mail notification to one or more recipients
  - Run a command or process, giving you virtually unlimited extensibility
  - Encrypt, decrypt or sign data using the included OpenPGP component
  - Move data to a network drive or to another server using a variety of protocols
- COM (Component Object Model) for automating time-consuming tasks or integrating into your custom application
- Synchronization tools for mirroring content across systems
- Tools for monitoring and publishing content change

EFT Architecture

EFT Server provides the enterprise with a secure and reliable file management system using industry standard protocols and customizable automation tools. It integrates rapidly into existing electronic data exchange processes. The complete EFT Server solution involves a client such as the built-in EFT Web Transfer Client, a DMZ Gateway Server, EFT Server, Auditing and Reporting module and Secure Ad Hoc Transfer Module.



GlobalSCAPE's Enhanced File Transfer Solution

EFT Server

EFT Server is the core of the EFT solution: a secure, reliable server with extensive automation capabilities and support for a wide range of protocols, all controlled from a lucid, logical interface, making integration with existing data exchange systems—yours or a trading partner's—easy.

EFT Server

EFT Server Security

EFT Server provides a robust security architecture for meeting business and regulatory requirements. It ensures that encrypted transactions occur only with the appropriate entities and that data confidentiality and integrity are preserved during transport and storage. The technology required to meet these objectives are:

- Registration & Authorization
- Authentication
- Life-cycle Management
- Data Transport Security
- Data Storage Security

Registration and Authorization

Registration adds new trading partner user accounts to an environment. Authorization establishes the permissions for those accounts. GlobalSCAPE EFT Server supports multiple methods for adding, storing and controlling permissions for accounts. User profiles can be managed internally or externally through NTLM, Active Directory (AD), LDAP, or ODBC data sources.

Methods for adding new user accounts

- **Manually –** User accounts can be created from a Windows-based administrator interface (locally or remote).
- **Programmatically –** The EFT COM (Component Object Model) interface can register and authorize thousands of users in seconds.
- **Implicitly –** EFT Server can query of existing user domains (such as Active Directory), LDAP, or ODBC data stores.

Methods for storing user accounts

- **Virtual users –** EFT Server provides a proprietary database for storing user accounts and permissions. These accounts are isolated from the operating system accounts and they are only authorized to access the services provided by the server.
- **LDAP and Windows Active Directory users –** EFT Server queries the LDAP or Active Directory Database on the domain of the system that is running the server or queries the Primary Domain Controller for the domain and adds all users. This is helpful for organizations that have a large number of users and have already configured Active Directory or LDAP permissions.
- **ODBC users –** The server can query any ODBC compatible database. This allows user management (addition, modification, removal, etc.) from any application that can communicate with the database or through its COM interface. ODBC users also have the benefit of isolation from operating system users.

Permission controls

Authorizing users for system resource (bandwidth, directories, files, etc.) access is accomplished through numerous granular permission controls. Resources can be controlled down to bandwidth limits and hard disk space utilization, to IP address and file type restrictions. EFT Server user and account controls include:

- Folder permissions (read, write, exec, list, create, rename, delete, etc.)
- Maximum transfer speed allowed
- Maximum concurrent connections per user account
- Maximum concurrent connections per same IP address
- Maximum concurrent connections to the server (from all users)
- Maximum uploads/downloads per session per user
- Maximum uploads/download size per session per user
- Maximum disk space allowed (quota) per user
- Disable account after defined number of incorrect login attempts
- Ban IP after defined number of invalid commands
- Allow certain commands (NOOP, XCRC, etc.)
- Allow protocols (FTP, FTPS (SSL/TLS), SFTP (SSH), HTTP, HTTPS (SSL), SFTP)
- Require client certificates for FTPS (SSL) sessions
- Require client public keys for SFTP (SSH) sessions
- Allow password type (standard, OTP, or anonymous)
- Define user's root login folder
- Restrict access to a defined IP address
- Listen on a specific IP address and port
- File type exclusion filter
- IP address grant/deny access list
- Flooding/hammering auto-ban sensitivity

