9700 HMS Version 3.20 PA-DSS Compliance Documentation

General Information

About This Document

This document is intended as a quick reference guide to provide information concerning MICROS' adherence to the PCI Data Security Standard and Payment Application Data Security Standard (PA-DSS) compliance. This document relates specifically to *MICROS 9700 Version 3.20 Hospitality Management System* software.

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 Payment Card Industry (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].

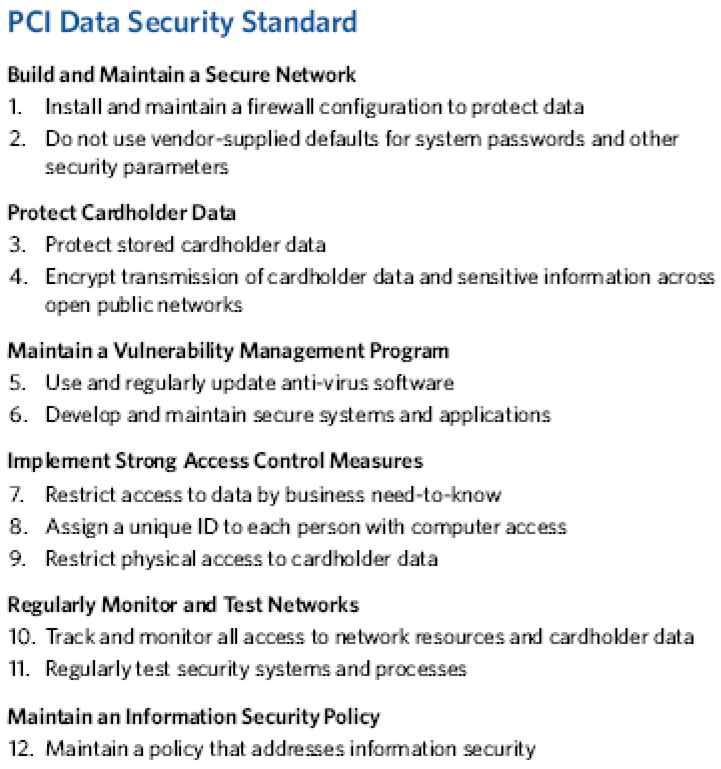
For more detailed information concerning PCI compliance, please refer to the PCI Security Standards Council website, https://www.pcisecuritystandards.org/.

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

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 Payment Card Industry (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, shown below, consists of twelve basic requirements supported by more detailed sub-requirements:[2]



PCI Data Security Standard

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect 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 and sensitive information across open public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
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

[2] Reprinted from “CISP_overview.pdf”, <http://usa.visa.com/download/business/accepting_visa/support_center/cisp_overview.pdf?it=c|/business/accepting_visa/ops_risk_management/cisp%2Ehtml|CISP%20Overview>.

Who Should be Reading This Document

This document is intended for the following audiences:

- MICROS Installers/Programmers
- MICROS Dealers
- MICROS Customer Service
- MICROS Training Personnel
- MIS Personnel
- 9700 Users

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 2000 or Windows 2003
- Familiarity with the 9700 HMS software
- Familiarity with operating MICROS peripheral devices

9700 HMS Version 3.20 and the PCI Data 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 9700 HMS Version 3.20 software conforms to The PCI Data Security Standard.

To ensure the payment application is implemented into a secure network environment, 9700 HMS 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/.

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data

Firewalls are computer devices that control computer traffic allowed into a company's network from outside, as well as traffic into more sensitive areas within a company's internal network. All systems need to be protected from unauthorized access from the Internet, whether for e-commerce, employees' Internet-based access via desktop browsers, or employees' email access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.[3]

In accordance with the PCI Data Security Standard, MICROS Systems Inc. mandates every site 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.

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.

[3] "Payment Card Industry (PCI) Data Security Standard.doc", p. 4, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

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.

The firewall configuration must also place the database in an internal network zone, segregated from the demilitarized zone (DMZ) with the web server. A DMZ can be used to separate the Internet from systems storing cardholder data.

Customers and resellers/integrators should establish and maintain payment applications so that cardholder data is not stored on Internet-accessible systems.

As a PCI compliant measure, 9700 HMS does not require the database server and web server to be on the same server.

