Oracle® Secure Payment Gateway for HSI Profit Series

PA-DSS Implementation Guide

July 2015

ORACLE

Contents

Document Information

Purpose

This document provides information pertaining to Secure Payment Gateway adherence with the *Payment Application Data Security Standard* (*PA-DSS*) version 1.2 that was developed by the *Payment Card Industry Security Standards Council* (*PCI-SSC*).

Standard Name	Standard Audience	Version Number
Payment Application Data Security Standard (PA-DSS)	Payment Application Vendor	1.2
Payment Card Industry Data Security Standard (PCI DSS)	Merchant	1.2

This guide will provide recommendations for steps that may be taken to secure the Secure Payment Gateway as to facilitate compliance with the *Payment Card Industry Data Security Standard* (*PCI DSS*) version 1.2. Although the software provided by HSI can be implemented in a PCI DSS compliant manner, it is the responsibility of the merchant, not HSI, to ensure the implementation of all software and processes meet or exceed the guidelines defined in the PCI DSS. This guide provides any Information Technology (IT) staff, IT consultants and implementations specialists the instructions for implementing the application in a compliant manner.

Versions

This document is valid for versions of the Secure Payment Gateway listed below:

Version Number	Release Date
1.2 SR3	January 2011
1.2 SR3 Patch 1	April 2011

The Secure Payment Gateway PA-DSS Implementation Guide is reviewed and updated with each version release. An updated copy of the PA-DSS Implementation Guide is provided to you with your initial Secure Payment Gateway installation and each version upgrade. Guides are also available for download at http://web.hsi-solutions.com/Solutions/Compliance/PA-DSS-Implementation-Guides.aspx

Assistance

Web References

The internet has many sites that can provide you with information about the PCI DSS. Here are just a few sites that provide information for merchants about PCI:

- https://www.pcisecuritystandards.org/
- http://pcianswers.com/
- http://pcidssfaq.org/
- http://www.pcicomplianceguide.org/

Consultants

A *Qualified Security Assessor (QSA)* can offer consultation services that provide you with answers to compliancy questions you may have. They may also be able to provide you with services and resources to assist you in achieving compliance with the PCI DSS. HSI *highly recommends* that you speak with a QSA on those requirements that exist outside of the Secure Payment Gateway. For a list of PCI approved QSA's, refer to the list provided at the PCI Web site:

https://www.pcisecuritystandards.org/approved_companies_providers/qualified_security_assessors.php

Hospitality Solutions International (HSI)

The recommendations in this guide indicate configuration and steps for compliance when using the Secure Payment Gateway. Should you have any questions regarding the compliancy of your Secure Payment Gateway not addressed in this guide, please contact an HSI Product Management representative during our normal business hours at (480) 596-5156.

You may also reach us via email at compliance@hsi-solutions.com.

Additional assistance may be provided by contacting the following numbers:

- **HSI Customer Support** **1-800-474-5022**
- **HSI Inside Sales** **1-480-596-5156**

IMPORTANT NOTE: **HSI representatives cannot adjust the configuration of your environment, systems or applications in a way that may compromise any sensitive data or violate the requirements of the PCI DSS.**

Recommendation Overview

HSI has provided the following recommendations as part of this PA-DSS Implementation Guide to assist you in achieving compliance with the PCI DSS. Recommendations are based upon HSI's review and interpretation of the requirements of the PCI DSS. Instructions on implementing these recommendations are provided throughout this guide.

