Self-Serve AdminCentral

# PA-DSS Implementation Guide

## Self-Serve AdminCentral Transaction Engine

Version 1.2.3

## What is PA-DSS?

Payment Application Data Security Standard (PA-DSS) is a set of standards for payment applications that are sold to merchants. PA-DSS is derived from the Payment Card Industry Data Security Standard (PCI DSS) with a focus to ensuring application developers use best practices when handling card data.

Specific PA-DSS program requirements are organized around the following principles:

1. Do not retain full track data, card verification code or value, or PIN block data
2. Protect stored cardholder data
3. Provide secure authentication features
4. Log payment application activity
5. Develop secure payment applications
6. Protect wireless transmissions
7. Test payment applications to address vulnerabilities and maintain payment application updates
8. Facilitate secure network implementation
9. Cardholder data must never be stored on a server connected to the Internet
10. Facilitate secure remote access to payment application
11. Encrypt sensitive traffic over public networks
12. Encrypt all non-console administrative access
13. Maintain a PA-DSS Implementation Guide for customers, reslers, and integrators
14. Assign PA-DSS responsibilities for personnel, and maintain training programs for customers, resellers, integrators

## Self-Serve AdminCentral Transaction Engine PA-DSS status

Self-Serve AdminCentral Transaction Engine version 1.2.3 is validated to be compliant with Payment Application – Data Security Standards (version 3.1). The Transaction Engine v 1.2.3 is part of Self-Serve AdminCentral version 1.4.2 and may be included in other Self-Serve AdminCentral releases.

Merchants must be compliant to PCI DSS. A PA-DSS validated payment application facilitates a merchant's PCI compliance, but it alone will not ensure compliance.

Neither the Self-Serve AdminCentral Transaction Engine nor Self-Serve AdminCentral has any implementation requirements that would compromise a merchant's PCI DSS compliance.

## Purpose of this guide

This guide describes how to implement the EFI Self-Serve and Payment system, incorporating the Self-Serve AdminCentral Transaction Engine, in a PCI DSS compliant manner. It is a condition of the Self-Serve AdminCentral Transaction Engine's PA-DSS compliance that we provide this information.

Refer to this guide for information about topics including:

- How the engine handles transaction data
- Logging
- Upgrading and installing

*This guide is updated when there is a change in the Self-Serve AdminCetnral Transaction Engine related to PA-DSS, and annually to reflect changes in PCI standards and the Self-Serve AdminCentral Transaction Engine. You can download the latest version of this guide from the EFI website.*

*Revision history:*

| Date | Self-Serve AdminCentral Transaction Engine version | Document Part Number |
|---|---|---|
| August 2014 | 1.0.0 | 45124401 |
| December 2014 | 1.1.0 | 45132131 |
| December 2015 | 1.2.0 | 45145023 |
| May 2016 | 1.2.3 | 45151739 |

# Table of Contents

# 1. WHAT IS THE SELF-SERVE ADMINCENTRAL TRANSACTION ENGINE?

The Self-Serve AdminCentral Transaction Engine is a required component in the EFI Self-Serve AdminCentral System. The Engine is responsible for all credit card processing functionality.

Self-Serve AdminCentral allows self-serve copy and printing under a pay-at-the-device concept.

## 1.1. Component overview

Self-Serve AdminCentral is a hosted system, with server components on a host machine that is managed by EFI. The system requires the web-based interface to the host called Self-Serve AdminCentral for configuration, and one or more M500 series devices as customer interfaces.

The M500 series device is installed on-site and configured to work with an MFP (multi-function printer) to offer copy, print, and receipt printing services on the MFP after the customer inserts a valid payment card. The system is scalable, with an implementation able to have as few as one and as many as hundreds of M500 devices.

The Self-Serve AdminCentral Transaction Engine component resides on the M500 and is responsible for all functions related to payment cards and charging on the M500 series device.

The following diagram illustrates the system architecture:

**What the merchant, reseller or integrator is responsible for**

The merchant, reseller or integrator is responsible for implementing the Self-Serve AdminCentral Transaction Engine in a PCI compliant manner, within the context of implementing Self-Serve AdminCentral as described in this document.

