Oracle® Hospitality e7 Point-of-Sale

PA-DSS 3.2 Implementation Guide
Release 4.3
E87112-01

September 2017

ORACLE

Contents

Preface

This document describes the steps that you must follow in order for your e7 Point-of-Sale installations to comply with Payment Application – Data Security Standards (PA-DSS). The information in this document is based on PCI Security Standards Council Payment Application - Data Security Standards program (version 3.2 dated June 2016). You can download the PCI PA-DSS 3.2 Requirements and Security Assessment Procedures from the PCI SSC Document Library.

Oracle Hospitality instructs and advises its customers to deploy Oracle Hospitality applications in a manner that adheres to the PCI Data Security Standard (v3.2). Subsequent to this, you should follow the best practices and hardening methods, such as those referenced by the Center for Internet Security (CIS) and their various benchmarks, in order to enhance system logging, reduce the chance of intrusion, increase the ability to detect intrusion, and other general recommendations to secure networking environments. Such methods include, but are not limited to, enabling operating system auditing subsystems, system logging of individual servers to a centralized logging server, disabling infrequently-used or frequently vulnerable networking protocols, and implementing certificate-based protocols for access to servers by users and vendors.

You must follow the steps outlined in this Implementation Guide in order for your e7 Point-of-Sale installation to support your PCI DSS compliance efforts.

Revision History

Date	Description of Change
September 2017	• Initial publication

This PA-DSS Implementation Guide is reviewed and updated on a yearly basis, when there are changes to the underlying application, or when there are changes to PA-DSS requirements. Go to the Hospitality documentation page on the Oracle Help Center at http://docs.oracle.com/en/industries/hospitality/ to view or download the current version of this guide, and refer to the e7 Point-of-Sale's Release Notes and this guide's Revision History to learn what has been updated or changed. In order to ensure your PCI DSS compliance, you need to subscribe to receive email Oracle Security Alerts by clicking the Critical Patch Updates link on the Oracle Technology Network at http://www.oracle.com/technetwork/index.html. This provides you timely information on any possible updates to the PA-DSS Implementation Guide that you need to know about in order to continue to use e7 Point-of-Sale in a PCI DSS compliant manner.

1 Executive Summary

e7 Point-of-Sale 4.3 has been Payment Application - Data Security Standard (PA-DSS) validated, in accordance with PA-DSS Version 3.2. For the PA-DSS assessment, we worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PAQSA):

Coalfire Systems, Inc.
11000 Westmoor Circle, Suite 450,
Westminster, CO 80021

Coalfire Systems, Inc.
1633 Westlake Ave N #100
Seattle, WA 98109

This document also explains the Payment Card Industry (PCI) initiative and the Payment Application Data Security Standard (PA-DSS) guidelines. The document then provides specific installation, configuration, and ongoing management best practices for using Oracle Hospitality e7 Point-of-Sale Version 4.3 as a PA-DSS validated application operating in a PCI DSS compliant environment.

PCI Security Standards Council Reference Documents

The following documents provide additional detail surrounding the PCI SSC and related security programs:

- Payment Card Industry Payment Applications - Data Security Standard (PCI PA-DSS)
  https://www.pcisecuritystandards.org/security_standards/index.php
- Payment Card Industry Data Security Standard (PCI DSS)
  https://www.pcisecuritystandards.org/security_standards/index.php
- Open Web Application Security Project (OWASP)
  http://www.owasp.org
- Center for Internet Security (CIS) Benchmarks (used for OS Hardening)
  https://benchmarks.cisecurity.org/downloads/multiform/