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

Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.[4]

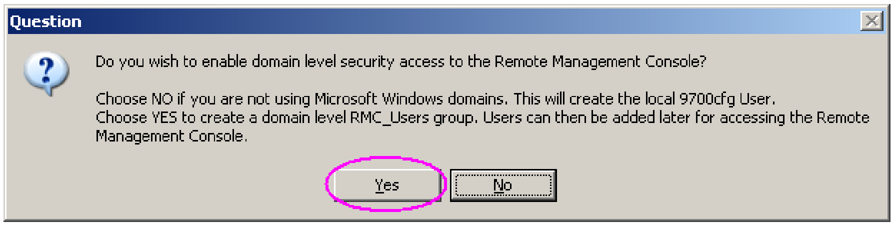
Previous versions of 9700 3.x installed with four default accounts with the original installation: “9700cfg,” “csremote,” “micros,” and “m9700.” MICROS Systems, Inc. previously advised that these defaults accounts be deleted, renamed, or disabled. To prevent compromised security and maintain PCI compliance, 9700 v. 3.20 has modified or removed these default accounts.

The “micros” and “csremote” legacy accounts will no longer be installed. These accounts have been removed from the installation process as they are not used and, when not securely deleted, can compromise PCI compliancy. When upgrading to 9700 v. 3.20 from a previous version, these accounts will be disabled after the upgrade process completes.

[4] “Payment Card Industry (PCI) Data Security Standard.doc”, p. 5, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

The legacy “m9700” account will be disabled after the 9700 v. 3.20 installation/ upgrade process completes.

The “9700cfg” account is used for remote Remote Management Console (RMC) access. This account will be disabled after the 9700 v. 3.20 installation/ upgrade process completes. If credit card transactions are performed through the 9700 system, this account must be deleted and the domain level security options must be enabled during the 9700 installation/upgrade process, as shown below.



Do you wish to enable domain level security access to the Remote Management Console?

Choose NO if you are not using Microsoft Windows domains. This will create the local 9700cfg User.
Choose YES to create a domain level RMC_Users group. Users can then be added later for accessing the Remote Management Console.

For more information, see the *9700 Secure Default Account Handling* document.

MICROS Systems, Inc. advises against using any administrative accounts, such as the “sa” account for application access to the database, for application logins. Customers and resellers/integrators are advised to always assign strong passwords to these default accounts even if these accounts are not used. These default accounts should then be disabled or not used.

Strong application and system passwords must be used whenever possible. MICROS Systems, Inc. mandates customers and resellers/integrators to always create PCI DSS-compliant complex password to access the payment application. For more information on how to create a PCI compliant password in the Enterprise Management Console (EMC), please see page 15.

For wireless environments, change wireless vendor defaults, including but not limited to, wireless equivalent privacy (WEP) keys, default service set identifier (SSID), password, and SNMP community strings. Disable SSID broadcasts. Enable Wi-Fi protected access (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

Encryption is the ultimate protection mechanism because even if someone breaks through all other protection mechanisms and gains access to encrypted data, they will not be able to read the data without further breaking the encryption. This is an illustration of the defense in depth principle.[5]

MICROS Systems Inc. uses credit card masking and Triple-DES 128-bit encryption to ensure credit card data is stored in a manner compliant with the PCI Data Standard.

As a PCI compliant measure to protect stored data, production 9700 HMS systems should never reside directly on the Internet and a firewall should always be placed between the 9700 HMS system and Internet/corporate network gateways.

9700 HMS does not allow unmasked credit card information to be printed 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) is displayed.

9700 does not support the transmission of card information via email or Instant Message (IM).

Historical data (magnetic stripe data, card validation codes, PINs, or PIN blocks) stored by previous versions of the 9700 software must be securely removed as a necessary component of PCI compliancy. Any cryptographic material, such as cryptographic keys used for computation or 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.

[5] “Payment Card Industry (PCI) Data Security Standard.doc”, p. 6, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

Conversions from 9700 v2.x to 9700 v3.x must therefore include securely erasing the legacy flat-file database and all old log files from the system after upgrading to 9700 v3.x. Historical data must be securely removed wherever it resides. The 9700 upgrade itself will encrypt all sensitive data in the 3.2 database when the initial database conversion occurs. For more information, refer to the *9700 Upgrade Best Practices* document.

