

**Oracle® Hospitality Payment Gateway Services**  
PA-DSS Implementation Guide  
Version 6.0

July 2015

Copyright © 2006, 2015, Oracle and/or its affiliates. All rights reserved.

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.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

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.

---

## Table of Contents

1	General Information.....	3
	About This Document.....	3
	About The PCI Security Standards Council .....	3
	About The PCI Data Security Standard(PCI DSS) .....	4
	Who Should Be Reading This Document.....	6
	What the Reader Should Already Know.....	6
2	MICROS Payment Gateway Version 6.0 And Payment Application Data Standard .....	7
	Build and Maintain a Secure Network.....	7
	1. Install and maintain a firewall configuration to protect cardholder data.....	7
	2. Do not use vendor-supplied defaults for system passwords and other security parameters	8
	Protect Cardholder Data.....	9
	3. Protect stored cardholder data.....	9
	4. Encrypt transmission of cardholder data across open, public networks.....	13
	Maintain a Vulnerability Management Program.....	14
	5. Use and regularly update anti-virus software or programs .....	14
	6. Develop and maintain secure systems and applications.....	15
	Implement Strong Access Control Measures .....	16
	7. Restrict access to cardholder data by business need-to-know.....	16
	8. Assign a unique ID to each person with computer access .....	16
	9. Restrict physical access to cardholder data.....	18
	Regularly Monitor and Test Networks.....	19
	10. Track and monitor all access to network resources and cardholder data .....	19
	11. Regularly test security systems and processes .....	21
	Maintain an Information Security Policy.....	22
	12. Maintain a policy that addresses information security for employees and contractors...	22

---

# 1 General Information

Oracle Corporation acquired MICROS and all further references to MICROS should be considered as Oracle Corporation.

## About This Document

MICROS Payment Gateway offers cost-effective and cutting-edge integrated payment card processing solutions. It seamlessly integrates with acquirer-side transaction processor and merchant-side management system. Via MICROS Payment Gateway, MICROS clients, using a MICROS-Fidelio information technology platform, will be able to acquire VISA, MasterCard, Amex, Diners Club and JCB transactions, as well as local transactions. It is the ideal integrated payment solution for hotels, restaurants and other franchises.

This document is intended as a quick reference guide to provide you with information concerning MICROS Payment Gateway adherence to the Payment Card Industries – Security Standards Council (PCI-SSC) concerning PA-DSS. This document relates specifically to MICROS Payment Gateway Version 6.0. This document is distributed to all relevant users on an annual basis or whenever there is a change on software or implementation requirement.

## About The PCI Security Standards Council<sup>[1]</sup>

The PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including: the Data Security Standard (DSS), Payment Application Data Security Standard (PA-DSS), and Pin-Entry Device (PED) Requirements.

<sup>[1]</sup> [https://www.pcisecuritystandards.org/organization\\_info/index.shtml](https://www.pcisecuritystandards.org/organization_info/index.shtml)

---

All of the five founding members have agreed to incorporate the PCI DSS as the technical requirements of each of their data security compliance programs. Each founding member also recognizes the QSAs and ASVs certified by the PCI Security Standards Council as being qualified to validate compliance to the PCI DSS.

A Limited Liability Corporation (LLC) chartered in Delaware, USA, the PCI Security Standards Council was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. All five payment brands share equally in the council's governance, have equal input to the PCI Security Standards Council and share responsibility for carrying out the work of the organization. Other industry stakeholders are encouraged to join the group and review proposed additions or modifications to the standards.

## **About The PCI Data Security Standard(PCI DSS)<sup>[2]</sup>**

The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

The PCI Security Standards Council will enhance the PCI DSS as needed to ensure that the standard includes any new or modified requirements necessary to mitigate emerging payment security risks, while continuing to foster wide-scale adoption.

