How EFT Addresses PCI DSS Requirements

EFT facilitates enforcing high security and compliance with the PCI Data Security Standard (PCI DSS), which provides detailed security compliance guidelines that can be used to provide hardened security for EFT, no matter which rules or standards by which your organization is measured. Each requirement and a description of how EFT helps comply with the requirements is described below. (Updated for PCI DSS v3.2)

Refer to the PCI Security Standards website for official documentation of the standard. You can download the PCI DSS *Security Audit Procedures* from https://www.pcisecuritystandards.org.

Compensating Controls

From the PCI DSS Security Auditing Procedures document:

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

When EFT warns you of a non-compliant setting, you will be given the choice to fix the problem or proceed with the non-compliant setting. If you choose to proceed in violation of the PCI DSS, you will be asked to specify a compensating control, i.e. an alternate hardware, software, or internal policy that satisfies the requirement in some other way (ref. "Compensating Controls" in the PCI DSS for more

information). The controls you document will appear in the PCI DSS Compliance report, which you can provide to Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs), individuals who are certified by the PCI Security Standards Council as being qualified to validate compliance to the PCI DSS.

PCI DSS Requirements Addressed

EFT facilitates compliance with applicable PCI DSS requirements. The PCI DSS requirements related to physical security and cardholder database security are not applicable to EFT; however, you should place the Server computer in a secured area, such as a locked server room or network operations center.

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

PCI DSS Requirement	How Requirement Is Addressed with EFT
1.1 Establish and implement firewall	Requires measures external to EFT

and
router
configuration
standards.

Requires
firewalls
and
routers
to
protect
cardholder
data
and/or
the
DMZ
Build
and
maintain
a
secure
network
and
systems
Requirement
1
Install
and
configure
EFT's
built-in
firewall
to
restrict
connections
between
untrusted
networks
and
any
system
components
in
the
EFT
environment.

Gateway.

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

Storing cardholder data in the DMZ is expressly prohibited by the PCI DSS (1.3.7). And for security best practices you should not allow inbound

connections
to
originate
from
untrusted
into
trusted
zones.

EFT's
optional
DMZ
Gateway
module solves
both
of
these
problems.
Refer
to
https://www.globalscape.com/managed-file-transfer/dmz-gateway
for
details
of
DMZ
Gateway.

EFT
Implement

a combination of DMZ and the DMZ Gateway module facilitates compliance with this requirement.

When EFT is installed in combination with the DMZ Gateway module, only authorized system components provide publicly accessible services, protocols, and ports.

1.3.2 Limit inbound Internet traffic to IP addresses in the DMZ

Gateway,
DMZ.
internal
inbound
ports
need
be
opened
into
the
trusted
network,
hence
all
inbound
traffic
will
be
restricted
to
IP
addresses
within
the
DMZ.

Requirement 1.3
Prohibit

anti-spoofing measures to detect and block forged source IP addresses from entering the network.

Requirement 1.3.4 Do not allow unauthorized outbound

EFT in combination with the DMZ Gateway module.

traffic from the cardholder data environment to the Internet.

EFT can be configured to permit only "established" connections into the DMZ Gateway as a SOCKS5 proxy for outbound traffic. Offloading files using

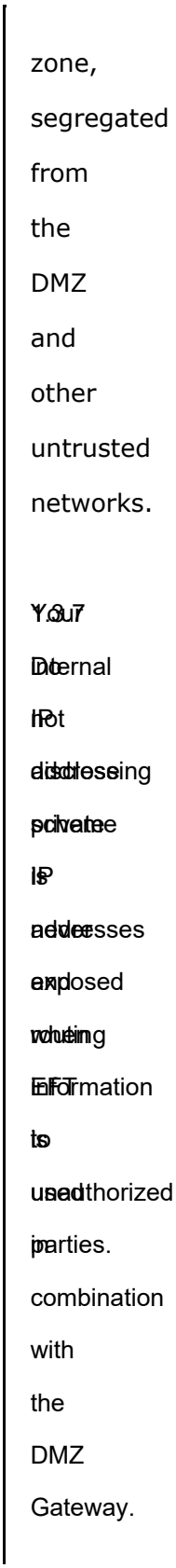
EFT
though
the
DMZ
Gateway
means
your
internal
IP
address
won’t
be
exposed
(1.3.48).
Additional
steps
may
be
required
to
fulfill
this
requirement,
such
as
DLP
and
deep
content
inspection

tools,
before
files
are
submitted
to
EFT
for
offloading.
*Requires
DMZ
Gateway.

