Oracle® MICROS e7 Version 3.3 or Higher

Payment Application-Data Security Standard (PA-DSS) Implementation Guide

General Information

About This Document

This document is intended as a quick reference guide to provide guidance and instructions for customers, resellers, and integrators to implement MICROS e7 software into a merchant environment in a PCI DSS compliant manner. This document relates specifically to Oracle MICROS e7 Version 3.3 and higher software.

Taking the appropriate steps to secure your system is required in order to be PCI compliant.

Revision History

Date	Initials	Brief Description of Change
4/2015	IB	Page 15: Added information about synchronizing time among components in the network.
12/2014	IB	The Implementation Guide was updated for v4.1 of e7.
8/2014	JM	The Implementation Guide was updated for v4.0 of e7.
10/2014	IB	Page 11: Removed paragraphs describing an encryption key sharing policy. Page 16: Removed paragraph describing the AES passphrase.
12/2012	RW	Updated e7 v3.3 and documentation to comply with the Payment Card Industry (PCI) Data Security Standard.pdf V 2.0

Declarations

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Introduction

About PCI Compliance

When customers offer their bankcard at the point of sale, over the Internet, on the phone, or through the mail, they want assurance that their account information is safe. That’s why the PCI Data Security Standard was instituted. The program is intended to protect cardholder data—wherever it resides—ensuring that members, merchants, and service providers maintain the highest information security standard[1].

For more detailed information concerning PCI compliance, please refer to the PCI Security Standards Council website, https://www.pcisecuritystandards.org/.

About The PCI Data Security Standard

PCI compliance is required of all merchants and service providers that store, process, or transmit cardholder data. The program applies to all payment channels, including retail (brick-and-mortar), mail/telephone order, and e-commerce. To achieve compliance with PCI, merchants and service providers must adhere to the PCI Data Security Standard, which offers a single approach to safeguarding sensitive data for all card brands. This Standard is a result of a collaboration among the credit card industry and is designed to create common industry security requirements, incorporating the PCI requirements.

Using the PCI Data Security Standard as its framework, PCI provides the tools and measurements needed to protect against cardholder data exposure and compromise across the entire payment industry. The PCI Data Security Standard, listed below, consists of twelve basic requirements supported by more detailed sub-requirements:

[1] Reprinted from “Cardholder Information Security Program”, <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>.

The PCI Data Security Standard[2]

Build and Maintain a Secure Network

- **Requirement 1:** Install and maintain a firewall configuration to protect cardholder data.

- **Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- **Requirement 3:** Protect cardholder data

- **Requirement 4:** Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- **Requirement 5:** Use and regularly update ant-virus software

- **Requirement 6:** Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- **Requirement 7:** Restrict access to cardholder data by business need-to-know

- **Requirement 8:** Assign a unique ID to each person with computer access

- **Requirement 9:** Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- **Requirement 10:** Track and monitor all access to network resources and cardholder data

- **Requirement 11:** Regularly test security systems and processes

Maintain an Information Security Policy

- **Requirement 12:** Maintain a policy that addresses information security

[2] Reprinted from the ‘PCI DSS Requirements and Security Assessment Procedures, v2.0’ document, available on the PCI Security Standards Council website, https://www.pcisecuritystandards.org/.

Who Should be Reading This Document

This document is intended for the following audiences:

- Installers/Programmers
- Dealers
- Customer Service
- Training Personnel
- IT Support Personnel

What the Reader Should Already Know

This document assumes that you have the following knowledge or expertise:

- Operational understanding of PCs
- Understanding of basic network concepts
- Experience with Microsoft Windows 2003, Windows XP, Windows Vista, Windows 7 or Windows 8
- Familiarity with the MICROS e7 software
- Familiarity with operating MICROS peripheral devices

MICROS e7 Version 4.0 and the PCI Data Standard

PCI Data Security Standard

While MICROS Systems Inc. recognizes the importance of upholding cardmember security and data integrity, certain parameters of the PCI Data Security Standard and PCI compliance are the sole responsibility of the client. This section contains a description of the 12 points of The PCI Data Security Standard. Information within this section pertains only to how the e7 Version 4.0 or later software conforms to The PCI Data Security Standard.

To ensure the payment application is implemented into a secure network environment, e7 does not interfere with the use of network address translation (NAT), port address translation (PAT), traffic filtering network device, anti-virus protection, patch or update installation, or use of encryption.

For a complete description of the PCI Data Security Standard, please consult the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

Document Conventions

This document is organized by each of the 12 basic requirements outlined in the PCI Data Security Standard. For each requirement, there is a MICROS Development response or recommendation that applies to e7 software.

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network.[3]

In accordance with the PCI Data Security Standard, MICROS Systems Inc. mandates every site, including wireless environments, install and maintain a firewall configuration to protect data. Configure your network so that databases and wireless access points *always* reside behind a firewall and have no direct access to the Internet.

[3] "Payment Card Industry (PCI) Data Security Standard.pdf", p. 20, V. 2.0, available on the PCI Security Standards Council website, https://www.pcisecuritystandards.org/.

