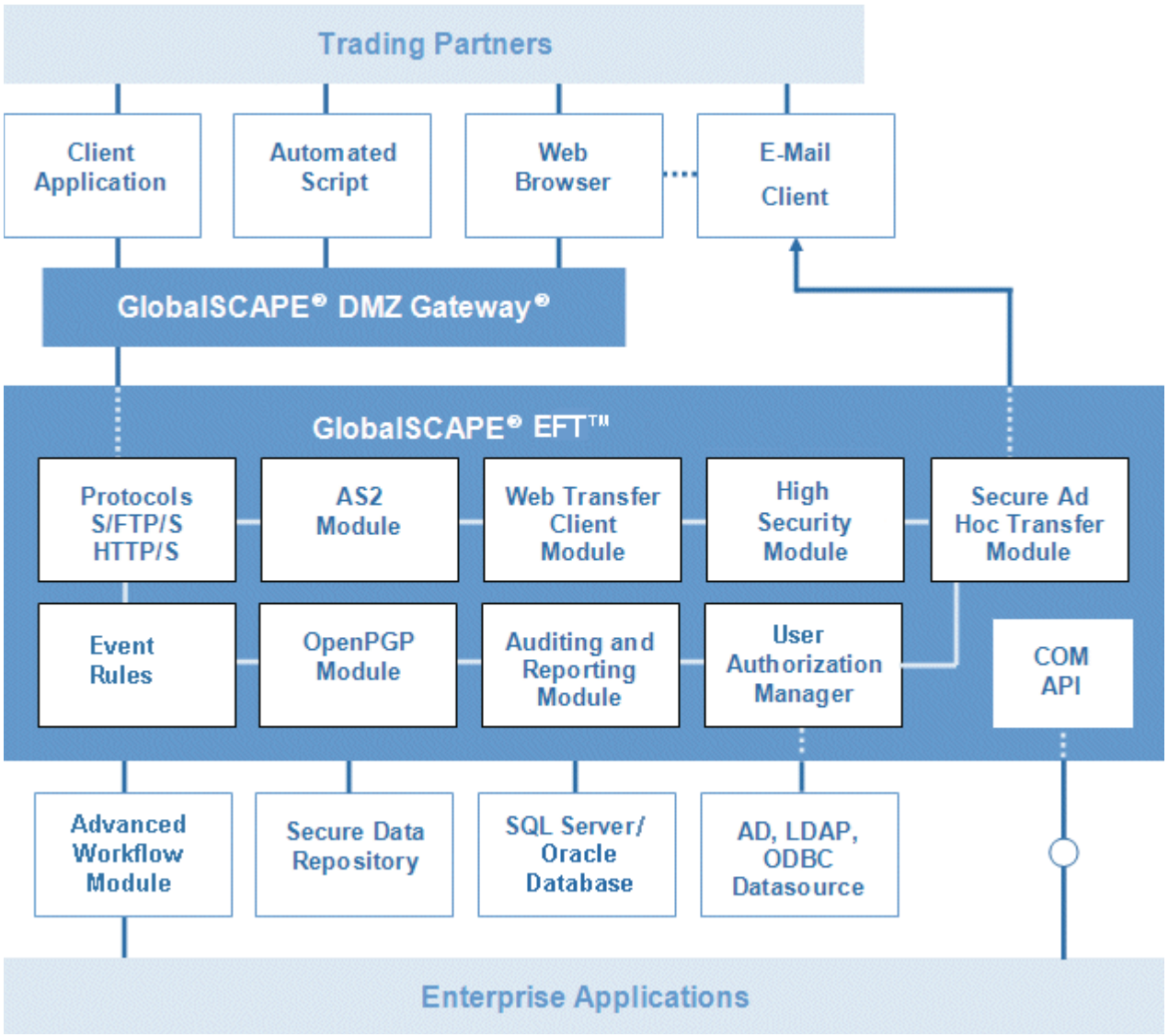
Introduction to EFT™ Managed File Transfer

More than just a managed file transfer (MFT) solution, EFT™ extends beyond standard MFT to allow you to connect with any industry-standard file-transfer client with a robust security architecture for meeting business and regulatory requirements, ensuring that encrypted transactions occur only with the appropriate entities, and that data confidentiality and integrity are preserved during transport and storage. EFT's modular form makes it affordable by allowing you to purchase just the functionality you need. You can add advanced features as your business needs change.