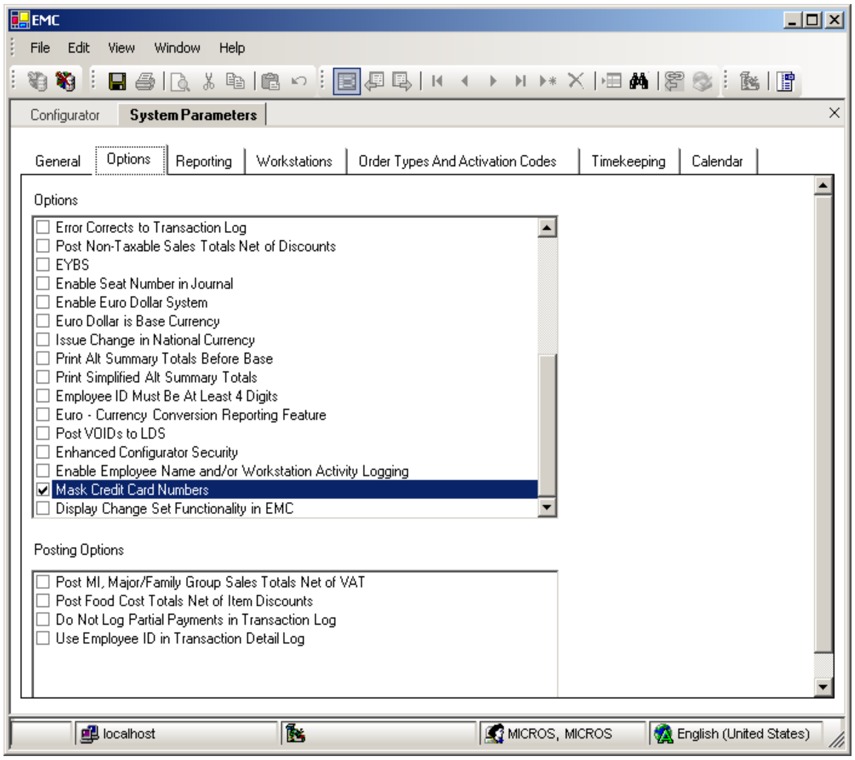
To ensure customer data is protected, MICROS Systems, Inc. mandates 9700 HMS resellers/integrators must only collect customer data (for example, sensitive authentication data, log files, debug files, databases, etc.) needed to solve a specific problem. Such data must only be stored in specific, known 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. For more information, refer to the *Customer Support Information Security Guidelines* document.

To be in compliance with Requirement 3 of the PCI Data Security Standard, please ensure the following Credit Card Masking options in the Enterprise Management Console (EMC) are configured as shown below.

Enabled Option

The following option is enabled by default:

- **System Information>Parameters>Options Tab>Options Section:** Mask Credit Card Numbers



Options

☐ Error Corrects to Transaction Log
☐ Post Non-Taxable Sales Totals Net of Discounts
☐ EYBS
☐ Enable Seat Number in Journal
☐ Enable Euro Dollar System
☐ Euro Dollar is Base Currency
☐ Issue Change in National Currency
☐ Print Alt Summary Totals Before Base
☐ Print Simplified Alt Summary Totals
☐ Employee ID Must Be At Least 4 Digits
☐ Euro - Currency Conversion Reporting Feature
☐ Post VOIDs to LDS
☐ Enhanced Configurator Security
☐ Enable Employee Name and/or Workstation Activity Logging
☑ Mask Credit Card Numbers
☐ Display Change Set Functionality in EMC

Posting Options

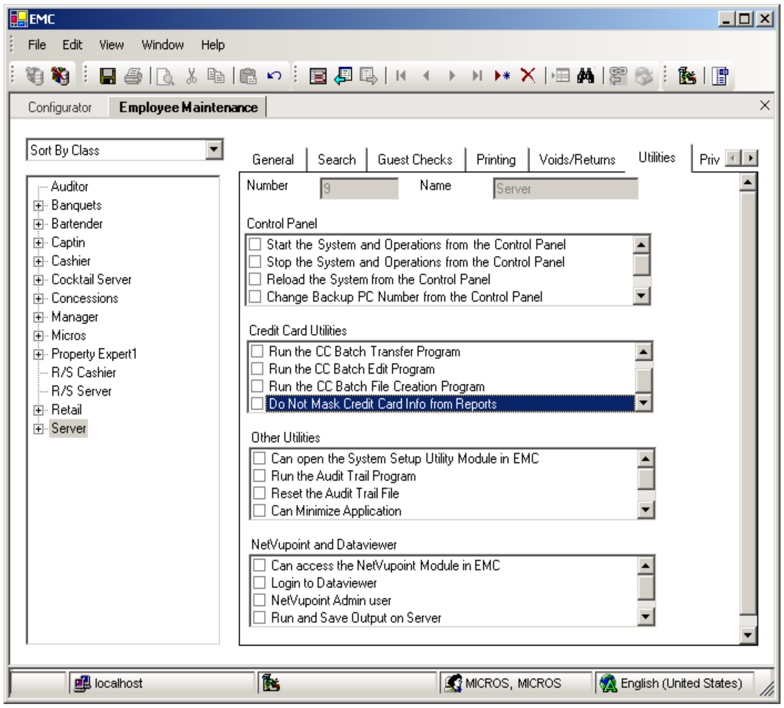
☐ Post MI, Major/Family Group Sales Totals Net of VAT
☐ Post Food Cost Totals Net of Item Discounts
☐ Do Not Log Partial Payments in Transaction Log
☐ Use Employee ID in Transaction Detail Log