<sup>[2]</sup> [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml)

---

Ongoing development of the standard will provide for feedback from the Advisory Board and other participating organizations. All key stakeholders are encouraged to provide input, during the creation and review of proposed additions or modifications to the PCI DSS.

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:<sup>[3]</sup>

### ***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 data
4. Encrypt transmission of cardholder data and sensitive information across 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

<sup>[3]</sup> [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml)

---

## Who Should Be Reading This Document

This document is intended for the following audiences:

- MICROS Customers
- MICROS Installers/Programmers
- MICROS Dealers/Resellers
- MICROS Customer Service
- MICROS Training Personnel
- MIS 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 the operating systems platforms supported by MICROS Payment Gateway
- Familiarity with operating MICROS Financial Services

---

## 2 MICROS Payment Gateway Version 6.0 And Payment Application Data Standard

While MICROS recognizes the importance of upholding card member security and data integrity, certain parameters of the PCI Data Security Standard and PCI-SSC 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 MICROS Payment Gateway Version 6.0 software conforms to The PCI Data Security Standard.

For a complete description of the PCI Data Security Standard, please consult the Payment Card Industries – Security Standards Council website found at <https://www.pcisecuritystandards.org>.

### Build and Maintain a Secure Network

#### 1. Install and maintain a firewall configuration to protect cardholder 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<sup>[4]</sup>.*

<sup>[4]</sup> "PCI DSS Requirements and Security Assessment Procedures", Page 20, Version 2.0, October 2010. [https://www.pcisecuritystandards.org/documents/pci\\_dss\\_v2.pdf](https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf)



---

In accordance with the PCI Data Security Standard, MICROS strongly recommends every site install and maintain a firewall configuration to protect data. Configure your network so that databases and servers always reside behind a firewall and have no direct access to the Internet.

MICROS recommends that only some predefined ports/services are allowed and block all other unauthorized access to/from MICROS Payment Gateway servers.

To make sure your firewall configuration is set up in compliance with Step 1 of the PCI Data Security Standard, “Install and maintain a firewall configuration to protect cardholder data”, please consult the Payment Card Industries – Security Standards Council website found at <<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 <sup>[5]</sup>.*

MICROS Payment Gateway Version 6.0 allows for all applications, operating system, and database passwords to be changed. There is no default username nor default password. MICROS Payment Gateway provides a configuration tool which only allows the users with operating system local administrator privilege to login via their own username and password. MICROS strongly recommend users login via their unique and strong user access credentials.

<sup>[5]</sup> “PCI DSS Requirements and Security Assessment Procedures”, Page 24, Version 2.0, October 2010.  
<[https://www.pcisecuritystandards.org/documents/pci\\_dss\\_v2.pdf](https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf)>

---

For all other system components, including operating system, network devices and access points, MICROS strongly recommends changing all vendor-supplied default passwords to complex passwords.

MICROS Payment Gateway is designed as such that no user access is needed for daily operation. MICROS strongly recommends that non-console administrative access to the Payment Gateway Servers be blocked, and recommends customer use SSH/VPN/SSL for encryption if customer has to use the non-console administrative access. Other than Java and database, MICROS Payment Gateway doesn't require any other software and/service. MICROS recommends that only some specific ports are allowed and all unnecessary and insecure services and protocols shall be removed.

For more information on Step 2 of The PCI Data Security Standard, "Do not use vendor-supplied defaults for system passwords and other security parameters", please consult the Payment Card Industries – Security Standards Council website found at <https://www.pcisecuritystandards.org>.

