Sierra Server

Version: 1.79.X.X

PA-DSS 3.2 Implementation Guide

Document Version: 2021

Date: April 23, 2021

Document Owners

Pamela Kellman

Technical Writer

Unitec, LLC.

Confidential Information

The information contained in this document is Unitec Inc. confidential. Distribution of this document outside of Unitec, LLC. is strictly prohibited. Do not copy or distribute without the permission of the Chief Technology Officer.

Table of Contents

Notice 3
About this Document 4
Revision Information 5
Executive Summary 6
Application Summary 7
Typical Network Implementation 10
Credit/Debit Cardholder Dataflow Diagram 11
Difference between PCI Compliance and PA-DSS Validation 13
Considerations for the Implementation of Payment Application in a PCI-Compliant Environment 14
Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4) 14
Handling of Sensitive Authentication Data (PA-DSS 1.1.5) 14
Secure Deletion of Cardholder Data (PA-DSS 2.1) 14
All PAN is Masked by Default (PA-DSS 2.2) 15
Cardholder Data Encryption & Key Management (PA-DSS 2.3, 2.4, and 2.5) 15
Removal of Historical Cryptographic Material (PA-DSS 2.6) 15
Set up Strong Access Controls (3.1 and 3.2) 15
Properly Train and Monitor Admin Personnel 17
Log settings must be compliant (PA-DSS 4.1.b, 4.4.b) 17
PCI-Compliant Wireless settings (PA-DSS 6.1.a and 6.2.b) 18
Services and Protocols (PA-DSS 8.2.c) 19
Never store cardholder data on internet-accessible systems (PA-DSS 9.1.c) 19
PCI-Compliant Remote Access (10.1) 19
PCI-Compliant Delivery of Updates (PA-DSS 10.2.1.a, 7.2.3) 20
PCI-Compliant Remote Access (10.2.3.a) 22
Data Transport Encryption (PA-DSS 11.1.b) 22
PCI-Compliant Use of End User Messaging Technologies (PA-DSS 11.2.b) 23
Network Segmentation 23
Maintain an Information Security Program 24
Payment Application Initial Setup & Configuration 24
Appendix A: Addressing Inadvertent Capture of PAN 25
Addressing Inadvertent Capture of PAN on WINDOWS OS 25

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 PCI PA-DSS and DSS.

The retailer may undertake activities that may affect compliance. For this reason, Unitec, LLC. 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 Server 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 3.2 dated June 2016)[1].

Unitec, LLC. instructs and advises its customers to deploy Unitec, LLC. applications in a manner that adheres to the PCI Data Security Standard (v3.2). 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 Server installation to support your PCI DSS compliance efforts.

[1] PCI PA-DSS 3.2 can be downloaded from the PCI SSC Document Library.

Revision Information

Name	Version	Date of Update	Summary of Changes
Will Severe	2017	1-July-2017	Release for 2017 under PA-DSS 3.2
Will Severe	2018	1-July-2018	Annual review of document. Increment Application Version to 1.77.X.X
Will Severe	2019	1-May-2019	Annual review of document. Increment Application Version to 1.78.X.X. Add info on Remote Software Update option.
John Williams	2020	1-Feb-2020	Increment Application Version to 1.79.X.X. • Revised versioning scheme Annual review of document.
Pamela Kellman	2021	8-April-2021	Increment Application Version to 1.79.X.X. Add info on: • Addition of BeyondTrust Remote Access support button • Encryption change from 128- to 256-bit • Addition of payment processors • Win10 support
John Williams	2021	23-April-2021	Address updates requested by Coalfire QSA

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 SUPPORT section of the Unitec WEB site at www.startwithunitec.com.

Unitec, LLC notifies our distribution network of changes, releases, and corresponding documentation, including this Implementation Guide, in the following ways:

- Website Updates
- Manual Updates
- Product Bulletins
- “Word of Mouth” via our Commercial Channel with regularly scheduled calls /updates with our Distribution network
- Will be sent via email upon request

Executive Summary

Sierra Server 1.79.X.X has been Payment Application - Data Security Standard (PA-DSS) validated, in accordance with PA-DSS Version 3.2. For the PA-DSS assessment, we worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PAQSA):

COALFIRE

Coalfire Systems, Inc. 11000 Westmoor Circle, Suite 450, Westminster, CO 80021	Coalfire Systems, Inc. 1633 Westlake Ave N #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 Unitec, LLC.'s Sierra Server Version 1.79.X.X as a PA-DSS validated Application operating in a PCI DSS 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 Card Industry Payment Applications - Data Security Standard (PCI PA-DSS)
  https://www.pcisecuritystandards.org/security_standards/index.php

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

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

- Center for Internet Security (CIS) Benchmarks (used for OS Hardening)
  https://benchmarks.cisecurity.org/downloads/multiform/