Authentication

Registered users who wish to establish a secure session should prove their identity before the session takes place. Traditionally, this consisted of password-based authentication mechanisms that were inherently weak because the password was transmitted across the network in plain text. EFT server provides state-of-the-art authentication choices for securing the session and establishing the validity of the authenticating user. These choices include:

- Digital Certificates
- Public-key Authentication
- One Time Password (OTP) Authentication
- Standard Password-based Authentication

Digital Certificates

Digital certificates are an electronic means of establishing a client or server's credentials. If signed by a trusted Certificate Authority (CA), it theoretically becomes tamper-proof and virtually impossible to forge. Digital certificates usually contain information about the subscriber, the identity of the organization who issued the certificate, the subscriber's public-key (used for encrypting and decrypting subsequent transmissions), the operational period for which the certificate is valid, and the signature of the issuing authority. EFT Server supports digital certificates in a variety of industry-standards such as PEM, Base64 Encoded X.509, DER Encoded X.509, PKCS#7, and PKCS#12. Additionally it includes a complete certificate management system that allows you to:

- Create certificates for signing by a Certificate Authority (CA), or self-sign them (implicit trust)
- Add or remove certificates from a trusted list
- Import certificates from a mutually trusted, third party
- Set a certificate expiration date
- Choose the certificate strength (bit-length), and type (how it is encoded)

Public Key Authentication

Public key authentication can be used in addition to or as a replacement for password-based authentication when establishing SFTP sessions (SSH2). Public keys are similar to digital certificates because they can be distributed to 3rd parties (unlike a password) as long as the private key is present on the system that is initiating the transaction. EFT Server includes provisions for creating and managing public/private key pairs, including the ability to import and export keys and add public keys to a trusted list.

One Time Passwords (OTP)

Secure solutions requiring advanced authentication protection, but not transport encryption or user validation such as an internal network with implicit trust, may wish to use an authentication mechanism like the One Time Password (OTP) system. OTP (RFC 2289) is an advanced password scheme based on Bellcore's S/Key protocol (RFC 1760). This system offers a secure alternative to standard password-based authentication mechanisms, as compromised passwords do not pose a security threat due to their single-use nature.

Standard Password-based Authentication

EFT Server also supports traditional password-based authentication, which consists of usernames and passwords being transmitted in plain-text. While not recommended for mission critical applications, certain business models avoid security altogether in favor of faster authentication and transfers. The typical scenario is a company in which files are made publicly available to any connecting user (called anonymous users), such as a public FTP site containing downloadable product demos, software drivers for a retail hardware component, or an HTTP site with publicly available documents.

User Account Management

Organizations often require the ability to quickly and efficiently remove users such as a departing employee or ex-partner, manage temporary accounts, as well as address the revocation and if necessary re-issuance of public-keys or certificates should they expire or become compromised. EFT Server addresses these needs through the use of life-cycle management tools giving you the ability to:

- Set an account expiration date
- Set a certificate expiration date
- Manually disable an account
- Automatically disable an account based on improper or suspicious activity
- Create new accounts using step-by-step wizards

Data Transport Security

Modern applications use Internet-based communication mechanisms to complete live financial transactions, transfer patient medical records, and move and transform data in the supply chain. Because of the public nature of the Internet, the confidentiality of such transactions should be preserved through strong encryption and security. The applications that perform electronic data exchange typically rely on protocols that are specifically geared towards enabling secure data transfer across public networks like the Internet. New standards, such as IPSec and S/MIME, have emerged, but they are often subject to vendor interpretation and not widely used. More established protocols such as SSL/TLS and SSH provide fewer interoperability problems and are generally more accepted across industries.

EFT Server uses industry standard security protocols to ensure interoperability with existing secure applications. Additionally, it employs FIPS compliant algorithms in accordance with U.S. Government Department of Defense (DoD) specifications in order to ensure maximum protection and confidentiality of data transmissions.

