PA DSS Implementation Guide

Sierra Server Software

Version 1.63

Jun 10, 2013

SS1000

Table of Contents

Notice

THE INFORMATION IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. UNITEC MAKES NO REPRESENTATION OR WARRANTY AS TO THE ACCURACY OR THE COMPLETENESS OF THE INFORMATION CONTAINED HEREIN. YOU ACKNOWLEDGE AND AGREE THAT THIS INFORMATION IS PROVIDED TO YOU ON THE CONDITION THAT NEITHER UNITEC NOR ANY OF ITS AFFILIATES OR REPRESENTATIVES WILL HAVE ANY LIABILITY IN RESPECT OF, OR AS A RESULT OF, THE USE OF THIS INFORMATION. IN ADDITION, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE SOLELY RESPONSIBLE FOR MAKING YOUR OWN DECISIONS BASED ON THE INFORMATION HEREIN.

Nothing herein shall be construed as limiting or reducing your obligations to comply with any applicable laws, regulations or industry standards relating to security or otherwise including, but not limited to, PA-DSS and DSS.

The retailer may undertake activities that may affect compliance. For this reason, UNITEC is required to be specific to only the standard software provided by it.

About this Document

This document describes the steps that must be followed in order for your Sierra product installations to comply with Payment Application – Data Security Standards (PA-DSS). The information in this document is based on PCI Security Standards Council Payment Application Data Security Standards program (version 2.0 dated October, 2010).

Unitec instructs and advises its customers to deploy UNITEC applications in a manner that adheres to the PCI Data Security Standard (v2.0). Subsequent to this, best practices and hardening methods, such as those referenced by the Center for Internet Security (CIS) and their various “Benchmarks”, should be followed in order to enhance system logging, reduce the chance of intrusion and increase the ability to detect intrusion, as well as other general recommendations to secure networking environments. Such methods include, but are not limited to, enabling operating system auditing subsystems, system logging of individual servers to a centralized logging server, the disabling of infrequently-used or frequently vulnerable networking protocols and the implementation of certificate-based protocols for access to servers by users and vendors.

You must follow the steps outlined in this *Implementation Guide* in order for your Sierra product installation to support your PCI DSS compliance efforts.

Revision Information

Version	Date	Summary of Changes
1.00	14-Apr-2009	Initial release
1.24	19-Apr-2010	Document was completely rewritten and released for software version 1.24.
1.24A	30-July-2010	Revised sections 4.3, 4.4, 4.6 and 4.7 with minor clarifications
1.24B	3-Nov-2010	Revised sections 1.0 and 4.1 through 4.11 with minor clarifications. Added new requirement ("Note: Should customers….systems") at the end of section 4.2.
1.34	23-May-2011	Reviewed document with release of version 1.34 software. Incremented document rev with no other changes made.
1.43	10-Apr-2012	Deleted 2nd paragraph in Sec 4.2 ("Sierra does not store any cardholder data that is not allowed per PCI DSS. As data cannot be stored, procedures for purging stored data are non-applicable") and added 4th paragraph ("Version 1.43 of Sierra….")
1.63	10-Jun-2013	Completely rewritten for compliance with version 2.0 of PA-DSS

Note: This PA-DSS Implementation Guide must be reviewed on a yearly basis, whenever the underlying application changes or whenever the PA-DSS requirements change. Updates should be tracked and reasonable accommodations should be made to distribute or make the updated guide available to users. A copy of this guide is included with products shipped from the factory and customers may also download the latest version from the MANUALS section of the Unitec WEB site at www.StartWithUnitec.com

Executive Summary

The Sierra Payment Application version 1.6 has been PA-DSS (Payment Application Data Security Standard) certified, with PA-DSS Version 2.0. For the PA-DSS assessment, we worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PAQSA):

Coalfire
IT Audit and Compliance

Coalfire Systems, Inc. 361 Centennial Parkway Suite 150 Louisville, CO 80027	Coalfire Systems, Inc. 1633 Westlake Avenue N. Suite 100 Seattle, WA 98109

This document also explains the Payment Card Industry (PCI) initiative and the Payment Application Data Security Standard (PA-DSS) guidelines. The document then provides specific installation, configuration, and ongoing management best practices for using Payment Application as a PA-DSS validated Application operating in a PCI Compliant environment.