# 2. CARD DATA HANDLING IN SELF-SERVE ADMINCENTRAL TRANSACTION ENGINE

The Self-Serve AdminCentral Transaction Engine (SSAC Transaction Engine) reads magnetic stripe data from credit cards. Data includes:

- PAN
- Expiry

The engine does not process PINs. The Engine does prompt the customer for CVC codes for some card gateways.

The Engine reads the information from a card and provides limited details (last 4 digits of card number, card type, and expired flag) to the M500 application. The M500 performs basic validation for card type support and if good, creates a transaction file. The transaction file only contains the last 4 digits of the card number and card type. The M500 application informs the Engine that validation passed, and the Engine creates a CardData file which contains the encrypted PAN and other card information. The encryption key is unique for each transaction under DUKPT. The engine derives the key for a particular transaction each time it is needed. Encryption uses 256-AES.

When the Engine must communicate with the card processing gateway for preauthorization or capture, it derives the encryption key and decrypts the PAN in memory. The engine deletes the PAN as soon as it is no longer needed.

Immediately after the transaction status changes to approved or declined, the Engine securely deletes the entire CardData file.

The CardData file that the Engine creates is the only place where card data is stored. The file only exists pre-authorization. The PAN is always stored in this table in encrypted form.

The file is named: D:\CloudData\CardData\CardData_*receipt#*.json

The transaction file created by the M500 application only holds the last 4 digits of the card number and card type.

The file is named: D:\CloudData\TransactionData\Tran*DateTime*.json

Post authorization, the Engine sends the transaction file to the host and deletes the local copy. The host never receives any card data other than the last 4 digits of the card number and card type,

After authorization, the M500 does not retain any cardholder data as both the CardData file and the transaction file are deleted.

The Activity log on the M500 contains only the first 2 and last 4 digits of card number and card type. The Event log on the M500 contains only the card type and last 4 digits. Logging on the M500 cannot be disabled.

The following security measures are implemented by EFI and the SSAC Transaction Engine to protect cardholder data:

- The PAN is always encrypted everywhere it is stored on the M500 before authorization to make it unreadable and unusable to an intruder.
- The PAN is securely deleted immediately after authorization to make it unreadable and unusable to an intruder.

- All transaction files are deleted from the M500 immediately after the transaction is sent to the host. The M500 does not retain any transaction files.
- All secure data deletion on the M500 uses 3 passes, in accordance with DoD 5220.22-M
- The Engine transmits data between the M500 and the host using HTTPS, using by default only PCI-DSS accepted secure TLS v1.2.
- The M500 never displays or prints the full PAN in the clear; the PAN is always masked wherever it is displayed.
  - On receipts, only the last 4 digits are displayed.
  - In Activity logs, only the first 2 and last 4 digits are logged
- The SSAC Transaction Engine never stores post-authorization data in non-volatile memory on the M500.
- The M500 is subject to physical security measures, including locked access panels.
- The host is never in possession of a PAN or any other sensitive cardholder data.

## 2.1. Self-Serve AdminCentral

Self-Serve AdminCentral is the interface to the host. Users at an organization log into Self-Serve AdminCentral to access configuration, M500 status, transactions, and sales reports. AdminCentral also provides a mechanism to retrieve activity logs from the M500.

The M500 sends transaction data that does not contain sensitive card data to the host, eliminating the possibility that sensitive card data can be accessed via any method from AdminCentral or any other access to the host.

The host does not have any other interface available to the organization.

# 3. IMPLEMENTING SELF-SERVE ADMINCENTRAL

The following sections contain information about what you must do to implement the Self-Serve AdminCentral system and the included SSAC Transaction Engine component in a PCI compliant manner.

The self-serve system does not have any implementation requirements that would prevent PCI compliance.

## 3.1. Do not retain full magnetic stripe, card validation code or value, or PIN block data

| PA-DSS Requirements | |
|---|---|
| PA-DSS | Description |
| 1.1.4 | Delete sensitive authentication data stored by previous payment application versions |
| 1.1.5 | Delete any sensitive authentication data (pre-authorization) gathered as a result of troubleshooting the payment application |
| 2.1 | Purge cardholder data after customer-defined retention period |
| 2.2 | Mask PAN when displayed so only personnel with a business need can see the full PAN |

| PA-DSS Requirements | |
|---|---|
| PA-DSS | Description |
| 2.3 | Render PAN unreadable anywhere it is stored |

These requirements ensure any cardholder data that is not necessary is deleted promptly and completely. These standards apply to the Engine's data handling and to EFI's and the merchant's or integrator's use of data for troubleshooting, diagnostics, or any business purpose.

