Configuration and Security Best Practices Checklist

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT, all versions

DISCUSSION

Below is a checklist of suggestions and guidelines for installing, configuring, and deploying EFT in a production environment, including best practices for security (after the Configuration Checklist).

Development Lab Environment

As with any mission-critical software or hardware, it is recommended that a testing, validation, development, or usability lab be established to provide a "sandbox" into which EFT and DMZ Gateway Server software can be deployed. This initial deployment allows for validation of the interoperability with other dependent components as well the validation of expected usage scenarios.

The lab environment should emulate (if not duplicate) the production environment at a network topography and application level. To do this, a clear vision of the production network and the proposed deployment of EFT and DMZ Gateway must exist. Typical deployments of EFT and DMZ Gateway consist of many other components from the enterprise, including Active Directory Server, SQL Server, SMTP Server, and a storage system such as a SAN. For DMZ Gateway, a firewall such as Microsoft ISA might be applicable. Finally, some deployments also include Clustering, in which case various components are replicated to provide clustered resources.

For increased business continuity and risk mitigation, you should use the development lab environment as the starting point for any configuration changes in the system. That is, make the change in development and validate it prior to making the change in production. A good testing tool is CuteFTP.

Configuration Checklist

The installation and configuration of EFT in either a lab or a production environment should be validated by EFT administrators/operators to ensure that the functions are working as expected.

Configuration and Security Best Practices Checklist

Service	
	Make sure that the EFT Server service is started on the computer.
	Make sure that the service is listening on the expected IP:PORT socket addresses on EFT. (To view the listening sockets, use "netstat -ona" from a command line or an application such as PrcView or TcpView.)
	Check the Event Viewer log to ensure that there are no errors in the Application log related to EFT or DMZ Gateway.
	Confirm that the administration interface shows the status of the system when it is launched and connected to EFT.
Server User Management	
	For each Site on EFT, ensure that the expected user accounts exist.
	To ensure that authentication is working as expected, attempt to log in to EFT as a user account on the system (using any protocol).
	To confirm that permissions for the user account are working as expected, attempt a file transfer.
Protocol/Network	
	For each protocol enabled on EFT, attempt a connection directly to EFT using a client that

supports that protocol.

For each protocol enabled through DMZ Gateway, attempt a connection to the appropriate DMZ Gateway IP:PORT and confirm that this route works as expected.

Auditing/Logging

View the audit traces generated by the validation steps above.

Confirm that the Auditing and Reporting module database has been populated with appropriate data (using either EFT Reporting interface or direct access to the SQL Server being used).

Confirm that the text log files generated by EFT have been populated with the appropriate data.

Event Rules/Workflow

Each customer has a unique set of Event Rule/workflow requirements, but these are the general validation steps. Confirm the following are working as expected:

E-mail notifications. Test e-mail notifications by triggering an Event Rule that has an e-mail notification Action to confirm that Event Rules fire and that the SMTP configuration is correct.

PGP operations. Confirm that OpenPGP keys are configured properly.

Move/Copy/Download actions. Initiate

Event Rules that perform remote file uploads/copies/download so that connectivity originating from EFT to a remote system is properly configured. In this step, also confirm that a log file is generated that audits outbound connection information (a "cl*.log" file in the designated Server Log File location).

Custom Commands. EFT is responsible for triggering those external commands, so that is what should be validated with respect to EFT. Any actions carried out by those external tools should be validated independently. Confirm that a "CMDOUT.LOG" file is generated as the result of an invoked Custom Command.

Folder Monitor Rules. Ensure that the Event Rules are properly enabled and responsive to files added to the folder being monitored.

Failover Testing

For failover cluster deployments, the failover and failback operations of the cluster should be confirmed. After a failover/failback, confirm that the newly active server behaves properly; that is, the failover is transparent and the configuration/operation is as expected. This can be summarized by the prior set of tests operating against the newly active node in the cluster.

Load Testing

If you expect high volumes of traffic or

	back-end processing within EFT, you should verify that the resource utilization levels on the Server are within acceptable tolerances. There are numerous load-testing tools available, ranging from simple batch files running command-line FTP to highly complex synthetic transaction generators. Globalscape's Quality Assurance team performs load testing of our servers as part of our standard validation process for releasing software.
Fine Tuning	
	Review Knowledgebase article #10438, Tuning Windows for TCP/IP performance Review Knowledgebase article #11214, Performance Tuning EFT HA Native mode
High Availability	
	It is always recommended to separate EFT's configuration share and site data shares to different servers. If possible, use a share server that is exclusive to EFT's configuration. This directly improves stability. DFS is not a supported platform for shared config. Refer to knowledgebase article #11569 Known Issues Using DFS on EFT for more information.