PCI Security Standards Council Reference Documents

The following documents provide additional detail surrounding the PCI SSC and related security programs (PA-DSS, PCI DSS, etc):

- Payment Applications Data Security Standard (PA-DSS)
  https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml

- Payment Card Industry Data Security Standard (PCI DSS)
  https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

- Open Web Application Security Project (OWASP)
  http://www.owasp.org

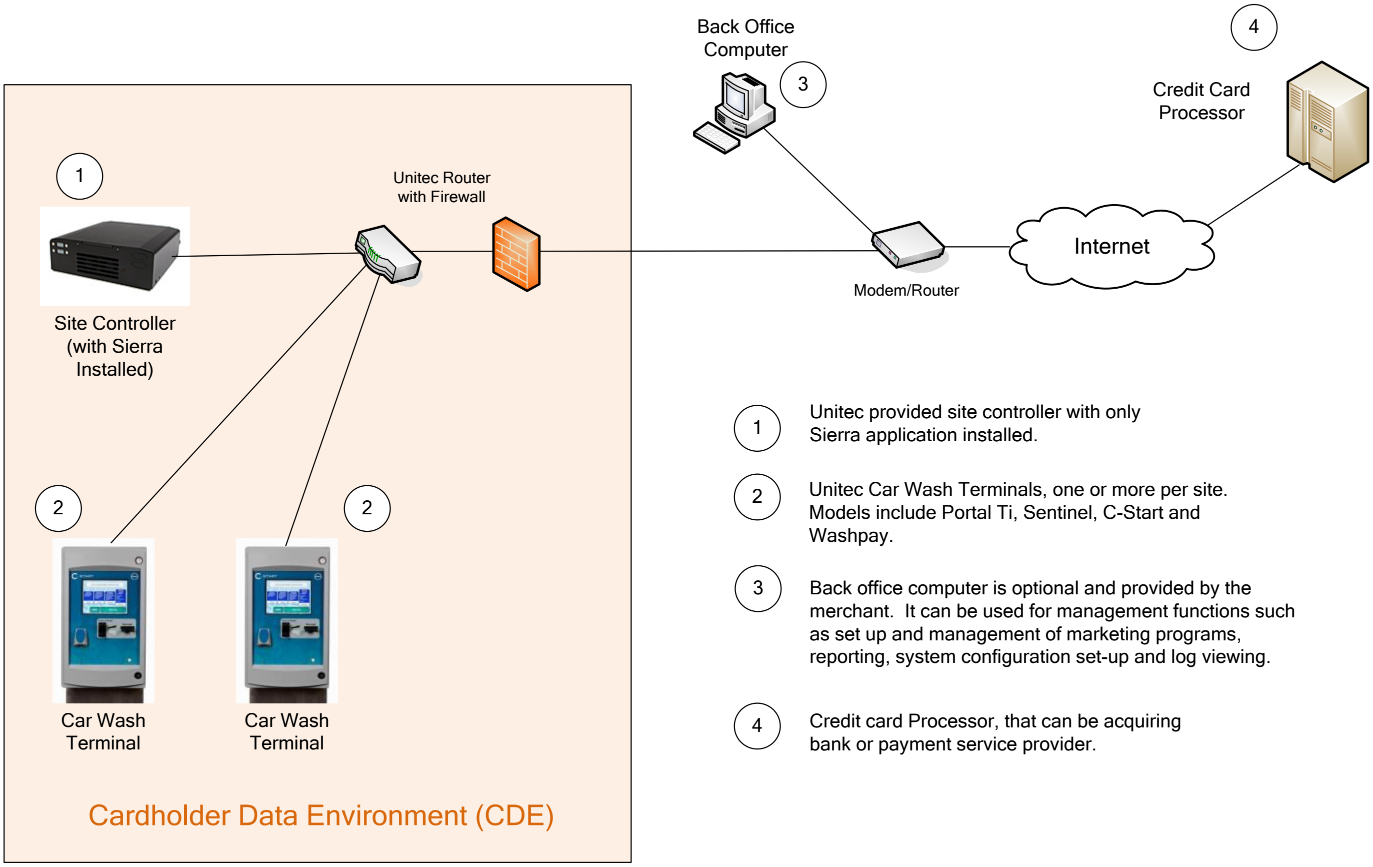
Application Summary

Payment Application Name:	Sierra Server
Payment Application Version:	1.63
Application Description:	The Sierra server application provides payment and management capabilities to Unitec Car Wash terminals. It is factory installed on a Unitec supplied site controller or the Car Wash terminal and operates with the Windows XP Embedded Operating System.
Application Target Clientele:	Sierra was designed for use in the Automatic Car Wash market
Components of Application Suite (i.e. POS, Back Office, etc.)	Sierra is the server application of a Unitec Car Wash system and works exclusively with 'client' software applications that run on a Unitec Portal Ti, Sentinel, C-Start or Washpay terminal. The system is supplied with a factory configured network router as shown in the Network Diagram (later in this document).
Required Third Party Payment Application Software:	No 3rd party payment application software is required. Unitec has however integrated a 3rd party application to accommodate processing with Mercury Payment Systems. This application, the DSI Client from Datacap Systems, is provided as a client for use in communicating with Datacap's Net ePay payment server. Net ePay is hosted at Mercury Payment Systems and it is a PADSS validated payment application)