Personal firewall software must be installed on any mobile and employee-owned computers with direct connectivity to the Internet, such as laptops used by employees, which are used to access the organization's network. The firewall software's configuration settings must not be alterable by employees.

Because of the PCI Data Security Standard, MICROS Systems Inc. mandates each site ensure that servers, databases, wireless access points, and any medium containing sensitive data reside behind a firewall. The firewall configuration must restrict connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks.

MICROS does not recommend that a specific vendor's firewall be installed. Work with the customers' network administrator to select a solution that works with their existing configuration. MICROS does sell a firewall that can be used for MICROS e7 sites. For information on the hardware firewall offered by MICROS, refer to *PMA05-828.*

Windows XP Pro, 2003, Vista, Windows 7 and Windows 8 have a built-in software firewall that should be enabled when running the MICROS e7 software. The firewall must be enabled before installing the MICROS e7 software.

To ensure your firewall configuration is set up in compliance with Requirement 1 of the PCI Data Security Standard, "Install and maintain a firewall configuration to protect data", please consult the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

2. Do not use vendor-supplied defaults for system passwords and other security parameters

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.[4]

The MICROS e7 software does not create any default accounts. After the MICROS e7 Version 4.0 software has been installed, any vendor-supplied passwords (including those used in wireless installations) must be changed to strong complex passwords that are in accordance with the Payment Application Data Security Standard before going live. This step is required in order to achieve PCI compliance.

[4] "Payment Card Industry (PCI) Data Security Standard.pdf", p. 24, V. 2.0, available on the PCI Security Standards Council website, https://www.pcisecuritystandards.org/.

Refer to the appropriate vendor-specific documentation for more information on changing vendor default passwords.

Strong application and system passwords are essential to maintaining a secure environment. MICROS Systems, Inc. mandates that customers and resellers/ integrators always create PCI compliant complex passwords. This is especially true for all users with administrative function access, and users accessing cardholder data. These groups of users must utilize complex passwords.

For wireless environments, the wireless vendor defaults must be changed to be PCI compliant. This includes, but is not limited to changing, wireless equivalent privacy (WEP) keys, default service set identifier (SSID), password, and SNMP community strings. Disable SSID broadcasts. Enable Wi-Fi protected access (WPA and WPA2) technology for encryption and authentication. For more information, refer to the *MICROS Wireless Networking Best Practices: A Payment Application Data Security Standard (PA-DSS) Implementation Guide Supplement* document.

All non-console administrative access must be encrypted using technologies such as SSH, VPN, or SSL/RLS (transport layer security) for web-based management and other non-console administrative access. Telnet or rlogin must never be used for administration.

For more information on Requirement 2 of The PCI Data Security Standard, “Do not use vendor-supplied defaults for system passwords and other security parameters”, please consult the PCI Security Standards Council website https:// www.pcisecuritystandards.org/.

Protect Cardholder Data

3. Protect stored data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.[5]

[5] “Payment Card Industry (PCI) Data Security Standard.pdf”, p. 28 V. 2.0, available on the PCI Security Standards Council website, https://www.pcisecuritystandards.org/.

MICROS Systems Inc. uses credit card masking and Triple-DES 128-bit encryption to ensure that credit card data is stored in a manner compliant with the PCI Data Standard. Each MICROS e7 workstation should always sit behind a firewall for protection from malicious Internet attacks.

MICROS e7 does not allow unmasked credit card information to appear on guest checks displayed on the workstation, customer receipts, and journals in order to comply with Requirement 3 of The PCI Data Security Standard. Only the last four digits of the Primary Account Numbers (PAN) are displayed.

All credit authorization data stored with guest checks are purged from the system on a nightly basis. When a site upgrades from an earlier version of MICROS e7 (versions 2.1 and lower) the database conversion process manages securing any historical data fields by removing the options to unmask the account number on the credit card voucher, guest check, and credit card batch utility.

Historical data (magnetic stripe data, card validation codes, PINs, or PIN blocks) stored by non-PCI compliant versions of the MICROS e7 software must be securely removed as a necessary component of PCI compliancy. Any cryptographic material, such as verification of cardholder data or sensitive authentication data stored by previous versions of the software, must also be securely removed as a necessary component of PCI compliancy.