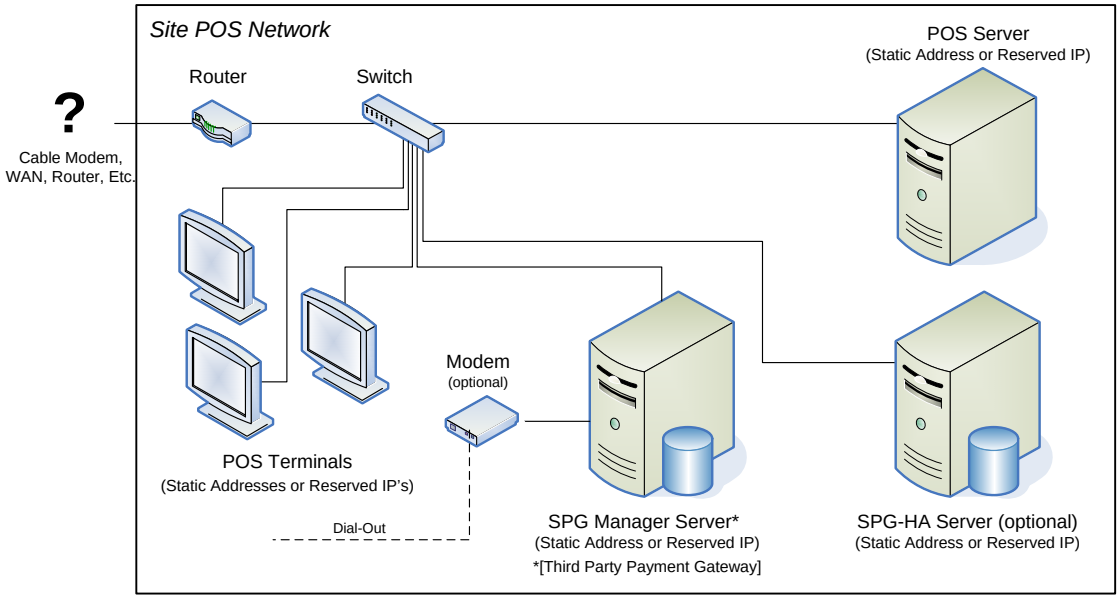
- HSI *highly recommends* that a professional organization or QSA familiar with the PCI DSS requirements assist you with your adherence to the requirements of the PCI DSS.
- HSI *highly recommends* that users change all default application and system passwords, including wireless and wired access to the network, and apply complex password rules.
- HSI *highly recommends* implementing procedures to manage the rotation of all passwords.
- HSI *highly recommends* that the use of two-factor authentication be implemented and maintained for all remote access to the site.
- HSI *highly recommends* that the HSISupport User account associated with remote access only be enabled when an authorized HSI Representative requires remote access.
- HSI *highly recommends* disabling the HSISupport User account after remote access is no longer required.
- HSI *highly recommends* the implementation of anti-malware software and its continued updating, use and review.
- HSI *highly recommends* that all applications and operating systems be kept up to date with latest approved patches and updates.
- HSI *highly recommended* that you take measures to secure any systems and applications that run within your environment from inappropriate electronic and physical access.
- HSI *highly recommends* that you take steps to enable monitoring of all systems and software used in your enterprise. This should include system level monitoring of data access for all users with administrative level access.
- HSI *highly recommends* periodic testing of security systems and processes based upon the merchant level of your site.
- HSI *highly recommends* maintaining a policy and training program that addresses information security.
- HSI *highly recommends* rotating encryption keys at a minimum annually.
- HSI *highly recommends* disabling any operating system Restore Points.

Implementation Instructions

The information provided in this section will define recommendations for securely implementing the Secure Payment Gateway (SPG).

Local Installation

The following diagram shows the recommended configuration for the Secure Payment Gateway with the optional Secure Payment Gateway High Availability Manager (SPG-HA). Installation occurs on the sites local POS network.



As a POS Server is typically located in an area that is open to many users, HSI *highly recommends* that the Secure Payment Gateway Manager (SPG Manager) be installed on a dedicated server that can be secured in an area that limits access to the computer. HSI recommends installing the Third Party Payment Gateway application on the same computer as the SPG Manager. A dedicated server is required to operate the SPG-HA which manages failover and provides load balancing for payment transactions.

Communications between the Secure Payment Gateway Agent (SPG Agent) on the terminals and the SPG Manager and SPG-HA requires the use of Static IP Addresses or Reserved IP Addresses. Configuration of these specific IP addresses will be required to ensure data is communicated correctly.

User Configuration

By default the Secure Payment Gateway is installed to utilize the Local System User account. If the Windows Local System user account does not have the appropriate rights this may render the SPG in-operable. HSI *highly recommends* the configuration of unique users and user groups to access and operate those applications related to payment card processing.

Recommended User Account Configuration

As part of the installation, the following User account is optionally created to allow the application secure access to those areas of the system that impact credit card activity:

Secure Payment Gateway Manager User

The Secure Payment Gateway Manager user account is utilized to run the Secure Payment Gateway, SQL Server and communicate with the Third Party Payment Gateway. It is critical that the user account remain active to allow continued operation of the Secure Payment Gateway application.

- **User name:** SPGM
- **Full name:** Secure Payment Gateway Manager
- **Password:** The SPGM password must be defined during installation by a Site Administrator to facilitate the site's compliance with Requirement 2.1 of the PCI-DSS.