EFT
When
system
with
that
DMZ
Gateway,
data
(such
as
database)
in
the
DMZ.

zone,
segregated
from
the
DMZ
and
other
untrusted
networks.

Your
Internal
IP
addresses
are
not
disclosed
to
untrusted
parties.



Requires Install external firewall EFT on any mobile and/or employee-owned computers	Requires Document external and procedures

Requirement 2: Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

How PCI Requirement Is Addressed with EFT	With

How EFT Addresses PCI DSS Requirements

Always change vendor-supplied defaults (for EFT Enterprise) disable the unnecessary Express Security before (installing EFT Express) and the high-security-enabled Site, EFT detects whether any default values are specified

for Admin login port (1100), DMZ Gateway port (44500), FTP banner message, or SFTP banner message, and will prompt you to change them.
No default passwords, usernames, certificates, or keys are

used.

2.2 Refer to the configuration standards for all system components.

2.2.1 Implement only one primary function per server.

2.2.2 Enable only the

2.2 Develop configuration standards for all system components.

EFT's primary function is to transfer files between server and the administrator to segregate servers.

apply
to necessary
the services,
protocols,
daemons,
etc.,
as
required
for
the protocol
function
is
necessary.
The
system
is
enabled
by
default.

2.2.3
Implement
additional
security
features
for
any
required
services,
protocols,

automatically detected* and are considered insecure to change them or present a compensating control.

*Requires Advanced Security module (for EFT Enterprise) or the Express Security module (for EFT

			Express) and creation of a PCI DSS Site.
2.2.4	With the Advanced Security module (for EFT Enterprise) or the Express Security module (for EFT Express) and a	Configure system security parameters to prevent misuse.	

PCI DSS Site, EFT monitors and warns when

- User login credentials persisted in memory beyond the absolute minimum time necessary (some configurations require this when reusing credentials for secondary

connections)

- Flood and DoS prevention settings set too low
- FTP Anti-timeout prevention scheme disabled or FXP (site-to-site) permitted

2.2.5 Remove all unnecessary functionality

It is up to the administrator to remove any scripts, custom commands,

AWE workflows or similar user-created files that are no longer in use.

2.3 Encrypt all non-console administrative access using strong cryptography.

The status of non-console (remote) access settings are monitored* and you are warned if SSL is

not enabled and given the option to either disable remote administration or enable SSL. *Requires Advanced Security module (for EFT Enterprise) or the Express Security module (for EFT Express) and creation of a PCI

DSS Requirement	How EFT Addresses PCI DSS Requirements
2.4 Maintain an inventory of system components for PCI DSS scope	EFT Site requires measures to maintain external IP addresses

Requirement 3: Protect Stored Cardholder Data

PCI DSS Requirement	How EFT Addresses PCI DSS Requirements
3.1 Keep cardholder	**EFT**

scheduled, automatic Clean-up Action*. Deleted files may be purged** by overwriting with pseudorandom data (PCI DSS 9.8). Disk quotas can be set to limit data storage.

*Requires

	EFT Enterprise. **Requires Advanced Security module (for EFT Enterprise) or the Express Security module (for EFT Express)	
3.2.1-3	Refers to not store sensitive authentication data (SAD), authorization (even if	

unencrypted).	
stored on the server.	
Use a third-party DLP or similar tool to detect and prevent SAD storage.	
3.3 Mask PAN when displayed	Not applicable to EFT, which does not display PAN. EFT cannot display that data.

How EFT Addresses PCI DSS Requirements

3.4 Encrypt PAN, or other sensitive data using EFT's optional OpenPGP encryption module or third-party encryption utilities.	
3.4.1 If disk encryption is used, logical access to encrypted data is managed	EFT will detect and warn if Microsoft Encrypting File System (EFS) is independently

being used. (Requires Advanced Security module (for EFT Enterprise) or the Express Security module (for EFT Express) and creation of a PCI DSS Site.)	
8.5 Do not use group, shared, or generic accounts and passwords, or other authentication methods.	Mostly operating system authentication and access control mechanisms.
10.5 Secure audit trails so they cannot be altered.	Document and measures

implement external
to procedures
to EFT; however
protect access
to keys
keys
through
the
administrator
interface
is
limited
to
administrator
roles
with
Site
or
Server
access
only.