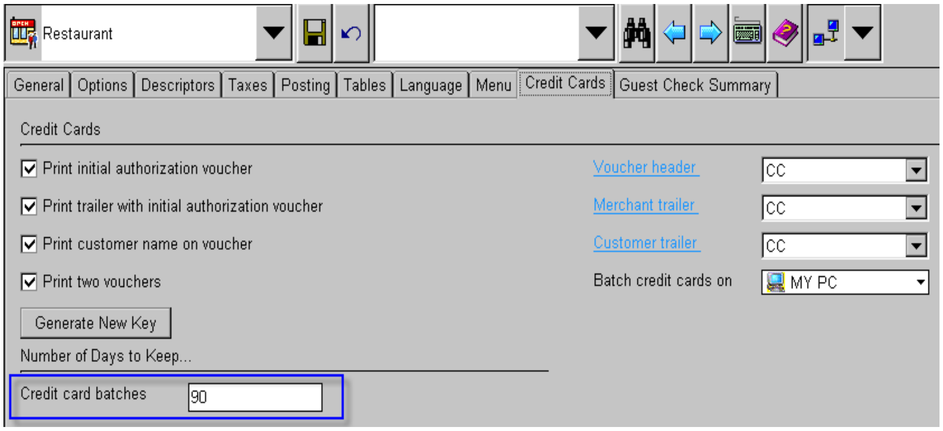
Therefore, conversions from a MICROS e7 non-PCI compliant version (versions 2.0 patch 2 and before) to a MICROS e7 PCI compliant version (versions 2.1 and higher) must include, securely erasing the legacy flat-file database and all old log files from the system after upgrading. Historical data must be securely removed wherever it resides. The MICROS e7 upgrade itself will encrypt all sensitive data in the 2.1 or higher database when the initial database conversion occurs. For more information, refer to the *MICROS e7 Upgrade Best Practices, MD0007-033* document, or consult the *Secure Data Storage Locations Within the MICROS e7 Product* section below.

The primary account number is never shown or logged unmasked. Masking is always used for the account number and the expiration date in all aspects of the MICROS e7 product.

Purging Cardholder Data

Cardholder data exceeding the merchant-defined retention period must be purged. Credit card batch purging is configured within the Configurator.

To configure credit card batch purging, navigate to the Credit Cards tab of the Restaurant form, as seen below. Within the 'Number of Days to Keep...' section, enter the number of days to save credit card batch files.



Credit Cards

☑ Print initial authorization voucher
☑ Print trailer with initial authorization voucher
☑ Print customer name on voucher
☑ Print two vouchers

Voucher header	CC
Merchant trailer	CC
Customer trailer	CC
Batch credit cards on	MY PC

Number of Days to Keep...

Credit card batches: 90

Secure Key Management Practices

Periodic Key Rotation

In order to achieve maximum security, MICROS Systems, Inc. mandates the system administrator regularly rotate the site's encryption keys.

PA-DSS requires that the passphrase used to generate the encryption key be changed periodically, at least once per calendar year. Always immediately replace known or suspected compromised keys.

Operating Conditions

MICROS e7 uses a Triple-DES 128-bit encryption scheme to encrypt credit card data with an encryption key. MICROS e7 allows the user to modify the passphrase used to generate the encryption key.

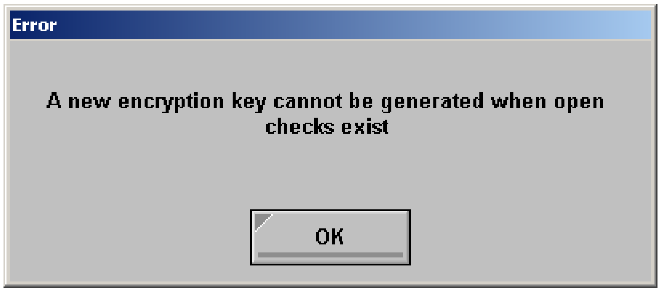
The MICROS e7 encryption key is generated at runtime in memory each time that the application needs to encrypt/decrypt sensitive data. The encryption key is resident only in memory, and the passphrase is not known to the user. The user is required to change the passphrase at least once per year in order to maintain PCI compliancy and must always replace known or suspected compromised keys immediately.

Warning!

This following procedure SHOULD ONLY be performed when the site is closed for business and all credit card batches have been settled*. MICROS recommends performing this operation at least two hours before the site opens for the day.*

Additionally, the following situations will cause the encryption key process to fail:

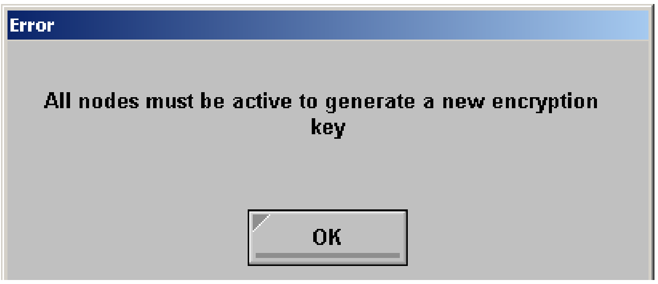
- *If there are any open checks on the system.*



Error

A new encryption key cannot be generated when open checks exist

- *If a node is offline.*



Error

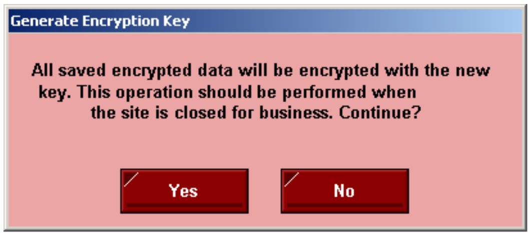
All nodes must be active to generate a new encryption key

Changing the Passphrase

Follow these steps to change the passphrase:

1. Go to the *MICROS e7 Configurator* | *Restaurant* | *Credit Cards* tab.
2. Select the **[Generate New Key]** button. This button will generate a new passphrase.
3. This operation will fail if there are open checks on the system, or if there are offline workstations. Do not continue until both of these issues are resolved.