> Site administrators may alternately choose to create a domain user account in place of the SPGM user account. If so, the domain user account must have all the rights that are required to access and operate (SPG, SQL Server).
>
> The password for the defined user account **must** be PCI compliant. Refer to Appendix B of this guide for instructions on password requirements.

User Groups

User groups limit access and operational control to those users registered to the group. HSI *highly recommends* that User Groups with permissions limited to the scope of access and functions be defined.

As part of the installation, the following User Group is optionally created to allow the application secure access those areas of the system that impact credit card activity:

- SPG Users

  This user group has restricted access to the <root path> in which the SPG was installed.

The SPGM User will be included as a member of this group in addition to the user group for SQL Server, allowing them access required to operate the SPG. If a domain user account is created in place of the SPGM user account it must also be made a member of the appropriate groups to ensure the SPG will function properly.

Application Services

It is *highly recommended* that the Secure Payment Gateway Manager and Backup Manager services be configured to log on using the defined user account for the SPG.

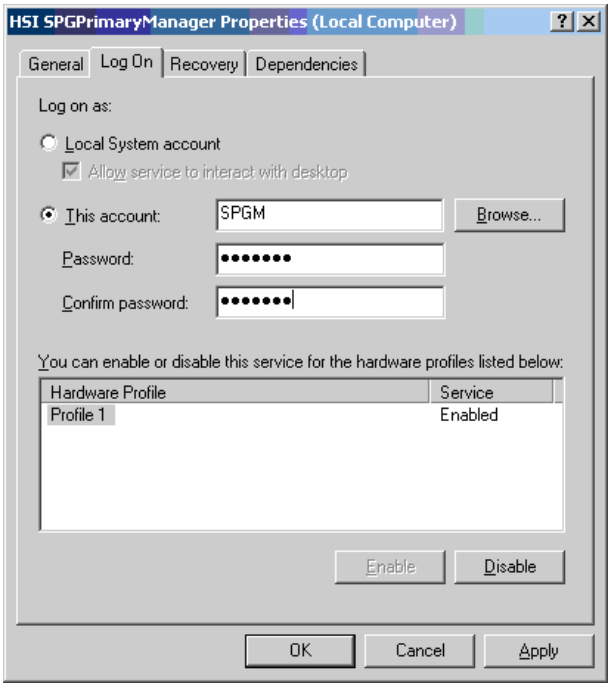
> Utilizing the user account for log on will require that the password be updated in the service configuration. Failure to update the password may render the Secure Payment Gateway in-operable.

Updating the service with the new password will require the Secure Payment Gateway and the High Availability SPG (if applicable) to be taken offline for a brief time where you will be unable to process credit cards.

Change Password on Service

To change the password on the service you may use the following instructions:

1. Open the *Computer Management* window (right-click **My Computer** > select **Manage**).
   In Server 2008, the window is called Server Manager.
2. In the left pane of the *Computer Management* window, expand **Services and Applications**.
   *In Server 2008, expand **Configuration**.*
3. Click the **Services** icon to display the list of services in the right pane.
4. Locate and highlight the **HSI SPGPrimaryManager** service.
5. Right-click **HSI SPGPrimaryManager** and select **Properties** from the drop-down menu.
6. In the *HSI SPGPrimaryManager Properties (Local Computer)* window, click the **Log On** tab to select.
7. To change the password of a local user (SPGM) or the user indicated in the *This account* field (for a domain user, type \\[domain]\[domain user name] in the *This account* field):
8. Type the new password created for the SPGM user in the *Password* and *Confirm password* fields.
9. Click the **Apply** button. Repeat steps 5 – 9 for the **HSI SPGBackupManager** service if applicable.



If the service does not start or the error appears, there may be a problem with the user or password. Open the service configuration and confirm the correct user account and password have been entered.

Other Configuration Information

Public Networks

While the Secure Payment Gateway does not directly pass data across public networks, it is *highly recommended* that a secure encryption transmission technology (IPSEC, VPN, SSL/TLS) be utilized if you plan on implementing the application to allow data over public networks. The Secure Payment Gateway does not impede the use of these technologies.

Wireless

If you choose to implement the Secure Payment Gateway in a wireless environment, it is *highly recommended* that the guidelines for implementing wireless connectivity published by the PCI Security Standards council (PCI-SSC) be utilized.

https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf

Restore Points

Some members of the PCI community *highly recommended* that any restore point features of your operating system be disabled. As this is a component of the operating system that does not impact the operation of your Secure Payment Gateway, your HSI Implementation Specialist will leave this feature in its default state. Please address the concerns of Restore Points with your individual QSA.