## Protect Cardholder Data

### 3. Protect stored cardholder data

*Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other network 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 PAN in unencrypted e-mails<sup>[6]</sup>.*

<sup>[6]</sup> "PCI DSS Requirements and Security Assessment Procedures", Page 28, Version 2.0, October 2010. [https://www.pcisecuritystandards.org/documents/pci\\_dss\\_v2.pdf](https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf)

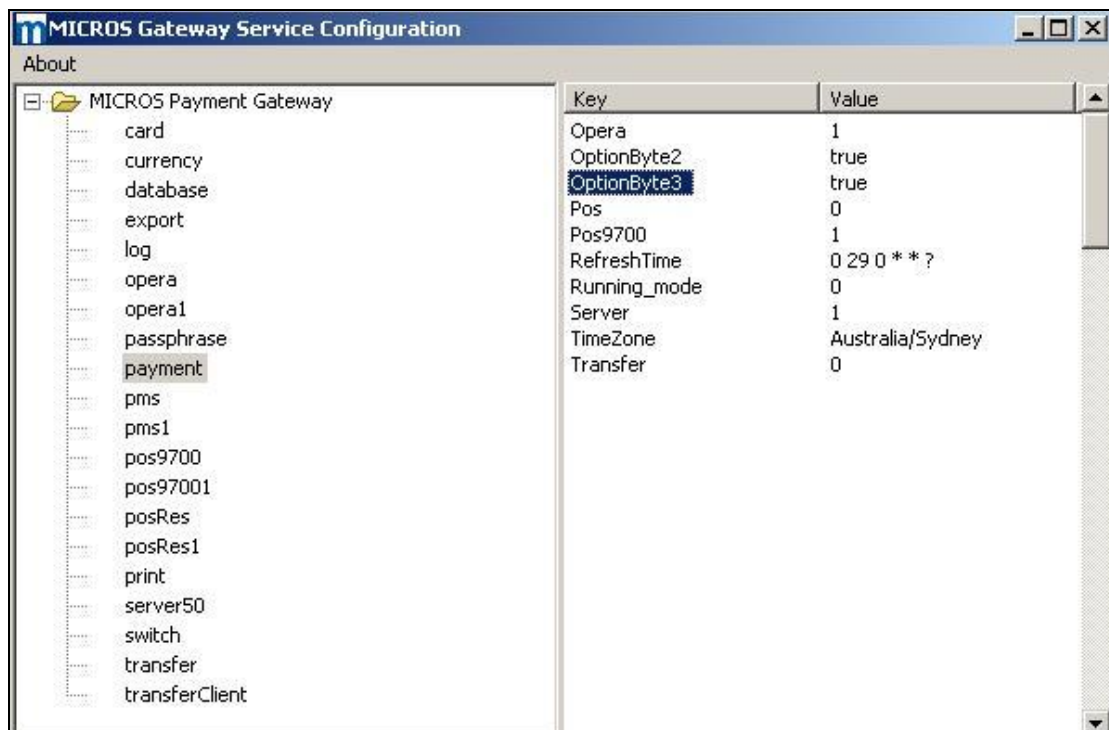
---

MICROS Payment Gateway Version 6.0 uses credit card masking and strong encryption (AES-256) to ensure credit card data is stored in a manner compliant with the PCI Data Standard. The Gateway Database Server should always sit behind a firewall for protection from malicious Internet attacks.

MICROS Payment Gateway never stores the full track information. Nor does it store the card validation code (CAV2/CID/CVC2/CVV2), or PIN/PIN Block. By default there is no full PAN ever stored in database, unless the acquiring banks/processors request a batch file or batch-upload at the end of day.

## I PAN Storage

Set “OptionByte3” to “true” in payment configuration in order to enable full PAN storage. By default it’s “false”, even if the entry of “OptionByte3” is absent.



When “OptionByte3” is set to true, full PANs and the expiry dates will be encrypted via strong encryption. In that case, Key Management Tool (refer to “MICROS

---

Payment Gateway Key Management Tool User Guide”) needs to be run and Key Custodian Form is required to be signed. In accordance with the PCI Data Security Standard, MICROS strongly recommends restrict access to keys to the fewest number of custodians necessary, store keys securely in the fewest possible locations and forms and render cryptographic material irretrievable.