### What the Self-Serve AdminCentral Transaction Engine does

Preauthorization, the Engine stores cardholder data in tables on the M500, described in "Card data handling in Self-Serve AdminCentral Transaction Engine" on page 6. The PAN is encrypted and unreadable at all times it is stored in these tables. The full PAN is never displayed on the M500 screen, printed in receipts, or logged.

Immediately after authorization, the Engine securely deletes the records containing the cardholder data. The Engine:

- securely deletes all card data records on the M500
- sends the transaction records to the host; the transaction records never contain sensitive data
- deletes all transaction records

The merchant cannot change any of these steps, including changing how long data is stored before it is deleted. There is no mechanism for the merchant or EFI to retrieve or view preauthorization cardholder data on the M500 for any reason, including troubleshooting. The Engine cannot be configured to show cardholder data under any circumstances.

Transaction information can be accessed after it is sent to the host via Self-Serve AdminCentral. A merchant user can only see the last 4 digits of the card number, card type, and total transaction amount. The PAN and other cardholder data are never sent to the Host, and therefore the PAN is not visible to any merchant user.

Previous versions of the Self-Serve AdminCentral Transaction Engine stored cardholder data in exactly the same way as version 1.2.3; data is not retained after authorization. There is no historical data to be deleted when you implement Self-Serve AdminCentral Transaction Engine version 1.2.3.

### What the merchant, reseller or integrator must do

PA-DSS requires EFI advise how to protect cardholder data in your possession. Cardholder data cannot be retrieved from the M500, however you must protect data you acquire from other systems or sources.

- Collect only data you need to solve a specific problem
- Encrypt sensitive data while it is in your possession
- Retain data for only the length of time you need it for legal, regulatory, or business purposes then securely delete it
- Store data in a specific, known location with limited access

## 3.2. Protect stored cardholder data

| PA-DSS Requirements | |
|---|---|
| PA-DSS | Description |
| 2.4 | Protect keys used to secure cardholder data |
| 2.5 | Implement key management processes and procedures for cryptographic keys |
| 2.6 | Render irretrievable cryptographic key material or cryptograms stored by the payment application |

These requirements ensure cryptographic keys used to secure cardholder data are protected to prevent disclosure and misuse.

### What the Self-Serve AdminCentral Transaction Engine does

Before authorization, the Engine stores the PAN in encrypted format at all times. The card reader encrypts the PAN before sending it to other Engine components.

The encryption key is unique for each transaction using a DUKPT scheme. When the Engine needs to decrypt the PAN for submission to the payment gateway, the engine derives the key and only holds the unencrypted PAN in memory. The unencrypted PAN is never saved. Encryption uses 256-AES.

The Engine never saves the encryption key for a transaction. Encryption methods are independent of Engine version and there is no data that needs to be deleted when the Engine is upgraded.

Post-authorization card data is not stored on the M500. When the transaction is authorized, the Engine securely deletes the card data record and sends the transaction to the host, and deletes the transaction completely.

### What EFI does

EFI takes several measures to ensure PANs are secure at all times, including:

- 256-AES encryption at all times when stored preauthorization
- Using encryption keys that change with each transaction
- Never storing encryption keys
- Securely deleting card data records at authorization to make the card data irretrievable
- Deleting the entire transaction from the M500
- Using secure deletion methods with 3 passes in accordance with DoD 5220.22-M
- Never logging the full PAN or writing it into any other file that remains on the M500
- Never displaying or printing the full PAN for customers or staff
- Never sending sensitive card data to the host

- EFI does not have any access to any preauthorization card data from the M500

EFI meets PA-DSS requirement 2.6 with the following measures:

- Using a secure procedure in which no data re-keying is required
- Using secure deletion methods with 3 passes in accordance with DoD 5220.22-M

**What the merchant, reseller or integrator must do**

PA-DSS requires EFI advise how to delete encryption keys used by previous versions of the Self-Serve AdminCentral Transaction Engine at upgrade.