Note *This option must remain configured as shown above, in order to comply with Requirement 3 of The PCI Data Security Standard.*

Disabled Option

The following option is disabled by default:

- **Personnel>Employees>Maintenance>Select Employee Class>Utilities Tab>Credit Card Utilities:** Do Not Mask CC Info from CC Reports



Number 9
Name Server

Control Panel
☐ Start the System and Operations from the Control Panel
☐ Stop the System and Operations from the Control Panel
☐ Reload the System from the Control Panel
☐ Change Backup PC Number from the Control Panel

Credit Card Utilities
☐ Run the CC Batch Transfer Program
☐ Run the CC Batch Edit Program
☐ Run the CC Batch File Creation Program
☐ Do Not Mask Credit Card Info from Reports

Other Utilities
☐ Can open the System Setup Utility Module in EMC
☐ Run the Audit Trail Program
☐ Reset the Audit Trail File
☐ Can Minimize Application

NetVupoint and Dataviewer
☐ Can access the NetVupoint Module in EMC
☐ Login to Dataviewer
☐ NetVupoint Admin user
☐ Run and Save Output on Server

Note *These options must remain configured as shown above to comply with Requirement 3 of The PCI Data Security Standard.*

Cardholder data must be purged after it exceeds the customer-defined retention period from all locations within the payment application where customer data is stored.

In some situations, MICROS RES resellers/integrators might be tasked with troubleshooting an issue with the system. To ensure cardholder data is protected, MICROS Systems, Inc. mandates MICROS RES resellers/integrators must only collect customer data (for example, sensitive authentication data, log files, debug files, databases, etc.) needed to solve a specific problem. 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.

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 and sensitive information across public networks

Sensitive information must be encrypted during transmission over the Internet, because it is easy and common for a hacker to intercept and/or divert data while in transit.[6]

The 9700 HMS application requires that all POS clients and the server must be established over a secure, private network to make sure that no traffic (including transmission of cardholder data) between 9700 components will be sent over a public network, or Internet. MICROS requires that customers and resellers/ integrators establish and maintain secure transmissions of cardholder data.

Wireless transmissions of cardholder data must be encrypted over both public and private networks. Encrypt transmissions by using Wi-Fi Protected Access (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. For more information, please refer to the *MICROS Wireless Networking Best Practices: A Payment Application Data Security Standard (PA-DSS) Implementation Guide Supplement* document.

Because of the PCI Data Security Standard, MICROS Systems Inc. mandates each site use some sort of encryption (VPN, SSL, etc) when sending any sensitive information over the Internet, including wireless connections, E-mail, and when using services such as Telnet, FTP, etc.

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.

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/.

[6] “Payment Card Industry (PCI) Data Security Standard.doc”, p. 7, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software

Many vulnerabilities and malicious viruses enter the network via employees' email activities. Anti-virus software must be used on all email systems and desktops to protect systems from malicious software.[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 must 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 via vendor security patches, and all systems should have current software patches to protect against exploitation by employees, external hackers, and viruses. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.[8]

MICROS Systems Inc. uses separate development and production environments to ensure software integrity and security. Updated patches and security updates 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 patches, depend on site specific protocol and practices.

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/.