Protocol	Transport Encryption	Integrity	Certificate Authentication
FTP over SSL	Optional	No	Yes
TLS (SSL v3)	Optional	No	Yes
SFTP (SSH2)	Entire Session	Yes	Yes
HTTP/S	Entire Session	No	Yes

Secure protocols supported by EFT Server

Secure Socket Layer/Transport Security Layer (SSL/TLS)

The SSL protocol is widely used by Internet Web browsers and Web servers for session authentication and confidentiality. GlobalSCAPE EFT Server supports Secure Socket Layer (SSL) and its newer version, Transport Layer Security (TLS), for protecting data transmissions over both FTP and HTTP protocols.

Secure Shell (SSH2)

Popular among academic institutions and UNIX/Linux organizations, SSH has become the protocol of choice for secure remote login and other secure network services (SFTP, SCP) over a typically unsecured network. EFT Server supports SFTP, including password and public-key based authentication mechanisms.

While both SSL and SSH accomplish pretty much the same goal, there are pros and cons to each protocol. It is often easier to configure access to an SFTP server through a firewall due to the dedicated SSH connection port (22). SSH also offers public-key authentication so that no passwords are required. SSL is more widespread than SSH, and is formally ratified (various RFCs) and offers greater identity validation support through certificate chains of trust.

Hyper Text Transfer Protocol/Secure (HTTP/S)

In addition to FTP over SSL or the equivalent SSH2 version of FTP (SFTP), GlobalSCAPE EFT Server supports HTTP and HTTP over SSL (HTTPS) sessions. Regardless if your trading partner, remote employee or customer is using an FTP client or a Web browser, they can connect to, authenticate, browse, and transfer files using either protocol, in plain-text or secure implementations.

Data Storage Security

Data transmission over a public network such as the Internet is not only at risk during transport, it is also at risk when stored on Internet-accessible servers, such as those residing in "Demilitarized Zones" (DMZs). Placing a server in the DMZ creates a reliable mechanism for distributing data among business partners, remote employees, customers, and suppliers. Using an EFT DMZ Gateway Server in the DMZ gives you the same reliable mechanism without having to risk placing any data at all in the DMZ. EFT Server extends this inherent security with the ability to:

- OpenPGP encrypt, decrypt or sign files
- Push files to another EFT or 3rd party server using secure protocols

- Pull data securely from Enhanced File Transfer Server from within the network
- Streaming repository encryption
- Any combination of the above

OpenPGP

Organizations transferring mission critical or classified documents, or requiring increased data security on Internet-accessible systems, may wish to encrypt data as it is received and subsequently stored on disk. GlobalSCAPE EFT Server can generate public/private PGP key pairs or import existing public keys. OpenPGP support includes:

- Create public and private key pairs
- Establish key expiration dates
- Import public keys only or key pairs
- Set a default site key for encrypting and signing data
- Encrypt, decrypt or sign based on a timer event, incoming or outgoing file event, or other events

Streaming Repository Encryption

EFT's streaming repository encryption can encrypt files stored on disk in the EFT Virtual File System (VFS) transparently to a read or write operation of the file server. The advantage to this is that only encrypted data is ever stored—even temporarily—on disk. When a file is requested and read by an authorized client, it is decrypted for transmission, but still remains encrypted on the filesystem.

Data Push or Pull

Sensible security practices dictate that confidential data transferred to a publicly accessible server should not remain on that server due to the risk of exposure or compromise. If the publicly accessible server is configured to broker the incoming transactions with a server inside the corporate firewall, it safeguards the files since they reside on a secure corporate intranet, inaccessible from public networks.

GlobalSCAPE EFT Server can automatically move uploaded files to another FTP, Web, or EFT Server inside the enterprise firewall, or any other location using any of the protocols it supports. This is accomplished using Event Rules that trigger an action (based on a variety of customizable conditions) to copy or move uploaded files within the integral file system or to a remote system using any of the following protocols: FTP, FTPS, SFTP, or HTTP/S protocols.