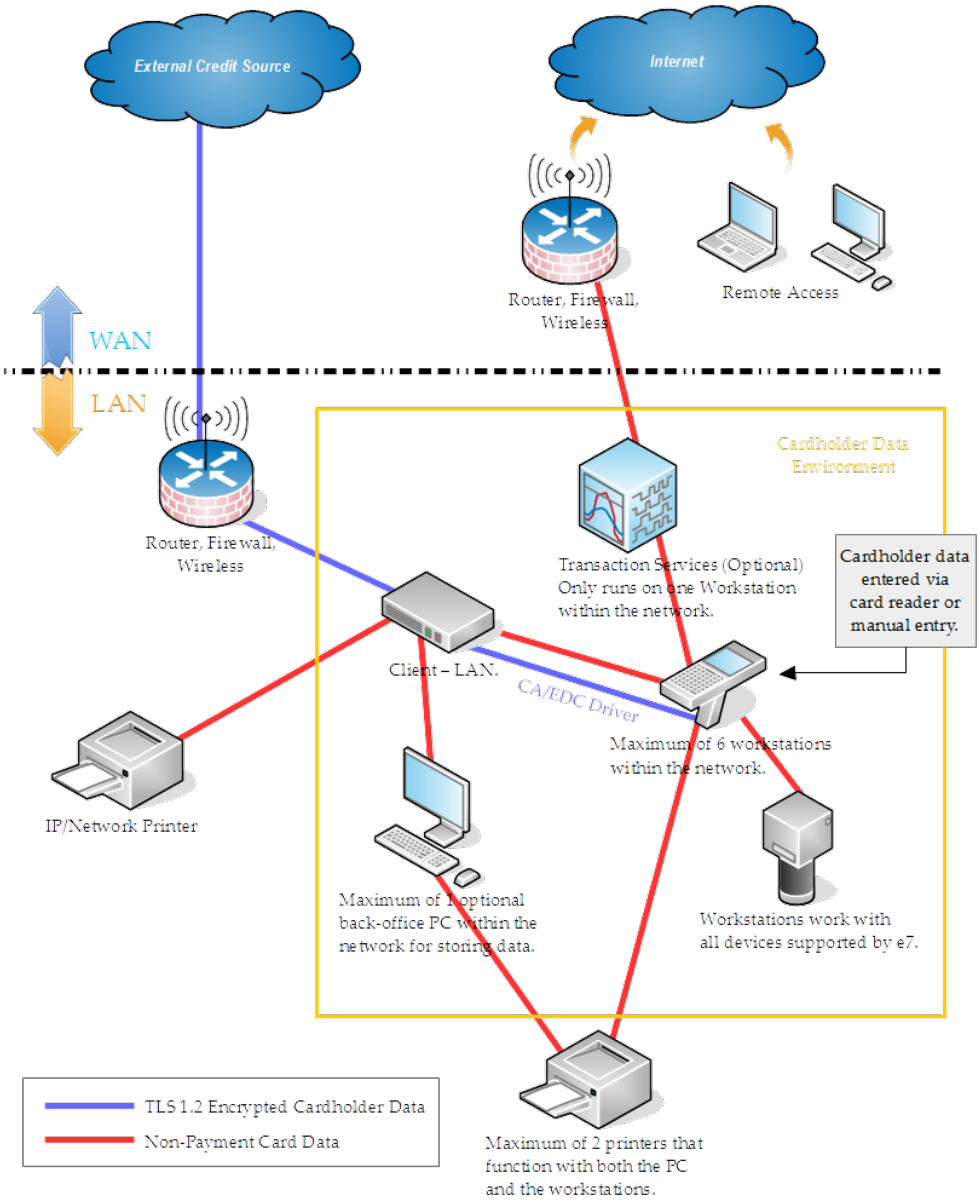
Payment Application Summary

<table>
<tr><td>Payment Application Name</td><td colspan="2">e7 Point-of-Sale</td><td>Payment Application Version</td><td colspan="2">4.3.X.X</td></tr>
<tr><td>Payment Application Description</td><td colspan="5">e7 operates as a full, standalone payment implementation and allows privileged users to:
Enter customer sales, perform employee operations, print receipts, void checks, generate and print system reports, assign cash drawers, and so on.
Create, edit and settle electronic draft data to the credit card processor.
View and print detailed information about each record in a credit card batch or batch transfer.</td></tr>
<tr><td>Typical Role of the Payment Application</td><td colspan="5">Used as a POS in a restaurant.</td></tr>
<tr><td rowspan="3">Target Market for Payment Application (check all that apply)</td><td>☐</td><td>Retail</td><td>☐</td><td>Processors</td><td>☐ Gas/Oil</td></tr>
<tr><td>☐</td><td>e-Commerce</td><td>☒</td><td colspan="2">Small/medium merchants</td></tr>
<tr><td>☐</td><td colspan="4">Others (please specify):</td></tr>
<tr><td rowspan="4">Stored Cardholder Data</td><td colspan="5">The following is a brief description of files and tables that store cardholder data.</td></tr>
<tr><td colspan="3">File or Table Name</td><td colspan="2">Description of Stored Cardholder Data</td></tr>
<tr><td colspan="3">ClosedCheckDetails.bin
ccbYYYYMMDD_batchsequence.bin
SalesTransactions.bin</td><td colspan="2">Card account numbers
Expiration dates
Customer names</td></tr>
<tr><td colspan="5">Individual access to cardholder data is logged as follows:
The application does not log full PAN data. The application logs the last four digits of the PAN for troubleshooting purposes.</td></tr>
<tr><td rowspan="2">Components of the Payment Application</td><td colspan="5">The following are the application-vendor-developed components which comprise the payment application:</td></tr>
<tr><td colspan="5">e7.exe – Payment application.</td></tr>
<tr><td rowspan="2">Required Third Party Payment Application Software</td><td colspan="5">The following are additional third party payment application components required by the payment application:</td></tr>
<tr><td colspan="5">Not applicable.</td></tr>
<tr><td>Supported Database Software</td><td colspan="5">The following are database management systems supported by the payment application:</td></tr>
</table>

<table>
<tr><td></td><td colspan="6">Not applicable.</td></tr>
<tr><td rowspan="2">Other Required Third Party Software</td><td colspan="6">The following are other third party software components required by the payment application:</td></tr>
<tr><td colspan="6">o Microsoft .NET Framework Runtime 3.5.1
o Microsoft Visual C++ Runtime</td></tr>
<tr><td rowspan="2">Supported Operating System(s)</td><td colspan="6">The following are Operating Systems supported or required by the payment application:</td></tr>
<tr><td colspan="6">Latest Supported Versions of:
• Microsoft Windows 10 (32-bit and 64-bit)
• Microsoft Windows 8.1 (32-bit and 64-bit)
• Microsoft Windows 7 Professional (32-bit and 64-bit)</td></tr>
<tr><td>Payment Application Authentication</td><td colspan="6">POS Application Terminal (transactions)
The Employee can use one of several methods to authenticate on the POS Application Terminal, they include:
• Employee Magnetic Card
• Employee Number/Pin
Configuration Interface
The Configurator utility requires:
• Unique Username.
• Password – must contain Uppercase, Number, Symbol and a minimum of 9 characters.
• Passwords are hashed with SHA256 with random salt.</td></tr>
<tr><td>Payment Application Encryption</td><td colspan="6">See e7 4.2 Security Design for information about payment application encryption.</td></tr>
<tr><td>Supported Payment Application Functionality</td><td>☐</td><td>Automated Fuel Dispenser</td><td>☐</td><td>POS Kiosk</td><td>☐</td><td>Payment Gateway/ Switch</td></tr>
<tr><td></td><td>☐</td><td>Card-Not-Present</td><td>☐</td><td>POS Specialized</td><td>☐</td><td>Payment Middleware</td></tr>
<tr><td></td><td>☐</td><td>POS Admin</td><td>☒</td><td>POS Suite/General</td><td>☐</td><td>Payment Module</td></tr>
<tr><td></td><td>☐</td><td>POS Face-to-Face/POI</td><td>☐</td><td>Payment Back Office</td><td>☐</td><td>Shopping Card & Store Front</td></tr>
<tr><td>Payment Processing Connections</td><td colspan="6">Table Service
The operator drops off a check at the customer table. The customer provides a payment card to the operator; the card is authorized using the POS terminal. The terminal communicates directly with</td></tr>
</table>

	the payment processor using secure transmission protocols. The authorization is approved and the card data is saved in the transaction detail and a voucher is printed. The operator returns the voucher to the customer and typically gratuity is added and the customer signs the voucher. The operator then returns to the POS terminal and makes final payment on the transaction and fills in gratuity field. The transaction is now finalized. **Quick Service** The cashier asks directly for payment from the customer after the ordering process. The customer provides a payment card to the operator; the card is authorized using the POS terminal. The terminal communicates directly with the payment processor using secure transmission protocols. Once authorization is complete, the POS makes final payment on the transaction. The transaction is now finalized. A customer receipt or voucher is often presented to the customer for signature. **Approved Payment Processors:** o Merchant Link o First Data o Heartland o RBS o SecureNet
Description of Listing Versioning Methodology	Oracle implements wildcard versioning and follows a versioning methodology for the application in the format of [N].[N].[N].[N] (where N represents a number): • Changes made at the Major level include architectural changes to the application and impact PA-DSS requirements or the security of the application. • Changes made at the Minor level include minor changes to the application that may or may not impact PA-DSS requirements. o Additional hardware platform and OS support can be added at the Minor level that may result in high level impact to PA-DSS requirements. • Changes at the Patch level include one or more changes made at the Interim level, and do not impact PA-DSS requirements or the security of the application. • Changes at the Interim level do not impact PA-DSS requirements or the security of the application. The versions of the payment application listed on the PCI SSC web site are listed as Major.Minor.X.X.