.telerik-reTable-4 { border-collapse: collapse; border: solid 0px; font-family: Tahoma; } .telerik-reTable-4 tr.telerik-reTableHeaderRow-4 { border-width: 1.0pt 1.0pt 3.0pt 1.0pt; margin-top: 0in; margin-right: 0in; margin-bottom: 10.0pt; margin-left: 0in; line-height: 115%; font-size: 11.0pt; font-family: "Calibri" , "sans-serif"; width: 119.7pt; background:

#4F81BD; padding: 0in 5.4pt 0in 5.4pt; color: #FFFFFF; } .telerik-reTable-4 td.telerik-reTableHeaderFirstCol-4 { padding: 0in 5.4pt 0in 5.4pt; } .telerik-reTable-4 td.telerik-reTableHeaderLastCol-4 { padding: 0in 5.4pt 0in 5.4pt; } .telerik-reTable-4 td.telerik-reTableHeaderOddCol-4 { padding: 0in 5.4pt 0in 5.4pt; } .telerik-reTable-4 td.telerik-reTableHeaderEvenCol-4 { padding: 0in 5.4pt 0in 5.4pt; } .telerik-reTable-4 tr.telerik-reTableOddRow-4 { border-width: 1pt; color: #666666; vertical-align: top; border-bottom-style: solid; border-bottom-color: #4F81BD; } .telerik-reTable-4 tr.telerik-reTableEvenRow-4 { color: #666666; vertical-align: top; } .telerik-reTable-4 td.telerik-reTableFirstCol-4 { border-width: 1pt; border-color: #4F81BD; padding: 0in 5.4pt 0in 5.4pt; border-bottom-style: solid; border-left-style: solid; } .telerik-reTable-4 td.telerik-reTableLastCol-4 { border-width: 1pt; border-color: #4F81BD; border-bottom-style: solid; border-right-style: solid; padding: 0in 5.4pt 0in 5.4pt; } .telerik-reTable-4 td.telerik-reTableOddCol-4 { border-width: 1pt; border-color: #4F81BD; padding: 0in 5.4pt 0in 5.4pt; border-bottom-style: solid; } .telerik-reTable-4 td.telerik-reTableEvenCol-4 { border-width: 1pt; border-color: #4F81BD; padding: 0in 5.4pt 0in 5.4pt; border-bottom-style: solid; } .telerik-reTable-4 tr.telerik-reTableFooterRow-4 { color: #355C8C; background-color: #FFFFFF; vertical-align: top; padding: 0in 5.4pt 0in 5.4pt; } .telerik-reTable-4 td.telerik-reTableFooterFirstCol-4 { border-width: 1pt; border-color: #4F81BD; border-bottom-style: solid; border-left-style: solid; padding: 0in 5.4pt 0in 5.4pt; } .telerik-reTable-4 td.telerik-reTableFooterLastCol-4 { border-width: 1pt; border-color: #4F81BD; border-bottom-style: solid; border-right-style: solid; padding: 0in 5.4pt 0in 5.4pt; } .telerik-reTable-4 td.telerik-reTableFooterOddCol-4 { border-width: 1pt; border-color: #4F81BD; border-bottom-style: solid; padding: 0in 5.4pt 0in 5.4pt; } .telerik-reTable-4 td.telerik-reTableFooterEvenCol-4 { border-width: 1pt; border-color: #4F81BD; border-bottom-style: solid; padding: 0in 5.4pt 0in 5.4pt; }
Numerous other features can be validated within EFT. The above set represents the key elements that are most often used and are the most critical to successful operation in a production environment.

Security Best Practices Checklist

The following settings are recommended for increased security.

Administration Security	
	Create a specific AD account on which EFT's service is to run with the minimum necessary permissions.

Create an Event Rule to back up the entire Server configuration to a separate drive at least daily.

Do not use any default administrator names (e.g., "admin").

Do not use the default administration port (1100).