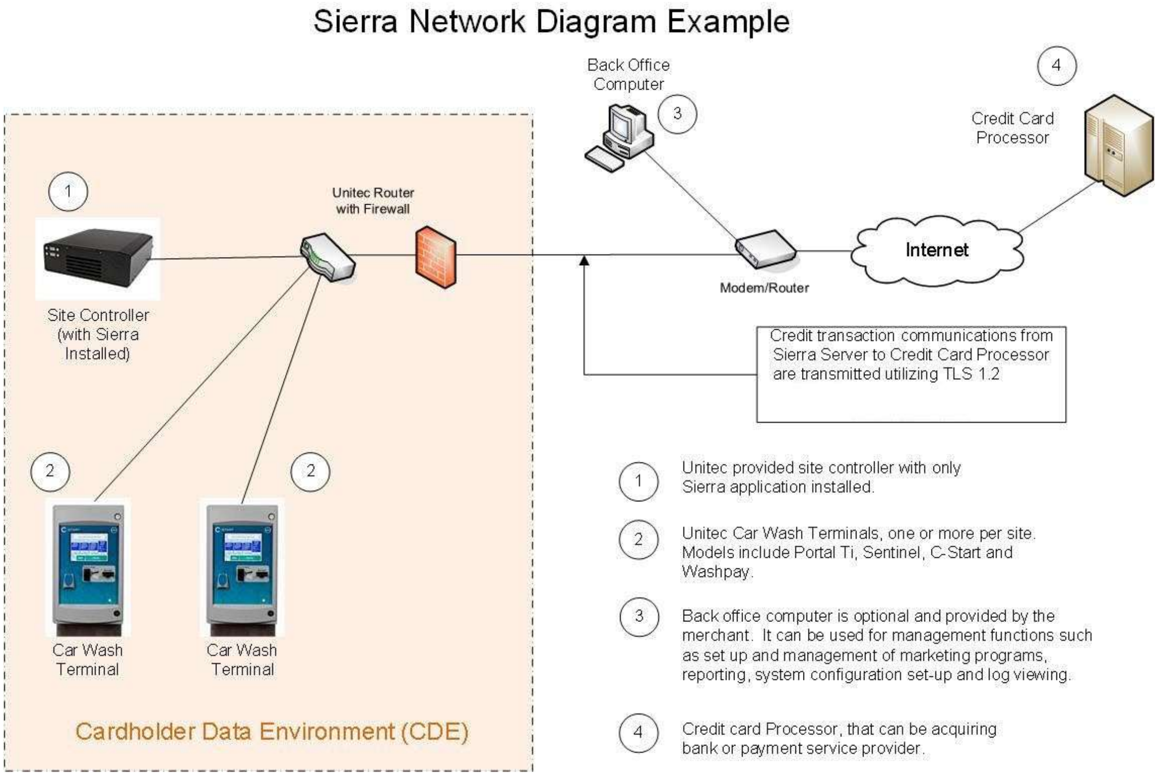
Application Summary

<table>
<tr><td><b>Payment Application Name</b></td><td>Sierra Server</td><td><b>Payment Application Version</b></td><td>1.79.X.X</td></tr>
<tr><td><b>Application Description</b></td><td colspan="3">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 Embedded POSReady 7 and Windows 10 Operating Systems.</td></tr>
<tr><td><b>Typical Role of Application</b></td><td colspan="3">Sierra Server was designed for use in the Automatic Car Wash market</td></tr>
<tr><td><b>Target Market for Payment Application</b></td><td colspan="3">
<table>
<tr><td colspan="6"><b>Target Market for Payment Application (check all that apply)</b>:</td></tr>
<tr><td>X</td><td>Retail</td><td></td><td>Processors</td><td>X</td><td>Gas/Oil</td></tr>
<tr><td></td><td>e-Commerce</td><td>X</td><td>Small/medium merchants</td><td></td><td></td></tr>
<tr><td></td><td colspan="5">Others (please specify):</td></tr>
</table>
</td></tr>
<tr><td rowspan="4"><b>Stored Cardholder Data</b></td><td colspan="3">The following is a brief description of files and tables that store cardholder data:</td></tr>
<tr><td colspan="2">File or Table Name</td><td>Description of Stored Cardholder Data</td></tr>
<tr><td colspan="2">No card holder data is stored by the application.</td><td>N/A</td></tr>
<tr><td colspan="3"><b>Individual access to cardholder data is logged as follows:</b>
Card holder data is not retained or accessible at any time.</td></tr>
<tr><td rowspan="2"><b>Components of the Payment Application</b></td><td colspan="3">The following are the application-vendor-developed components which comprise the payment application:</td></tr>
<tr><td colspan="3">Sierra Server 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).</td></tr>
<tr><td rowspan="2"><b>Required Third-Party Payment Application Software</b></td><td colspan="3">The following are additional third-party <u>payment application</u> components required by the payment application:</td></tr>
<tr><td colspan="3">None</td></tr>
<tr><td rowspan="2"><b>Database Software Supported</b></td><td colspan="3">The following are database management systems supported by the payment application:</td></tr>
<tr><td colspan="3">Sierra Server databases use SQL Express 2012 database software</td></tr>
<tr><td></td><td colspan="3">The following are other required third-party software components required by the payment application:</td></tr>
</table>

Other Required Third Party Software	.Net Framework version 4.5 (Microsoft) IIS Version 7.5 (Microsoft) Director Enterprise Reporting and Management System (SaaS) from Unitec (optional to support Remote Software Updating)
Required Hardware	The following are Hardware Systems required by the payment application:
	Unitec Portal TI Kiosk Unitec Sentinel Kiosk Unitec C-Start Kiosk Unitec Washpay Paynode **PTS Devices** EMV for Canada on Moneris • Verifone UX100, UX300/UX301 and UX400/UX401 EMV for USA on Chase Payment (Datacap and Bluefin) • IDTech VP6800 EMV on Payment Express (Windcave) • Windcave SCR200 Reader, SKP200 Secure Key Pad and BRF210 Contactless NFC antenna
Operating System(s) Supported	The following are Operating Systems supported or required by the payment application:
	Windows Embedded POSReady 7 Windows 10
Application Authentication	The Sierra Server application is accessed via a set of web pages, the Sierra Management Interface, which are hosted on the system where the application is running. Access is controlled by a username/password authentication mechanism which follows PA-DSS 3.2. Passwords are protected by using the SHA-512 hash function in conjunction with a cryptographically secure pseudo-random number generated 64-byte salt (new salt per password creation), and stored in the SQL database.
Application Encryption	Sierra Server utilizes a 256-bit implementation of the Rijndael Algorithm to encrypt cardholder data in transit, as well as while in RAM. CHD is never written to any database or file storage location.

<table>
<tr><td><b>Application Functionality Supported</b></td><td><b>Payment Application Functionality (check only one):</b><table>
<tr><td></td><td>Automated Fuel Dispenser</td><td>X</td><td>POS Kiosk</td><td></td><td>Payment Gateway/Switch</td></tr>
<tr><td></td><td>Card-Not-Present</td><td></td><td>POS Specialized</td><td></td><td>Payment Middleware</td></tr>
<tr><td></td><td>POS Admin</td><td></td><td>POS Suite/General</td><td></td><td>Payment Module</td></tr>
<tr><td></td><td>POS Face-to-Face/POI</td><td></td><td>Payment Back Office</td><td></td><td>Shopping Cart & Store Front</td></tr>
</table></td></tr>
<tr><td><b>Payment Processor Options:</b></td><td>Sierra Server communicates with card processors via:
• TLS 1.2
• or third-party middleware (such as DSIClientX for IP Tran-LT)</td></tr>
<tr><td><b>Description of Listing Versioning Methodology</b></td><td>Unitec uses a Major-Minor-Quarter-Revision versioning scheme, such as <b>X.YY.Z.abcd</b>
• X – The major version number. Updates only when major changes, like an entire re-design of a significant portion of the solution are made. These changes require a full PA-DSS validation.
• YY – An incremental, minor portion of the version number. These changes require a no-impact, low-impact, or high-impact change PA-DSS validation.
• Z – An incremental revision counter. This is a Wildcard incremented for changes that do not require PA-DSS validation.
• abcd – Source code build counter. Always available, but not displayed anywhere for official, proper releases. This is a Wildcard incremented for changes that do not require PA-DSS validation.</td></tr>
<tr><td><b>Resellers</b></td><td>Unitec partners with partners with a Distribution network, providing them with training and support for everything from simple tasks and installation to diagnosing the most complex issues in the field. To complement the service our Distributors provide, we have expanded our technical support to provide direct Operator Support with three different levels of phone support available.</td></tr>
</table>