The engine uses encryption to secure the PAN before authorization. Each transaction uses a unique key. The key is never stored, but is uniquely derived each time it is needed.

This method means:

- There is no key to delete when you upgrade.
- There is no encryption key management process required, therefore none of the following apply
  - Generation of strong cryptographic keys
  - Secure cryptographic key distribution
  - Secure cryptographic key storage
  - Cryptographic key changes for keys that have reached the end of their cryptoperiod
  - Retirement or replacement of keys when the integrity of keys has been weakened or suspected of being compromised
  - Split knowledge and dual control for any manual clear-text cryptographic key management operations supported by the payment application
  - Prevention of unauthorized substitution of cryptographic keys
- There is no process required to render encryption keys irretrievable when they are stored.

## 3.3. Provide secure authentication features

| PA-DSS Requirements | |
|---|---|
| PA-DSS | Description |
| 3.1 | Use unique user IDs and secure authentication for administrative access and access to cardholder data |
| 3.2 | Use unique user IDs and secure authentication for access to PCs, servers, and databases with payment applications |
| 3.3 | Secure payment application passwords during transmission and storage |

These requirements cover access controls to the M500 and the cardholder data on the host.

### What the Self-Serve AdminCentral Transaction Engine does

The Engine is a component that is installed on the M500 device and that is invoked by the M500 software as needed. The Engine does not have a user interface, and does not support any user logon or access, or provide access to cardholder data.

The engine does not generate, manage or otherwise support authentication credentials for administrative access or access to cardholder data. It does not generate or support user credentials or administration credentials. Credentials are not transmitted.

The M500 device does not allow user access to the Engine or cardholder data, either remote or local. The M500 software and the Self-Serve AdminCentral Transaction Engine are pre-installed on the M500 device and cannot be installed on another computer or device.

### What the merchant, reseller or integrator must do

PA-DSS requires EFI advise how to change and create authentication credentials for accounts with access to cardholder data.

Cardholder data cannot be accessed or retrieved by any means from the M500. There is no process or interface for configuring credentials to secure such access. If you have cardholder data in your possession, obtained from another system or source, you must establish and maintain unique user IDs and secure authentication per PCI requirements.

- Change default passwords
- Use unique user IDs
- Authentication requires at least 1 of the following methods
    - Something you know, such as a password or passphrase
    - Something you have, such as a token device or smartcard
    - Something you are, such as a biometric
- Do not use group, shared, or generic accounts and passwords
- Passwords are at least 7 characters long and contain numeric and alphabetic characters
- Require passwords to be changed at least every 90 days
- New passwords are different from the past 4
- Lock out the user for a minimum of 30 minutes after 6 logon attempts
- Require re-logon after 15 minutes idle
- Render credentials unreadable during transmission using strong one-way cryptographic algorithm; this must include concatenating a unique input variable with the password before encryption
- Render credentials unreadable where stored using strong one-way cryptographic algorithm; this must include concatenating a unique input variable with the password before encryption

## 3.4. Log Payment application activity

| PA-DSS Requirements | |
|---|---|
| PA-DSS | Description |
| 4.1 | PCI compliant log settings |
| 4.4 | Payment application facilitates centralized logging |

These requirements ensure all access to cardholder data is logged.

### What the Self-Serve AdminCentral Transaction Engine does

The M500 application and the Engine automatically create two types of logs on the M500. Logging cannot be disabled.

*Activity:* The activity log is a .txt file that details all automated and customer activity on the M500. It contains the first 2 and last four digits of the card number only. The activity log is useful for troubleshooting. The full PAN is never logged.

The activity log can be retrieved from the M500 when required for troubleshooting. The merchant can trigger the log download from Self-Serve AdminCentral, and the EFI support team can then access the log.

*Event:* The M500 event log is a .csv format file that comprehensively details activity related to and performed by the Self-Serve AdminCentral Transaction Engine. The log contains the last 4 digits of the card number and card type.

The event logs are automatically created and cannot be paused, disabled, or configured to contain more or less data. The M500 event log is in .csv format to be compatible with many centralized logging services.

The log is uploaded daily to SFTP using the credentials configured in Self-Serve AdminCentral. At the same time the log is uploaded, a new log is automatically created. You must configure the SFTP settings for the event log to be uploaded.