Only turn on remote administration if necessary. If remote administration is needed, then ban all IPs except those trusted IPs necessary to access the server for administration.

Turn on SSL/TLS if using remote administration.

Create sub-administrator accounts with the least amount of privileges necessary for help desk or operational administrators.

Do not give sub-administrators access to COM or the ARM (report) module unless absolutely necessary

If giving ARM (report) access to a sub-administrator, use the ReportsConnectionString registry override to define an alternate (least privileged) database connection string for database queries.

Set administrator passwords to expire every 90 days (or according to internal best

	practices/policies).
	Enable and define a complex security scheme for administrator passwords to include a minimum password length of 12 to 16 characters.
	Prohibit reuse of previous 99 passwords.
	Lockout administrators for an extended period after multiple failed login attempts.
	Run a PCI DSS report to detect any lax security configuration settings (either manually or on a schedule with an Event Rule).
	Periodically check the Globalscape support site for the latest version and upgrade accordingly. One or more high priority fixes for security vulnerabilities are often included.
User/Password Security	
	Expire accounts that are inactive for 90 days.
	Set user passwords to expire every 60 or 90 days.
	Enable and define a complex password security scheme for users.
	Prohibit reuse of previous 99 passwords.
	When using HTTP/S and/or SFTP protocols, require that the user reset their password

	upon initial use (requires KIA support by the SFTP client. FTP/S protocol does not support password reset upon initial login).
	Briefly lockout users after repeated failed logins.
	Automatically ban IP addresses with repeated failed username attempts.
	E-mail user login credentials separately or only send username and communicate password via phone or other means (i.e., out-of-band delivery).
	Allow users to reset their passwords and force them to do so upon first login.
File System Security	
	Segregate user's folders. (Do not share folders/resources across users when possible.)
	Restrict users to their home folders and set the home folder as ROOT for that user.
	Use Settings Templates to inherit user permissions rather than modifying them for each user.
	Use Groups to simplify control over user access to resources.
	Limit resource permissions to the minimum necessary.

Configuration and Security Best Practices Checklist

Auditing Security

- Enable verbose logging (Log Type).
- Rotate logs daily and encrypt+sign using an Event Rule.
- Always use extended auditing (ARM).
- Examine audit logs at least weekly for anomalous behavior

Data Security

- Encrypt data at rest using EFS encryption, OpenPGP, or 3rd-party encryption.
- Keep data separate (DAS/SAN/NAS).
- Define data recovery procedures in case of data corruption/loss/theft.
- Scan uploaded files for viruses (3rd-party tool required).
- Never store data in the DMZ, even temporarily. (Instead, install DMZ Gateway® in the DMZ and then store/manage data on EFT and other storage locations.)
- Create a legacy data clean-up rule according to your company policy.
- Enable data wiping for sanitizing deleted data.

	Add a banned file type rule and disallow all extensions except those required by the business.
Protocols Security	
	Be extremely selective when choosing which IPv4 or IPv6 addresses to bind to for a specific Site (listener). Only bind to IPv6 addresses if your organization is aware of and mitigating against IPv6-specific attacks at the edge of your network.
	If possible, allow only secure protocols (SSL/TLS, SSH, HTTPS, AS2).
	Disable all unused services or features that may adversely affect security, including Web Services, any unused protocol listeners, and using username and password credentials for use in Event Rule context variables, if not needed by any Event Rule.
	Always choose the strongest ciphers, hashes, and key lengths.
	The following are considered weak ciphers:
	• TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TTLS_RSA_WITH_AES_128_CBC_SHA • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_GCM_SHA384

Not configuring SSL/TLS securely increases the likelihood that user credentials would be compromised by decrypting the session. If these ciphers are not required for supporting older browsers disable them. Additional changes may be required to avoid specific attacks. For example, to mitigate the BEAST exploit, move RC4 (a lesser strength but non-CBC cipher) to the top of the SSL/TLS cipher priority list, followed by AES 256, then AES128, etc.

In the Server **Security** tab, enable the most secure **SSL/TLS Compatibility** settings as needed for your environment.

Do not enable Clear Command Channel (CCC) nor unprotected data channel (PROT C), unless needed in your environment.

Disallow site-to-site (FXP) support for FTP/S protocol listeners, and block client anti-timeout attempts.

Have your server’s SSL/TLS certificate signed by Certificate Authority (CA).

