Security Best Practices Checklist

The following settings are recommended for increased security. For a PDF of the Configuration Validation checklist, refer to:

http://help.globalscape.com/help/eft6-3/validationchecklist.pdf

Administration Security	
☐	Create a specific AD account on which EFT Server's service is to run.
☐	Create an Event Rule or manually backup the entire Server configuration at least daily.
☐	Do not use any default administrator names (e.g., "admin").
☐	Do not use the default administration port.
☐	Only turn on remote administration if absolutely essential.
☐	Turn on SSL if using remote administration.
☐	Create sub-administrator accounts with the least amount of privileges necessary for helpdesk or operational administrators.
☐	Set administrator passwords to expire every 60 or 90 days.
☐	Set a complex security scheme for administrator passwords.
☐	Lockout administrators upon 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 latest version, security patches, etc. and upgrade accordingly.
User/Password Security	
☐	Expire accounts that are non-active for a specified period.
☐	Set user passwords to expire every 60 or 90 days.
☐	Define complex password security scheme for users.
☐	Prohibit password reuse/history.
☐	Automatically kick or ban 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.
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.
☐	Specify a maximum disk space (quota) for each user (or Settings Template).

Auditing Security	
☐	Enable verbose logging (Log Type).
☐	Rotate logs daily and encrypt+sign using an Event Rule.
☐	Always use extended auditing (ARM).
Data Security	
☐	Encrypt data at rest using EFS encryption, PGP, 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. (Use DMZ Gateway instead.)
☐	Create a legacy data clean-up rule according to your company policy.
☐	Enable data wiping for deleted data.
Protocols Security	
☐	Only allow secure protocols (SSL, SSH).
☐	Only allow high security ciphers, hashes, key lengths.
☐	Mask the server identity by using generic banner messages.
☐	Specify a maximum limit for connections and transfers for each user/template.
☐	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 a Server 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, GlobalSCAPE Continuous Data Protection (CDP), or even a simple script file.
- **Database Backup and Truncation** - If you are using the Auditing and Reporting module (ARM), the SQL Server to which the audit records are stored should include EFT Server 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 Server. 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 EFT Server Log Files (CMDOUT.log found in the application folder, and all other logs found in the Log folder specified at the EFT Server level).
- **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 Server 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 Server service to ensure optimal health.

- **Performance Counter Monitoring** - DMZ Gateway provides a Performance Counter object to the computer on which it is installed. This object provides a standard Windows mechanism to view activity through DMZ Gateway and, in general, assess the fundamental health of the system as a whole. It is recommended that the enterprise operations practices include monitoring the key performance counters (automatically is preferred) by adding the "Gateway" performance object to Microsoft's Perfmon, and monitoring items such as "Active Sites" (indicates up/down state of EFT Server through DMZ Gateway) and "Active Client Connections" (indicates activity through the DMZ Gateway to EFT Server).
- **Event Log Alerting** - EFT Server will log error conditions to the standard Windows Event Viewer. It is recommended that the operations team for an enterprise include EFT Server error checks in their monitoring techniques, looking for an ERROR event generated with a source of "EFT Server" or "GlobalSCAPE Gateway" service.

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 Server 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 Server and DMZ Gateway. If DMZ Gateway is configured to allow only one EFT Server 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 Server 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 Server 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 Server 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.

For detailed procedures, refer to:

http://help.globalscape.com/help/eft6-3/index.htm#best_practices_for_configuration_and_validation.htm