Typical Network Implementation



Sierra Network Diagram Example

Credit transaction communications from Sierra Server to Credit Card Processor are transmitted utilizing TLS 1.2

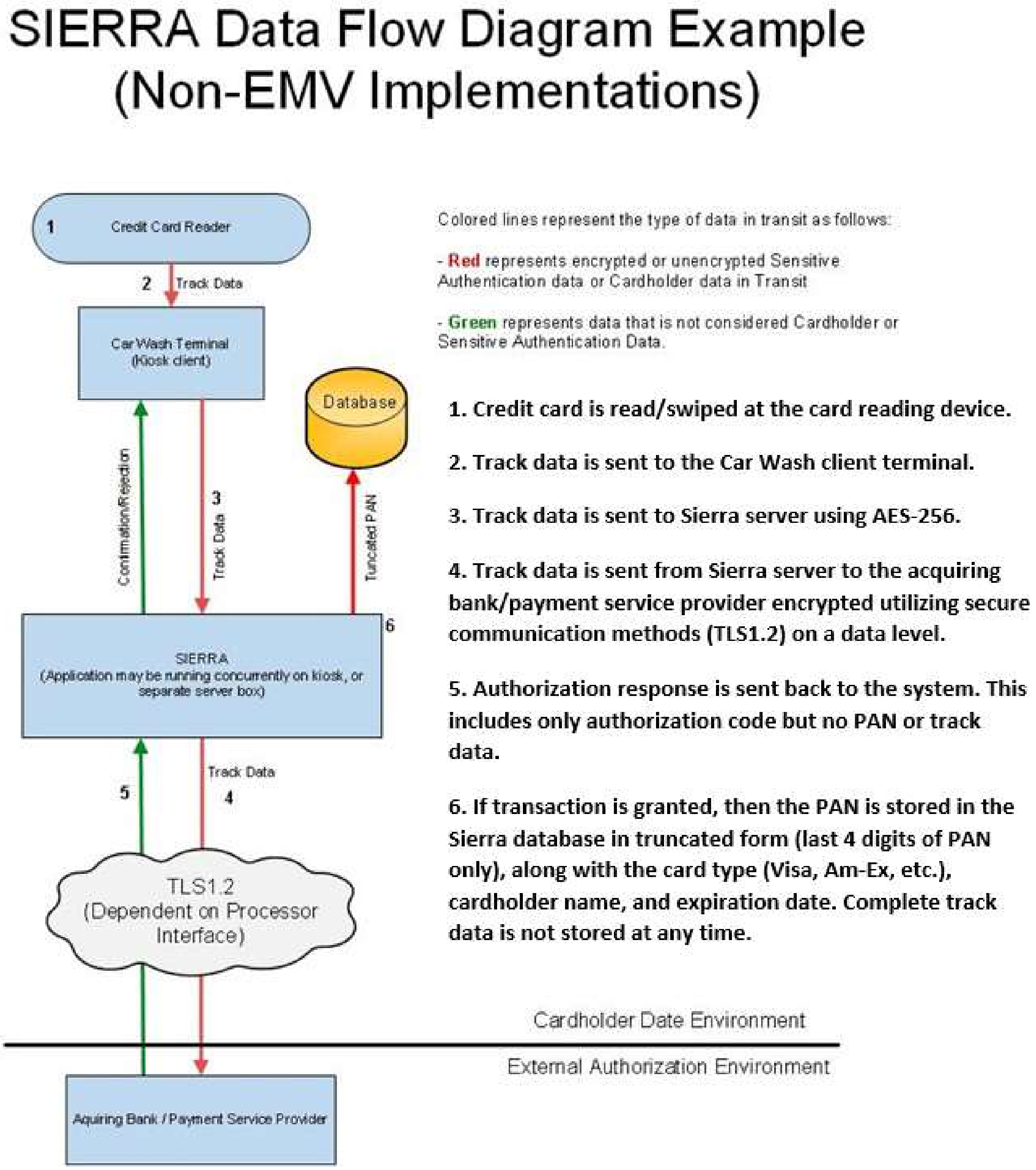
1 Unitec provided site controller with only Sierra application installed.

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.

Credit/Debit Cardholder Dataflow Diagram



SIERRA Data Flow Diagram Example
(Non-EMV Implementations)

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 using AES-256.

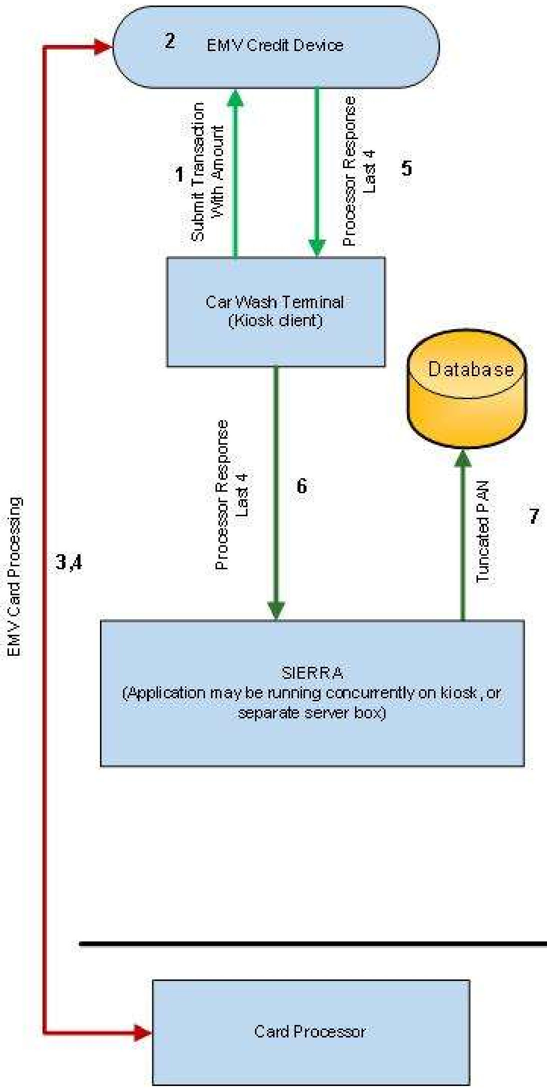
4. Track data is sent from Sierra server to the acquiring bank/payment service provider encrypted utilizing secure communication methods (TLS1.2) on a data level.