Reliability

Transferring files over the Internet can be a complex, time-consuming and hands-on process. Deficiencies in protocol and network reliability often inhibit critical data transfers from taking place. One weakness is that certain protocols do not inherently support the capability to retransmit data if the target host becomes temporarily unavailable. Another problem is the lack of positive verification that a file was transferred successfully and that the transmitted data arrived intact and uncorrupted. Because of these limitations, the person initiating the transfer is often forced to oversee the entire transfer process through to completion. The following shows how EFT Server solves reliability problems with state-of-the-art data and transaction technology.

Guaranteed Delivery

When you initiate a transfer, EFT Server's guaranteed delivery mechanisms ensure integrity and completion. Typical problems associated with file transfer include:

- **Interrupted transfers –** Remote connections are frequently interrupted (network error, server disconnect, etc.) EFT Server supports auto-resume attempts from file transfer clients with resume transfer capability, such as CuteFTP Professional.
- **Transfer paused by initiator –** Transfers in progress can be paused and restarted at any time while using a supporting client. This is often referred to as checkpoint restart or manual restart.

Data Integrity Checking

Data integrity is a critical part of electronic data transmissions, especially when mission critical or classified data is involved. All TCP/IP packets arriving at the destination does not guarantee that a transfer is successful. The actual data being transferred may be corrupted in transit or during the storage phase. Typical scenarios include compromised transmissions where data is replaced in transit, or a failed disk I/O operation, such as when a disk becomes full. Most protocols and applications provide only minimal data integrity verification mechanisms. Aside from inherent measures built into the underlying protocols used, EFT Server offers the following additional measures to protect against corrupted data:

- **Cyclical Redundancy Checking* (CRC).** CRC is the process of comparing the checksum of a transferred file compared to its original source. The source and destination file checksums are compared once the transfer is finished. If the checksums match, the file transfer is considered complete. If they don't match, an error is reported and the transfer is retried until the checksums match.
- **MAC checking**. Message Authentication Code (MAC) checking is similar process to CRC checking except that it applies only to SSH2 connections. The transferring packets are verified; however, no further validation occurs once the transfer is completed and the data is stored on disk.

**CRC checking requires use of a supporting client, such as CuteFTP Professional, EFT Web Transfer Client, or CuteFTP Mac Pro.*

Accelerated Transfers

Business managers often recognize that confidential company data must not be compromised; yet they demand fast and inexpensive data transfer capabilities. Securing data during transport or upon storage is a bandwidth and CPU intensive process that takes a direct toll on the speed and efficiency of the transfer. Even non-encrypted transfers of massive files such as multi-media, ISO images, or complete system backups may require hours, if not days, to complete, especially when transferred over large geographical distances or through multiple Internet hops. Typical acceleration methods in the past have included everything from SSL hardware accelerators to costly direct physical links between systems. Most of these solutions limit transfers to sequential operations (one file at a time), which is grossly inefficient when large amounts of data are involved. EFT Server solves this problem using accelerated transfer technology:

- **Multi-part* Accelerated Transfers (Segmented Delivery) –** This cutting-edge approach to transferring large files can accelerate transfers by over 400%. A file is segmented (split) into multiple equally sized parts, and each part is then transferred simultaneously over a separate thread. Once all segments are received, the resulting parts are recombined back into a whole file.

- **Simultaneous Transfers (Concurrent Delivery) –** When used with a supporting client such as CuteFTP Professional, EFT server can permit multiple simultaneous sessions over FTP/S, HTTP/S or SFTP. EFT Server can handle as many simultaneous connections as allowed by the underlying hardware, and allowed sockets by the operating system.
- **Mode Z Compression* –** Allow users to compress transfers on the fly to speed up delivery and increase bandwidth efficiency with streaming compression.