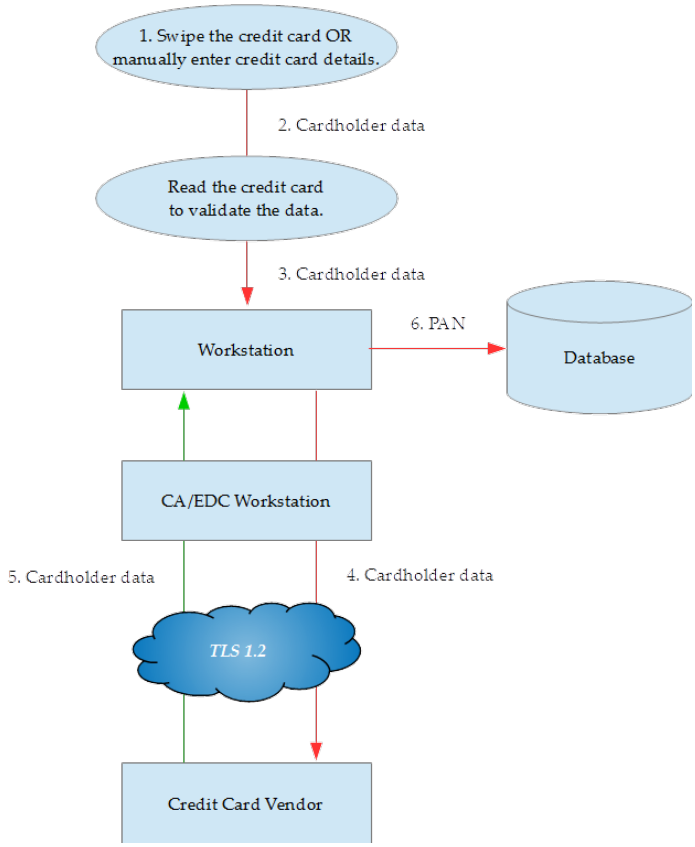
Typical Network Implementation



The e7 environment requires a device with a win32 operating system, either a back-office PC or a win32 workstation such as MICROS Workstation 6, to host credit card drivers in order to process credit card payments using Transport Layer Security 1.2.

Credit/Debit Cardholder Dataflow Diagram

Authorization Data Flow Diagram

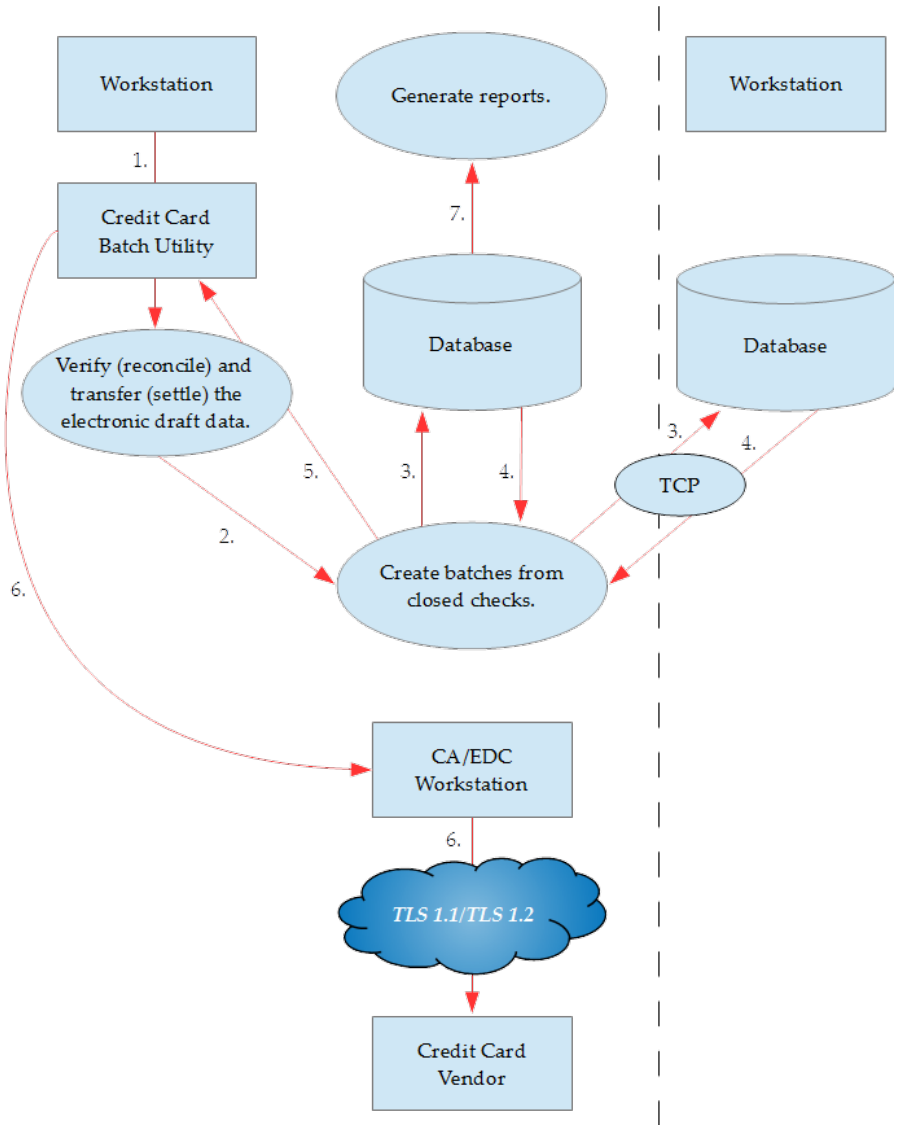


1. Read the credit card at the card-reading device.
2. Validate the data by reading the credit card itself.
3. Track data is sent to the Workstation.
4. Track data is sent through CA/EDC to the Credit Card Vendor by using a secure communication method (TLS 1.2).
   Note: CA/EDC can be hosted on a different node
5. An authorization response (Confirmation/Rejection) is sent to the system.
6. Credit card draft data (this may include the cardholder's credit card account number, the expiration date, purchase (payment) amount, and an authorization code) is stored in the database.

Red lines represent encrypted or unencrypted Sensitive Authentication data or Cardholder data in Transit.