[7] "Payment Card Industry (PCI) Data Security Standard.doc", p. 8, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

[8] "Payment Card Industry (PCI) Data Security Standard.doc", p. 8, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

Implement Strong Access Control Measures

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

This ensures critical data can only be accessed in an authorized manner.[9]

MICROS Systems Inc. recognizes the importance of data control, and does so by establishing access based upon employee job 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

This ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.[10]

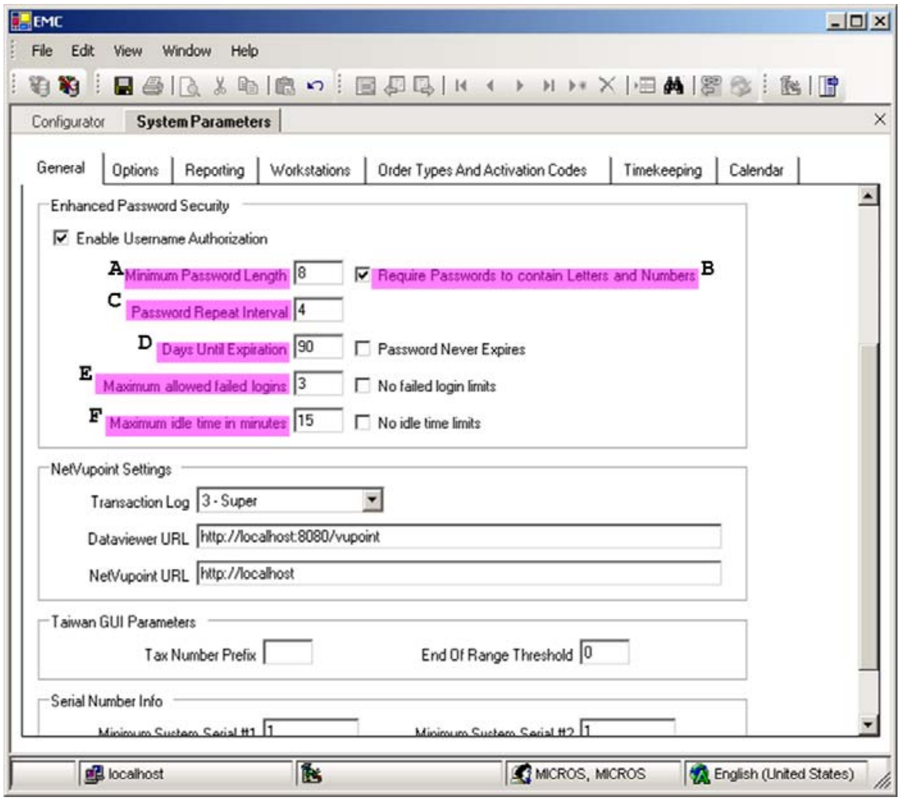
MICROS Systems Inc. recognizes the importance of establishing unique IDs for each person with computer access. No two MICROS users can have the same ID, and each person’s activities can be traced provided the client site maintains proper configuration and adheres to privilege level restrictions based on a need-to-know basis. 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 management for non-consumer users and administrators, for all system components, depend on site specific protocol and practices. To ensure strict access control of the 9700 HMS application always assign unique usernames and complex passwords to each account. MICROS Systems Inc. mandates applying these guidelines to not only MICROS passwords, but to Windows passwords as well.

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.

[9] “Payment Card Industry (PCI) Data Security Standard.doc”, p. 9, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

[10] “Payment Card Industry (PCI) Data Security Standard.doc”, p. 10, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

To be in compliance with Requirement 8 of the PCI Data Security Standard, please ensure the following options in the Enterprise Management Console (EMC) are configured as shown below.



Enhanced Password Security

☑ Enable Username Authorization

A Minimum Password Length: 8 — ☑ Require Passwords to contain Letters and Numbers B

C Password Repeat Interval: 4

D Days Until Expiration: 90 — ☐ Password Never Expires

E Maximum allowed failed logins: 3 — ☐ No failed login limits

F Maximum idle time in minutes: 15 — ☐ No idle time limits

NetVupoint Settings

Transaction Log: 3 - Super

Dataviewer URL: http://localhost:8080/vupoint

NetVupoint URL: http://localhost

Taiwan GUI Parameters

Tax Number Prefix:

End Of Range Threshold: 0

Serial Number Info

Minimum System Serial #1: 1

Minimum System Serial #2: 1

In the EMC>System Information>Parameters>General Tab>Enhanced Password Security Tab, ensure these options (above in pink) are configured as follows:

- A: Ensure "Minimum Password Length" is at least 8
- B: Ensure "Require Passwords to contain Letters and Numbers" is checked
- C: Ensure "Password Repeat Interval" is at least 4
- D: Ensure "Days Until Expiration" is not greater than 90
- E: Ensure "Maximum Allowed Failed Logins" is not greater than 6
- F: Ensure "Maximum Idle Time in Minutes" is not greater than 15

MICROS Systems, Inc. mandates changing your master username password in the EMC, following the above guidelines, after logging in for the first time.