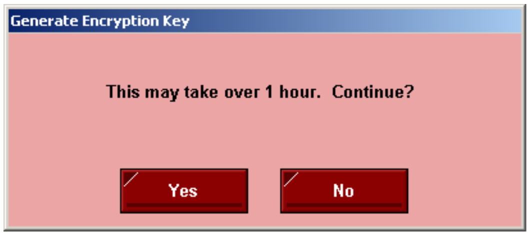
If the system satisfies these requirements, then the following verification prompt will appear:



All saved encrypted data will be encrypted with the new key. This operation should be performed when the site is closed for business. Continue?

Select **[Yes]** to continue, or select **[No]** to stop**.**

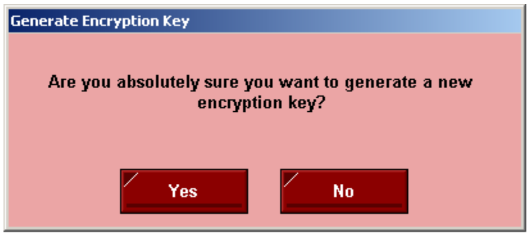
4. The following verification prompt will appear:



This may take over 1 hour. Continue?

Select **[Yes]** to continue, or select **[No]** to stop**.**

5. The following final verification prompt will appear:



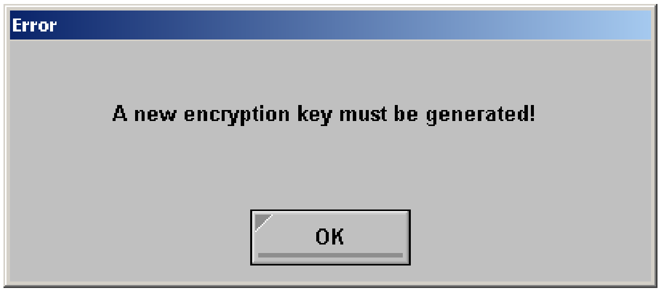
Are you absolutely sure you want to generate a new encryption key?

Select **[Yes]** to continue, or select **[No]** to stop**.**

The prompting is intended to ensure that the key is not changed accidentally.

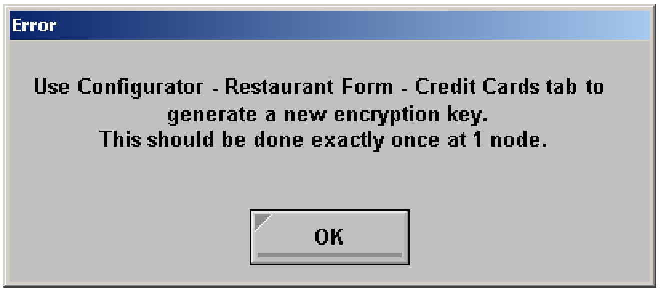
Upgrade Prompting

Following a MICROS e7 upgrade to Version 2.8, each node will display a prompt that a new key must be generated. The key will only need to be generated on one node (any node) and the key will be changed everywhere.



A new encryption key must be generated!

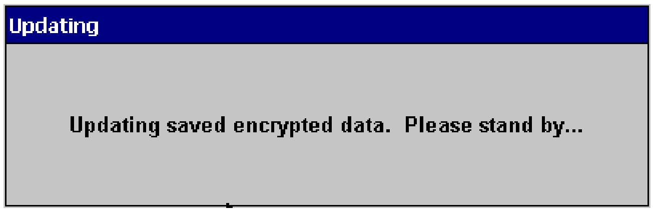
After selecting **[Ok]**, the user is prompted to navigate to the *MICROS e7 Configurator* | *Restaurant* | *Credit Cards* tab to change the key:



Use Configurator - Restaurant Form - Credit Cards tab to
generate a new encryption key.
This should be done exactly once at 1 node.

If the key is generated from the PC, then an hourglass will display until the process is complete.

If the key is generated from a workstation, then an hourglass will display along with the following dialog box:



Updating saved encrypted data. Please stand by...

Once this process is complete, the dialog box will disappear and the hourglass will return to the normal mouse cursor.

Secure Data Storage Locations Within the MICROS e7 Product

The table below lists the locations and the names of the files where secure data is stored. All of the files listed below contain card account numbers, expiration dates, and customer names:

File Name	Path
ClosedCheckDetails.bin	\MICROS\e7\db\ClosedChecks\
OpenCheckDetails.bin	\MICROS\e7\db\OpenChecks\
ccbYYYYMMDD_{BatchSeq}.bin	\MICROS\e7\db\CreditCardBatches\Pending\
ccbYYYYMMDD_{BatchSeq}.bin	\MICROS\e7\db\CreditCardBatches\Settled\
cctYYYYMMDD_{BatchSeq}.bin	\MICROS\e7\db\CreditCardBatches\Settled\
SalesTransactions.bin	\MICROS\e7\db\ReportDetail\bdYYYYMMDD\

Synchronizing time within the MICROS e7 Product

PCI DSS 10.4 - *Define and document process for obtaining and distributing a time signal (system time) to all components within the cardholder network.*

1. Sign in to a workstation with sufficient privileges to use Manager Procedures, then click **Workstations**.
2. Select the workstation you used to sign in.
3. Click **Set Date and Time** and set the time.
4. Select **Update all workstations** and click **Update**.