Events against the following components and activities are logged:

- Event log
- M500 Application
- Self-Serve AdminCentral Transaction Engine files
- Card Reader DLL
- D:\TransactionData folder
- Card data file
- Software updates

The event log audits the elements required by PCI-DSS 10.1 and 10.2 including:

- Initialization, stopping or pausing of audit logs
- Creation and deletion of system level objects
- Actions by administrators
- Access to audit logs
- Invalid logical access attempts

The log contains details to allow recreation of activity and identifies:

- User
- Type of event
- Date and time
- Success or failure
- Origination of event
- Affected data, system component or resource

M500 event log is compatible with Central Logging repositories that support CSV, including, but not limited to, Cisco Secure ACS and Dell SecureWorks Log Retention Service.

The event log is uploaded to a defined SFTP site daily between 1am and 5am as soon as the M500 is idle. Each log file contains a single day's events. At the time the log is uploaded to SFTP, the next log is automatically created.

Log name:

Location–DeviceName-MAC Address–YYYYMMDD-HHMMSS

Log entries use the following format:

date, time, timezone, user, type, result, origination, component

For example:

2015-03-20, 10:07:27:310, EST, SSAC Transaction Engine, Read Magnetic Stripe, Success, Card Reading, Card Reader DLL

**What the merchant, reseller or integrator must do**

- Define configuration settings to enable the uploading of the event log to your SFTP site. Configuration is defined in Self-Serve AdminCentral and applies to all your M500 devices. Configuration includes SFTP address, port, login username, and login password.
- Perform the necessary steps to use the event log in your centralized logging repository. You can import the log .csv file into your repository; you may need to put it through a conversion process or define rules to interpret the data.
- Do not take any measures to disable logging; disabling payment application logging will result in non-compliance with PCI DSS.
- Implement access controls to the SFTP site where the M500 event log is stored to restrict access to staff with a business reason
- Implement PCI DSS compliant access audit trails to any machine where the M500 event log is stored.

  Complete details are provided in PCI DSS requirements: 10.2 to 10.3.

  Auditing must allow you to reconstruct events including:

  - Individual access to the transaction files
  - All actions by individual with root or administrative privileges
  - Access to audit trails
  - Invalid logical access attempts

- Use of identification and authentication attempts
- Initialization of the audit logs
- Creation and deletion of system-level objects

Auditing must record for each event:

- User identification
- Type of event
- Date and time
- Success or Failure indication
- Origin of event
- Identity or name of affected data, system component or resource

## 3.5. Develop Secure Payment Applications

| PA-DSS Requirements | |
|---|---|
| PA-DSS | Description |
| 5.4.4 | Versioning methodology |

This requirement ensures merchants, resellers, and integrators understand which version of the Self-Serve AdminCentral Transaction Engine they are using and what type of changes have been made to each version.

**What EFI does**

The version of the Engine described in this document is version 1.2.3.

EFI uses the following schema for versioning: Major.Minor.Patch

*What is a major version?* If the Self-Serve AdminCentral Transaction Engine is rewritten, or if methods for encrypting data is changed. The major number could also change after the minor number reaches 9. A major release could have security impact.

*What is a minor version?* If a new payment gateway is added, or a new cash card processor. Could also be a defect fix related to card processing. A minor version update could indicate a security impact. The minor number could also change after the patch number reaches 9.

*What is a patch?* To fix a defect that is not related to card handling. A patch release does not have a security impact.

EFI does not use wildcards in its versioning methodology.

Note that the versioning for the M500 software or the Self-Serve AdminCentral is independent of the Engine.

## 3.6. Protect wireless transmissions

| PA-DSS Requirements | |
|---|---|
| PA-DSS | Description |
| 6.1 | Implement wireless technology securely |
| 6.2 | Implement strong encryption for authentication and transmission |
| 6.3 | Use wireless technology securely |

This requirement affects security around wireless technology implemented in the Self-Serve AdminCentral Transaction Engine and M500.

### What the Self-Serve AdminCentral Transaction Engine does

The Engine does not employ wireless network technology; the M500 has not been developed for use with wireless. EFI does not provide any wireless functionality.

The Self-Serve AdminCentral Transaction Engine is in full compliance with all PA-DSS standards related to wireless transmissions.