MICROS Systems, Inc. mandates 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 15 when creating the new, strong password. The new password must contain at least 8 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 Virtual Private Network (VPN) connection via a firewall before access is allowed. Logging functions must be enabled for security purposes. Access to customer passwords must always be restricted. For more information, refer to the *Webex 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 allows the opportunity to access devices or data, and remove systems or hardcopies, and should be appropriately restricted.[11]

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 users not store cardholder data on Internet-accessible systems. To ensure cardholder is not stored on Internet-accessible systems, the web server and data server must not be on the same server.

[11] "Payment Card Industry (PCI) Data Security Standard.doc", p. 11, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

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. The presence of logs in all environments allows thorough tracking and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.[12]

MICROS Systems Inc. provides a comprehensive audit trail utility, within the EMC, that allows privileged users to track MICROS specific activities. The advent of open database structure means that anyone with system level access to the database server (MS SQL or Oracle) has access to system components covered under this requirement, and thus would require logging of user access and activity as detailed in Requirement 10 of the PCI Data Security Standard.

[12] “Payment Card Industry (PCI) Data Security Standard.doc”, p. 12, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

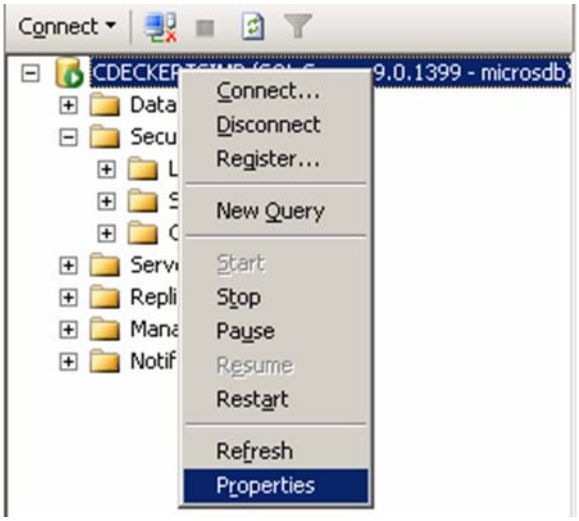
Enable Database Logging

Note *For maximum security and functionality, MICROS Systems, Inc. strongly recommends consulting with a SQL Server or Oracle Server database administrator to perform this task.*

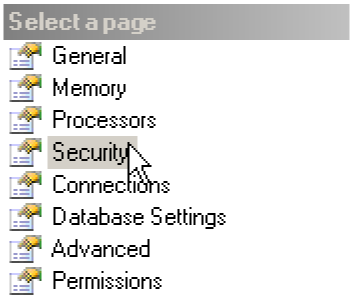
Microsoft® SQL Server

For MSSQL, enable the C2 audit tracing by following the steps below.