Security for MICROS e7 Resellers and Integrators

As mentioned previously, all sensitive data is stored in the database using 128-bit Triple-DES encryption. The cryptographic material used for encryption is generated at runtime and is resident in memory until the MICROS e7 application is exited. The MICROS e7 application does not require any manual interaction from merchants, resellers or integrators with regards to managing its cryptographic material.

In some situations, MICROS e7 resellers/integrators might be tasked with troubleshooting an issue with the system. To ensure cardholder data is protected, MICROS Systems, Inc. mandates MICROS e7 resellers/integrators must only collect customer data needed to solve a specific problem (for example, sensitive authentication data, log files, debug files, databases, etc.). Such data must only be stored in specific, known locations with limited access. Resellers/integrators must only collect the limited amount of data needed to solve a specific problem, and must encrypt such sensitive authentication data while stored. After such data is no longer used, it must be immediately deleted in a secure manner.

When troubleshooting customer issues, resellers and integrators must keep in mind the following when using databases from live customer sites:

- Collect live customer databases only when needed to solve a specific problem. If customer support requires the database, then it should be transferred to the MICROS customer support FTP site. Please refer to the *MICROS FTP Site File Transfer Policy*.

- Store databases in specific, known locations with limited access. Password protect zip archives used to store customer databases.

- Collect only the limited amount of data needed to solve a specific problem. Pull the latest known database backup, not every backup in the *\DbBackups* directory. The more files you retrieve, the more you have to manage through the troubleshooting process, and the more files you will have to destroy later. For information on destroying these files refer to the *MICROS Secure Wipe Tool* documentation.

- Securely delete such data immediately after use. This involves removing data from the PC or terminal where the troubleshooting occurred, and deleting it using a MICROS approved wipe tool. Detailed instructions on deleting this information can be found in the *MICROS Secure Wipe Tool* documentation.

For more information, refer to the *Customer Support Sensitive Information Security Policy & Handling Guidelines* document.

For more information on Requirement 3 of The PCI Data Security Standard, “Protect stored data”, please consult the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

4. Encrypt transmission of cardholder data across open,

public networks

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.[6]

MICROS Systems Inc., uses Triple-DES 128-bit encryption to ensure credit card data is transmitted across public networks in a manner compliant with the PCI Data Security Standard. When transmitting cardholder data over the Internet *always* use SSL and when transmitting wirelessly, *always* use the highest level of encryption available. For more information, please refer to the *MICROS Wireless Networking Best Practices: A Payment Application Data Security Standard (PA-DSS) Implementation Guide Supplement* document.

Wireless transmissions of cardholder data must be encrypted over both public and private networks. Encrypt transmissions by using Wi-Fi Protected Access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. Use one of the above methodologies in conjunction with WEP at 128 bit, and rotate shared WEP keys quarterly and whenever there are changes in personnel who have access to keys. WEP must be used with a minimum 104-bit encryption key and 24 bit-initialization value. Always restrict access based on media access code (MAC) address.

Be certain to rotate the site's encrytion key for the WPA/WPA2 frequently. At a minimum, this key should be rotated annually.

Because of the PCI Data Security Standard, MICROS Systems Inc. mandates each site use secure encryption transmission technology (for example, IPSEC, VPN, or SSL/TLS) when sending cardholder information over public networks, including when using wireless connections, E-mail, and when using services such as Telnet, FTP, etc. When sending credit card numbers via email, customers and resellers must use an email encryption solution.

Modems should not reside in application servers unless absolutely necessary. If a modem is installed, it should be kept powered off or disabled except when needed. For added security, the modem should be configured to use automatic call back and data encryption. Firewalls will not protect against attacks via the modem.

[6] "Payment Card Industry (PCI) Data Security Standard.pdf", p. 35 V. 2.0, available on the PCI Security Standards Council website, https://www.pcisecuritystandards.org/.

All non-console administrative access must be encrypted using technologies such as SSH, VPN, or SSL/RLS (transport layer security) for web-based management and other non-console administrative access. Telnet or rlogin must never be used for administration.

For more information on Requirement 4 of The PCI Data Security Standard, “Encrypt transmission of cardholder data and sensitive information across public networks”, please consult the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software

Malicious software, commonly referred to as ―malware‖—including viruses, worms, and Trojans—enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.[7]

In accordance with the PCI Data Security Standard, MICROS Systems Inc. mandates regular use and regular updates of anti-virus software. Anti-virus software should be deployed on the MICROS e7 PC on a regular basis.

Anti-virus software must also be deployed on all systems commonly affected by viruses, particularly personal computers and servers.