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 of PAN only), along with the card type (Visa, Am-Ex, etc.), cardholder name, and expiration date. Complete track data is not stored at any time.

1
Credit Card Reader
2
Track Data
Car Wash Terminal
(Kiosk client)
Database
Confirmation/Rejection
3
Track Data
Tuncated PAN
6
SIERRA
(Application may be running concurrently on kiosk, or separate server box)
5
Track Data
4
TLS1.2
(Dependent on Processor Interface)
Cardholder Date Environment
External Authorization Environment
Aquiring Bank / Payment Service Provider

SIERRA Data Flow Diagram Example (EMV Implementation)



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. Kiosk client submits transaction with amount to EMV Credit Device

2. EMV Card Data is entered at EMV Credit Device

3. EMV Credit Device immediately encrypts and forwards CHD to the Card Processor

4. Card Processor sends authorization response back to EMV Credit Device

5. EMV Credit Device forwards processor response and truncated PAN (last 4 digits of PAN only) to Kiosk Client

6. Kiosk Client forwards processor response and truncated PAN to Sierra Server Application

7. If transaction is granted then the truncated PAN is stored in the Sierra database along with the Card Type (VISA, AMEX etc..), Cardholder Name and, Expiration Date. Complete Track data is not stored at any time.

Cardholder Date Environment

External Authorization Environment

Difference between PCI Compliance and PA-DSS Validation

As a software vendor who develops payment applications, our responsibility is to be "PA-DSS Validated." We have performed an assessment and payment application validation review with our independent assessment firm (PAQSA), to ensure that our platform does conform to industry best practices when handling, managing and storing payment related information.

PA-DSS Version 3.2 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 called the Cardholder Data Environment (CDE).

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

The PA-DSS Validation is intended to ensure that Sierra Server will help you facilitate and maintain PCI Compliance with respect to how the 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 and Systems

1. *Install and maintain a firewall configuration to protect cardholder data*
2. *Do not use vendor-supplied defaults for system passwords and other security parameters*

Protect Cardholder Data

3. *Protect stored cardholder data*
4. *Encrypt transmission of cardholder data across open, public networks*

Maintain a Vulnerability Management Program

5. *Protect all systems against malware and regularly update anti-virus software or programs*
6. *Develop and maintain secure systems and applications*

Implement Strong Access Control Measures

7. *Restrict access to cardholder data by business need-to-know*
8. *Identify and authenticate access to system components*
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 for all personnel

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.

- ✓ Remove Historical Sensitive Authentication Data
- ✓ Handling of Sensitive Authentication Data
- ✓ Secure Deletion of Cardholder Data
- ✓ All PAN is masked by default
- ✓ Cardholder Data Encryption & Key Management
- ✓ Removal of Historical Cryptographic Material
- ✓ Set up Strong Access Controls
- ✓ Properly Train and Monitor Admin Personnel
- ✓ Log settings must be compliant

Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4)

Sierra Server never stores sensitive authentication data.

Handling of Sensitive Authentication Data (PA-DSS 1.1.5)

Unitec Sierra Server does not collect or 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 used for pre-authorization (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

Secure Deletion of Cardholder Data (PA-DSS 2.1)

Sierra Server does not store cardholder data and therefore there is no data to be purged by the application as required by PA-DSS v3.2.

Any cardholder data you store outside of the application must be documented and you must define a retention period at which time you will securely delete (render irretrievable) the stored cardholder data. When defining a retention period, you must take into account legal, regulatory, or business purpose.

All underlying software (this includes operating systems and/or database systems) must be configured to prevent the inadvertent capture of PAN. Instructions for configuring the underlying operating systems and/or databases can be found in **Appendix A**.

All PAN is Masked by Default (PA-DSS 2.2)

Sierra Server does not have the ability to display full PAN for any reason and therefore there is no configuration details to be provided as required for PA-DSS v3.2. Truncated PAN, limited to last 4 digits, can be found in the following locations:

- SQL Database (Unitec.mdf, DeferredPayment and HotFile tables) – Last 4 digits only.
- Application Logs (Unitec.Siteserver_yyyy-mm-dd.log, Unitec.CStart_yyyy-mm-dd.log) – Truncated PAN as either "*"+ last 4 digits, or only last 4.
- Customer receipts – Last 4 digits only.
- Transaction Reports (summary and detail) – Last 4 digits only.

Cardholder Data Encryption & Key Management (PA-DSS 2.3, 2.4, and 2.5)

Sierra Server 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 v3.2.

Removal of Historical Cryptographic Material (PA-DSS 2.6)

Sierra Server 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 and 3.2)

The PCI DSS requires that access to all systems in the payment processing environment, including all PCs, servers, and databases with cardholder data or with payment applications, 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.

The following roles within the application have administrative access:

- User Management
- Utilities (including access to the credit mode setup parameters and any other PCI-related setup)

All authentication credentials are generated and managed by the application. Secure authentication is enforced automatically by the payment application for all credentials by 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). To maintain PCI DSS compliance the following 11 points must be followed per the PCI DSS:

1. The payment application must not use or require the use of default administrative accounts for other necessary or required software (for example, database default administrative accounts) (PCI DSS 2.1 / PA-DSS 3.1.1)
2. The payment application must enforce the changing of all default application passwords for all accounts that are generated or managed by the application, by the completion of installation and for subsequent changes after the installation (this applies to all accounts, including user accounts, application and service accounts, and accounts used by Unitec, LLC. for support purposes) (PCI DSS 2.1 / PA-DSS 3.1.2)
3. The payment application must assign unique IDs for all user accounts. (PCI DSS 8.1.1 / PA-DSS 3.1.3)
4. The payment application must provide at least one of the following three methods to authenticate users: (PCI DSS 8.2 / PA-DSS 3.1.4)
    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
5. The payment application must NOT require or use any group, shared, or generic accounts and passwords (PCI DSS 8.5 / PA-DSS 3.1.5)
6. The payment application requires passwords to be at least 7 characters and includes both numeric and alphabetic characters (PCI DSS 8.2.3 / PA-DSS 3.1.6)
7. The payment application requires passwords to be changed at least every 90 days (PCI DSS 8.2.4 / PA-DSS 3.1.7)
8. The payment application keeps password history and requires that a new password is different than any of the last four passwords used (PCI DSS 8.2.5 / PA-DSS 3.1.8)
9. The payment application limits repeated access attempts by locking out the user account after not more than six logon attempts (PCI DSS 8.1.6 / PA-DSS 3.1.9)
10. The payment application sets the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. (PCI DSS 8.1.7 / PA-DSS 3.1.10)
11. The payment application requires the user to re-authenticate to re-activate the session if the application session has been idle for more than 15 minutes. (PCI DSS 8.1.8 / PA-DSS 3.1.11)