## I Tokenization

MICROS Payment Gateway supports the tokenization feature. With this feature turned on, full PANs are no longer stored in the database of MICROS Payment Gateway. Instead only tokens will be stored in the database.

The data retention period is controlled by parameter “OptionByte6”. It has the default value as 180, i.e. MICROS Payment Gateway by default will store the cardholder data for 180 days. There is a task procedure running automatically everyday to check the database and handle the data housekeeping. Any cardholder data after expiration, will be purged.

MICROS Payment Gateway doesn’t show the full account number in any display, log; all account numbers are masked. The first six and last four digits are the maximum number of digits to be showed in log and in screen. MICROS Payment Gateway doesn’t provide the capability to send email.

None of previous versions of MICROS Payment Gateway ever stored magnetic stripe data, card validation values or codes, and PINs or PIN block data. In accordance with the PCI Data Security Standard, for any existing MICROS Payment Gateway customer upgrading to V6.0, MICROS requests that all historic data and cryptographic material must be remove by using Eraser, an industry standard wipe tool included in MICROS Payment Gateway installation package. The whole Payment\_Gateway folder should be removed.

---

In case of support and/or trouble-shooting, only the masked PAN (First 6 digits and last 4 digits) are required as well as the authorization code, or the reference number.

In accordance with the PCI Data Security Standard, MICROS strongly recommends:

- Collect sensitive authentication 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 sensitive authentication data while stored
- Securely delete such data immediately after use

For more information on Step 3 of The PCI Data Security Standard, “Protect stored data”, please consult the Payment Card Industries – Security Standards Council website found at <<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 can be continued targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments<sup>[7]</sup>.*

MICROS Payment Gateway Version 6.0 uses SSL or IPSEC VPN to ensure credit card data is transmitted across public networks in a manner compliant with the PCI Data Security Standard. Lease line connection is also supported if acquiring banks/processors insists on such a connection. MICROS recommends the use of HTTPS/SSL over internet to connect to processors (and/or acquiring banks). If HTTPS/SSL over internet isn't allowed by the processors, IPSEC VPN should be deployed. If a site is connecting to a central MICROS Payment Gateway, a MICROS Payment Gateway SSLInterface is installed so that all traffic between the site and the central MICROS Payment Gateway is via HTTPS/SSL. For SSL connection, only SSL Version 3.0 (or above) is supported.

MICROS Payment Gateway doesn't facilitate the sending of PANs by end-user messaging technologies (email, instant messaging, chat etc). In accordance with the PCI Data Security Standard, if any site uses such a technology, MICROS strongly recommends that site renders the PAN unreadable or implements strong cryptography, or uses of strong cryptography to encrypt the PANs.

[7] "PCI DSS Requirements and Security Assessment Procedures", Page 35, Version 2.0, October 2010.  
<[https://www.pcisecuritystandards.org/documents/pci\\_dss\\_v2.pdf](https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf)>

---

MICROS Payment Gateway doesn't use wireless transmissions. Wireless access to that network, if permitted, would be the sites' responsibility. MICROS recommends when transmitting wirelessly, sites always use the PCI DSS-compliant settings and industry best practices to implement strong encryption for authentication and transmission of cardholder data.

For more information on Step 4 of The PCI Data Security Standard, "Encrypt transmission of cardholder data and sensitive information across public networks", please consult the Payment Card Industries – Security Standards Council website found at <<https://www.pcisecuritystandards.org>>.

## Maintain a Vulnerability Management Program

### 5. Use and regularly update anti-virus software or programs

*Malicious software, commonly referred to as "malware" - including viruses, worms, and Trojans - enters the network during many business approved activities including employees' 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<sup>[8]</sup>.*

In accordance with the PCI Data Security Standard, MICROS strongly recommends regular use and regular updates of anti-virus software or programs. Anti-virus software must be deployed on all systems commonly affected by viruses, particularly personal computers and servers. MICROS Payment Gateway is compatible with all industry standard anti-virus software or programs.