Application Information

Database Backup

The Secure Payment Gateway is designed to perform periodic backups of the application database as part of an application recovery process. These backup files may contain encrypted credit card account information for the current business day depending upon your preferred third party payment gateway provider. It is highly recommended that the locations these periodic backups are placed, whether on the local disk or external to the local disk, are protected from unauthorized access.

Data Retention

Requirement 3.1 of the PCI DSS indicates that storage of cardholder data must be kept to a minimum and limit the retention of the data to that which is required for business, legal and/or regulatory purposes. The Secure Payment Gateway is designed to work with your individual third party payment gateway's features for limiting storage of sensitive data.

If using the following payment provider middleware application, the HSI Secure Payment Gateway will not store any cardholder data after the cardholder data is swiped/keyed into the SPG:

- ***Dollars on the Net by Shift4***

If using any of the following payment providers middleware applications, the HSI Secure Payment Gateway will not store any cardholder data after an authorization request is generated:

- ***Fusebox by Elavon***
- ***ProtoBase by Elavon (Option 1)***

If using the following payment provider middleware application, the HSI Secure Payment Gateway will not store any cardholder data after the completion of the business day in which the transaction was settled:

- ***ProtoBase by Elavon (Option 2)***
- ***PropertyCard by Elavon***
- ***CreditLine by 911 Software***

> For information on retention of cardholder data within your Third Party Payment Gateway application, please refer to their PA-DSS Implementation Guide.

Application Upgrades

Upgrades for the Secure Payment Gateway will be made available as a new version release. An upgrade CD/DVD can be mailed to your site upon request. You may contact an HSI Customer Support Representative to schedule your application upgrade or to determine if an upgrade is available.

Security Release/Patch

Security releases or patches for the Secure Payment Gateway will be made available as soon as possible once a known security issue is recognized. These will be distributed as a patch accessible for download from the HSI secure FTP site. For information on security releases or patches you may visit our Web site at http://web.hsi-solutions.com/Solutions/Compliance.aspx and sign up to receive newsletter updates for your Secure Payment Gateway.

Application Logging

The Secure Payment Gateway performs logging of various activities that takes place during the course of the business day depending upon the logging level. Files and locations listed below are based upon the standard installation procedure of the Secure Payment Gateway. The location of the log files may have been changed to an alternate path during the installation.

> None of the logs generated by the application are capable of capturing clear text payment card data.

C:\Program Files\HSI\Secure Payment Gateway\[Application Version]\SPGPrimaryManager\[Manager Unique ID]\Logs

- ***Error.<yyyymmdd>.log***

The Error log is an error and warning log file for the entire Secure Payment Gateway. This log may contain all system errors and warnings that are generated by the application. Information written to the Error log is also written to the System log. The default logging level for this log is "Warning" which will capture all errors and warnings. This log file is always enabled and cannot be disabled.

- ***Maintenance.<yyyymmdd>.log***

The Maintenance log is a connectivity log file for the entire Secure Payment Gateway. This log contains communication pings that confirm connectivity by the application. This log file is always enabled and cannot be disabled.

- ***Security.<yyyymmdd>.log***

The Security log is a security specific error and warning log file for the entire Secure Payment Gateway. This log may contain all security errors and warnings that are generated by the application. The default logging level for this log is "Warning" which will capture all errors and warnings. This log file is always enabled and cannot be disabled.

- ***System.<yyyymmdd>.log***

The System log is a general log file for the entire Secure Payment Gateway. This log may contain all system activity; errors and tracing that are generated by the application. The default logging level for this log is "Warning" which will capture all errors and warnings. This log file is always enabled and cannot be disabled.

> If implementing the High Availability Manager application these same files will also be present in the C:\Program Files\HSI\Secure Payment Gateway\[Application Version]\SPGBackupManager\[Manager Unique ID]\Logs directory on the backup server.

File Monitoring

The Secure Payment Gateway is comprised of various configuration and data files that are required to operate the application. In your efforts to perform file monitoring in accordance with PCI DSS requirement 11.5, you may choose to include the follow folders and files:

Configuration Files

- *C:\Program Files\HSI\Secure Payment Gateway\[Application Version]\SPGPrimaryManager\Config\MerchantConfiguration.xml*
- *C:\Program Files\HSI\Secure Payment Gateway\[Application Version]\SPGPrimaryManager\Config\SecurePaymentGatewayConfiguration.xml*
- *C:\Program Files\HSI\Secure Payment Gateway\[Application Version]\SPGPrimaryManager\Config\SecurePaymentTypeConfiguration.xml*
- *C:\Program Files\HSI\Secure Payment Gateway\[Application Version]\SPGPrimaryManager\Config\TransportConfiguration.xml*

If implementing the High Availability Manager application these same files will also be present in the C:\Program Files\HSI\Secure Payment Gateway\[Application Version]\SPGBackupManager\Config directory on the backup server.