Sierra Server is shipped with a factory default Administrative account. Upon first login with default user credentials, the user will be prompted and required to change the account password. Once the new admin account is created, the default admin account can and should be deleted. The password for this account can be changed at any time as follows:

1. After log-in, select SET-UP from the main menu options
2. Select USERS from the sub-menu that's shown on the left side of the page
3. 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.
4. 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 5 passwords used).

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.

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

4.1.b: Sierra Server 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 Server in any way will result in non-compliance with PCI DSS. Logs may be accessed by:

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.

Implement automated assessment trails for all system components to reconstruct the following events:

PCI Requirement
10.2.1 All individual user accesses to cardholder data from the application
10.2.2 All actions taken by any individual with administrative privileges in the application
10.2.3 Access to application audit trails managed by or within the application
10.2.4 Invalid logical access attempts
10.2.5 Use of the application's identification and authentication mechanisms (including but not limited to creation of new accounts, elevation of privileges, etc.) and all changes, additions, deletions to application accounts with root or administrative privileges
10.2.6 Initialization, stopping, or pausing of the application audit logs
10.2.7 Creation and deletion of system-level objects within or by the application

Record at least the following assessment trail entries for all system components for each event from 10.2.x above:

PCI Requirement
10.3.1 User identification
10.3.2 Type of event
10.3.3 Date and time
10.3.4 Success or failure indication
10.3.5 Origination of event
10.3.6 Identity or name of affected data, system component, or resource.

Disabling or subverting the logging function of Sierra Server in any way will result in non-compliance with PCI DSS.

4.4.b: Sierra Server facilitates centralized logging.

Payment application logs required per the PA-DSS can be retrieved through the Sierra Management Application and saved on to a thumb drive or other media for use in a centralized logging system. Sierra Server 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 and navigating through the Management application, refer to the Sierra Server User's Manual.

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

Sierra Server 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:

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

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.

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.

Services and Protocols (PA-DSS 8.2.c)

Sierra Server does not require the use of any insecure services or protocols. In addition to the default services that come with Windows, Sierra requires the following Microsoft services and protocols:

- Application Host Helper Service
- Client for NFS
- Dialog Box Filter
- Keyboard Filter
- LPD Service
- Message Queuing
- Message Queuing Triggers
- Net.Msmq Listener Adapter
- Net.Pipe Listener Adapter
- Net.Tcp Listener Adapter
- RIP Listener
- Simple TCP/IP Services
- SQL Server (SQLEXPRESS)
- SQL Server VSS Writer
- Windows Process Activation Service
- WinHTTP Web Proxy Auto-Discovery ServiceWorkstation

And the following non-Microsoft services:

- EasyMail SMTP Express (Email delivery system)
  - For sending application alerts and status. Sensitive data (PAN, consumer details) is never included.
- Site Server (The Sierra server)
- Tbupddwu (Touch screen driver)

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

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

For customers who wish to enable access from the Internet to the Sierra Management Application, the system must be installed behind a properly configured firewall, with port 9810 forwarded to the Sierra Server host system for TCP (HTTP) communications. It is not recommended to configure the system to a DMZ.

Incoming 9810 will support HTTP access to the web page. Outbound traffic will be limited to encrypted credit transactions (TLS1.2), and possibly outgoing email messages.

PCI-Compliant Remote Access (10.1)

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 Server does not accommodate remote access by default but does allow Remote Desktop (RD) or BeyondTrust Remote Access to be temporarily enabled for troubleshooting purposes. This action requires an Administrative password for Sierra Server access (Something you know) and a unique activation code (or token) that is issued by Unitec (something you have). The activation code is valid for one day only.

Unitec uses the BeyondTrust Remote Access platform to remotely support our customers. Only Unitec employees have access to the BeyondTrust Remote Access platform which is configured to authenticate utilizing Duo's mutli-factor authentication. BeyondTrust Remote Access supports the following security features:

- Duo multi-factor authentication
- Encryptions of non-console access to the cardholder data environment using SSH, VPN, or TLS
- Automatic software and configuration updates
- Security logs configuration to include reports and screen scrape type detail
- IP Address-based restrictions to only allow access from Unitec controlled assets
- Unlimited remote computer access by DRB In Bay Support personnel
- A secure, maintainable installation that can be PCI DSS-compliant.

BeyondTrust Remote Access automatically logs a user out after 15 minutes of inactivity. Once disconnected after 15 minutes, the user is required to re-authenticate.

PCI-Compliant Delivery of Updates (PA-DSS 10.2.1.a, 7.2.3)

Unitec delivers patches and updates 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 regularly testing Sierra Server with a security scanning tool (such as Nessus Vulnerability Scanner). Once we identify a relevant vulnerability, we work to develop & test a product update that helps protect Sierra Server against the specific, new vulnerability.

In most cases, the update will require a change to the Windows Operating System (OS) and depend on associated patches issued by Microsoft. These patches are incorporated by Unitec, tested and released as a new OS version. When a new OS version is released, an update program (or utility) is developed for applying the OS update to previously deployed units. New OS versions and update programs are issued quarterly, and all resellers and customers are notified of release and availability via Unitec's website, www.startwithunitec.com, as well as electronics newsletters and direct mailings.

Unitec offers two methods of delivery for updates to the Sierra Application. For most customers, software updates are provided as a utility that's loaded onto a USB thumbdrive that can be ordered from Unitec, LLC. Sierra Server uses a digital signature technique based on a salted SHA-

512 hash of the utility contents to ensure the integrity of an update program. This security measure ensures any update applied to Sierra Server is from a known and trusted source and eliminates the possibility of installing invalid files or programs.

The process for manually installing a software update is as follows:

1. Acquire the update program from your Unitec distributor (USB Thumb Drives containing the update utility are ordered and shipped from Unitec, LLC. via UPS/FedEx/USPS).