To make sure your anti-virus software is set up in compliance with Step 5 of the PCI Data Security Standard, "Use and regularly update anti-virus software or programs", please consult the Payment Card Industries – Security Standards Council website found at <<https://www.pcisecuritystandards.org>>.

<sup>[8]</sup> "PCI DSS Requirements and Security Assessment Procedures", Page 37, Version 2.0, October 2010. <[https://www.pcisecuritystandards.org/documents/pci\\_dss\\_v2.pdf](https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf)>

---

## 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 vendorprovided 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. ...For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques<sup>[9]</sup>.*

MICROS uses separate development and production environments to ensure software integrity and security. Updated patches and security updates are available via the MICROS product website, [www.micros.com](http://www.micros.com) . While MICROS makes every possible effort to conform to Step 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 make sure your site develops and maintains secure systems and applications in compliance with Step 6 of The PCI Data Security Standard, “Develop and Maintain Secure Systems and Applications”, please consult the Payment Card Industries – Security Standards Council website found at <https://www.pcisecuritystandards.org>.

<sup>[9]</sup> “PCI DSS Requirements and Security Assessment Procedures”, Page 38, Version 2.0, October 2010. [https://www.pcisecuritystandards.org/documents/pci\\_dss\\_v2.pdf](https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf)



---

## 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<sup>[10]</sup>.*

MICROS recognizes the importance of data control and recommends access to sensitive information is restricted, password protected, and granted on a need-to-know basis.

For more information on Step 7 of The PCI Data Security Standard, “Restrict access to cardholder data by business need-to-know”, please consult the Payment Card Industries–Security Standards Council website found at <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<sup>[11]</sup>.*

MICROS recognizes the importance of establishing unique ID’s for each person with computer access and strongly recommends a unique ID be assigned to each person with Payment Gateway server access.

[10] “PCI DSS Requirements and Security Assessment Procedures”, Page 44, Version 2.0, October 2010. [https://www.pcisecuritystandards.org/documents/pci\\_dss\\_v2.pdf](https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf)

[11] “PCI DSS Requirements and Security Assessment Procedures”, Page 46, Version 2.0, October 2010. [https://www.pcisecuritystandards.org/documents/pci\\_dss\\_v2.pdf](https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf)

---

The installation of MICROS Payment Gateway requires the operating system administrative account access and the database administrative account access. MICROS recommends sites setup complex passwords for those accounts and change the passwords on a regular basis following PCI guidelines for password management.

During the installation, a database user will be created for MICROS Payment Gateway to access database. MICROS Payment Gateway doesn't request a default name for this user. Sites are able setup the user name and the password at ease. MICROS recommends sites setup complex password for this account.

For any administrator account, MICROS strongly recommend that customer

- 1) change default password immediately after first time login
- 2) change the password at least every 90 days
- 3) use passwords of at least 7 characters
- 4) use passwords containing both numeric and alphabetic characters
- 5) not use a new password that is the same as any of the last four passwords he or she has used

MICROS Payment Gateway is installed as system service and runs automatically without any human interference. For daily operation, no access to MICROS Payment Gateway application system is needed. The MICROS Payment Gateway Configuration tool/GUI uses the operating system authentication and only users with local administrative privileges can logon. MICROS recommends the Payment Gateway Server only be accessed by site's IT manager.

MICROS Payment Gateway doesn't provide any remote access service nor does it require the use of remote access. MICROS strongly recommends remote access be authenticated using a two factor authentication mechanism if any site utilizes the remote access.

While MICROS makes every possible effort to conform to Step 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. In accordance with the PCI Data Security Standard, MICROS strongly recommends sites control access, via unique user ID and PCI DSS compliant secure authentication, to any PCs, servers, and databases with payment applications and cardholder data.