**Multi-Part Transfers and Mode Z Compression require use of a supporting client.*

Auditability

A compromised server or transmission often results in the manipulation or destruction of data. It is often necessary to determine the When/What/Where of these types of events and if necessary prove that an event was conducted by a specific user. Auditability is the degree to which sufficient records are kept to document a specific transaction or event and is typically achieved through detailed logging, non-

repudiation of receipt (NRR), and message disposition notification (MDN). GlobalSCAPE's auditability features satisfy the most sought after auditability requirements by organizations today.

Detailed Logging

EFT Server logs all incoming and outgoing transactions to the following log file formats:

- W3C
- NSA
- Microsoft IIS (Extended)

EFT Server can rotate logs on a daily, weekly, or monthly basis. Selection of the rotation period is based on administrator preference and the amount of server traffic. Since an access log file typically grows 1 MB or more per 10,000 requests, even a moderately busy server will generate large log files.

Connection Monitoring

Troubleshoot problem connections with connection monitoring. Examine per-connection logs in real-time, search for text, filter results, and configure monitoring options.

Message Notification

Message Notification is the process by which a message is returned to the originator of a transaction indicating that the transaction has been completed successfully. A completed transaction can trigger an event that will send an e-mail to the administrator, the originator of the transaction, or a 3rd party, informing them of the fact that the transaction was completed successfully. This process helps provide peace of mind and assurance, without having to constantly check the server or ask the administrator if the data has arrived.

Non-Repudiation

Non-repudiation is a security mechanism that makes it difficult or impossible for a user to deny performing an operation or initiating a particular transaction. It ensures that both transactions and activities are binding to the user that performed them. EFT Server provides a level of NRR using the following:

- **Digital Signatures.** EFT Server supports digital signatures for user authentication.
- **Encrypted/Signed Logs.** EFT Server can encrypt and sign logs upon rotation as part of its Event Rules launching a custom script.
- **Detailed Logging.** EFT Server not only logs FTP and HTTP transactions, it also logs the source and destination file CRC checksums upon completing a transfer. This information helps prove that a file was received successfully and not corrupted during transit.

Automation

Modern organizations benefit from Internet-based technologies such as FTP and HTTP due to the speed, reliability and wide spread acceptance of these protocols. These benefits are especially apparent when large numbers of trading partners and routine, batch-processed transactions are involved. Many organizations often require additional capabilities, such as scheduling, unattended automated operations, pre- and post-transaction processing, and data translation/transformation services. Traditional solutions, such as EDI applications come with high price tags and implementation costs that can run into the millions of dollars. The high cost and instability of the EDI services market has caused the emergence of transactional delivery mechanisms such as Web Services. EFT Server can integrate with Web Services and provides the automation, provisioning and management capabilities required by most organizations in an affordable, easily deployed package.

Event Rules & Actions

Post transaction data and management capabilities are an integral part of EFT Server's comprehensive event-based rules system. With it, you can automatically perform pre-defined actions when specific events occur and conditions are met. A powerful Custom Commands mechanism is also included for client-initiated actions that fall outside of standard FTP operations. Customization and extensibility are

powerful capabilities provided by the robust architecture of the server. Through use of existing or custom-developed web services and/or scripts, used in conjunction with Custom Site Commands and Event Rules, the possibilities for expansion of the server are nearly limitless. A few examples of actions you can perform are:

- Send an e-mail notification upon file arrival
- Send an e-mail notification when quota limit exceeded
- Send an e-mail warning a user if connected using the wrong protocol or attempted to upload a banned file type, etc.
- Move a file to a new folder upon arrival
- Move a file securely to another server upon arrival
- Encrypt a file upon arrival
- Encrypt and archive server logs upon log rotation
- Delete an account upon login
- Start an application and pass certain parameters to it
- Check a file extension against a filter and automatically delete it
- Compress files upon arrival

Component Object Model (COM) Interface SDK

Another valuable benefit of EFT Server and CuteFTP professional for Windows is how they expose their primary functionality through a Component Object Model (COM) interface.