### What the merchant, reseller or integrator must do

If wireless technology is implemented around access to any machine where any cardholder data is stored or the M500 event logs are stored, it is the merchant, reseller, or integrator's responsibility to:

- Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission per PCI DSS 2.1.1
- Install a firewall per PCI DSS requirements 1.2.3, 2.1.1, and 4.1.1
  - Install a perimeter firewall between a wireless network and the store server per PCI DSS 1.2.3; this firewall must deny or control any access from the wireless environment to the cardholder data
  - Change the wireless vendor's default settings per PCI DSS 2.1.1
    - Encryption keys must be changed from default at installation, and must also be changed anytime anyone with knowledge of the keys leaves the company or changes positions
    - Default SNMP community strings on wireless devices were changed
    - Default passwords/passphrases on access points were changed
    - Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks (for example, WPA/WPA2)
    - Other security-related wireless vendor defaults, if applicable

- Ensure the wireless application was developed under industry best practices to include or make available strong encryption for authentication and transmission per PCI DSS 4.1.1. WEP is prohibited

## 3.7. Facilitate secure network implementation

| PA-DSS Requirements | |
|---|---|
| PA-DSS | Description |
| 8.2 | Use only necessary and secure services, protocols, daemons, components, and dependent software and hardware |

This requirement ensures services and components required by the Transaction Engine are secure.

**What the Self-Serve AdminCentral Transaction Engine does**

The engine does not require any insecure services. The necessary services are:

- Protocols Https TCP
- Ports TCP 443 TCP 9100
- Services AES 256 encryption
- Third party protocols WINHTTP provided by Microsoft provides HTTPS
- Third party ports TCP 443 WINHTTP
- Self-Serve AdminCentral for card processor configuration

## 3.8. Test payment applications to address vulnerabilities and facilitate secure remote access to payment application

| PA-DSS Requirements | |
|---|---|
| PA-DSS | Description |
| 7.2 | Software vendors must establish a process for timely development and deployment of security patches and upgrades |
| 10.1 | Use two-factor authentication for all remote access to the payment application that originates outside the customer environment |
| 10.2 | Implement secure remote access into the payment application |
| 10.2.1 | Securely deliver updates via remote access to customer networks |
| 10.2.3 | Implement remote access security features |

These requirements affect M500 software update deployment and the security around remote access to the Self-Serve AdminCentral Transaction Engine on the M500.

### What the Self-Serve AdminCentral Transaction Engine does

The M500 and the Engine do not support remote access. All access to the M500 is restricted to Self-Serve AdminCentral for configuration, software updates, monitoring, and downloading activity logs. The M500 and the Engine do not accept communications from any other source.

The M500 pulls software updates from the host when the software update is triggered from Self-Serve AdminCentral.

The M500 authenticates the host and uses a checksum to validate the update package is genuine. The update is applied to the M500 when the unit is idle.

### What EFI does

EFI does not automatically deploy software updates to your M500 devices. EFI does not use remote access products to access M500 devices in your store.

EFI may update software for new features, fixes, or to address security vulnerabilities.

EFI constantly monitors for newly identified security vulnerabilities and we act quickly when we identify a potential impact on security. EFI will provide a software update via Self-Serve AdminCentral; it is your responsibility to deploy the updates to your store's M500 devices in a timely manner.

EFI's release process for software updates that result from vulnerability detection is the same as that for other updates. EFI places software updates on the host as soon as possible. Self-Serve AdminCentral displays an alert that an update is available. Follow the workflow to deploy the update.

EFI uses MD5 cryptographic hashes to verify the integrity of the files we release. EFI runs the Microsoft File Checksum Integrity Verifier (FCIV) utility against a file being released. The M500 also generates a checksum against the update file to ensure it is valid.

### What the merchant, reseller or integrator must do

It is your responsibility to log into Self-Serve AdminCentral and trigger the application of the update to your M500 devices. Updates can only be applied through Self-Serve AdminCentral; they cannot be applied remotely or by any other means.

Each release is accompanied by release notes describing the changes in the version and/or changes to the PA-DSS Implementation Guide. Summary notes are viewable from within Self-Serve AdminCentral, full notes are available on the EFI website. Review these notes when you are deciding when to apply a software update. You must deploy M500 updates as quickly as possible to protect the integrity of your M500 and keep cardholder data secure.