Database Software Supported:	Sierra uses SQL Express 2008 r2 database software
Other Required Third Party Software:	.Net Framework version 4.0 (Microsoft) and IIS Version 5.5 (Microsoft)
Operating System(s) Supported:	Windows XP Embedded
Application Functionality Supported	Select one or more from the following list: ☐ **POS Suite** ☐ **POS Admin** ☐ **Shopping Cart & Store Front** ☐ **POS Face-To-Face** ☐ **Payment Middleware** ☐ **Others (Please Specify):** ☒ **POS Kiosk** ☐ **Payment Back Office** ☒ **POS Specialized** ☐ **Payment Gateway/Switch**
Payment Processing Connections:	Credit card processing will require an Internet connection. As processing requires transmittal of sensitive cardholder data, communications from Sierra to the card processor are secured via SSL V3 (as required by the PADSS and PCI-DSS).
Description of Versioning Methodology:	Sierra Server versioning has three levels, Major (X), Minor(Y), and incremental (Z): X.YZ • Major changes include significant functional changes or

	changes to accommodate a new platform (hardware or Operating System) and would have an impact on PA-DSS requirements. • Minor changes include small changes such as minor enhancements and may or may not have an impact on PA-DSS requirements. • Incremental changes include bug fixes and would have no negative impact on PA-DSS requirements.
List of Resellers/Integrators (If Applicable):	Sierra is sold exclusively through a network of over 400 Unitec distributors. Authorized distributors can be found through the "Car Wash Operator" Menu option at www.startwithunitec.com

Typical Network Implementation

Sierra Network Diagram Example



1 Unitec provided site controller with only Sierra application installed.

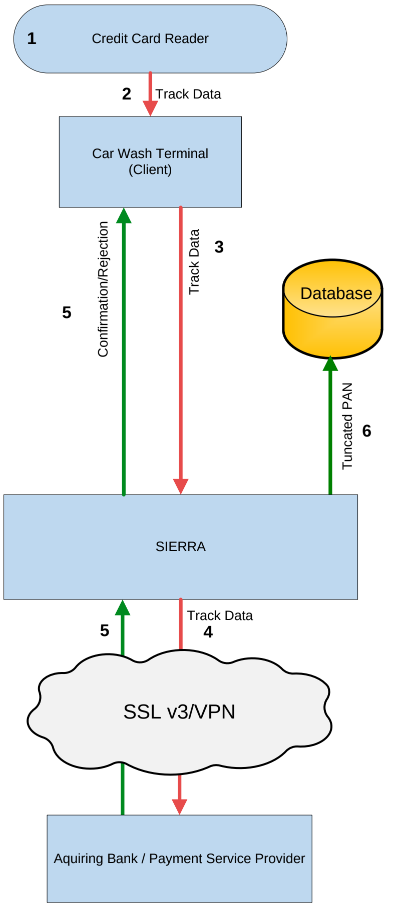
2 Unitec Car Wash Terminals, one or more per site. Models include Portal Ti, Sentinel, C-Start and Washpay.