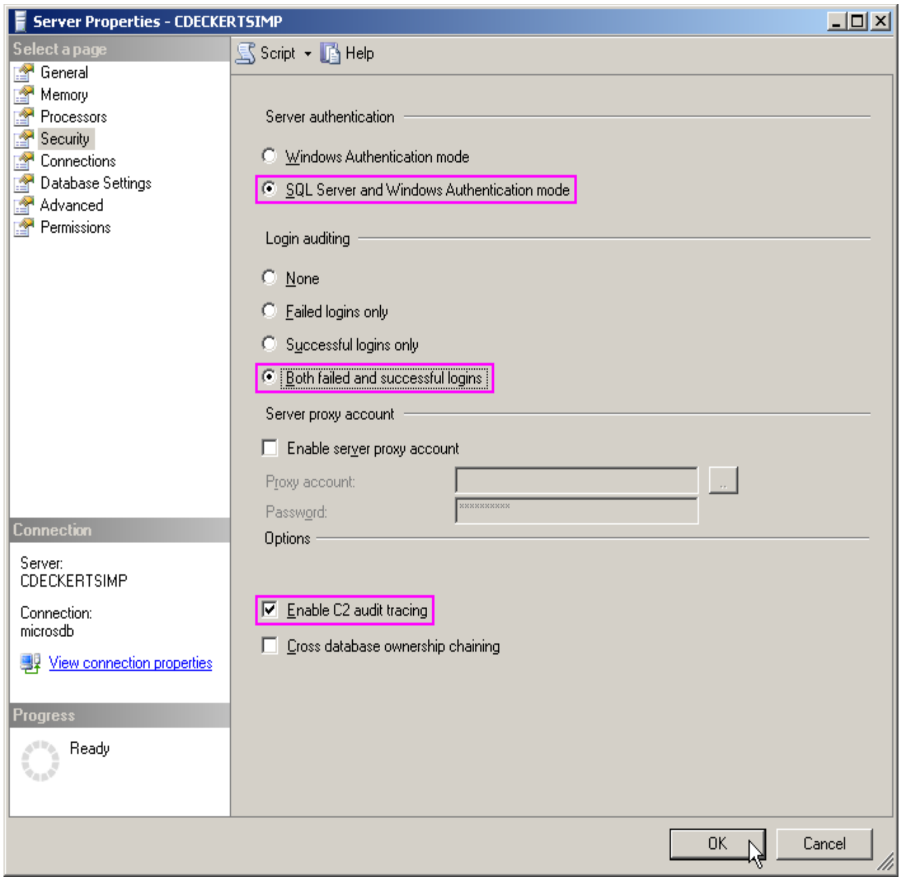
1. Within Microsoft® SQL Server Management Studio, select the Server until it highlights. Right-click the server and select *Properties*.



2. Select *Security* until it highlights.



3.



Server: CDECKERTSIMP

Connection: microsdb

Ready

Server authentication

○ Windows Authentication mode

● SQL Server and Windows Authentication mode

Login auditing

○ None

○ Failed logins only

○ Successful logins only

● Both failed and successful logins

Server proxy account

□ Enable server proxy account

Proxy account:

Password: **********

Options

☑ Enable C2 audit tracing

□ Cross database ownership chaining

- Within the Server authentication section, select the “SQL Server and Windows Authentication mode” option, as seen circled above.

- Within the Login auditing section, select the “Both failed and successful logins” option.

- Within the Options section, select the “Enable C2 audit tracing” option.

Note *These options must remain configured as shown above in order to comply with Requirement 10 of The PCI Data Security Standard.*

For more information, see the *SQL Server 2000 C2 Administrator’s and User’s Security Guide* available for download from Microsoft’s website, http://www.microsoft.com/technet/prodtechnol/sql/2000/maintain/sqlc2.mspx.

Oracle® Server

1. To enable the Oracle® server audit trail, set the `AUDIT_TRAIL` static parameter within the Parameter file, which has the following properties:

    ```
    AUDIT_ TRAIL = { none | os | db |db, extended
    |xml |xml,extended }
    ```

    The following list provides a description of each setting:

    - `none` or `false`: Auditing is disabled.
    - `db` or `true`: Auditing is enabled with all audit records stored in the database audit trail (SYS.AUD$).
    - `db,extended`: As db, but the SQL_BIND and SQL_TEXT columns also populated.
    - `xml`: Auditing is enabled, with all audit records stored as XML format OS files.
    - `xml,extended`: As xml, but the SQL_BIND and SQL_TEXT columns are also populated.
    - `os`: Auditing is enabled with all audit records directed to the operating system's audit trail.

Note *The `AUDIT_TRAIL` static parameter **cannot** be equal to '`none`' or '`false`' in order to comply with Requirement 10 of The PCI Data Security Standard.*

The `AUDIT_SYS_OPERATIONS` static parameter enables or disables the auditing of operations issued by users connecting with SYSDBA or SYSOPER privileges, including the SYS user. All audit records are written to the OS audit trail.

Note *The `AUDIT_SYS_OPERATIONS` static parameter must be set to '`true`' to comply with Requirement 10 of The PCI Data Security Standard.*

The AUDIT_FILE_DEST parameter specifies the OS directory used for the audit trail when the os, xml and xml,extended options are used. It is also the location for all mandatory auditing specified by the AUDIT_SYS_OPERATIONS parameter.

Note *Privileged access to the database, starting and stopping of the database, and structural changes (such as adding a datafile) will now be audited.*

No audit actions are captured yet until audit actions are defined. For instruction on how to define audit actions, see the Oracle® Database Security Guide.