Green lines represent data that is not considered Cardholder or Sensitive Authentication Data.

Batch Settlement Data Flow Diagram



1. At the end of each processing day, electronic draft data is verified (reconciled) and transferred (settled) to the Credit Card Processor.
2. The Credit Card Batch Utility creates a batch containing the transaction records that require payment.
3. The Credit Card Batch Creation processing method retrieves guest check files from all remote workstations.
4. Closed check details are sent to the settlement node.
5. Electronic draft data (credit card transactions from other workstations) are sent to the batch utility for reconciling and settling the electronic draft data.
6. During settlement, the batch is sent to the Credit Card Vendor/Processor for payment against customer credit card accounts.
7. Generate the Batch Transfer Status Report and Batch Detail Report.

Difference between PCI Compliance and PA-DSS Validation

As the software and payment application developer, our responsibility is to be PA-DSS validated. We have tested, assessed, and validated the payment application against PA-DSS Version 3.2 with our independent assessment firm (PAQSA) to ensure that our platform conforms to industry best practices when handling, managing, and storing payment-related information.

The PA-DSS Validation is intended to ensure that e7 Point-of-Sale will help you facilitate and maintain PCI Compliance with respect to how the payment application handles user accounts, passwords, encryption, and other payment data related information.

The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the PCI Data Security Standard (DSS). The security requirements defined in the DSS apply to all members, merchants, and service providers that store, process, or transmit cardholder data.

The PCI DSS requirements apply to all system components within the payment application environment which is defined as any network device, host, or application included in, or connected to, a network segment where cardholder data is stored, processed or transmitted.

PCI Compliance is an assessment of your actual server (or hosting) environment called the Cardholder Data Environment (CDE). It is the responsibility of you, as the merchant, and your hosting provider to work together to use PCI compliant architecture with proper hardware & software configurations and access control procedures.

The 12 Requirements of the PCI DSS:

Build and Maintain a Secure Network and Systems

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Protect all systems against malware and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know
8. Identify and authenticate access to system components
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for all personnel

2 Considerations for the Implementation of Payment Application in a PCI-Compliant Environment

Oracle provides functionality within e7 Point-of-Sale to enter sensitive personal information (including passport, date of birth, and credit card numbers) in specific fields on the user interface. The form fields that are intended to receive this information are clearly labeled, and are designed with heightened security controls such as data masking in the form and encryption of data at rest. Entering this sensitive personal information in any other field (for example, in a Notes or Comments field), does not provide it with these heightened security controls and is not consistent with the requirements for protecting cardholder data as detailed in the Payment Card Industry Data Security Standards (PCI DSS).

The following areas must be considered for proper implementation in a PCI-Compliant environment.

- Remove Historical Sensitive Authentication Data
- Handling of Sensitive Authentication Data
- Secure Deletion of Cardholder Data
- All PAN is masked by default
- Cardholder Data Encryption & Key Management
- Removal of Historical Cryptographic Material

Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4)

Sensitive Authentication Data (SAD) includes security-related information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions. Refer to the Glossary of Terms, Abbreviations, and Acronyms in the PCI SSC for the definition of Sensitive Authentication Data.

The following previous versions of e7 Point-of-Sale stored SAD:

- 1.0
- 1.5 and 1.5 Patch 1
- 2.0
- 2.0, 2.0 Patch 1, and 2.0 Patch 2
- 2.7

Historical SAD stored by previous versions of e7 Point-of-Sale must be securely deleted and removal is absolutely necessary for PCI DSS compliance. See Removing Historical Sensitive Data for information and instructions.

Handling of Sensitive Authentication Data (PA-DSS 1.1.5)

Oracle Hospitality does not store Sensitive Authentication Data (SAD) for any reason, and we strongly recommend that you do not do this either. However, if for any reason you should do so, the following guidelines must be followed when dealing with SAD used for pre-authorization (swipe data, validation values or codes, PIN or PIN block data):

- Collect SAD only when needed to solve a specific problem
- Store such data only in specific, known locations with limited access
- Collect only the limited amount of data needed to solve a specific problem
- Encrypt such data while stored
- Securely delete such data immediately after use

Secure Deletion of Cardholder Data (PA-DSS 2.1)

The following guidelines must be followed when dealing with Cardholder Data (Primary Account Number (PAN); Cardholder Name; Expiration Date; or Service Code):

- A customer defined retention period must be defined with a business justification.
- Cardholder data exceeding the customer-defined retention period or when no longer required for legal, regulatory, or business purposes must be securely deleted.
- Here are the locations of the cardholder data you must securely delete:

Database table	**Information**
ReferenceDbDetailTable	ExpDate, RefEntry
ReferenceTransDbDetailTable	ExpDate, RefEntry
CCBatchItemTable	CardAccountNumber, ExpDate, Track2Data, CustomerName
CCBatchTransferItemStatusTable	CardAccountNumber, ExpDate
CreditAuthDbDetailTable	CardAccountNumber, ExpDate, Track2Data, CustomerName
CaVoucherDbDetailTable	CardAccountNumber
File name	**Information from databases**
db\ClosedChecks\ businessDateFolder\ ClosedCheckDetails.bin	ReferenceDbDetailTable, CreditAuthDbDetailTable, CaVoucherDbDetailTable
db\OpenChecks\OpenChecks\ checkNumber.chk	ReferenceDbDetailTable, CreditAuthDbDetailTable, CaVoucherDbDetailTable

db\ReportDetail\ businessDateFolder\ SalesTransaction.bin	ReferenceTransDbDetailTable
db\CreditCardBatches\Pending\	CCBatchItemTable
db\CreditCardBatches\Settled\	CCBatchTransferItemStatusTable

- e7 Point-of-Sale automatically securely deletes Cardholder Data by:
  - Removing data on the OpenChecks file once the check is closed, and then moving the data to closedcheckdetals.bin.
  - Removing data on closedcheckdetails.bin by End of Day (EOD), and transferring the check data to CcBatchItemTable in the Pending folder as part of EOD operations.
  - Transferring the data to the Settled folder when settling the batch, and keeping the data for 90 days (duration can be configured.)
- All underlying software (this includes operating systems and/or database systems) must be configured to prevent the inadvertent capture of PAN. Instructions for configuring the underlying operating systems and/or databases can be found in Inadvertent Capture of PAN.