For more information on Step 8 of the PCI Data Security Standard, “Assign a unique ID to each person with computer access”, please consult the Payment Card Industries – Security Standards Council website found at <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<sup>[12]</sup>.*

In accordance with the PCI Data Security Standard, MICROS strongly recommends restricting physical access to cardholder data. This includes physical access to the Payment Gateway servers and any computer consoles capable of accessing the Payment Gateway servers, as well as restricting physical access to sites’ other credit card payment-related application servers (Opera, MICROS 3700, MICROS 9700, MICROS Symphony etc).

MICROS recommends that sites secure their server in a locked office controlled by a Card Key based access control system to protect both internal and external access.

MICROS mandates the MICROS Payment Gateway Database Server should always sit behind a firewall for protection from malicious Internet attacks.

<sup>[12]</sup> “PCI DSS Requirements and Security Assessment Procedures”, Page 51, Version 2.0, October 2010. [https://www.pcisecuritystandards.org/documents/pci\\_dss\\_v2.pdf](https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf)

---

To make sure your site is set up in compliance with Step 9 of The PCI Data Security Standard, “Restrict physical access to cardholder data”, please consult the Payment Card Industries – Security Standards Council website found at <https://www.pcisecuritystandards.org>.

## Regularly Monitor and Test Networks

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

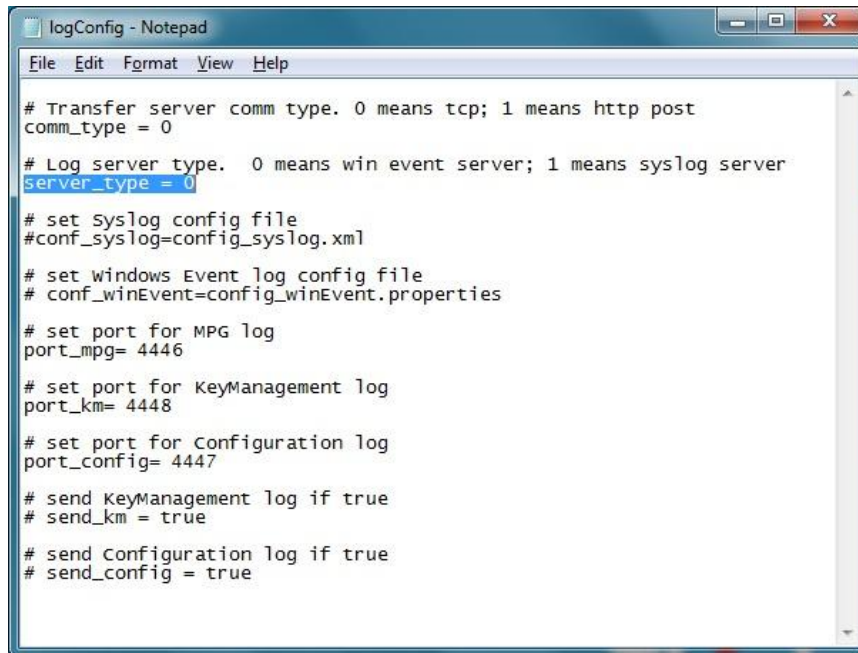
*Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs<sup>[13]</sup>.*

MICROS Payment Gateway is installed as system service and runs automatically without any human interference. For normal operation, no user is needed to access the resources and data. MICROS recommends the Payment Gateway Server only be accessed by site’s IT manager.

In accordance with the Payment Card Industries - Security Standards Council standard, MICROS strongly recommends logging of activity on the MICROS Payment Gateway database server. From the application server standpoint, MICROS Payment Gateway has the ability to log all Payment Gateway service related system activity and every payment transaction processed. Those logs are automatically enabled when installation and they can’t be disabled. MICROS recommends that the logs be archived for at least 1 year.