EFT is offered in a small-to-medium business Standard Edition and EFT Enterprise Edition. EFT Standard Edition is built on the same code as EFT Enterprise Edition, with Enterprise-specific features disabled, but visible so that you can see features that you might want to add later. That is, all module features are available during the trial period for both Standard and Enterprise Editions. Module features that require licensing and activation separate from the Standard Edition are identified in the user interface and in this user guide.

The illustration below shows the various EFT components.



EFT™ Standard and EFT Enterprise™ each provide the following features:

- **Data Protection and Encryption** - EFT protects intellectual property, trade secrets, and customer files transferred over the Internet using secure protocols including FTPS (SSL/TLS), SFTP (SSH2), and HTTP/S (SSL).
- **Guaranteed Delivery and Data Integrity** - EFT extends the industry-standard FTP protocol with strong reliability features, including post transmission integrity verification, mid-file recovery, and automatic restart.
- **Tracking and Auditing** - Secure data delivery requires strong audit trails for tracking and non-repudiation. EFT provides industry-standard logging (W3C, NCSA, Microsoft IIS Extended), e-mail notification of completed transactions, and digital certificates for proof of identity.
- **Programmatic Interface** - EFT can be controlled through its administration interface or through its Component Object Model (COM) interface. The COM API is a programmatic interface that lets you control EFT from your own custom applications using any COM-enabled programming language.
- **Accelerated Transfers** - EFT supports multi-part (segmented) transfers for faster delivery of large files over large geographical distances. Multi-part transfers require the use of compatible clients such as CuteFTP.
- **Life-Cycle Management** - EFT helps you quickly and efficiently manage users, temporary accounts, and expired or compromised public-keys or certificates.
- **Authentication and Authorization** - EFT supports password, public-key, or one-time-password authentication. User profiles can be managed internally or externally through NTLM, Active Directory (AD), or ODBC data sources.
- **User and Group Management** - Manage system resources including bandwidth, folder access, file types, and more using granular or Site-wide controls provided for user and group management. Visually manage folder permissions via the Windows Explorer-like Virtual File System (VFS). Inherit or override permissions, grant administrative, guest, or anonymous permissions, or deny access altogether. Manage client connections with real-time monitoring and on-the-spot disconnection of users. Administrators can force users to reset their passwords upon initial login, require complex passwords, remove/disable inactive accounts automatically.
- **Specify SSL ciphers and version levels** - EFT provides administrators the ability to specify symmetric key cipher(s) and the ordering of those ciphers for establishing SSL sessions. EFT validates inbound SSL sessions and allows or denies connections based on specified or approved ciphers.

EFT Enterprise™ provides each of the features of EFT™ Standard, plus:

- SFTP (SSH) and HTTPS modules are included
- LDAP authentication functionality
- SSL certificate-only authentication
- Delegated administration for user-only, Site-only, or Server-only management
- ARM support for Oracle database (with optional ARM module)
- DMZ Gateway multi-site configuration (with optional DMZ Gateway®)
- AS2 support (with optional AS2 module)

The available modules include:

HTTPS (Included in the Enterprise edition) - The HTTPS add-on module allows you to set up a secure connection to anyone in minutes using any Web browser. The HTTPS module adds the HTTPS protocol to EFT, enabling you to support secure browser-based transfers without having to install a Web server. HTTPS encrypts the session data using the SSL (Secure Socket Layer) protocol, which provides protection from eavesdroppers and man-in-the-middle attacks.

SFTP (Included in the Enterprise edition) - SFTP is a subset of the popular SSH protocol and is a platform independent, secure transfer protocol. SFTP provides a single connection port for easy firewall navigation, password and public key authentication, and strong data encryption, to prevent login, data, and session information from being intercepted and/or modified in transit. The SFTP module enables EFT to authenticate and transfer data securely with SFTP-ready FTP clients, such as CuteFTP Professional.

AS2 (Available in EFT Enterprise only) **-** The AS2 (Applicability Statement 2) specification supports the exchange of structured business data securely on top of the HTTP or HTTP/S protocol.

OpenPGP - EFT employs industry-standard OpenPGP (based on the open source implementation of Pretty Good Privacy) technology to safeguard data at rest. The OpenPGP data encryption or decryption process is directed by Event Rules that specify how data files are treated in a particular context. EFT uses OpenPGP to encrypt uploaded data and the off-load capabilities of EFT to move the file to another location.