3 Back office computer is optional and provided by the merchant. It can be used for management functions such as set up and management of marketing programs, reporting, system configuration set-up and log viewing.

4 Credit card Processor, that can be acquiring bank or payment service provider.

Dataflow Diagram

SIERRA Data Flow Diagram Example



Colored lines represent the type of data in transit as follows:

- **Red** represents encrypted or unencrypted Sensitive Authentication data or Cardholder data in Transit

- **Green** represents data that is not considered Cardholder or Sensitive Authentication Data.

1. Credit card is read / swiped at the card reading device

2. Track data is sent to the Car Wash client terminal

3. Track data is sent to SIERRA server.

4. Track data is sent from Sierra server to the acquiring bank/payment service provider and must be encrypted utilizing secure communication methods (VPN/SSL v3) on a data level.

5. Authorization response is sent back to the system. This includes only authorization code but no PAN or Track data

6. If transaction is granted then the PAN is stored in the Sierra database in truncated form (last 4 digits preceded with asterisks in place of PAN digits) along with the Card Type (VISA, AMEX etc..), Cardholder Name and, Expiration Date. Complete Track data is not stored at any time.

Difference between PCI Compliance and PA-DSS Validation

As a software vendor, our responsibility is to be "PA-DSS Validated."

We have performed an assessment and certification compliance review with our independent assessment firm, to ensure that our platform does conform to industry best practices when handling, managing and storing payment related information.

PA-DSS is the standard against which Payment Application has been tested, assessed, and validated.

PCI Compliance is then later obtained by the merchant, and is an assessment of your actual server (or hosting) environment.

Obtaining "PCI Compliance" is the responsibility of the merchant and your hosting provider, working together, using PCI compliant server architecture with proper hardware & software configurations and access control procedures.

The PA-DSS Validation is intended to ensure that the Payment Application will help you achieve and maintain PCI Compliance with respect to how Payment Application handles user accounts, passwords, encryption, and other payment data related information.

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

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

The 12 Requirements of the PCI DSS:

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*

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

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

- Sensitive Authentication Data requires special handling
- Remove Historical Cardholder Data
- Set up Good Access Controls
- Properly Train and Monitor Admin Personnel
- Key Management Roles & Responsibilities
- PCI-Compliant Remote Access
- Use SSH, VPN, or SSLV3/TLS 1.0 or higher for encryption of administrative access
- Log settings must be compliant
- PCI-Compliant Wireless settings
- Data Transport Encryption
- PCI-Compliant Use of Email
- Network Segmentation
- Never store cardholder data on internet-accessible systems
- Use SSLV3 for Secure Data Transmission
- Delivery of Updates in a PCI Compliant Fashion

Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4.a)

Sierra retains only cardholder data elements that are allowed per the PCI DSS. It should be noted however that version 1.12 did store full track 2 contents – in encrypted form – prior to authorization. This data was deleted from the database upon authorization but there are no tools available to securely wipe trace data from the storage device (the D-Drive flash card). To comply with this requirement, Sierra installations with version 1.12 should be updated as follows:

- Acquire a software upgrade utility to update Sierra from version 1.12 to 1.24 and a new D-Drive from Unitec.

- Apply the software upgrade in accordance with the instructions provided with the upgrade utility.

- Save a database back up onto a thumbdrive by following the procedures described in the Operator's Manual.

- Install the new D-drive that contains the compliant version of Sierra. Use the restore function to copy the database from the thumbdrive onto the new D-Drive. Use of the restore function does not transfer either historic or cryptographic material including track data.