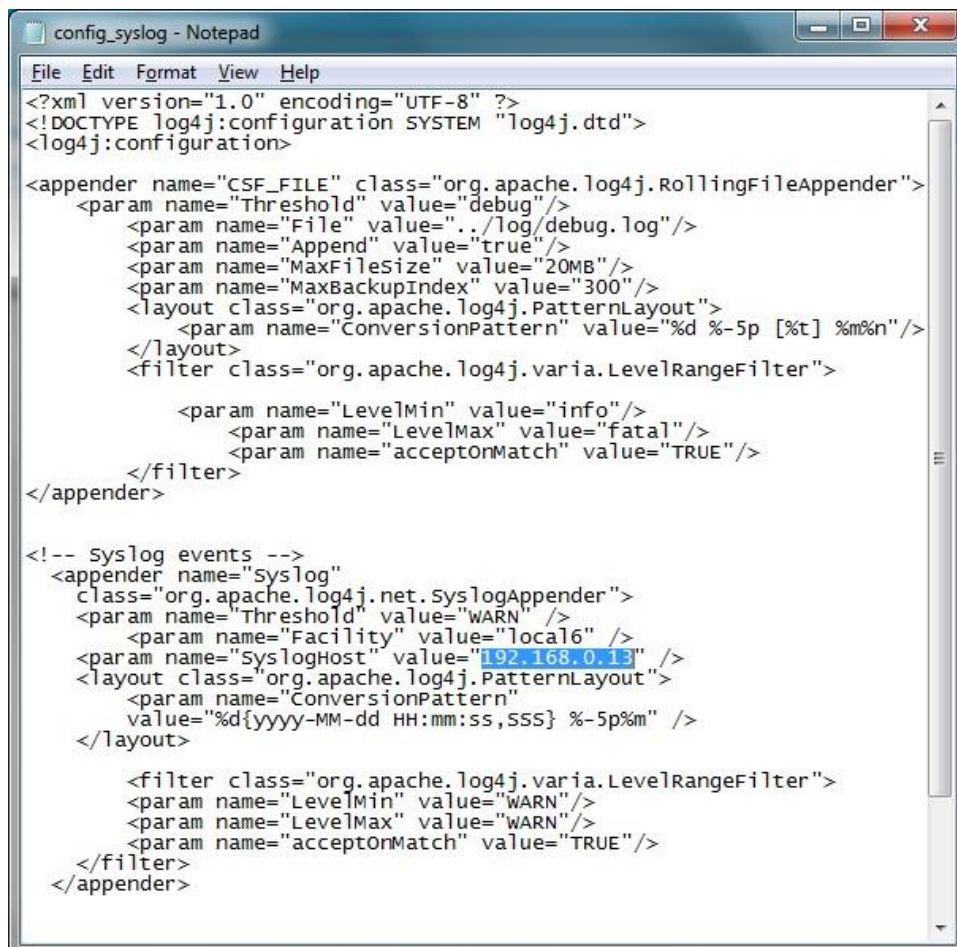
MICROS Payment Gateway also facilitates the ability to assimilate logs into merchant’s centralized log server, with logging via either industry standard log file mechanisms. Either Syslog or Windows Event is supported, defined by the parameter “server\_type” in logConfig.properties.

<sup>[13]</sup> “PCI DSS Requirements and Security Assessment Procedures”, Page 55, Version 2.0, October 2010.  
[https://www.pcisecuritystandards.org/documents/pci\\_dss\\_v2.pdf](https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf)



```
logConfig - Notepad
File Edit Format View Help
# Transfer server comm type. 0 means tcp; 1 means http post
comm_type = 0
# Log server type. 0 means win event server; 1 means syslog server
server_type = 0
# set syslog config file
#conf_syslog=config_syslog.xml
# set windows Event log config file
# conf_winEvent=config_winEvent.properties
# set port for MPG log
port_mpg= 4446
# set port for KeyManagement log
port_km= 4448
# set port for Configuration log
port_config= 4447
# send KeyManagement log if true
# send_km = true
# send Configuration log if true
# send_config = true
```