Database Files

- *C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data\SPGManager_[Application Version].mdf*
- *C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data\SPGManager_[Application Version_log.ldf*

Database Backup Files

- *C:\DBMaintenance\SPGManager_V1.2.0\SPGManager_v1.2.0FullDBBackup_yyyymmddhhmm.bak*
- *C:\DBMaintenance\SPGManager_V1.2.0\SPGManager_v1.2.0DiffDBBackup_yyyymmddhhmm.bak*

Encryption

The Secure Payment Gateway encrypts all aspects of the customer's credit card account (account number, expiration and cardholder name) using proven encryption technologies. For security reasons, specific details on the encryption technologies have been excluded.

Key Management

Managing the security of the encryption keys is vital to the security of your data. HSI highly recommends that you restrict access to the Secure Payment Gateway directory structure to only those users required to administer the application. Preventing unauthorized access to the network environment and directory structure will aid in safeguarding your encryption keys.

Key Rotation

Rotation of the encryption keys changes the keys used to perform the encryption/decryption of any sensitive data in the application. Requirement 3.6.4 of the PCI DSS calls for the periodic changing of keys:

- As deemed necessary
- At least annually

Key Rotation is a manual process that requires a key rotation utility designed for your specific application version. Rotation of your data encryption key can be scheduled by contacting an HSI Customer Support Representative.

HSI *highly recommends* that you rotate the data encryption key at a minimum annually.

As part of your annual assessment, you may be required to provide evidence of a successful key rotation. Upon the completion of the key rotation, the key rotation event will be logged in the system.yyyymmdd.log file for the day in which the key was rotated. These log files are retained by default for 3 days so a copy of this log file should be saved to a location in which it can be recalled. This is a simple text file and does not require any special application to view.

If you have not had your keys rotated since the installation of your Secure Payment Gateway, unique keys were generated during the installation. Please refer to your installation date as the last recorded changing of keys.

Secure Data Deletion

As part of your application upgrade, the original application directory structure was left intact to ensure an immediate uptime in the event of an upgrade issue. Upon the successful completion of the upgrade, it will be necessary to securely delete the previous versions directory structure to be compliant with requirement 9.10.2 of the PCI-DSS. This directory structure must be securely deleted to ensure it cannot be reconstructed.

HSI has provided and installed a freeware version of a secure file deletion utility on the HSI file server. This utility will allow for the secure deletion of the previous versions directory structure.

Install/Configure Eraser

Eraser must be installed and configured properly to support the correct type of secure file deletion required by PCI.

1. Place your SPG Pre-Installation CD into the CD-ROM drive of the POS file server.

   > The CD is designed to auto run the pre-installation. When the console for the pre-installation is displayed, select the Cancel option to stop the process.

2. Using Windows Explorer, navigate to the **\\Software\Eraser** folder on the CD-ROM drive.
3. Double-click the **EraserSetup32.exe** file to begin the installation.
4. Follow the prompts to install Eraser (accept license, default install path, available to anyone).
5. Upon the completion of the Eraser installation, select the Run Eraser Now option and press Finish.
6. From the Eraser console, press **Ctl+E** on your keyboard to open the Erasing Preferences option.
7. On the Files Tab, select Option Number 3 (*US DoD 5220.22-M (8-306. /E*) and press **OK**.
8. Close the Eraser console.

Delete Data Structure

A secure deletion of the old directory structure on the hard drive of the file server is absolutely necessary for PCI-DSS compliance. Utilize the following steps to securely delete the old directory structure.

1. Open Windows Explorer
2. Navigate to the **[HSI Home Path]\Secure Payment Gateway\v1.x.x.x** folder on POS file server.

   > This path will typically be C:\Program Files\HSI\Secure Payment Gateway\v1.x.x.x based upon the default installation path of the application. It is important that only the previous version of the SPG be securely deleted as any files that are securely deleted CANNOT be recovered.

3. Right-click the **\v1.x.x.x folder** and select the **Erase** option.
4. When prompted to confirm the deletion, click YES to securely delete the directory structure.