To ensure your anti-virus software is set up in compliance with Requirement 5 of the PCI Data Security Standard, “Use and regularly update anti-virus software”, please consult the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

6. Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.[8]

[7] “Payment Card Industry (PCI) Data Security Standard.pdf”, p. 37 V. 2.0, available on the PCI Security Standards Council website, https://www.pcisecuritystandards.org/.

[8] “Payment Card Industry (PCI) Data Security Standard.pdf”, p. 38 V. 2.0, available on the PCI Security Standards Council website, https://www.pcisecuritystandards.org/.

MICROS Systems Inc., uses separate development and production environments to ensure software integrity and security. Updated service packs and hot fixes are available via the MICROS product website, <*http://www.micros.com*>. While MICROS Systems Inc. makes every possible effort to conform to Requirement 6 of the PCI Data Security Standard, certain parameters, including following change control procedures for system and software configuration changes, and the installation of available security fixes, depend on site specific protocol and practices.

In order to comply with Requirement 6 of the PCI standard, all Operating System (OS) must be patched and updated regularly. When a critical update is released, the site must install that update to ensure that system security is as strong as possible. Antivirus definitions must also be installed on all PCs, and should be kept up to date with the most recent virus definitions. Check the documentation provided by your antivirus software provided as well as for your Operating System for steps to ensure that your software is up to date.

Microsoft Windows XP Pro feature System Restore must be disabled and remain disabled to maintain PCI compliancy. To disable System Restore, follow the steps below:

1. From the *Start Menu* go to the *My Computer | Properties | System Properties | System Restore* tab and enable either the **Turn off System Restore** option or the **Turn off System Restore on all drives** option.
2. Select **[Ok]**.
3. When prompted with the following message, click **[Yes]** to confirm that you would like to turn off the System Restore:

   ```
   You have chosen to turn off System Restore. If you
   continue, all existing restore points will be deleted,
   and you will not be able to track or undo changes to
   your computer.
   Do you want to turn off System Restore?
   ```

4. The *System Properties* dialog box will close. Follow the steps to turn on System Restore.

Follow these steps to turn on System Restore:

1. From the *Start Menu* go to the *My Computer | Properties | System Properties | System Restore* tab.
2. Clear the **Turn off System Restore** option or the **Turn off System Restore on all drives** option.

3. Click **[Ok]**.
4. The *System Properties* dialog box will close.

To ensure your site develops and maintains secure systems and applications in compliance with Requirement 6 of The PCI Data Security Standard, “Develop and Maintain Secure Systems and Applications”, please consult the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.[9]

MICROS Systems Inc., recognizes the importance of data control, and does so by establishing access based upon employee class level. This mechanism ensures access to sensitive information is restricted, password protected, and based on a need-to-know basis.

Access to customer passwords by resellers/integrator personnel must be restricted.

For more information on Requirement 7 of The PCI Data Security Standard, “Restrict access to data by business need-to-know”, please consult the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

8. Assign a unique ID to each person with computer access

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.[10]

MICROS Systems Inc., recognizes the importance of establishing unique ID’s for each person with computer access. No two MICROS e7 users can have the same ID. While MICROS Systems Inc., makes every possible effort to conform to Requirement 8 of the PCI Data Security Standard, certain parameters, including proper user authentication, remote network access, and password

[9] “Payment Card Industry (PCI) Data Security Standard.pdf”, p. 44 V. 2.0, available on the PCI Security Standards Council website, https://www.pcisecuritystandards.org/.

[10] “Payment Card Industry (PCI) Data Security Standard.pdf”, p. 46 V. 2.0, available on the PCI Security Standards Council website, https://www.pcisecuritystandards.org/.

management for non-consumer users and administrators, for all system components, depend on site specific protocol and practices. This requirements must be complied with in order for the site to be PCI compliant.

To ensure strict access control of the MICROS e7 application, always assign unique usernames and complex passwords to each account. MICROS Systems Inc. mandates applying these guidelines to both MICROS passwords, and to Windows passwords.

Furthermore, MICROS Systems, Inc. advises users to control access, via unique usernames and PCI-compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data.

Creating Secure Passwords

To comply with Requirement 8 of the PCI Data Security Standard, follow the standards below:[11]

- Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.
- Verify user identity before performing password resets.
- Set first-time passwords to a unique value for each user and change immediately after the first use.
- Immediately revoke access for any terminated users.
- Remove/disable inactive user accounts at least every 90 days.
- Enable accounts used by vendors for remote maintenance only during the time period needed.
- Communicate password procedures and policies to all users who have access to cardholder data.
- Do not use group, shared, or generic accounts and passwords.
- Change user passwords at least every 90 days.
- Require a minimum password length of at least seven characters.
- Use passwords containing both numeric and alphabetic characters.

[11] “Payment Card Industry (PCI) Data Security Standard.doc”, p. 38–41, V. 1.2, October, 2008. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-2.pdf>.

- Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
- Limit repeated access attempts by locking out the user ID after not more than six attempts.
- Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.
- If a session has been idle for more than 15 minutes, require the user to re-enter the password to reactivate the terminal.
- Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.