High Security Module (HSM) **-** The High Security module (HSM) achieves or exceeds security practices mandated by PCI DSS, HIPAA, and Sarbanes-Oxley for data transfer, access, and storage. The HSM protects data in transit by enforcing the use of secure protocols, strong ciphers and encryption keys, and maintaining strict password policies. For a list of features in the HSM, refer to Features of the High Security Module.

Auditing and Reporting Module (ARM) - The Auditing and Reporting module captures all of the transactions passing through EFT. You can query the data and create/view reports from within EFT's administration interface. A new database is created when upgrading to version 6. (The Standard edition does not offer support for Oracle databases.)

Web Transfer Client (WTC) - The Web Transfer Client (WTC) can deploy automatically upon client connection to EFT and can be used by any trading partner using virtually any Web browser that supports Java and DHTML. (Limited to 5 concurrent users in the Standard edition.)

Secure Ad Hoc Transfer (SAT) - The Secure Ad Hoc Transfer (SAT) module allows you to exchange files without the problems associated with having to manually create temporary FTP accounts, the size limitations and security issues of regular e-mail, or the time delays and high costs of overnight and physical shipments. (Neither edition is compatible with prior versions of the Secure Ad Hoc Transfer module.)

Advanced Workflow Engine (Available in EFT Enterprise only) - Similar to EFT's Commands, EFT's Advanced Workflows add additional automation capabilities, allowing you to add scripting and variables to *Workflow Tasks*, then add these reusable Workflows to Event Rules. A Workflow is a series of steps that can perform file transfers, batch data processing, application testing, and so on, and are defined to run automatically when started by some event.

DMZ Gateway Module **-** DMZ Gateway is used in combination with EFT to create a multi-tier security solution for data storage and retrieval. The DMZ Gateway resides at the edge of the network, brokering data between EFT residing behind your corporate firewall and your clients in the outside world. (Multiple-Site configuration is only available in Enterprise edition.)

Mail Express Module - Mail Express™ allows you to send large email file attachments to recipients inside or outside of your organization quickly, reliably, and securely, while reducing the load on your mail server.

Secure Mobile Access Module - The Secure Mobile Access (SMA) module for EFT™ allows you to access EFT-managed files on your mobile devices.

COM API - Using the COM API, you can interact directly with EFT from your own custom applications using any COM-enabled programming language such as Visual Basic (VB), Java, or C++. You can create a script with the development IDE of your choice.

What's New in v6.5?

Release notes/version history for EFT Standard and Enterprise is available online at http://www.globalscape.com/mft/history.aspx.

EFT v6.5 includes the following changes:

- EFT v6.5 can be integrated with Mail Express v3.3 or later for mailing attachments in a browser or in Outlook.
- Changes were made to the COM API to accommodate updates such as Mail Express integration and Unicode support. Refer to the COM API reference for details.
- Unicode changes:
    - Unicode has been added/improved throughout EFT. (Refer to Unicode Exceptions.)
    - Unicode filenames are detected prior to trying to create a PGP SDA.
    - Updated the ODBC SQL scripts to Unicode.
    - Added support for both UTF8 and UTF-8 formats in FEAT and OPTS
    - A **Filename encoding** option was added to the Copy/Move and Download Actions (**Advanced Options**) to specify UTF-8 or ASCII encoding.
    - **Encoding** option added to the Site's **FTP Settings** dialog box to specify Auto-detect or UTF-8 character sets for inbound FTP/S file path names.
    - Logs can be encoded in UTF-8 format.
    - Internationalized domain name (IDN) support
- OpenSSL version was updated to 0.9.8t
- AS2 component version was updated to v8.2.4462.0.
- AWE was updated to version 8.0.9.0
- Incorporated new database utility (DBUtility.exe) for creating and upgrading the ARM database; ARM database is now upgraded separately from EFT
- Added AES-128CTR and AES-246 CTR ciphers for both FIPS and non-FIPS for encrypting SFTP sessions on a Site. They are enabled by default.
- Added ability to stop in-progress transfers and show % progress complete on the **Status** tab in the administration interface.
- Added an icon next to check boxes in the administration interface to indicate that a setting is inherited from its parent node.
- Added ability to control the administrator account timeout (while maintaining PCI DSS compliance)