All PAN is Masked by Default (PA-DSS 2.2)

e7 Point-of-Sale masks all PAN by default in all locations that display PAN (screens, paper receipts, printouts, reports, etc.) by displaying only the last 4 digits. The payment application displays PAN in the following locations:

- Guest check receipt – masks all but the last four digits of the PAN.
- CA voucher receipt – masks all but the last four digits of the PAN and masks the expiration date.
- Batch Detail Report – masks all but the last four digits of the PAN and masks the expiration date.
- Batch Transfer Report – masks all but the last four digits of the PAN and masks the expiration date.

e7 Point-of-Sale does not have the ability to display full PAN for any reason and therefore there is no configuration details to be provided as required for PA-DSS v3.2.

Cardholder Data Encryption & Key Management (PA-DSS 2.3, 2.4, and 2.5)

e7 Point-of-Sale does store cardholder data and does have the ability to output PAN data for storage outside of the payment application. All PAN must be rendered unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs). To perform key encryption, click **Generate New Key** in the Configurator.

A list of all locations where PAN may be output by the merchant includes:

- Logs: contains masked PAN in \micros\e7\etc\.
- Database Backup: contains encrypted PAN in \micros\e7\DbBackups\.

NOTE: All PAN output by the merchant, to be stored in the merchant environment must be rendered unreadable using strong cryptographic methods.

e7 Point-of-Sale uses a dynamic key encryption.

- Generation of strong cryptographic keys.
  e7 uses AES-128, AES-192, or AES-256 encryption.
- Secure cryptographic key distribution.
  e7 programmatically generates keys and does not distribute them outside of the system.
- Secure cryptographic key storage.
  e7 encrypts the keys with AES-128, AES-192, or AES-256 using a dynamic key, then stores the encrypted keys in the proprietary database.
- Cryptographic key changes for keys that have reached the end of their cryptoperiod.
  - e7 Point-of-Sale does not enforce key change.
- e7 does not retire or replace keys when the integrity of the key has been weakened and/or when known or suspected compromise.
- e7 does not support manual clear-text cryptographic key-management procedures.
- e7 does not allow any substitution of cryptographic keys.

Removal of Historical Cryptographic Material (PA-DSS 2.6)

e7 Point-of-Sale has the following versions that previously encrypted cardholder data:

- e7 v4.2
- e7 v4.1
- e7 v4.0

If the historical Cardholder data is no longer needed, the following must be completed to ensure PCI Compliance:

- All cryptographic material for previous versions of the payment application (encryption keys and encrypted cardholder data) must be rendered irretrievable when no longer needed.
- e7 Point-of-Sale uses previously validated encryption algorithms that are PCI Compliant. Therefore there is no need to render historical cryptographic keys or cryptograms irretrievable as they are still in use by the payment application.

Set up Strong Access Controls (PA-DSS 3.1 and 3.2)

The PCI DSS requires that access to all systems in the payment processing environment be protected through use of unique users and complex passwords. Unique user accounts indicate that every account used is associated with an individual user and/or process with no use of generic group accounts used by more than one user or process.

All authentication credentials are generated and managed by the application. Secure authentication is enforced automatically by the payment application for all credentials by the completion of the initial installation and for any subsequent changes (for example,

any changes that result in user accounts reverting to default settings, any changes to existing account settings, or changes that generate new accounts or recreate existing accounts). To maintain PCI DSS compliance the following 11 points must be followed per the PCI DSS:

1. The payment application must not use or require the use of default administrative accounts for other necessary or required software (for example, database default administrative accounts) (PCI DSS 2.1 / PA-DSS 3.1.1)
2. The payment application must enforce the changing of all default application passwords for all accounts that are generated or managed by the application, by the completion of installation and for subsequent changes after the installation (this applies to all accounts, including user accounts, application and service accounts, and accounts used by Oracle Hospitality for support purposes) (PCI DSS 2.1 / PA-DSS 3.1.2)
3. The payment application must assign unique IDs for all user accounts. (PCI DSS 8.1.1 / PA-DSS 3.1.3)
4. The payment application must provide at least one of the following three methods to authenticate users: (PCI DSS 8.2 / PA-DSS 3.1.4)
    a. Something you know, such as a password or passphrase
    b. Something you have, such as a token device or smart card
    c. Something you are, such as a biometric
5. The payment application must NOT require or use any group, shared, or generic accounts and passwords (PCI DSS 8.5 / PA-DSS 3.1.5)
6. The payment application requires passwords to be at least 7 characters and to include both numeric and alphabetic characters (PCI DSS 8.2.3 / PA-DSS 3.1.6)
7. The payment application requires passwords to be changed at least every 90 days (PCI DSS 8.2.4 / PA-DSS 3.1.7)
8. The payment application keeps password history and requires that a new password is different than any of the last four passwords used (PCI DSS 8.2.5 / PA-DSS 3.1.8)
9. The payment application limits repeated access attempts by locking out the user account after not more than six logon attempts (PCI DSS 8.1.6 / PA-DSS 3.1.9)
10. The payment application sets the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. (PCI DSS 8.1.7 / PA-DSS 3.1.10)
11. The payment application requires the user to re-authenticate to re-activate the session if the application session has been idle for more than 15 minutes. (PCI DSS 8.1.8 / PA-DSS 3.1.11)

You must assign strong passwords to any default accounts (even if they won't be used), and then disable or do not use the accounts.

e7 does not include any additional applications or databases that require the account and password criteria from the above 11 requirements.

Configure Restaurant Security

Configure security settings for the restaurant:

1. From the e7 Configurator, select **Restaurant** and then select **Security**.

2. Select **Enable Enhanced Security**.
3. In the **Days Until Password Expire** field, enter the amount of days between 1 and 90 before requiring users to change their password.
4. In the **Minimum Password Length** field, enter the minimum number of characters between 9 and 40 that are required for a password.
5. In the **Minimum Uppercase Character**, **Minimum Lowercase Character**, **Minimum Numeric Character**, and **Minimum Special Character** fields, enter number of characters between 2 and 20 that are required for a password.
6. In the **Maximum Idle Time** field, enter the number of minutes between 1 and 15 that the Configurator remains open after being idle.
7. In the **Maximum Failed Logins** field, enter the number of failed login attempts between 1 and 6 before the account is set to inactive.
8. In the **Password Repeat Intervals** field, enter the number of previous passwords between 4 and 10 that are remembered to prevent a user from using a recent, previous password.

Configure Employee Account Security

Add employees who will need access to the e7 Configurator and configure their security settings:

1. From the e7 Configurator, select **Employee** and then select **Security**.
2. Select **Update Enhanced Security** and then fill out the form:
    - User ID
    - Password
    - Confirm User Password
    - User Must Change Password: select this option to force the user to change their password after their first login.
    - User Account Disabled: select this option to revoke access to the e7 Configurator.