Remote Access

MICROS Systems, Inc. mandates a two-factor authentication for remote access to the site's network by MICROS Systems, Inc. employees, administrators, and third parties. Technologies such as remote authentication and dial-in service (RADIUS), terminal access controller access control system (TACACS) with tokens, or VPS based on SSL/TLS or IPSEC with individual certificates must be used.

Remote access software security features must always be used and implemented. Therefore, default settings in the remote access software must be changed so that a unique username and complex password is used for each customer.

Never use the default password and adhere to the PCI DSS password requirements established on page 21 when creating the new, strong password for the remote access software. Adhere to the same PCI DSS password requirements when creating customer passwords. Passwords must contain at least seven characters, including a combination of numbers and letters.

Connections must only be allowed from specific, known IP/MAC addresses. Strong authentication or complex passwords for logins must be used. Encrypted data transmission and account lockout after a certain number of failed attempts must be enabled. The systems must be configured so that a remote user must establish a VPN connection via a firewall before access is allowed.

Logging functions must be enabled for security purposes. Disabling logs should not be done and will result in non-compliance with PCI DSS. Access to customer passwords must always be restricted to authorized reseller/integrator personnel. For more information, refer to the *MICROS Customer Support Remote Support Access Policy* document.

For more information on Requirement 8 of the PCI Data Security Standard, “Assign a unique ID to each person with computer access”, please consult the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

9. Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, ―onsite personnel‖ refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A ―visitor‖ refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. ―Media‖ refers to all paper and electronic media containing cardholder data.[12]

In accordance with the PCI Data Security Standard, MICROS Systems Inc. mandates the restriction of physical access to cardholder data. Inbound and outbound traffic to the cardholder data environment must be restricted.

MICROS Systems, Inc. mandates that users cannot store cardholder data on Internet-accessible systems. To ensure cardholder data is not stored on Internet-accessible systems, the web server and data server must not be on the same server.

To ensure your site is set up in compliance with Requirement 9 of The PCI Data Security Standard, “Restrict physical access to cardholder data”, please consult the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.[13]

[12] “Payment Card Industry (PCI) Data Security Standard.pdf”, p. 51 V. 2.0, available on the PCI Security Standards Council website, https://www.pcisecuritystandards.org/.

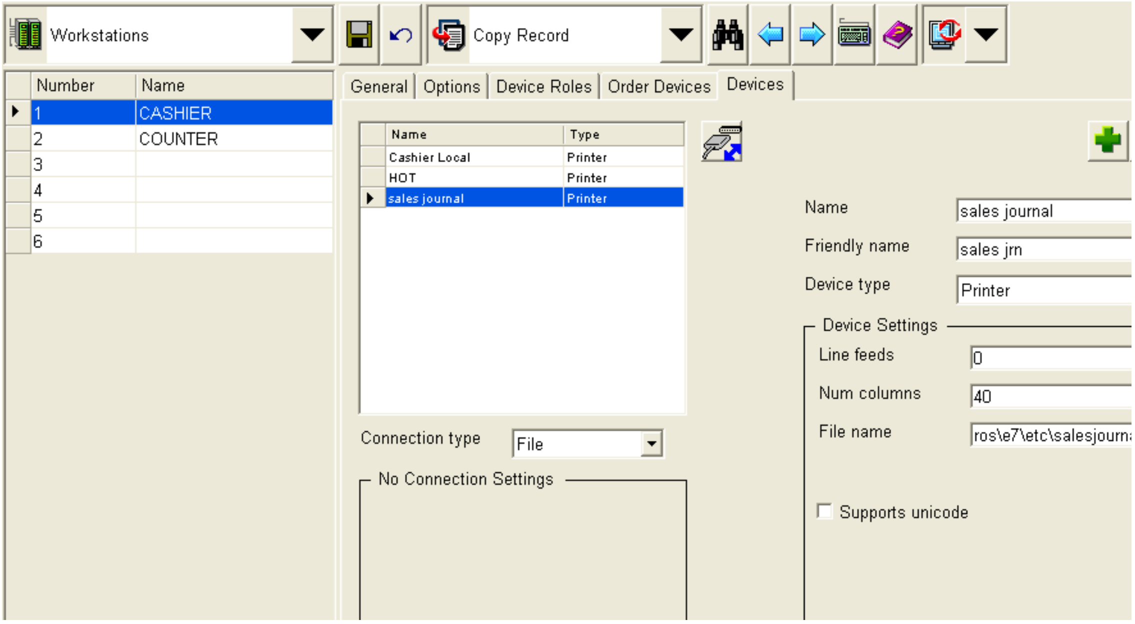
[13] “Payment Card Industry (PCI) Data Security Standard.pdf”, p. 55 V. 2.0, available on the PCI Security Standards Council website, https://www.pcisecuritystandards.org/.

MICROS e7 uses a proprietary (closed) database, which allows no general purpose access to the database, such as SQL. There is no database engine or off-the-shelf database server.

The MICROS e7 system does not store cardholder track data and always masks the primary account number and expiration date.