Organizations wanting to deploy custom applications internally or externally, automate administrative tasks, simplify or hide transfer interfaces for their partners, customers or employees, can do all these things using COM to communicate with EFT Server and CuteFTP Professional.

The extensibility provided by COM allows EFT Server to integrate into most organization's custom processes.

EFT Server COM capabilities

EFT Server's COM exposed interface provides enterprise integration capabilities. The server is made up of two components, the Administrator Interface and the Server Service (or Server Engine). The Server Service runs as a Windows service and starts automatically when your computer starts up. It can be controlled by the Administrator Interface, or through COM. The COM interface allows you to control the server from your own custom applications using any COM enabled programming language such as Visual Basic (VB), Java, .NET's C#, C++, and many others. Virtually every aspect of the server is exposed through the COM interface. Tasks you can perform using the server COM interface include:

- Add new users (for example, to automate the addition of thousands of users)
- Start and stop the server from listening (receiving new connections)
- Change server, site, and user settings
- Change directory permissions for users and groups
- Manage the file system (create physical folders, virtual folders, etc.)
- Manage certificates
- Change the server's IP address
- Query the server for information on users and export to a spreadsheet
- Remove users, groups, sites, and settings levels

Client Connectivity

Enterprise class file transfer suites require the availability of thin or "clientless" connectivity options. Ideal thin clients rely on industry standard protocols for trading partner connectivity. This eliminates the need for trading partners to rely on a particular vendor's file transfer client or proprietary protocol implementation.

Client Connectivity

The benefit to your trading partners of using industry standard Internet protocols and clientless connectivity options include:

- Reduced cost
- Reduced setup and implementation time
- Cross-platform connectivity
- Small footprint uses minimal system resources
- Zero maintenance
- Connect from anywhere

EFT Server offers a variety of Trading Partner connectivity options:

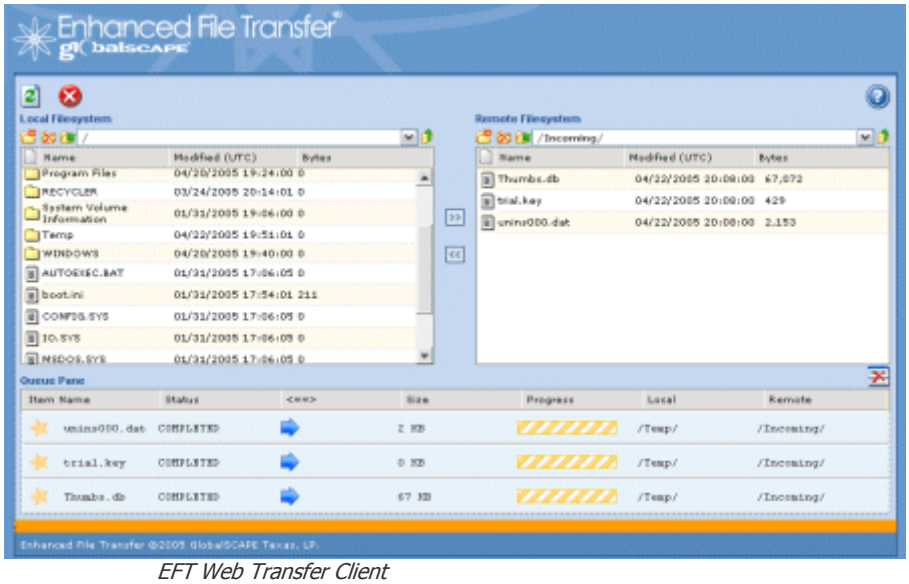
- EFT Web Transfer Client, a browser-based thin client
- GlobalSCAPE CuteFTP Professional file transfer clients
- Third party file transfer clients

Enhanced File Transfer Web Transfer Client

EFT Web Transfer Client is the ideal choice if ease of use and transparent deployment are priorities. It has broad compatibility, allowing you to support any partner without requiring them to invest in a client solution. The EFT Web Transfer client deploys automatically and can be used by any trading partner using virtually any Web browser.