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

5. To restart Sierra Server (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).

Customers who subscribe to the Unitec Director Enterprise Management System have the option of receiving Sierra Application updates delivered directly via a secure download. These update MSI packages are secured by using a Microsoft Authenticode signing certificate from DigiCert which provides information to authenticate the signer as well as to ensure that the software has not been subsequently modified. The signature includes the company's details, payload hash and timestamp information.

The MSI update's build & packaging process has a work flow to create a payload with a file name structure of Connector_<Major>.<Minor>.<Build>.<Revision>.msi. The final phase of the build pipeline securely fetches the public key and password from an Azure Key Vault and uses Microsoft Signtool.exe to sign the package with SHA-256 algorithm and time stamp. The signed package is uploaded by Unitec into the Director cloud and scheduled to be installed per site. The Sierra Server at each location polls the Director cloud for any available update and if one is found, it downloads a zip file which includes the MSI package and a scheduler file containing details of how to apply the updater.

The downloaded package will be placed in a local "staging" folder, extracted, and the MSI package checked for the proper MSI header signature (to make sure it is a valid MSI package) and to verify the secure signature using Microsoft "WinVerifyTrust" API.

If the MSI verification is successful, the site server will repackage the MSI and scheduler files as a new ZIP and broadcast the package to all connected Sierra systems. Each system will then repeat the verification process before applying the update.

If the MSI verification fails, then both the MSI package and the downloaded zip will be deleted immediately from the staging folder, and an entry will be logged to indicate that the package failed security validation.

PCI-Compliant Remote Access (10.2.3.a)

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, etc. to access other hosts within the payment processing environment, special care must be taken.

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). 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 Server allows Remote Desktop or BeyondTrust Remote Access 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 TLS 1.2 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). Only trusted keys and/or certificates are utilized.

PCI DSS requirement 4.1: Use strong cryptography and security protocols such as transport layer security (TLS 1.2) 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 Server.

Sierra Server is not designed or developed to use any wireless components.

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

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

PCI requires that cardholder information sent via any end user messaging technology must use strong encryption of the data.

Non-console administration and Multi-Factor Authentication (PA-DSS 12.1, 12.2)

Although Sierra Server does not support non-console administration and we do not recommend using non-console administration, should you ever choose to do this, you must use SSH, VPN, or TLS 1.2 or higher for encryption of this non-console administrative access along with a multi-factor authentication solution.

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 Server.

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

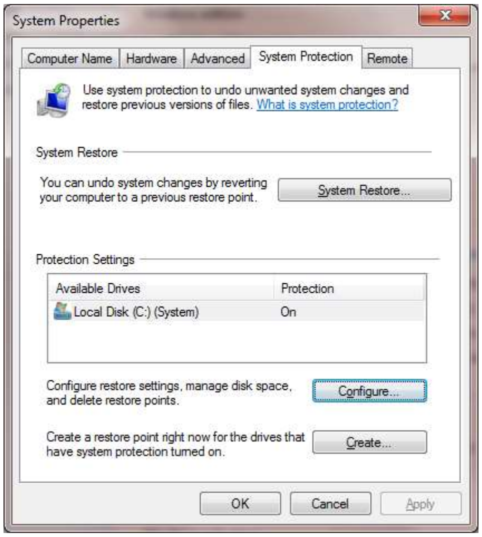
As Sierra Server is factory installed onto Unitec proprietary hardware products, there’s no field installation of software required and minimal set-up. To ensure compliance with PCI-DSS, the merchant must remember to reset the default password for the Administrative account.

Appendix A: Addressing Inadvertent Capture of PAN

Addressing Inadvertent Capture of PAN on WINDOWS OS

Disabling System Restore

- Open File Explorer
- Right-click on **My Computer** or right-click **This PC** and then select **Properties**
- Select **System Protection** on the top-left list. The following screen appears:



Use system protection to undo unwanted system changes and restore previous versions of files. What is system protection?

System Restore

You can undo system changes by reverting your computer to a previous restore point.

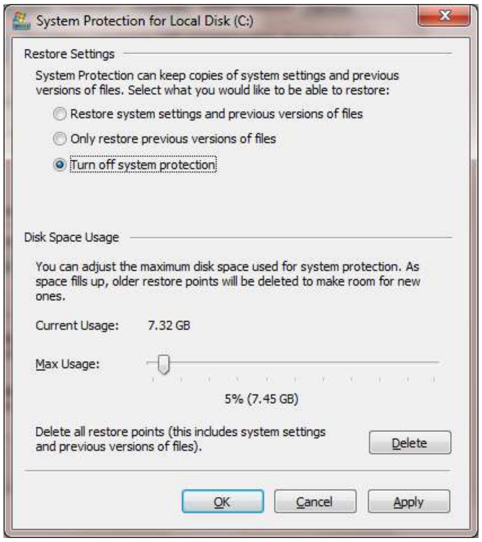
Protection Settings

Available Drives	Protection
Local Disk (C:) (System)	On

Configure restore settings, manage disk space, and delete restore points.

Create a restore point right now for the drives that have system protection turned on.

- Select **Configure**. The following screen appears.



Restore Settings

System Protection can keep copies of system settings and previous versions of files. Select what you would like to be able to restore:

○ Restore system settings and previous versions of files

○ Only restore previous versions of files

● Turn off system protection

Disk Space Usage

You can adjust the maximum disk space used for system protection. As space fills up, older restore points will be deleted to make room for new ones.

Current Usage: 7.32 GB

Max Usage: 5% (7.45 GB)

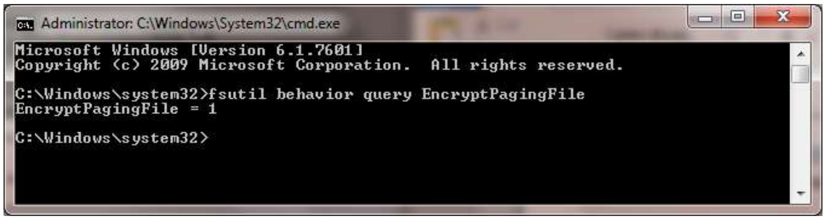
Delete all restore points (this includes system settings and previous versions of files).

- Select **Turn off system protection**.
- Click **Apply**, and **OK** to close the **System Protection** window.
- Click **OK** again to close the **System Properties** window.
- Reboot the computer.

Encrypting PageFile.sys

* Please note that in order to perform this operation, the hard disk must be formatted using NTFS.