The replaced D Drive may house sensitive data and must be securely destroyed. Unitec uses a 3rd party service to handle the destruction of these drives. Upon completion of the update process described above, any replaced D Drive older than version 1.24 must be returned to Unitec Customer Service through a secure courier (e.g. Fed-ex, UPS) so it can be destroyed. Unitec ensures the secure handling and destruction of all received D Drives through contract with a media destruction service who incinerates the drives in a secured environment and provides Certificates of Destruction which are archived at Unitec.

Sensitive Authentication Data requires special handling (PA-DSS 1.1.5.c)

UNITEC does not store Sensitive Authentication data for any reason, and we strongly recommend that you do not do this either. However, if for any reason you should do so, the following guidelines must be followed when dealing with sensitive authentication data (swipe data, validation values or codes, PIN or PIN block data):

- Collect sensitive authentication data 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

Purging of Cardholder Data (PA-DSS 2.1)

SIERRA does not store cardholder data and therefore there is no data to be purged by the application as required by PA-DSS v2.0.

Any cardholder data you store outside of the application must be documented and you must define a retention period at which time you will purge (render irretrievable) the stored cardholder data.

Cardholder Data Encryption Key Management (PA-DSS 2.5.c and 2.6.a)

SIERRA does not store cardholder data in any way nor does it provide any configurability that would allow a merchant to store cardholder data, therefore no encryption of cardholder data is required for PA-DSS v2.0.

Removal of Cryptographic material (PA-DSS 2.7.a)

SIERRA Version 1.12 encrypted cardholder data that was stored pre-authorization. As there are no tools available for removing cryptographic materials, customers using version 1.12 should upgrade their products following the procedure previously described (under the section titled “Remove Historical Sensitive Authentication Data”)

Set up Strong Access Controls (3.1.a and 3.2)

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

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

All authentication credentials are provided by the application. For both the completion of the initial installation and for any subsequent changes (for example, any changes that result in user accounts reverting to default settings, any changes to existing account settings, or changes that generate new accounts or recreate existing accounts), the following 10 points must be followed per PCI 8.1, 8.2, and 8.5.8-15:

1. The application must assign unique IDs for user accounts. (8.1)
2. The application must provide at least one of the following three methods to authenticate users: (8.2)
    a. Something you know, such as a password or passphrase
    b. Something you have, such as a token device or smart card
    c. Something you are, such as a biometric
3. The application must NOT require or use any group, shared, or generic accounts or passwords.(8.5.8
4. The application requires passwords to be changed at least every 90 days (8.5.9)
5. The application requires passwords must to be at least 7 characters (8.5.10)
6. The application requires passwords to include both numeric and alphabetic characters (8.5.11)
7. The application keeps password history and requires that a new password is different than any of the last four passwords used. (8.5.12)
8. The application limits repeated access attempts by locking out the user account after not more than six logon attempts. (8.5.13)
9. The application sets the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. (8.5.14)
10. The application requires the user to re-authenticate to re-activate the session if the application session has been idle for more than 15 minutes.

SIERRA is shipped with a factory default Administrative account. The password for this account must be changed as follows:

- After log-in, select SET-UP from the main menu options

- Select USERS from the sub-menu that's shown on the left side of the page

- Click on the EDIT button shown for the default account and enter a new password. As described above, your password must be at least 7 characters and include both alpha and numeric characters.

- Re-enter your new password in the 'confirm password' box then click on the SAVE button to complete the change.

Your password will be valid for 90 days only. As your password expiration date approaches, you will be notified that the password will expire each time you log in to the management application and prompted to reset your password. Follow the procedure described above to enter a new password (Note - Your new password must not be the same as any of the last passwords used).

[Note: These password controls are not intended to apply to employees who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by employees with administrative capabilities, for access to servers with cardholder data, and for access controlled by the application.]

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

Properly Train and Monitor Admin Personnel

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

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

Sierra Administrative Accounts are those configured with access privileges to the USER MANAGEMENT and UTILITIES functions enabled.

Log settings must be compliant (PA-DSS 4.1.b, 4.4.b)

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

4.4.b: SIERRA facilitates centralized logging.