Benefits of the EFT Web Transfer Client:

- Small footprint is easy on system resources
- Thin client deploys automatically, making integration easy
- Rebrandable interface allows customized partner interface: modify the .css yourself and just drop in your own images to give the client your own look.
- Works in most browsers—no need for additional software
- Works in most OSs, including Windows, Linux, and OS X
- Validates transfer success through automatic data integrity checksums
- Guarantees delivery of interrupted transfers using manual or automatic checkpoint restart
- Drag 'n drop file transfers (IE only)
- Multiple concurrent transfers for fast delivery
- Transfer queue support for management of transactions



EFT Web Transfer Client

CuteFTP Professional

If FTPS/SFTP protocol support, or any of the extended features EFT Server includes, is a requirement for your solution, CuteFTP Professional fully support all of EFT Server's features, including multi-protocol support, the ability to accelerate transfers, auto-resumption of interrupted transfers, and data integrity validation upon transfer completion.

Key features:

- Cross platform (Windows and Mac)
- Multi-protocol support (FTP over SSL/TLS, SFTP (SSH2), and HTTP/S
- Automatic and manual checkpoint restart
- Data integrity checking
- Accelerated multi-part (segmented) transfer technology
- Compressed (streaming compression) technology
- Easy to use drag and drop interface
- Low cost per seat

Third Party File Transfer Clients

EFT Server supports a wide variety of industry standard Internet protocols. Your trading partners can connect to EFT Server using their client of choice, whether existing or new. EFT Server can work with any third party client that supports the appropriate protocols, but use of third party clients does introduce some limitations:

- Little or no support for the extended file transfer features such as automatic resume, data integrity checking, accelerated and compressed transfers, and others, that EFT Server offers.
- Limited extensibility
- Transfers are often limited to one, or at most, two protocols

DMZ Gateway

EFT's DMZ Gateway provides highly secure data transmission from a Demilitarized Zone (DMZ) through a firewall to a back-end area such as a company intranet. When set up, the DMZ Gateway becomes a virtual extension in the DMZ of EFT Server. As far as external users can tell, they are accessing the EFT Server directly. The DMZ Gateway handles all external requests in the DMZ for the EFT Server, effectively creating a virtual EFT Server in the DMZ without the risk of exposing data there.

EFT DMZ Gateway

The EFT Server establishes an outbound connection initiated from the back end to the DMZ Gateway, and the DMZ Gateway then passes all user requests through socket level channels initiated from EFT Server. The result is that inbound holes through the firewall are not necessary. The DMZ Gateway acts transparently; and allows EFT Server, including sensitive data like authentication databases, to remain safely behind the firewall.

Peer Notification

The EFT DMZ Gateway handles requests to EFT Server through a two-way socket originating from EFT Server. This peer notification channel acts as a proxy for all transmission through the DMZ Gateway; the result is that the EFT server in the back-end can use the same logic and methods for processing requests. Peer notification channels replace the traditional inbound socket connection method for socket communication.

DMZ Security

EFT's DMZ Gateway adds multi-tier security for organizations that want to implement DMZ security best practices for authentication, data storage and retrieval, and firewall security.

DMZ Gateway best practice advantages include:

- No data ever stored in the DMZ
- Acts as a proxy server for authentication and directory listings, keeping them safely out of the DMZ
- No inbound holes in the firewall—all connections are East-to-West (initiated from behind the firewall to outbound).
- Transparent for the user; they do not even know the DMZ Gateway is there.
- No performance difference from reaching the EFT Server in the back-end; and a performance gain if the DMZ Gateway is replacing a server in the DMZ.
- No synchronization or replication of user database needed in DMZ—because there is no user database ever exposed in the DMZ.