Live sites should ensure that sales journals are enabled for each workstation. This file will track all transactions that occur on the workstation. Follow these steps to set up a Sales Journal in the MICROS e7 Configurator.

1. Go to the *Workstations* form and highlight the appropriate workstation.
2. Go to the *Devices* tab and select the Green Plus Sign to add a new device record.
3. Configure the following fields:



Number	Name
1	CASHIER
2	COUNTER
3	
4	
5	
6	

Name	Type
Cashier Local	Printer
HOT	Printer
sales journal	Printer

Connection type: File

No Connection Settings

Name: sales journal
Friendly name: sales jrn
Device type: Printer

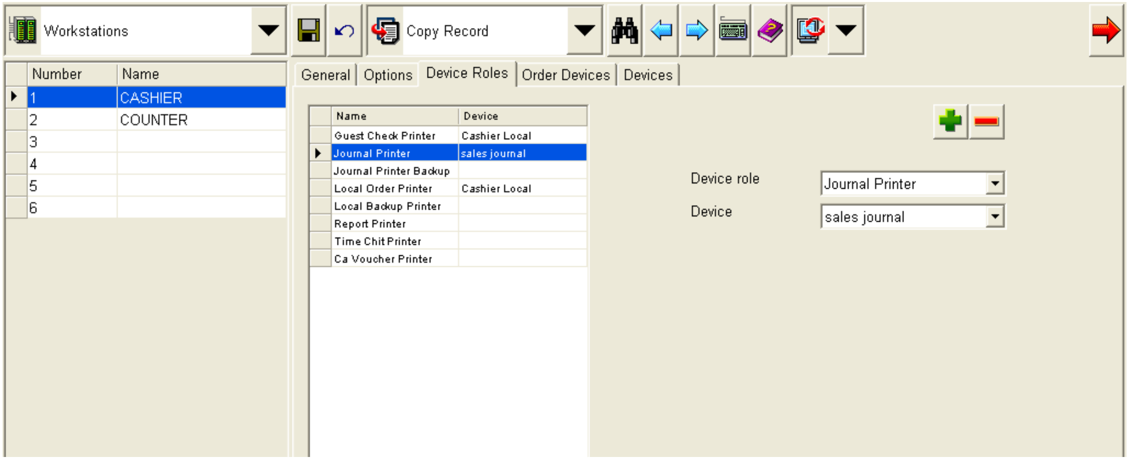
Device Settings
Line feeds: 0
Num columns: 40
File name: ros\e7\etc\salesjourn

□ Supports unicode

- In the **Name** field, enter a friendly descriptor to identify this record (e.g., Sales Journal).
- In the **Device Type** drop-down box select *Printer.*
- In the **Connection Type** drop-down select *File*.
- Use the **File Name** field to identify the path and name of the outputted file.

- Configure other fields as desired.

4. Save all changes.
5. Go to the *Device Roles* tab and select the Green Plus Sign to add a new record.



Number	Name
1	CASHIER
2	COUNTER
3	
4	
5	
6	

Name	Device
Guest Check Printer	Cashier Local
Journal Printer	sales journal
Journal Printer Backup	
Local Order Printer	Cashier Local
Local Backup Printer	
Report Printer	
Time Chit Printer	
Ca Voucher Printer	

Device role: Journal Printer
Device: sales journal

6. From the **Device Role** drop-down select *Journal Printer.*
7. From the **Device** drop-down select *Sales Journal*.
8. Save all changes.
9. Repeat steps 1-8 for all workstations.

After installation is complete, a debug log file is installed on each MICROS e7 workstation for troubleshooting and investigative purposes. The debug log is always enabled, and requires no merchant, reseller, or integration interaction. This log file is located at the following path unless otherwise specified by the user:

\Micros\e7\etc

To ensure your site is in compliance with Requirement 10 of The PCI Data Security Standard, “Track and monitor all access to network resources and cardholder data”, please consult the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

11. Regularly test security systems and processes

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.[14]

In accordance with the PCI Data Security Standard, MICROS Systems Inc. mandates regular testing of security systems and processes.

To ensure your site's security systems and processes are setup in compliance with Requirement 11 of The PCI Data Security Standard, "Regularly test security systems and processes", please consult the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, ―personnel‖ refers to full-time and part-time employees, temporary employees, contractors and consultants who are ―resident‖ on the entity's site or otherwise have access to the cardholder data environment.[15]

In accordance with the PCI Data Security Standard, MICROS Systems Inc. mandates a maintained policy that addresses information security.

A site's maintained information security policy should include information on physical security, data storage, data transmission, and system administration.

To ensure your information security policy is setup in compliance with Requirement 12 of The PCI Data Security Standard, "Maintain a policy that addresses information security", please consult the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

[14] "Payment Card Industry (PCI) Data Security Standard.pdf", p. 59 V. 2.0, available on the PCI Security Standards Council website, https://www.pcisecuritystandards.org/.

[15] "Payment Card Industry (PCI) Data Security Standard.pdf", p. 64 V. 2.0, available on the PCI Security Standards Council website, https://www.pcisecuritystandards.org/.