If you do allow remote access to any non-EFI machine or system where you are storing cardholder data, you are responsible for implementing it securely according to PCI requirements 1, 2, 8, and 10, 12.3.9. Measures include:

- Enabling remote access technologies only when in use
- Changing default settings in the remote-access software
- Allow connections only from known IP/MAC addresses
- Use 2-factor authentication for logins
- Enable encrypted data transmission

- Enable account logout after a certain number of failed login attempts
- Establish a VPN connection or high-speed connection via a firewall
- Enable logging
- Restrict access

## 3.9. Cardholder data must never be stored on a server connected to the Internet

| PA-DSS Requirements | |
|---|---|
| PA-DSS | Description |
| 9.1 | Database and web servers do not need to be on same server or in the same DMZ |

This requirement ensures card data cannot be accessed over the Internet.

### What the Self-Serve AdminCentral Transaction Engine does

The transaction engine is not public-facing and it does not require cardholder data to be stored in the same network zone as a web server. The Engine does not require a database server.

The Engine communicates with the host and credit card processing gateways over https on port 443. The M500 uses port 9100 for printing under the RAW protocol, or port 515 for printing under LPR.

The Self-Serve AdminCentral Transaction Engine is in full compliance with all PA-DSS standards related to this PA-DSS requirement.

### What the merchant, reseller or integrator must do

If you store cardholder data obtained from another system or source, ensure the data is on an internal network zone segregated from the DMZ and other untrusted networks. Refer to PCI DSS 1.3.7.

## 3.10. Encrypt sensitive traffic over public networks

| PA-DSS Requirements | |
|---|---|
| PA-DSS | Description |
| 11.1 | Use strong cryptography and security protocols |
| 11.2 | Use solution to render the PAN unreadable when sending via end-user messaging technologies |

These requirements ensure cardholder data is secured during transmission.

### What the Self-Serve AdminCentral Transaction Engine does

The engine communicates with the card processing gateway for authorization. The engine uses HTTPS for all communication with the card processor.

The engine does not transmit or facilitate transmitting any data over end-user messaging technologies and does not include any function to enable such transmission. The engine does not support any methodology to retrieve cardholder data from the M500 that could be sent by the merchant over a public network or end-user messaging technology.

The Self-Serve AdminCentral Transaction Engine is in full compliance with all PA-DSS standards related to encrypting data over public networks.

### What the merchant, reseller or integrator must do

PA-DSS requires EFI advise about how to secure cardholder data you send over public networks or over end-user messaging technologies such as email, instant messaging, or chat.

Cardholder data cannot be retrieved from the M500. In accordance to PCI requirements 4.1 and 4.2, if you have cardholder data obtained from another source or system, and you transmit it over public networks or over end-user messaging technologies you must:

- Render the PAN unreadable or implement strong cryptology
- Verify that only trusted keys and/or certificates are accepted
- Verify the encryption strength is appropriate for the encryption methodology in use
- Employ secure encryption transmission technology, such as IPSEC, VPN, or TLS version 1.1 or higher

## 3.11. Encrypt all non-console administrative access

| PA-DSS Requirements | |
|---|---|
| PA-DSS | Description |
| 12.1 | Encrypt non-console administrative access |
| 12.2 | Configure the payment application to use strong cyryptography for non-console administrative access |

This requirement is for the encryption of non-console access to the M500 and the Self-Serve AdminCentral Transaction Engine.

### What the Self-Serve AdminCentral Transaction Engine does

Direct administrative access, including non-console administrative access, to the M500 is not possible. Configuration changes and software updates can only be performed via interaction with the Self-Serve AdminCentral interface.

Any change made in AdminCentral is pulled by the M500 and applied only after it is verified as valid. The drives, folders, and files on the M500 cannot be accessed via any method.

Logs are the only files that can be retrieved from the M500 by any method. Logs do not contain cardholder data. The download of activity logs must be triggered from Self-Serve AdminCentral and they can then be accessed by EFI from their downloaded location. Event logs are automatically uploaded to SFTP daily.

The Self-Serve AdminCentral Transaction Engine is in full compliance with all PA-DSS standards related to non-console administrative access.