   > This process may take a few minutes to complete the secure deletion of the directory structure. Do NOT stop the process

5. When completed, you will be presented with an Erasing Report. It is recommended that this report be saved as a record of the secure deletion being performed upon the directory structure and kept on file for any potential inquiries.

Application Support

Remote Access

Requirement 8.3 of the PCI DSS requires the use of two-factor authentication for any remote access to the network. HSI *highly recommends* that the use of two-factor authentication be implemented and maintained for all remote access to the site.

HSI uses Symantec Corp's pcAnywhere® and Bomgar® to provide remote support to your site. Please see the HSI Remote Access Guide for additional information about using these remote access applications within your environment. The Remote Access Guide should have been provided to you along with this PA-DSS Implementation Guide. If you require a copy, please contact an HSI Customer Support representative for a replacement copy of the Remote Access Guide.

The Secure Payment Gateway does not support email or non-console administrative access in accordance with requirement 4.2 of the PCI DSS.

Troubleshooting

During the course of troubleshooting any issues that may arise with your Secure Payment Gateway, it may be necessary to use greater levels of logging to capture additional details. None of these additional levels will capture any sensitive credit card data.

HSI is very serious about the security of your system and data and has developed internal policies and procedures to ensure the secure handling of all your data while resolving your issue.

Appendix A: Technical Information

Directory Structure

This section lists the directories or folders which the Secure Payment Gateway may create as part of the product installation. Some folders and directories may not exist on every system because the directory structure is based on the options purchased and installed.

> All paths documented in this guide are based upon default installation path of the application (C:\Program Files\HSI). Users may optionally change the path for all folders and files during the installation.

Secure Payment Gateway Manager

- <root directory>\Secure Payment Gateway\[Version Number]\SPGPrimaryManager

Approved Operating Systems

- Microsoft Windows XP Professional SP3
- Microsoft Windows Server 2003
- Microsoft Windows Embedded for XP
- Microsoft Windows Server 2008
- Microsoft Windows 7

Secure Payment Gateway High Availability Manager

- <root directory>\Secure Payment Gateway\[Version Number]\SPGBackupManager

Approved Operating Systems

- Microsoft Windows XP Professional SP3
- Microsoft Windows Server 2003
- Microsoft Windows Embedded for XP
- Microsoft Windows Server 2008
- Microsoft Windows 7

Secure Payment Gateway Agent

- <root directory>\Secure Payment Gateway\[Version Number]\SPGAgent

Approved Operating Systems

- Microsoft Windows XP Professional SP3
- Microsoft Windows Server 2003
- Microsoft Windows WePOS
- Microsoft Windows 7
- Microsoft Windows Server 2008
- Microsoft Windows POSReady2009

Secure Payment Gateway External Agent

- <root directory>\Secure Payment Gateway\[Version Number]\SPGExternalAgent

Approved Operating Systems

- Microsoft Windows XP Professional SP3
- Microsoft Windows Server 2003
- Microsoft Windows Embedded for XP
- Microsoft Windows Server 2008
- Microsoft Windows 7

Services

This section provides a description of services that are utilized by the Secure Payment Gateway.

Required Services

This is a list of OS services that are required and utilized by the Secure Payment Gateway.

Display Name	Service Name	Executable File Name/Command	Default Startup Type	Notes
Computer Browser	Browser	svchost.exe -k netsvcs	Automatic	
DHCP Server	DHCPServer	tcpsvcs.exe	Automatic	DHCP Server Role
DNS Server	DNS	dns.exe	Automatic	DNS Server or DC role(s).
Event Log	Eventlog	services.exe	Automatic	
Message Queuing	MSMQ	mqsvc.exe	Automatic	Mechanism for SPG application inter-processing communications
Net Logon	Netlogon	lsass.exe	Manual	On a domain member, this service is started automatically.
Network Connections	Netman	svchost.exe -k netsvcs	Manual	This service starts automatically when the startup type is Manual and Network Connections is running.
Network Location Awareness (NLA)	NLA	svchost.exe -k netsvcs	Manual	This service automatically starts when the startup type is Manual.
NT LM Security Support Provider	NtLmSsp	lsass.exe	Manual	
Remote Procedure Call (RPC)	RpcSs	svchost -k rpcss	Automatic	
Remote Procedure Call (RPC) Locator	RpcLocator	locator.exe	Manual	On a domain controller, this service is started automatically.
Remote Registry	RemoteRegistry	svchost.exe -k regsvc	Automatic	
Security Accounts Manager	SamSs	lsass.exe	Automatic	
Server	lanmanserver	svchost.exe -k netsvcs	Automatic	
Windows Time	W32Time	svchost.exe -k netsvcs	Automatic	
Windows Internet Name Service (WINS)	WINS	Wins.exe	Automatic	WINS Server Role
Workstation	lanmanworkstation	svchost.exe -k netsvcs	Automatic	

Secure Payment Gateway Services

This is a list of services that are installed by the Secure Payment Gateway dependent upon the options purchased.