Note: These password controls are not intended to apply to employees who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by employees with administrative capabilities, for access to systems with cardholder data, and for access controlled by the application. The requirements apply to the payment application and all associated tools used to view or access cardholder data.

PA-DSS 3.2: Control access, via unique username and PCI DSS-compliant complex passwords, to any PCs or servers with payment applications and to databases storing cardholder data.

Properly Train and Monitor Admin Personnel

It is your responsibility to institute proper personnel management techniques for allowing admin user access to cardholder data, site data, etc. You can control whether each individual admin user can see credit card PAN (or only last 4).

In most systems, a security breach is the result of unethical personnel. Pay special attention to whom you trust into your admin site and who you allow to view full decrypted and unmasked payment information.

Log Settings must be Compliant (PA-DSS 4.1.b and 4.4.b)

4.1.b: e7 Point-of-Sale has PA-DSS compliant logging enabled by default. This logging is not configurable and may not be disabled. Disabling or subverting the logging function of e7 Point-of-Sale in any way will result in non-compliance with PCI DSS.

Implement automated assessment trails for all system components to reconstruct the following events:

10.2.1 All individual user accesses to cardholder data from the application

10.2.2 All actions taken by any individual with administrative privileges in the application

10.2.3 Access to application audit trails managed by or within the application

10.2.4 Invalid logical access attempts

10.2.5 Use of the application's identification and authentication mechanisms (including but not limited to creation of new accounts, elevation of privileges, etc.) and all changes, additions, deletions to application accounts with root or administrative privileges

10.2.6 Initialization, stopping, or pausing of the application audit logs

10.2.7 Creation and deletion of system-level objects within or by the application

Record at least the following assessment trail entries for all system components for each event from 10.2.x above:

10.3.1 User identification

10.3.2 Type of event

10.3.3 Date and time

10.3.4 Success or failure indication

10.3.5 Origination of event

10.3.6 Identity or name of affected data, system component, or resource.

4.4.b: e7 Point-of-Sale supports delimited text and fixed length data fields for centralized logging. You can leverage the header record for each file, which denotes the delimiters and fixed length fields contained within the log file, to implement centralized logging.

3 PCI-Compliant Wireless Settings (PA-DSS 6.1.a and 6.2.b)

e7 Point-of-Sale does not support wireless technologies. However, should the merchant implement wireless access within the cardholder data environment, the following guidelines for secure wireless settings must be followed per PCI Data Security Standard 1.2.3, 2.1.1 and 4.1.1:

1.2.3: Perimeter firewalls must be installed between any wireless networks and systems that store cardholder data, and these firewalls must deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

2.1.1: Change wireless vendor defaults per the following 5 points:

1. Encryption keys must be changed from default at installation, and must be changed anytime anyone with knowledge of the keys leaves the company or changes positions.
2. Default SNMP community strings on wireless devices must be changed.
3. Default passwords/passphrases on access points must be changed.
4. Firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks.
5. Other security-related wireless vendor defaults, if applicable, must be changed.

4.1.1: Industry best practices (for example, IEEE 802.11.i) must be used to implement strong encryption for authentication and transmission of cardholder data.

Note: The use of WEP as a security control was prohibited as of June 30, 2010.

4 Services and Protocols (PA-DSS 8.2.c)

e7 Point-of-Sale does not require the use of any insecure services or protocols. Here are the services and protocols that e7 Point-of-Sale does require:

- Simple Object Access Protocol (SOAP) used by the Extensible Markup Language (XML) Web Service.
- Transmission Control Protocol/Internet Protocol (TCP/IP) and a proprietary protocol.
- Transport Layer Security (TLS) 1.2.

e7 requires the following third-party software:

- Microsoft .NET Framework Runtime
- Microsoft Visual C++ Runtime

Never Store Cardholder Data on Internet-Accessible Systems (PA-DSS 9.1.c)

Never store cardholder data on Internet-accessible systems (e.g., web server and database server must not be on same server.)

PCI-Compliant Remote Access (PA-DSS 10.1)

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism. The means two of the following three authentication methods must be used:

1. Something you know, such as a password or passphrase
2. Something you have, such as a token device or smart card
3. Something you are, such as a biometric

PCI-Compliant Delivery of Updates (PA-DSS 7.2.3, 10.2.1.a)

e7 Point-of-Sale delivers patches and updates in a secure manner:

This section describes how payment application updates and patches are delivered to the merchant. The method used must provide a secure chain of trust per requirements in PA-DSS 7.2.a, including:

- Timely development and deployment of patches and updates. Starting in January 2011, Critical Patch Updates (CPU) are released on the Tuesdays closest to the 17th of the months of January, April, July, and October. The Critical Patch Updates and Security Alerts page on Oracle's web site always list the dates of release for the next four Critical Patch Updates, thus effectively providing a one-year notice to customers.
  On the Thursday before the release of each CPU, a Pre-Release Advisory is published by Oracle. Both the Pre-Release Advisory and the CPU Release Documentation are posted on the Critical Patch Updates and Security Alerts

page on Oracle's web site located at http://www.oracle.com/technetwork/topics/security/alerts-086861.html.

- Delivery in a secure manner with a known chain-of-trust. Software patches and updates are delivered from the My Oracle Support webpage.

As outlined in the Oracle Customer Support Security Practices document:

My Oracle Support is the key website service for providing interactions with Global Customer Support (GCS) for Oracle programs and hardware, including (Service Request) SR access, knowledge search/browse, support communities and technical forums.

My Oracle Support employs the following security controls:

- My Oracle Support is an HTTPS extranet website service using Secure Socket Layer (SSL) encryption.
- Your registration on My Oracle Support uses a unique Customer Support Identifier (CSI) linked to your Support contract(s).
- **Delivery in a manner that maintains the integrity of the deliverable.**

  When a patch is downloaded from My Oracle Support's Automated Release Updates (ARU) page, the patch's digital signature should be verified. This is a relatively simple manual process.

  There are several free file integrity validation tools available on the web that can verify the Message Digest 5 (MD5) or Secure Hash Algorithm (SHA-1) checksum for the downloaded patch file. You can use a tool like the Microsoft File Checksum Integrity Verifier, or a similar MD5 and SHA-1 checksum utility.

  Choose and download the validation tool that you want to use. Once a patch has been downloaded, run your file integrity validation tool against it and compare the hash value generated by the validation tool to the hash value that corresponds to the patch on the ARU page. Both hash values should exactly match each other to confirm the file's integrity. Once you have validated the patch file's integrity, deploy the patch as soon as possible.