**What the merchant, reseller or integrator must do**

- Restrict access to Self-Serve AdminCentral by managing the user accounts with logon credentials to prevent any change to configuration; AdminCentral cannot provide access to PANs or any other cardholder data.
- Restrict access to the SFTP site where event logs are uploaded to prevent any alterations of the logs. Access control and other security to your SFTP site is completely your responsibility.

# 4. INSTALLING THE SELF-SERVE SYSTEM

EFI provides a *Setup and Administration Guide* that describes a complete, non-merchant specific system installation and configuration.

Installation requires two general phases:

- System software configuration in Self-Serve AdminCentral
- M500 hardware assembly and connection

The M500 arrives at your location pre-loaded with all the required software components, including the Self-Serve AdminCentral Transaction Engine. If there is an updated version of software available, it will be automatically downloaded and applied when the M500 begins communicating with the host. The process is described in "Test payment applications to address vulnerabilities and facilitate secure remote access to payment application" on page 16.

## 4.1. Self-Service AdminCentral log in credentials

Self-Serve AdminCentral requires log in to access all of its functions, including configuration, software updating, and reporting.

User accounts are defined within AdminCentral, and a designated user receives an email inviting them to define their own password.

AdminCentral accounts or passwords should never be shared. Accounts should be deleted (deactivated) immediately if a staff member leaves your organization.

To create or delete an account, log into Self-Serve AdminCentral and click the Staff Account tab. You cannot define passwords for other users.

## 4.2. SFTP site requirements

The M500 automatically creates event logs.

The event logs created by the M500 satisfy PCI DSS requirements 10.2 and 10.3. You cannot disable logging or change any aspects of what is logged or how it is logged.

The event log can be uploaded daily to an SFTP site of your choosing, so you can use the log in your central logging server. You must enable log uploading to SFTP by configuring your specific site parameters in Self-Serve AdminCentral.

EFI does not provide or maintain this SFTP site. Managing the site and implementing PCI compliant security to the site is your responsibility.

Disabling logging will result in non-compliance with PCI DSS.

## 4.3. M500 security

You must manage the physical security of the M500. The M500 has a locked panel to protect cable connections and components from tampering. Keep the M500 keys in a secured location.

You must implement physical security controls to the M500 according to PCI standards (PCI DSS version 3.1 section 9). This includes but is not limited to:

- implementing restrictions on access to the M500 network jacks
- periodically inspecting the M500 device for evidence of tampering or substitution
- training personnel to be aware of suspicious behavior, and creating processes for reporting such behavior
- creating processes to verify the identity of third party persons claiming to be repair or maintenance personnel

# 5. UPGRADING TO SELF-SERVE ADMINCENTRAL TRANSACTION ENGINE VERSION 1.2.3

This section describes what you must do during an upgrade of the M500 components of the self-serve system, including the Self-Serve AdminCentral Transaction Engine.

Upgrades can introduce new features, defect fixes, or fixes to address vulnerabilities.

The Self-Serve AdminCentral version 1.4.2 contains the engine version 1.2.3 plus other components.

The Host and Self-Serve AdminCentral are upgraded by EFI. You must trigger the updating of your M500 devices.

## 5.1. Upgrading the M500 software

EFI posts M500 software update packages, and you can trigger their application to your M500 devices using the Self-Serve AdminCentral interface. When an update is available, an alert bar is visible across the top of the Self-Serve AdminCentral screen.

You can review information about the release within the update workflow, including the components being upgraded.

Once you trigger the update process, the remaining steps are automatic and do not require any intervention. When the M500 is idle, the M500 authenticates the update server, pulls the update package, verifies the package authenticity by checksum, and unencrypts the package. Only then is the upgrade process launched. Upgrade completely replaces the affected files on the M500.

After the upgrade, the M500 is ready for customer use again. Existing configuration is maintained after an upgrade.

There is no other way to upgrade any software on the M500.

## 5.2. Back-out process

To back-out of an upgrade, EFI posts a release that will apply earlier versions of software. You can apply the upgrade under the usual method. Alternatively, you must swap out the M500.

PA-DSS Implementation Guide
Self-Serve AdminCentral Transaction Engine v 1.2.3 ---Last revised 30-May-16