- Open Command Prompt.
    - Win 7: Click on the Windows “Orb” and in the search box type in **cmd**
    - Win 10: Click on the search icon located on the task bar and type in **cmd**
- Right-click on **cmd.exe** and select **Run as Administrator**.
- To Encrypt the Pagefile, type the following command: **fsutil behavior set EncryptPagingFile 1**

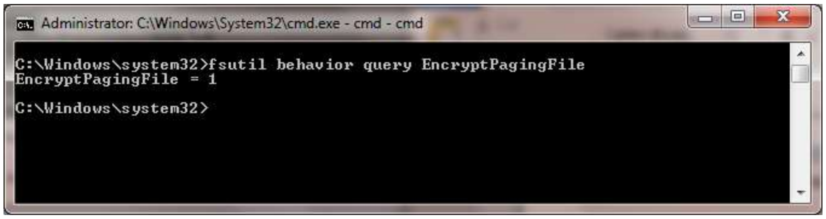


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>fsutil behavior query EncryptPagingFile
EncryptPagingFile = 1

C:\Windows\system32>
```

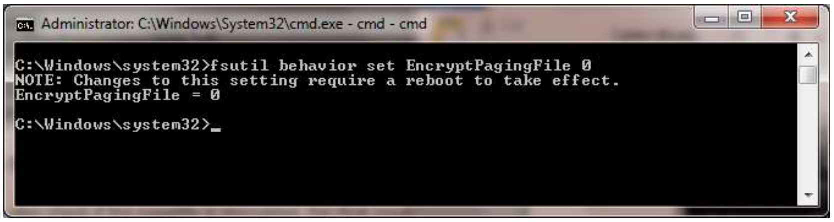
- To verify configuration, type the following command: **fsutil behavior query EncryptPagingFile**



```
C:\Windows\system32>fsutil behavior query EncryptPagingFile
EncryptPagingFile = 1

C:\Windows\system32>
```

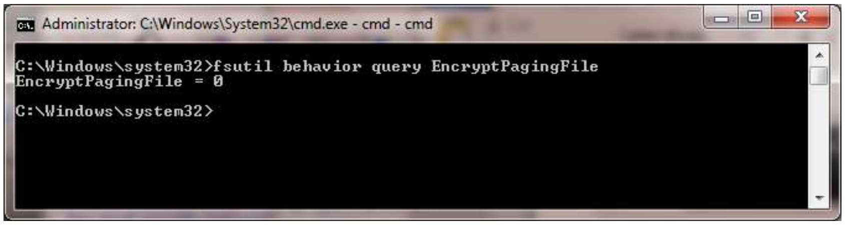
- If encryption is enabled, **EncryptPagingFile = 1** should appear
- In the event you need to disable PageFile encryption, type the following command: **fsutil behavior set EncryptPagingFile 0**



```
C:\Windows\system32>fsutil behavior set EncryptPagingFile 0
NOTE: Changes to this setting require a reboot to take effect.
EncryptPagingFile = 0

C:\Windows\system32>_
```

- To verify configuration, type the following command: **fsutil behavior query EncryptPagingFile**



```
C:\Windows\system32>fsutil behavior query EncryptPagingFile
EncryptPagingFile = 0