PCI-Compliant Remote Access (PA-DSS 10.3.2.a)

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism (username/ password and an additional authentication item such as a token or certificate).

In the case of vendor remote access accounts, in addition to the standard access controls, vendor accounts should only be active while access is required to provide service. Access rights should include only the access rights required for the service rendered, and should be robustly audited.

As outlined in *Oracle Global Customer Support Security Practices*, Oracle Global Customer Support (GCS) uses two main collaboration tools to review issues reported to Oracle: Oracle Web Conferencing (OWC) for programs and Oracle Shared Shell for hardware. Both tools share the following common features:

- You control and participate actively in all sessions. You control the session, what navigation is undertaken, what data is displayed and what commands are issued. You also have the ability to shut down the session at any time for any reason.

- Secure Socket Layer (SSL) encryption is provided for data transmitted over the Internet.

Additional details about OWC and Shared Shell:

If users and hosts within the payment application environment may need to use third-party remote access software such as Oracle Web Conferencing (OWC), Oracle Shared Cell, to access other hosts within the payment processing environment, special care must be taken.

In order to be compliant, every such session must be encrypted with at least 128-bit encryption (in addition to satisfying the requirement for two-factor authentication required for users connecting from outside the payment processing environment).

When requesting support from a vendor, reseller, or integrator, customers are advised to take the following precautions:

- Change default settings (such as usernames and passwords) on remote access software (e.g. VNC).
- Allow connections only from specific IP and/or MAC addresses.
- Use strong authentication and complex passwords for logins according to PA-DSS 3.1.1 – 3.1.10 and PCI DSS 8.1, 8.3, and 8.5.8-8.5.15.
- Enable encrypted data transmission according to PA-DSS 12.1 and PCI DSS 4.1.
- Enable account lockouts after a certain number of failed login attempts according to PA-DSS 3.1.8 and PCI DSS 8.5.13.
- Require that remote access take place over a VPN via a firewall as opposed to allowing connections directly from the internet.
- Enable logging for auditing purposes.
- Restrict access to customer passwords to authorized reseller/integrator personnel.
- Establish customer passwords according to PA-DSS 3.1.1 – 3.1.10 and PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.

Data Transport Encryption (PA-DSS 11.1.b)

The PCI DSS requires the use of strong cryptography and encryption techniques with at least a 128 bit encryption strength (either at the transport layer with TLS or IPSEC; or at the data layer with algorithms such as RSA or Triple-DES) to safeguard cardholder data during transmission over public networks (this includes the Internet and Internet accessible DMZ network segments).

PCI DSS requirement 4.1: Use strong cryptography and security protocols such as transport layer security (TLS 1.1/TLS 1.2) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

Examples of open, public networks that are in scope of the PCI DSS are:

- The Internet
- Wireless technologies
- Global System for Mobile Communications (GSM)
- General Packet Radio Service (GPRS)

Refer to the Dataflow diagram for an understanding of the flow of encrypted data associated with e7 Point-of-Sale

PCI-Compliant Use of End User Messaging Technologies (PA-DSS 11.2.b)

e7 Point-of-Sale does not allow or facilitate the sending of PANs via any end user messaging technology (for example, e-mail, instant messaging, and chat).

Non-Console Administration and Multi-Factor Authentication (PA-DSS 12.1, 12.2)

Although e7 Point-of-Sale does not support non-console administration and we do not recommend using non-console administration, should you ever choose to do this, you must use SSH, VPN, or TLS 1.1 or higher for encryption of this non-console administrative access along with a multi-factor authentication solution.

Network Segmentation

The PCI DSS requires that firewall services be used (with NAT or PAT) to segment network segments into logical security domains based on the environmental needs for internet access. Traditionally, this corresponds to the creation of at least a DMZ and a trusted network segment where only authorized, business-justified traffic from the DMZ is allowed to connect to the trusted segment. No direct incoming internet traffic to the trusted application environment can be allowed. Additionally, outbound internet access from the trusted segment must be limited to required and justified ports and services.

Refer to the standardized Network diagram for an understanding of the flow of encrypted data associated with e7 Point-of-Sale.

Maintain an Information Security Program

In addition to the preceding security recommendations, a comprehensive approach to assessing and maintaining the security compliance of the payment application environment is necessary to protect the organization and sensitive cardholder data.

The following is a very basic plan every merchant/service provider should adopt in developing and implementing a security policy and program:

- Read the PCI DSS in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.
- Once the gaps are identified, determine the steps to close the gaps and protect cardholder data. Changes could mean adding new technologies to shore up firewall and perimeter controls, or increasing the logging and archiving procedures associated with transaction data.
- Create an action plan for on-going compliance and assessment.
- Implement, monitor and maintain the plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities should complete annual self-assessments using the PCI Self-Assessment Questionnaire.

- Call in outside experts as needed.

Application System Configuration

Below are the operating systems and dependent application patch levels and configurations supported and tested for continued PCI DSS compliance.

- Microsoft Windows 10
- Microsoft Windows 8.1
- Microsoft Windows 7 SP1
- Microsoft Windows Compact Edition (CE) 6
- Microsoft Windows Embedded Compact 7

Payment Application Initial Setup & Configuration

Additional Resources:

- Oracle Hospitality e7 Installation Guide
- e7 Security Model

Appendix A Inadvertent Capture of PAN

This appendix provides instructions for addressing the inadvertent capture of PAN on the following supported operating systems:

- Microsoft Windows 10
- Microsoft Windows 8 and Microsoft Windows 8.1
- Microsoft Windows 7

Microsoft Windows 10

Disable System Restore

1. Click the **Start** button, enter `System Restore`, and click **Create a restore point**.
2. On the **System Protect** tab, click **Configure**.
3. Select **Turn off system protection**, click **Apply**, and then click **OK** until you return to the System dialog box.
4. Restart the computer.

Disable System Management of PageFile.sys

1. Click the **Start** button, select **File Explorer**, and then right-click **This PC**..
2. On the System dialog box, click **Advanced system settings**.
3. On the **Advanced** tab, click **Settings** for Performance.
4. On the **Advanced** tab, click **Change**.
5. Deselect **Automatically manage page file size for all drives**, select **Custom size**, and set the following fields:
    a. Initial Size: the amount of Random Access Memory (RAM) available.
    b. Maximum Size: 2x the amount of RAM.
6. Click **OK** until you return to the System dialog box.
7. Restart the computer.