Auditing and Reporting Module

Enhanced File Transfer Server's Auditing and Reporting Module (ARM) captures all of the transactions passing through the EFT system and then allows you to query the data and view reports from EFT Server's Administrative console. You can analyze captured data immediately using the preconfigured reports, or custom design your own with the included report designer.

Auditing

EFT with ARM captures significantly more data points than standard file logging. Data is stored in real time in a relational database, which you can then query from the EFT Server Administrator, or query directly from your own reporting system.

Reporting

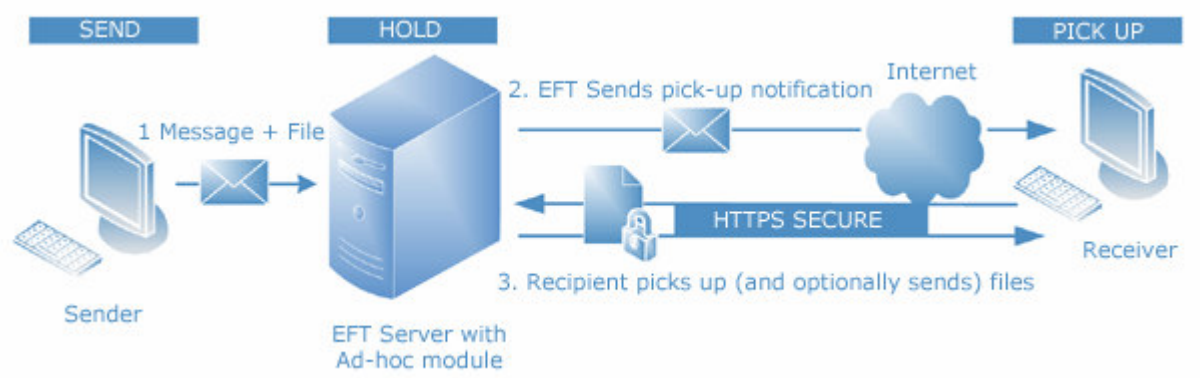
Query live data and pull it into a report in seconds. When a report is executed, EFT with ARM connects to the database and retrieves audited data based on the specified criteria and generates a report you can view directly in the EFT Server Administrative console. Use the preconfigured reports, or create your own reports using the visually-based report designer.

Search for a particular transaction from a specified date range. You can also select a report and then perform searches on them for even more granular analysis, filtering the results based on multiple criteria such as time, protocol, IP, file name, or bytes transferred. EFT with ARM enables you to find out what is happening and analyze why quickly and efficiently. You can export reports in .html, .pdf, .vp, or .txt formats.

Included, preconfigured reports have been carefully selected based on extensive interviews and research into the most important reporting needs. For example, we've created reports targeted especially for troubleshooting, nonrepudiation, billing, and trending.

Secure Ad Hoc Transfer Module

EFT Server's Secure Ad Hoc Transfer module enables an organization's employees to send and receive sensitive or business-critical files securely and reliably in an ad hoc, instantaneous manner, without the administrative overhead of creating, maintaining, and removing temporary FTP accounts. And since the delivery process is bi-directional, recipients can securely deliver files back to the sender. Auditing and receipt notifications afford built in non-repudiation of receipt for data that has been sent and/or received.



1. Users simply fill out a web form with sender and recipient information, and attach one or more files to send.
2. The Secure Ad-hoc Transfer modules then interacts with EFT Server in the back-end, automating the process of setting up a temporary user account, storage space, and login credentials. An e-mail notification is then sent to the recipient alerting them that one or more files are available for the recipient to pick up. The e-mail includes a secure link and login credentials to the temporary account created by EFT Server.
3. When the recipient logs in to the server, they will see the list of files which can be easily downloaded with a single mouse-click. If given permission, the recipient will be able to upload files back to the server for the sender to retrieve at a later time. Temporary accounts are disabled and deleted after a brief period of time as configured by the EFT Server administrator.

For more information about EFT Server and other GlobalSCAPE products, contact corporate sales at 1-800-290-5054 or visit our website at http://www.globalscape.com/.