3.6 Mostly
Fully requires
documents measures
and external
to implement
EFT; however, all
key per

3.6.1 Implement procedures for the creation of 512 or lesser certificate/key bit lengths. Default bit-length is set to 2048 bits for new keys. When importing SSL or SFTP keys,

3.6.1 Implement procedures for the creation of 512 or lesser certificate/key bit lengths. Default bit-length is set to 2048 bits for new keys. When importing SSL or SFTP keys,

a warning will appear if a weak key is imported. *Requires Advanced Security module (for EFT Enterprise) or the Express Security module (for EFT Express) and creation of

a PCI DSS Site 8.7 Requires Document external and procedures	

Requirement 4: Encrypt Transmission of Cardholder Data across Open, Public Networks

PCI DSS Requirement	**How EFT Addresses Requirement with EFT**
4.1 Use protocols such as SSL, TLS, and SFTP (SSH2)	Secure strong cryptography and security protocols

are provided for data transmission. Secure data transmission is enforced* by automatically redirecting incoming HTTP traffic to HTTPS.

*Requires Advanced Security module (for EFT Enterprise) or the Express Security module

		(for EFT Express)
4.2 – 4.3 Never send unprotected PANs by end-user messaging technologies; document security policies and procedures		Requires measures external to EFT

Requirement 5: Use and Regularly Update Anti-Virus Software

PCI DSS Requirement	How Requirement is Addressed with EFT

Requires measures 5.1 External to Anti-virus EFT requirements.

Requirement 6: Develop and Maintain Secure Systems and Applications

How PCI DSS Requirement is Addressed with EFT
Requirement 6.1 Establish processes for identifying security vulnerabilities discovered in EFT, including

an escalation process, a risk assessment that includes Common Vulnerability Scoring System (CVSS) risk ranking, and a process for notifying customers of critical patches or workarounds.

The

How EFT Addresses PCI DSS Requirements

Ensure that each system component and software is protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

Ensure that each system component and software is protected from known vulnerabilities by installing applicable vendor-supplied critical security patches. Install critical security patches within one month of release.

	the designated one-month window.
6.3 Develop internal and external software applications securely.	Globalscape takes a number of steps to develop software, as documented here: https://kb.globalscape.com/KnowledgebaseArticle11061.aspx.
6.3.1 Removal of custom application accounts, user IDs, and passwords prior	Only applies to Professional Services engagements and should be verified before

applications
deployment.
active
or
are
released
to
customers

6.3.2
Applies
to
Professional
Services
engagements
and
should
be
performed
prior
to
deployment.
Review
custom
code
prior
to
release
to
production
or
customers
in
order
to
identify
any
potential
coding
vulnerability.

How EFT Addresses PCI DSS Requirements

6.4 Requires Follows external to control procedures for all changes to system components.

6.5 GlobalSCAPE Addresses common coding vulnerabilities in software-development processes as documented here: https://kb.globalscape.com/KnowledgebaseArticle11061.aspx.

6.6 Requires For public-facing web

applications, addressing new threats and vulnerabilities as they emerge.

However, the dynamic nature of the threat landscape also underscores the importance of routine third-party security scans of EFT's public-facing web interfaces as part of its quality assurance process.

Requirement 6.7

Document external and internal procedures for EFT.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

PCI DSS Requirement	How EFT Addresses Requirement
7.1	EFT provides complete control over system and user access to data resources, with only those individuals completely segregated from such access.

7.2 Segregation Establish control access control system for systems using unique accounts, permissions that restrict access, based on templates and control need administrator access, and is accomplished via delegated, role-based administrator accounts

unless specifically allowed.

