

# FORTRA

DATASHEET (Globalscape)

## EFT™ Administrator Course

### A Foundation Course for EFT Administrators

Administrators and power users that are responsible for Globalscape Enhanced File Transfer™ (EFT™) and must interact with end users and internal processors would benefit from this two-day course. The EFT Administrator Course provides full coverage for everyday administrative guidelines, user account control, management, reporting, module configuration, and troubleshooting.

### Objectives of This Course

After successfully completing this course, you will understand:

- Installing, upgrading, and activating EFT
- Administration, configuration, and monitoring of EFT
- Creating and managing user accounts
- Troubleshooting connection issues
- The Event Rule system
- Custom commands
- Ways to log and track issues
- Limitations of using the administration interface
- Copying and creating backups of configuration files
- Navigating the VFS system
- Identifying permissions on the VFS tab using GS Auth/LDAP/ODBC
- AD authentication permissions and how they work
- Creating virtual directories and why they are used
- Troubleshooting login issues for user and/or administrator accounts
- EFT clients

### Agenda

#### Module 1: Introduction to EFT

- › File Transfer Technologies
- › MFT technologies
- › Capabilities of file transfer
- › Automation
- › Deployment scenarios
- › EFT modules
- › Features
- › Purpose of EFT
- › Architecture
- › IPv6
- › Virtual machines
- › Unicode
- › IDN

### KEY INFORMATION



#### Duration

- › 2 Days



#### Target Audience

- › Administrator (System, User, File Transfer, Network, Storage Admins)
- › Application Manager
- › Application Operations
- › Account Managers
- › Support Analyst
- › Developers
- › Engineers
- › DevOps
- › Security Admins
- › Security Associates
- › Security Auditors
- › Architects



#### Prerequisites

- › None

**Module 2: Server Administration**

- › Installation (MSI and silent installer)
- › Update process
- › Administration interface
- › Profiles for remote access
- › Authentication
- › Globalscape authentication
- › Windows Active Directory (NTLM/AD) authentication
- › LDAP
- › ODBC
- › RADIUS
- › SAML (WebSSO)
- › SMS authentication
- › RSA SecurID®
- › CAC
- › Forensics reports
- › Admin management and delegated administration
- › Viewing server statistics
- › Stopping the EFT server service
- › User database refresh interval
- › Changing the Server Listening IP Address and Port
- › Backup & Restore

**Module 3: Managing Connections to EFT**

- › File transfer technologies
- › Protocols configuration
- › FTPS
- › PASV port range
- › SFTP
- › HTTPS
- › FIPS
- › UTF-8
- › Monitor inbound/outbound transfers in real time
- › Configuring Site security
- › File transfer reporting

**Module 4: User Account Management**

- › EFT accounts
- › Settings Templates
- › Security settings
- › Permissions groups
- › Set limits

**Module 5: VFS**

- › Virtual folders and access to remote servers
- › Home folders
- › Permissions groups
- › EFS

**Module 6: HSM Module**

- › EFT PCI Sites
- › Stricter security settings
- › Expire inactive accounts
- › Expire passwords
- › Expiration reminder
- › Data sanitization
- › Reporting
- › PCI DSS monitor, report, compensating controls (CCs)

**Module 7: AS2 Module**

- › Introduction to AS2
- › How EFT supports AS2
- › AS2 authentication
- › Multi-directional AS2 transactions
- › Exchange structured business data securely using the HTTP or HTTPS protocol.

**Module 8: DMZ Gateway®**

- › Introduction to DMZ Gateway
- › Installing and configuring DMZ Gateway
- › Administering DMZ Gateway
- › Profile management
- › IP Access management

**Module 9: EFT HA**

- › High Availability Overview
- › Deployments
- › Server drain, maintenance, auto-restart
- › Unicast vs Multicast
- › High Availability Message Queuing
- › Installing and upgrading EFT in HA cluster
- › HA troubleshooting
- › Load balanced folder monitor
- › Performance tuning in EFT
- › NAS storage in HA mode
- › Mirroring EFT HA cluster to an another cluster
- › Changing path to shared configuration folder

**Module 10: Web-Based File Sharing**

- › Introduction
- › Exchange files using EFT over HTTP or HTTPS using a Web browser
- › Accessing WTC
- › Password reset
- › File management and filtering › Generate logs

**Module 11: Web Transfer Client Administration**

- › Configuring WTC
- › Localization settings
- › Disabling CRC
- › Terms and conditions
- › Customizations

**Module 12: Sharing Files and Folders**

- › Introduction Workspaces
- › Workspaces
- › Invitations
- › Notifications
- › Permissions
- › Transactional Workspaces
- › Activity reports
- › Email interface
- › Drop-off Portal

**Module 13: Workspaces Administration**

- › Workspaces permissions
- › Workspaces related variables
- › Workspaces conditions

**Module 14: Sending files using Outlook Add-In**

- › Configuration EFT Outlook Add-In › Sending files
- › Mail profiles with multiple accounts › Activity reports

**Module 15: Sending files using Outlook Add-in**

- › EFT Outlook Add-in Configuration

**Module 16: Desktop Clients**

- › Transferring files using CuteFTP
- › Transferring file using scClient

**Module 17: Mobile Transfer Client**

- › Introduction to Mobile Transfer Client › Transferring files with MTC

**Module 18: Accelerate Module**

- › Introduction to the Accelerate Module
- › Configuration and deployment scenarios
- › Acceleration using Event Rules
- › Using scClient

**Module 19: Troubleshooting EFT**

- › Inbound error logs
- › Outbound error logs
- › ARM schema and results
- › WTC error messages
- › Event Rules

# FORTRA

Fortra.com

**About Fortra**

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at [fortra.com](https://fortra.com).