Payment application logs required per the PA-DSS can be retrieved through the Sierra management application and saved on to a thumbdrive or other media for use in a centralized logging system. Sierra log files are saved as .CSV files. To access the log files:

1. Log in to the Sierra Management Application and select the UTILITIES option.

2. Select LOGS from the list of functions shown in the Utilities menu

3. Select System.Log from the drop down list provided in the ‘Log File’ menu box and click on the *VIEW LOG* button to display the log contents.

4. To save the log file (in .CSV format) click on the *SAVE* button, select the SAVE option and the drive and folder where the log is to be saved.

It should be noted that a log file’s size is limited and when its capacity is reached, a new file will start. The current file will be named System.log and previous files will be appended with a sequential digit as System.log1, System.log2 etc… up to System.log7 with System.log1 being the most recent. The (8) most recent log files will be stored.

For more details on accessing in navigating through the Management application, refer to the Sierra User’s Manual.

Services and Protocols (PA-DSS 5.4.c)

SIERRA does not require the use of any insecure services or protocols. A list of services and protocols that SIERRA does require is below. These are enabled on start-up and no reseller or merchant actions are required to configure or use these services properly.

Client Service for NetWare
COM+ Event System
COM+ System Application
Computer Browser
Cryptographic Services
DCOM Server Process Launcher
DHCP Client
Distributed Transaction Coordinator
DNS Client
Error Reporting Service
Event Log
HID Input Service
HTTP SSL
IIS Admin
IPSEC Services
Logical Disk Manager
Message Queuing
Message Queuing Triggers
Network Location Awareness (NLA)
NT LM Security Support Provider
Plug and Play
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Procedure Call (RPC)
Remote Registry
Security Accounts Manager
Server
Shell Hardware Detection
Simple Mail Transfer Protocol (SMTP)
Smart Card
SQL Server (SQLEXPRESS)
SQL Server VSS Writer
SSDP Discovery Service
System Event Notification
Task Scheduler
TCP/IP NetBIOS Helper
Telephony
Terminal Services
Themes
Universal Plug and Play Device Host
Windows Audio
Windows Management Instrumentation
Windows Presentation Foundation Font Cache 4.0.0.0
Wireless Zero Configuration
Workstation
World Wide Web Publishing

PCI-Compliant Wireless settings (PA-DSS 6.1.f and 6.2.b)

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

> 1.2.3: Perimeter firewalls must be installed between any wireless networks and systems that store cardholder data, and these firewalls must deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.
>
> 2.1.1: Change wireless vendor defaults per the following 5 points:
>
> 1. Encryption keys must be changed from default at installation, and must be changed anytime anyone with knowledge of the keys leaves the company or changes positions.

2. Default SNMP community strings on wireless devices must be changed
3. Default passwords/passphrases on access points must be changed.
4. Firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks.
5. Other security-related wireless vendor defaults, if applicable, must be changed.

4.1.1: Industry best practices (for example, IEEE 802.11.i) must be used to implement strong encryption for authentication and transmission of cardholder data.
Note: The use of WEP as a security control was prohibited as of June 30, 2010.

Never store cardholder data on internet-accessible systems (PA-DSS 9.1.b)

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

PCI-Compliant Remote Access (10.2)

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

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

SIERRA does not accommodate remote access by default but does allow Remote Desktop (RD) to be temporarily enabled for troubleshooting purpose. This action requires an Administrative password for Sierra Access (something you know) and a unique activation code (or token) that is issued by Unitec technical support (something you have). The activation code allows RD to be enabled for 24 hours only.

PCI-Compliant Delivery of Updates (PA-DSS 10.3.1)

UNITEC delivers patches and updates for Sierra in a secure manner.

As a development company, we keep abreast of the relevant security concerns and vulnerabilities in our area of development and expertise. We do this by subscribing to Microsoft security alert services and by lab testing SIERRA with a vulnerability scanning tool (Nessus Vulnerability Scanner). Should we identify a relevant vulnerability in Sierra, we work to promptly develop, test and, issue a product update that helps protect SIERRA against the specific, new vulnerability.