7.3 Requires documented policies and procedures.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

PCI DSS Requirement	How EFT Addresses Requirement	Addressed with EFT
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators	EFT enforces unique usernames for both users and administrators	✓

(8.1.1), user identification and administrative controls over user provisioning and authorization (8.1.2), allows user and admin account revocation (8.1.3), provides automatic removal of inactive users after 90 days (8.1.4),

includes controls for temporarily enabling/disabling users (8.1.5), auto-locks users after six failed login attempts (8.1.6), either for a period of time or permanently until the admin unbans (8.1.7), and

automatically expires sessions after 15 minutes of inactivity (8.1.8)

EFT supports various combinations of password, certificate, two-factor, and public-key authentication methods.

EFT supports various combinations of password, certificate, two-factor, and public-key authentication methods. (8.2), secures passwords during transmission (assumes

SSL
or
SSH),
and
storage
(with
a
one
way
[uniquely
salted]
hash)(8.2.1),
verifies
identity
before
allowing
password
reset
or
lost
username
retrieval
according
to
OWASP
guidelines
(8.2.2),
includes

minimum length and a number of complexity options (8.2.3), expires and forces password change after 90 days (8.2.4), disallows password re-use, internal dictionary match, or username match (8.2.5),

and can force first time use password reset (8.2.6).

8.3 Incorporate two-factor authentication for remote network access.

Although EFT supports 2FA, this requirement is about network access, such as what is normally done over a

NOTE: EFT does not provide multifactor authentication for

> Remote (non-console) administrator access.
>
> PCI DSS v3.2, you should disable remote (non-console) administrator access.
>
> From the PCI DSS v3.2, "Multi-factor authentication is not required at both the system-level

and
application-level
for
a
particular
system
component.
Multi-factor
authentication
can
be
performed
either
upon
authentication
to
the
particular
network
or
to
the
system
component."

Requires
Requirement
Document
external

to communicate EFT authentication procedures and policies

8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods (for EFT Enterprise) or the Express Security module

8.5 The "Anonymous" password type is disallowed on high-security-enabled sites (requires Advanced Security module

(for EFT Express). To comply with 8.5.1 you will need to create unique accounts for service provider access, should there ever be a need to provide such

access.

Requires
Requirements
external
unique
EFT
controlled
access
using
standard
authentication
physically
provisioned
to
the
user.

EFT
provides
granular
controls
over
database
administrators
cardholder
data
EFT's

restricted.

from

within

the

EFT

Server

console;

however

controls

over

access

to

the

database

(including

the

data

itself)

requires

measures

external

to

EFT.

Req

Requires

measures

external

to

EFT.

EFT procedures.

Requirement 9: Restrict Physical Access to Cardholder Data

PCI DSS Requirement	How EFT Addresses Requirement
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	EFT helps you meet requirements related to physical access to the cardholder environment.
9.8 Destroy media when it is no longer needed for business or legal reasons.	EFT supports data wiping

How EFT Addresses PCI DSS Requirements

it algorithm
is for
no sanitizing
longer deleted
needed data
for on
business disk.
or (Requires
legal Advanced
reasons. Security
module Cardholder
(for data
EFT on
Enterprise) electronic
or media
the must
EX be
Secure rendered
module unrecoverable
(for via
EFT a
Express) secure
.) wipe
program

9.9 Requires
Protect measures
devices external

that
EFT
can capture
payment
card
data
via
direct
physical
interaction

Requires
documented
external
and
EFT
procedures.

Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data

PCI DSS Requirement
10.1 Implement audit trails to link all access to system components to each individual user
10.2 Implement automated audit trails for all system components

10.3 Record audit trail entries for all system components
10.4 Synchronize critical system clocks and times
10.5 Secure audit trails so that they cannot be altered.
10.6 Review log sand security events for all system components (10.6.1) at least daily
10.7 Retain audit trail history for at least one year
10.8 Implement a process for the timely detection and reporting of failures of critical security control sys
10.9 Document policies and procedures

Requirement 11: Regularly Test Security Systems and Processes

PCI DSS Requirement	**How EFT Addresses PCI DSS Requirement**
11.1	Requires

11.6 Requirements relating to regular testing of security systems and processes.	- measures external to EFT.

Requirement 12: Maintain a Policy that Addresses Information Security

PCI DSS Requirement	How EFT Addresses Requirement Addressed with EFT
12.1 Requires a policy	- measures external to EFT.
12.1.0 Maintain an EFT policy	-

> that
>
> addresses
>
> information
>
> security
>
> for
>
> all
>
> personnel