Display Name	Service Name	Executable File Name/Command	Default Startup Type	Notes
HSI SPGPrimaryManager	HSI SPGPrimaryManager	SPGPrimaryManagerService.exe	Automatic	-
HSI SPGAgent	HSI SPGAgent	SPGAgentService.exe	Automatic	-
SQL Server	MSSQL$<servername>	sqlservr.exe" –s<servername>	Automatic	Required on database servers only – MS SQL Server application process
SQL Server Browser	SQLBrowser	sqlbrowser.exe	Automatic	Required on database servers only – naming service for MS SQL Server Express
Visual Studio 2005 Remote Debugger	msvsmon80	msvsmon.exe /service msvsmon80	Disabled	Installed with SQL Server 2005. Leave disabled.

Optional Services

This is a list of services that are optional with the Secure Payment Gateway.

Display Name	Service Name	Executable File Name/Command	Default Startup Type	Notes
911 Credit Server	Credit Server	Ccv_server.exe	Automatic	Only required when using CreditLine for payment card processing
Distributed Transaction Coordinator	MSDTC	msdtc.exe	Automatic	Required on HA database servers only – MS Distributed Transaction Support
Global Card Services Property Card	gcs-propcard	Wrapper.exe -s C:\GCS\etc\wrapper.conf	Automatic	Only required when using GCS for payment card processing
HSI SPGBackupManagerService	HSI SPGBackupManagerService	SPGBackupManagerService.exe	Automatic	-
HSI SPGExternalAgent	HSI SPGExternalAgent	SPGExternalAgentService.exe	Automatic	Only required if implementing Ordering Interface
Shift4 NetApi	frmNetApiService	NetApiSvc.exe	Automatic	Only required when using $$$ on the Net for payment card processing
Shift4 UTG (v2)	frmUtg2Service	Utg2Svc.exe	Automatic	Only required when using $$$ on the Net for payment card processing
Stunnel	stunnel	stunnel.exe	Automatic	Only required when using Fusebox for payment card processing
Vigilix Agent Guardian	Vigilix Agent Guardian	vxagentguardian.exe	Automatic	Only required when using Vigilix Monitoring
Vigilix Agent	Vigilix Agent	vxagent.exe	Automatic	Only required when using Vigilix Monitoring

Protocols

This section provides a description of the networking protocols that may be utilized by the Secure Payment Gateway.

Network Protocols Used

Number	Keyword	Protocol	References
1	ICMP	Internet Control Message	RFC792,JBP
6	TCP	Transmission Control	RFC793,JBP
17	UDP	User Datagram	RFC768,JBP

Secure Payment Gateway - Application Ports Used

Application/Service	Protocol	Client / Server Port Request	Service Port Incoming	Service Port Outgoing
HSI SPGPrimaryManager	TCP (MSMQ Send, MSMQ Receive)	-	1801	1801
HSI SPGPrimaryManager	UDP (MSMQ Naming Send/Receive)	-	1801	1801
HSI SPGBackupManager	TCP (MSMQ Send, MSMQ Receive)	-	1801	1801
HSI SPGBackupManager	UDP (MSMQ Naming Send/Receive)	-	1801	1801
HSI SPGAgent	TCP (MSMQ Send, MSMQ Receive)	-	1801	1801
HSI SPGAgent	UDP (MSMQ Naming Send/Receive)	-	1801	1801
HSI SPGExternalAgent	TCP (MSMQ Send, MSMQ Receive)	-	1801	1801
HSI SPGExternalAgent	UDP (MSMQ Naming Send/Receive)	-	1801	1801
HSI SPGExternalAgent	TCP (Interface Order Request)	-	22555*	-
Profit Series Ordering Interface	TCP (Interface Order Request)	-	22554*	-
911 Credit Server	HTTPS (CreditLine batch transmission)	-	-	443
Elavon (Fusebox)	TCP (Fusebox batch transmission)	-	-	10001
Elavon (PropertyCard)	TCP (PropertyCard batch transmission)	-	-	Confirm Port with Elavon
Elavon (ProtoBase)	TCP (ProtoBase batch transmission)	-	-	Confirm Port with Elavon
Shift 4	TCP (Shift 4 batch transmission)	-	-	26880
Shift 4	TCP (Shift 4 batch transmission)	-	-	26881