We do not deliver software updates via remote access to customer networks. Instead, software updates are provided as a utility that's loaded at Unitec onto a USB thumbdrive and made available to merchants through Unitec distributors. Sierra uses a SHA-2 hash verification to ensure the integrity of an update program. This security measure ensures any update applied to Sierra is from a known and trusted source and eliminates the possibility of installing invalid files or programs.

The process for installing a software update is as follows:

1. Acquire the update program from your Unitec distributor (updates are loaded onto a USB Thumb Drive).

2. Connect the thumbdrive with the update program to a USB port on the site server or terminal (depending on which device Sierra is installed).

3. Log on to the management system and select the UTILITIES Menu tab

4. From the Utilities page, select FILES from the list of Utilities functions and click on the 'Load Update Files' button. A message will be displayed when the file loading is complete. The update will be installed the next time Sierra is restarted.

5. To restart Sierra (and install the update), select SYSTEM from the list of Utilities functions and click on the 'Restart Server' button at the bottom of the page (Note: As this will cause the system to go out of service temporarily, confirm that the site is idle before restarting the server.

PCI-Compliant Remote Access (10.3.2.b)

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

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

If users and hosts within the payment application environment may need to use third-party remote access software such as <Remote Desktop (RDP)/Terminal Server, PCAnywhere>, etc. to access other hosts within the payment processing environment, special care must be taken.

In order to be compliant, every such session must be encrypted with at least 128-bit encryption (in addition to satisfying the requirement for two-factor authentication required for users connecting from outside the payment processing environment). For <RDP/Terminal Services> this means using the high encryption setting on the server, and for <PCAnywhere> it means using symmetric or public key options for encryption. Additionally, the PCI user account and password requirements will apply to these access methods as well.

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

- Change default settings (such as usernames and passwords) on remote access software (e.g. VNC)
- Allow connections only from specific IP and/or MAC addresses
- Use strong authentication and complex passwords for logins according to PA-DSS 3.1.1 – 3.1.10 and PCI DSS 8.1, 8.3, and 8.5.8-8.5.15
- Enable encrypted data transmission according to PA-DSS 12.1 and PCI DSS 4.1
- Enable account lockouts after a certain number of failed login attempts according to PA-DSS 3.1.8 and PCI DSS 8.5.13

- Require that remote access take place over a VPN via a firewall as opposed to allowing connections directly from the internet
- Enable logging for auditing purposes
- Restrict access to customer passwords to authorized reseller/integrator personnel.
- Establish customer passwords according to PA-DSS 3.1.1 – 3.1.10 and PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.

As previously mentioned, SIERRA allows Remote Desktop to be temporarily enabled for troubleshooting. As outlined in the text above any use of this feature outside of the secure network must be secured through a VPN.

Data Transport Encryption (PA-DSS 11.1.b)

The PCI DSS requires the use of strong cryptography and encryption techniques with at least a 128 bit encryption strength (either at the transport layer with SSLV3 or IPSEC; or at the data layer with algorithms such as RSA or Triple-DES) to safeguard cardholder data during transmission over public networks (this includes the Internet and Internet accessible DMZ network segments).

PCI DSS requirement 4.1: Use strong cryptography and security protocols such as secure sockets layer (SSLV3) / transport layer security (TLS 1.0 or higher) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

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

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

Refer to the Dataflow diagram for an understanding of the flow of encrypted data associated with SIERRA.

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

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

Non-console administration (PA-DSS 12.1)

SIEERA allows non-console administration, so you must use SSH, VPN, or SSLV3/TLS 1.0 or higher for encryption of this non-console administrative access. As previously stated, Administrative accounts are those with access to the USER MANAGEMENT and UTILITIES functions.

Network Segmentation

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

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

Maintain an Information Security Program

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

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

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

Payment Application Initial Setup & Configuration

As Sierra Server is factory installed onto Unitec proprietary hardware products, there's no field installation of software required and minimal set-up. To ensure compliance with PCI-DSS, the merchant must remember to reset the default password for the Administrative account.