If possible, require that the connecting clients provide a certificate proving their identify in addition to their authentication credentials.

Mask the server's identity by using generic banner messages.

	Specify a maximum limit for connections and transfers for each template.
	Specify a maximum limit of 5 connections and transfers for each user.
	Enable EFT's Denial of service settings, disconnecting and banning users that issue an excessive numbers of invalid commands (weighted over a given period) and permanently banning IP addresses that exceed the server's Flood/hammer value. Non HTTP/S setups should set the Flood/hammer slider to Very High, vs. the default Medium setting.
	Specify allowed IP address ranges for user/partner connections when possible, denying connections from all other IP addresses.

Prescriptive Guidance for Maintenance

The following are guidelines for maintaining the good health of an EFT and DMZ Gateway deployment and reducing long-term costs of maintenance and operation.

- **Configuration Backup** - For disaster recovery and business continuity, it is important to keep backups of the Server and DMZ Gateway configuration. Backing up the configuration can be accomplished with a variety of tools such as Symantec Backup Exec, Ghost / VMWare to make images of the system, or even a simple script file.
- **Database Backup and Truncation** - If you are using the Auditing and Reporting module (ARM), the database to which the audit records are stored should include EFT ARM tables as part of the typical database maintenance plan. This includes proper monitoring of the tables and transaction logs, backing up the data and having a retention policy to archive (or purge) old data.
-

Data Archival and Retention - You should put into place and enforce a policy by which old data is periodically archived and/or purged, because no disk is limitless and performance can degenerate as more files are added to EFT. Therefore, a storage management policy should include regular inspection of available hard disk space and health (error count, fragmentation, etc.) as well as archiving and/or purging user data and Server Log Files (CMDOUT.log found in the application folder, and all other logs found in the Log folder specified on the Server).

- **Restarting Services** - Given the facility of the Microsoft Cluster in failing over and failing back while providing high resource availability, it is recommended that you design a maintenance schedule in which the EFT service is cycled at least once per quarter to once per month. Failing over to the backup node, restarting the service, then failing back and restarting the other node would suffice in re-establishing a baseline state of the EFT service to ensure optimal health.

- **Event Log Alerting** - EFT will log error conditions to the standard Windows Event Viewer. It is recommended that the operations team for an enterprise include EFT error checks in their monitoring techniques, looking for an ERROR event generated with a source of "EFT," "EFT Enterprise," or "Globalscape."

Procedure for Cold Standby Setup

Below are few recommendations for achieving a backup server image that is ready to be turned on quickly and accept "real" traffic.

In all situations, if you are copying a configuration file from one system to another, care must be taken with hardware-specific resources, such as IP addresses, physical paths/partitions, and so on. If possible, it is recommended that the EFT configuration use the generic "All Incoming" IP Address for incoming socket connections so that differences in computer IP addresses do not prevent proper operation of the system if the Cold Standby comes online.

Furthermore, you must take care with the connections and IP-access restriction lists between EFT and DMZ Gateway. If DMZ Gateway is configured to allow only one EFT IP address to connect to it, then the Cold Standby server must have the same IP address to connect; alternately, the DMZ Gateway IP access list must include all possible IP addresses (possibly a Class C subnet) so that multiple servers from the approved network segment

may connect.

- **Virtualization Software** - A great solution from a cost- and resource-saving standpoint, virtualization software is also quite easy to manage due to the "software" nature of the solution. The approach would be to create an image within a virtual system (using a tool such as VMWare or Microsoft Virtual PC) by installing and activating the EFT or DMZ Gateway software. Once this is done, the steps required to bring the system online include first copying the configuration files (which were backed up using a process described above), then bringing the virtual image online and starting the service.

- **System Backup Software** - Another quick and easy option is to create a disk or system image of a configured EFT or DMZ Gateway (using a product such as Norton Ghost); when a Cold standby needs to be "stood up" and made hot, the image can be installed on a computer, backup configuration copied, and the service started.

- **Periodic Backup to Cold Standby Machine** - If resources permit, the quickest way to get a "Cold" computer to become "Hot" is to have a computer dedicated to this function. It should have EFT and/or DMZ Gateway installed and activated, but the service should be stopped. A process to copy the configuration periodically from the "Hot" server to the "Cold" server would keep the two in synch, and if the "Hot" system goes down, the "Cold" system can simply start the service.