Security Best Practices Checklist

The following settings are recommended for increased security.

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.