Disable Error Reporting

1. Click the **Start** button, enter `regedit`.
2. Right-click **Registry Editor** and select **Run as Administrator**..
3. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\
4. Right-click Disabled and select **Modify**.
5. Set the value to 1 and click **OK**.

Microsoft Windows 8 and Microsoft Windows 8.1

Disable System Restore

1. Right-click **Computer** and select **Properties**.
2. On the System dialog box, click **Advanced system settings**.
3. On the **System Protection** tab, click **Configure**.
4. Select **Turn off system protection**, click **Apply**, and then click **OK** until you return to the System dialog box.
5. Restart the computer.

Encrypt PageFile.sys

Your hard disk must be formatted using NTFS to perform this operation.

1. Click the **Start** button and enter `cmd`.
2. Right-click **Command Prompt** and select **Run as Administrator**.
3. Enter the command: `fsutil behavior set EncryptPagingFile 1`
   To disable encryption, enter 0 instead of 1.
4. Enter the command: `fsutil behavior query EncryptPagingFile`
5. Verify that the command prompt returns: `EncryptPagingFile = 1`

Clear the System PageFile.sys on Shutdown

You can enable the option to clear PageFile.sys on system shutdown to purge temporary data. This ensures that information such as system and application passwords and cardholder data are not inadvertently kept in the temporary files. Enabling this feature may increase the time it takes for system shutdown.

1. Click the **Start** button and enter `regedit`.
2. Right-click **Registry Editor** and select **Run as Administrator**.
3. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\
4. Right-click ClearPageFileAtShutdown and select **Modify**.
   If ClearPageFileAtShutdown does not exist, right-click the Memory Management folder, select **New**, and select **DWORD (32-bit) Value**.
5. Set the **Value data** field to 1 and click **OK**.

Disable System Management of PageFile.sys

8. Right-click **Computer** and select **Properties**.
9. On the System dialog box, click **Advanced system settings**.
10. On the **Advanced** tab, click **Settings** for Performance.
11. On the **Advanced** tab, click **Change**.
12. Deselect **Automatically manage page file size for all drives**, select **Custom size**, and set the following fields:

a. Initial Size: the amount of Random Access Memory (RAM) available.
b. Maximum Size: 2x the amount of RAM.

13. Click **OK** until you return to the System dialog box.
14. Restart the computer.

Disable Error Reporting

1. Click the **Start** button and enter `Control Panel`.
2. Click **Control Panel**, then click **Action Center**.
3. Click **Change Action Center settings**, then click **Problem reporting settings**.
4. Select **Never check for solutions**, then click **OK**.

Microsoft Windows 7

Disable System Restore

1. Right-click **Computer** and select **Properties**.
2. On the System dialog box, click **Advanced system settings**.
3. On the **System Protection** tab, click **Configure**.
4. Select **Turn off system protection**, click **Apply**, and then click **OK** until you return to the System dialog box.
5. Restart the computer.

Encrypt PageFile.sys

Your hard disk must be formatted using NTFS to perform this operation.

1. Click the **Start** button and enter `cmd` in the search field.
2. Right-click cmd.exe and select **Run as Administrator**.
3. Enter the command: `fsutil behavior set EncryptPagingFile 1`
   To disable encryption, enter 0 instead of 1.
4. Enter the command: `fsutil behavior query EncryptPagingFile`
5. Verify that the command prompt returns: `EncryptPagingFile = 1`

Clear the System PageFile.sys on Shutdown

You can enable the option to clear PageFile.sys on system shutdown to purge temporary data. This ensures that information such as system and application passwords and cardholder data are not inadvertently kept in the temporary files. Enabling this feature may increase the time it takes for system shutdown.

1. Click the **Start** button and enter `regedit` in the search field.
2. Right-click regedit.exe and select **Run as Administrator**.
3. Navigate to
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\

4. Right-click ClearPageFileAtShutdown and select **Modify**.
   If ClearPageFileAtShutdown does not exist, right-click the Memory Management folder, select **New**, and select **DWORD (32-bit) Value**.
5. Set the **Value data** field to 1 and click **OK**.

Disable System Management of PageFile.sys

1. Right-click **Computer** and select **Properties**.
2. On the System dialog box, click **Advanced system settings**.
3. On the **Advanced** tab, click **Settings** for Performance.
4. On the **Advanced** tab, click **Change**.
5. Deselect **Automatically manage page file size for all drives**, select **Custom size**, and set the following fields:
   a. Initial Size: the amount of Random Access Memory (RAM) available.
   b. Maximum Size: 2x the amount of RAM.
6. Click **OK** until you return to the System dialog box.
7. Restart the computer.

Disable Error Reporting

1. Click the **Start** button, select **Control Panel**, and then click **Action Center**.
2. Click **Change Action Center settings**, then click **Problem reporting settings**.
3. Select **Never check for solutions**, then click **OK**.

Appendix B Removing Historical Sensitive Data

This appendix provides instructions for removing historical sensitive data when upgrading from an e7 version that was not PCI-compliant.

Virtual Memory

The Microsoft Windows operating system uses virtual memory to optimize the use of RAM and disk memory. MICROS e7 can write sensitive data to the virtual memory during data swap process between the RAM and virtual memory.

To configure the operating system to automatically clear virtual memory whenever a MICROS e7 PC reboots:

1. Click the **Start** button, select **Control Panel**, and then select **Administrative Tools**.
2. Double-click **Local Security Policy**, select **Local Policies**, and then double-click **Security Options**.
3. Depending on your operating system, double-click the policy listed in the following table:

Operating System	Policy Name
Microsoft Windows Vista Business	Clear Virtual Memory Page File When System Shuts Down
Microsoft Windows 10 Microsoft Windows 8.1 Microsoft Windows 8 Microsoft Windows 7 Professional	Shutdown: Clear Virtual Memory Pagefile

4. Select **Enabled** and then click **OK**.

Database Copies and Logs

Use a database removal utility to wipe data from the system. The utility must overwrite data with garbage data to prevent access to the original information. The operating system delete function does not comply with PCI security standards because it unlinks the filename from the data but leaves the data intact on the system.

You must remove all database copies, logs, and any other files that contain customer data. If you do not think you can locate all files that must be removed, security compliance recommends reinstalling the system on a reformatted hard drve.

Do not wipe current database files stored in the \MICROS\e7\db\ folder.

Database Backup

Back up the current database:

1. In the e7 Configurator, select **Functionality**, then select **Backup the Database**. e7 creates and stores the database backup file (backup.001.gz or backup.002.gz) in the =MICROS\e7\dbbackups\ folder.
2. Make a copy of the backup file in a secure location.