2. Use the AUDIT statement to setup detailed auditing. The AUDIT statement can be used to track the occurrence of SQL statements in subsequent user sessions, specific SQL statements or all SQL statements authorized by a particular system privilege, and track operations on a specific schema object.

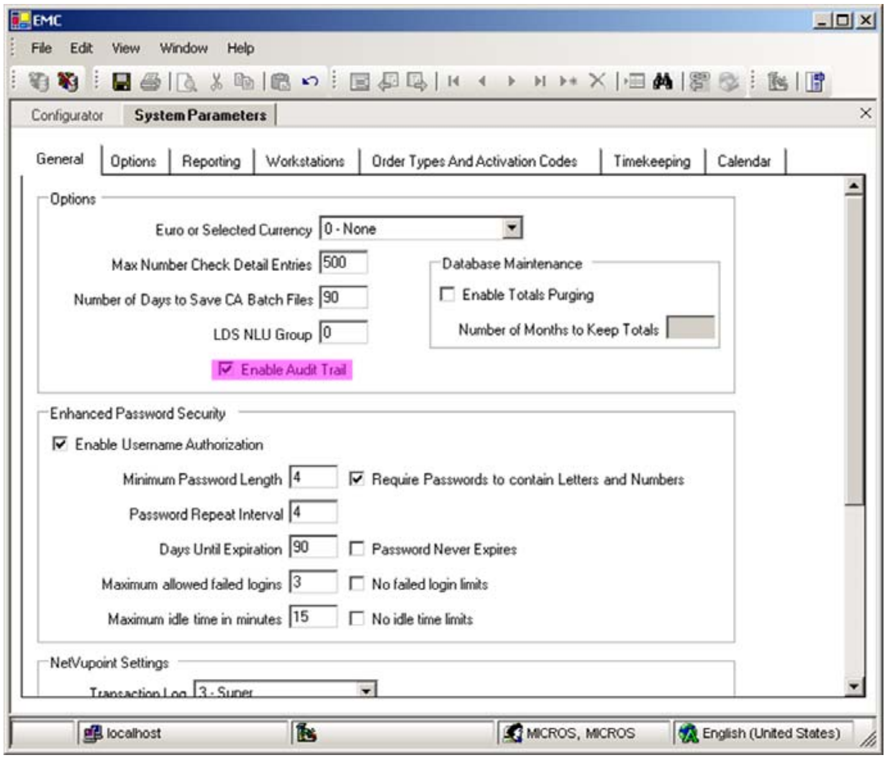
   For detailed information on using the AUDIT statement, see the “AUDIT” section of the *Oracle® Database SQL Reference*, http://download.oracle.com/docs/cd/B19306_01/server.102/b14200/statements_4007.htm#i2059073.

For more information, please see the “Database Auditing: Security Considerations” chapter within the *Oracle® Database Security Guide* available for download from Oracle’s website, www.oracle.com.

The EMC Audit Trail

In accordance with the PCI Data Security Standard, MICROS Systems Inc. mandates activity logging on the database server for all actions taken by any individual with root or administrative privileges via enabling the audit trail feature. Always enable audit logs for systems that store, process, and transmit cardholder data.

To enable audit trail, navigate to the System Information | System Parameters module | General Tab within the EMC and check the option "Enable Audit Trail", as shown below.



Options
Euro or Selected Currency 0 - None
Max Number Check Detail Entries 500
Number of Days to Save CA Batch Files 90
LDS NLU Group 0
☑ Enable Audit Trail

Database Maintenance
☐ Enable Totals Purging
Number of Months to Keep Totals

Enhanced Password Security
☑ Enable Username Authorization
Minimum Password Length 4 ☑ Require Passwords to contain Letters and Numbers
Password Repeat Interval 4
Days Until Expiration 90 ☐ Password Never Expires
Maximum allowed failed logins 3 ☐ No failed login limits
Maximum idle time in minutes 15 ☐ No idle time limits

NetVupoint Settings
Transaction Log 3 - Super

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 continually being discovered by hackers/researchers and introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is being maintained over time and through changes.[13]

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 company, and lets employees know what is expected of them. All employees should be aware of the sensitivity of the data and their responsibilities for protecting it.[14]

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/.

[13] "Payment Card Industry (PCI) Data Security Standard.doc", p. 13, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

[14] "Payment Card Industry (PCI) Data Security Standard.doc", p. 14, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.