For Windows Event logging, MICROS Gateway log service needs to be installed on the log server. For Syslog logging, an extra configuration item “SyslogHost” in config\_syslog.properties needs to be set for the syslog server.



```
config_syslog - Notepad
File Edit Format View Help
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE log4j:configuration SYSTEM "log4j.dtd">
<log4j:configuration>
<appender name="CSF_FILE" class="org.apache.log4j.RollingFileAppender">
  <param name="Threshold" value="debug"/>
  <param name="File" value="./log/debug.log"/>
  <param name="Append" value="true"/>
  <param name="MaxFileSize" value="20MB"/>
  <param name="MaxBackupIndex" value="300"/>
  <layout class="org.apache.log4j.PatternLayout">
    <param name="ConversionPattern" value="%d %-5p [%t] %m%n"/>
  </layout>
  <filter class="org.apache.log4j.varia.LevelRangeFilter">
    <param name="LevelMin" value="info"/>
    <param name="LevelMax" value="fatal"/>
    <param name="acceptOnMatch" value="TRUE"/>
  </filter>
</appender>
<!-- syslog events -->
<appender name="syslog"
  class="org.apache.log4j.net.SyslogAppender">
  <param name="Threshold" value="WARN" />
  <param name="Facility" value="local6" />
  <param name="SyslogHost" value="192.168.0.13" />
  <layout class="org.apache.log4j.PatternLayout">
    <param name="ConversionPattern"
      value="%d{yyyy-MM-dd HH:mm:ss,SSS} %-5p%m" />
  </layout>
  <filter class="org.apache.log4j.varia.LevelRangeFilter">
    <param name="LevelMin" value="WARN"/>
    <param name="LevelMax" value="WARN"/>
    <param name="acceptOnMatch" value="TRUE"/>
  </filter>
</appender>
```

---

To make sure your site is in compliance with Step 10 of The PCI Data Security Standard, “Track and monitor all access to network resources and cardholder data”, please consult the Payment Card Industries – Security Standards Council website found at <<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<sup>[14]</sup>.*

In accordance with the PCI Data Security Standard, MICROS strongly recommends regular testing of security systems and processes.

To make sure your site’s security systems and processes are setup in compliance with Step 11 of The PCI Data Security Standard, “Regularly test security systems and processes”, please consult the Payment Card Industries – Security Standards Council website found at <<https://www.pcisecuritystandards.org>>.

[14] “PCI DSS Requirements and Security Assessment Procedures”, Page 59, Version 2.0, October 2010.  
<[https://www.pcisecuritystandards.org/documents/pci\\_dss\\_v2.pdf](https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf)>

---

## Maintain an Information Security Policy

### **12. Maintain a policy that addresses information security for employees and contractors**

*A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of this requirement, “employees” refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are “resident” on the company’s site<sup>[15]</sup>.*

In accordance with the PCI Data Security Standard, MICROS strongly recommends maintaining a policy that addresses information security. It is ultimately the responsibility of the sites to enforce the recommended security recommendations.

MICROS doesn’t require the remote access to deliver/update MICROS Payment Gateway. In accordance with the PCI Data Security Standard, MICROS strongly recommends

- sites activate remote access technologies only when needed and immediately deactivate them after use, if any update is delivered via remote access
- sites properly configure a firewall or a personal firewall product to secure “always on” connections, if any update is delivered via VPN or other high speed connection

To make sure your information security policy is setup in compliance with Step 12 of The PCI Data Security Standard, “Maintain a policy that addresses information security for employees and contractors”, please consult the Payment Card Industries – Security Standards Council website found at <<https://www.pcisecuritystandards.org>>.

[15] “PCI DSS Requirements and Security Assessment Procedures”, Page 64, Version 2.0, October 2010. <[https://www.pcisecuritystandards.org/documents/pci\\_dss\\_v2.pdf](https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf)>