** the default value which may be configured.*

Secure Payment Gateway - OS Service Ports Used

Service	Protocol	Client / Server Port Request	Service Port Incoming	Service Port Outgoing
DHCP lease	TCP (request)	-	-	67
DHCP lease	TCP (response)	-	-	68
DNS (client to server lookup)	TCP or UDP (depends on software)	1024 - 5000	53	53
DNS (server to server lookup)	TCP or UDP (depends on software)	53	53	53
DNS (primary to secondary zone trnsf)	TCP	53	53	1024 - 5000
DNS (prim to second soa record trnsf)	UDP	53	53	53
File shares	UDP (name lookup)	-	-	137
File shares	TCP (session)	-	-	139
FTP-data	TCP	-	-	20
FTP	TCP	-	-	21
HTTP	TCP	-	-	80
HTTP-Secure Sockets Layer (SSL)	TCP	-	-	443
LDAP	TCP	-	-	389
LDAP (SSL)	TCP	-	-	636
Microsoft-DS	TCP	1024 – 5000	-	445
Microsoft-DS	UDP	-	-	445
NTP	UDP	-	-	123
PPTP	PPTP (protocol 47, GRE)	-	-	1723
RPC	TCP (port mapper)	-	-	135
RPC	TCP (session ports)	-	-	Dynamic
SNMP	UDP	-	-	161
SNMP Trap	UDP	-	-	162
SQL Server (TCP client)	UDP/TCP (name lookup)	-	-	53
SQL Server (TCP client)	TCP (session)	-	-	1433
Wins registration	UDP (NetBIOS over TCP/IP name svc)	-	-	137
Wins replication	TCP	-	-	42
Windows Challenge/Response auth	TCP (NetBIOS over TCP/IP session svc)	-	-	139

HSI Customer Support - TCP/IP Ports

Application / Tool	Source Port	Transport	Destination Port	Transport
Bomgar	80	TCP	-	-
Bomgar	443	TCP	-	-
RDP	3389	TCP	-	-
Vigilix	443	TCP	-	-

HSI Customer Support - ICMP Protocols

Application / Tool	Protocol	Type	Code	Name
Ping / PathPing / TracerT	ICMP	0	0	Echo Reply
Ping / PathPing / TracerT	ICMP	3	0 – 15	Destination Unreachable
Ping / PathPing / TracerT	ICMP	8	0	Echo Request
Ping / PathPing / TracerT	ICMP	11	0	Time Exceeded

HSI Customer Support - VPN

Application / Tool	Protocol	Client / Server Port Request	Service Port In	Service Port Out
PPTP	47, GRE	-	-	1723

Appendix B: Password & User Security

HSI *highly recommends* implementing procedures to manage user accounts and passwords. User accounts and passwords are critical to the continued operation of your Secure Payment Gateway.

> ***It is the responsibility of the site to maintain passwords on all user accounts in accordance with section 8 of the PCI DSS.***

The following are recommended practices for password security within your network environment.

- Ensure all users are assigned a unique ID with password; do not allow generic accounts and passwords
- Ensure that user passwords are changed at least every 90 days and inactive accounts removed after 90 days
- Immediately revoke access to any terminated user
- Use alphanumeric passwords that meet these requirements:
    - Must be between 7 and 15 characters
    - Must contain alpha characters
    - Must contain one capitalized alpha character
    - Must contain at least one numeric character
    - Must have an alpha character before and after any numeric character
    - Must be different from previous four passwords

Appendix C: Punch List

This punch list provides you with a recommended list of tasks to perform within Secure Payment Gateway to ensure compliancy is maintained once implemented.

Secure Payment Gateway PCI DSS Punch List

Quarterly	Annually
Confirm all applicable users have or are configured to rotate passwords every 90 days	All Quarterly Items
Change the User Password for user accounts (SPGM/domain user account) that impact your credit card processing applications	Visit the HSI Web Site for the latest information on any available upgrades or patches
Update Secure Payment Gateway Manager and Backup Manager Services (if applicable) with updated password for defined user account.	Visit the HSI Web Site for the latest information on compliance
Verify that the recommendations expressed in this guide are still in-place	Rotation of Data Encryption Keys
Document and resolve any discrepancies	