C:\Windows\system32>
```

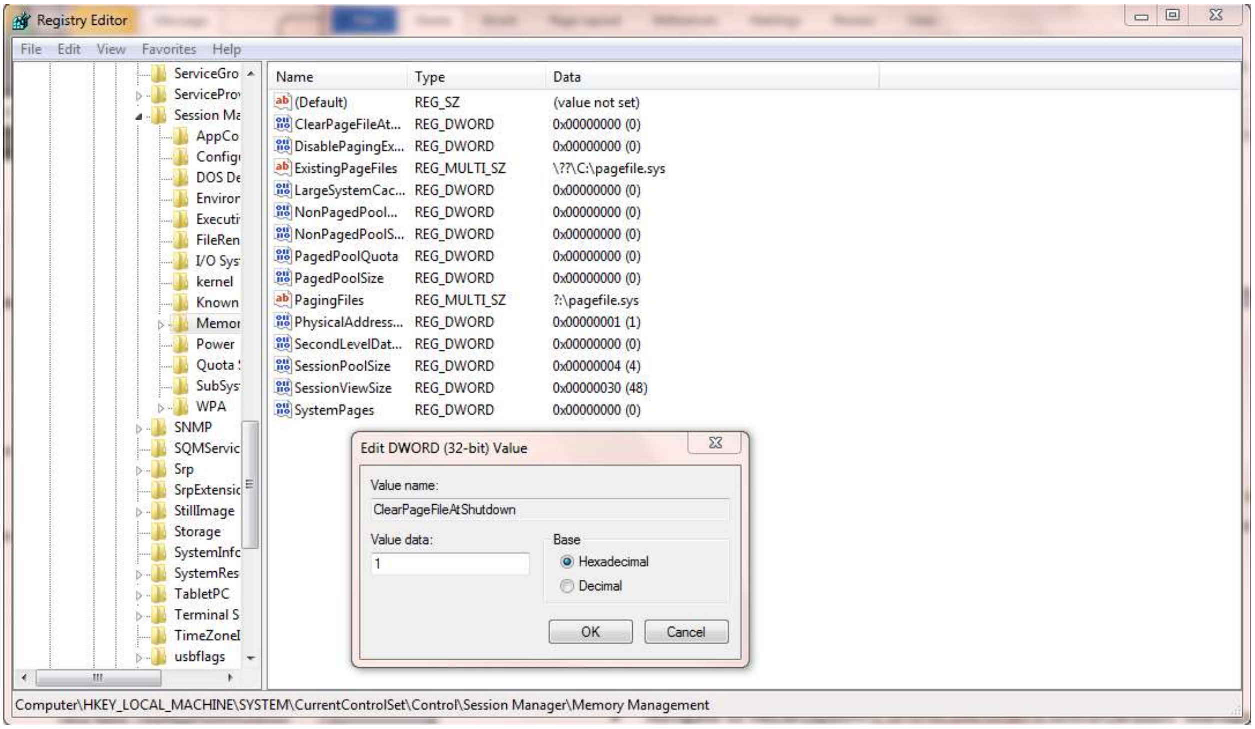
- If encryption is disabled, **EncryptPagingFile = 0** should appear

Clear the System Pagefile.sys on shutdown

Windows can clear the Pagefile.sys upon system shutdown. This will purge all temporary data from the pagefile.sys (temporary data may include system and application passwords, cardholder data (PAN/Track), etc.).

NOTE: Enabling this feature may increase windows shutdown time.

- Open Windows Registry
  - Win 7: Click on the Windows “Orb” and in the search box type in **regedit**
  - Win 10: Click on the search icon located on the task bar and type in **regedit**
- Right-click on **regedit.exe** and select **Run as Administrator**
- Navigate to **HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management**
- Select **ClearPageFileAtShutdown**
- Change the value from **0** to **1**
- Click **OK** and close Regedit



Name	Type	Data
(Default)	REG_SZ	(value not set)
ClearPageFileAt...	REG_DWORD	0x00000000 (0)
DisablePagingEx...	REG_DWORD	0x00000000 (0)
ExistingPageFiles	REG_MULTI_SZ	\??\C:\pagefile.sys
LargeSystemCac...	REG_DWORD	0x00000000 (0)
NonPagedPool...	REG_DWORD	0x00000000 (0)
NonPagedPoolS...	REG_DWORD	0x00000000 (0)
PagedPoolQuota	REG_DWORD	0x00000000 (0)
PagedPoolSize	REG_DWORD	0x00000000 (0)
PagingFiles	REG_MULTI_SZ	?:\pagefile.sys
PhysicalAddress...	REG_DWORD	0x00000001 (1)
SecondLevelDat...	REG_DWORD	0x00000000 (0)
SessionPoolSize	REG_DWORD	0x00000004 (4)
SessionViewSize	REG_DWORD	0x00000030 (48)
SystemPages	REG_DWORD	0x00000000 (0)

Edit DWORD (32-bit) Value

Value name: ClearPageFileAtShutdown

Value data: 1

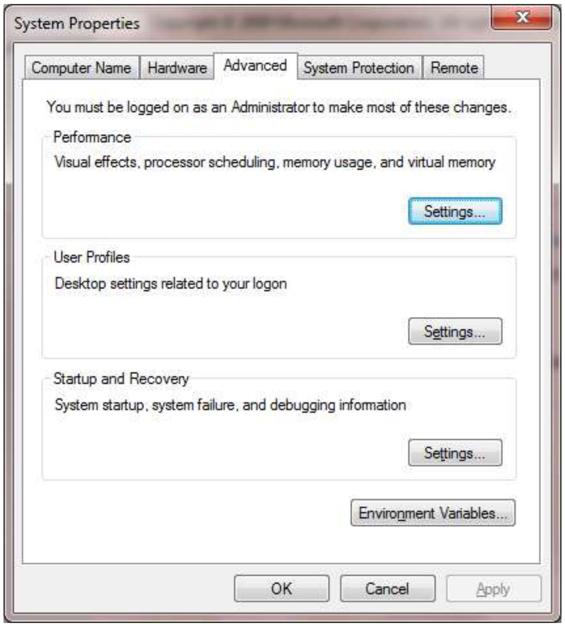
Base: ● Hexadecimal ○ Decimal

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management

- If the value does not exist, add the following:
  - Value Name: **ClearPageFileAtShutdown**
  - Value Type: **REG_DWORD**
  - Value: **1**

Disabling System Management of PageFile.sys

- Open File Explorer
- Right-click on **My Computer** or **This PC** >**Properties**>**Advanced System Settings** on the top-left list. The following screen appears:



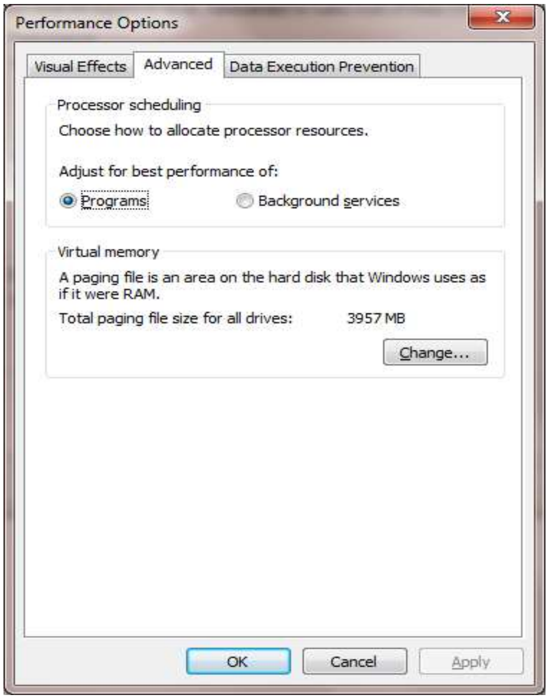
You must be logged on as an Administrator to make most of these changes.

Performance
Visual effects, processor scheduling, memory usage, and virtual memory

User Profiles
Desktop settings related to your logon

Startup and Recovery
System startup, system failure, and debugging information

- Under **Performance**, select **Settings** and navigate to the **Advanced** tab. The following screen appears:

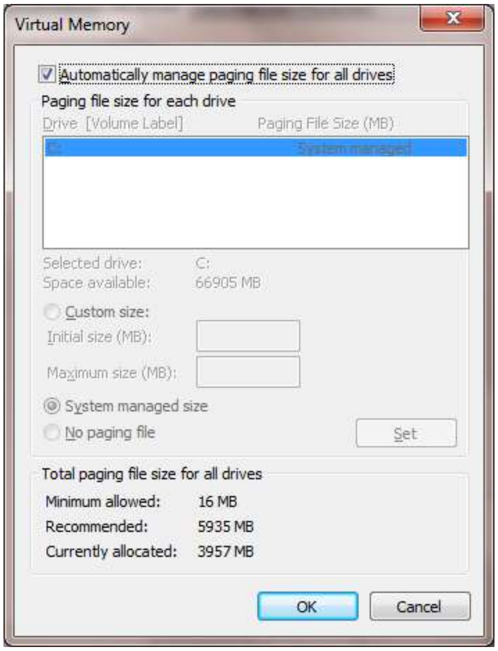


Processor scheduling
Choose how to allocate processor resources.

Adjust for best performance of:
● Programs ○ Background services

Virtual memory
A paging file is an area on the hard disk that Windows uses as if it were RAM.
Total paging file size for all drives: 3957 MB

- Select **Change** under **Virtual Memory**. The following screen appears:



Virtual Memory

☑ Automatically manage paging file size for all drives

Paging file size for each drive

Drive [Volume Label]	Paging File Size (MB)
C:	System managed

Selected drive: C:

Space available: 66905 MB

○ Custom size:

Initial size (MB):

Maximum size (MB):

● System managed size

○ No paging file

Total paging file size for all drives

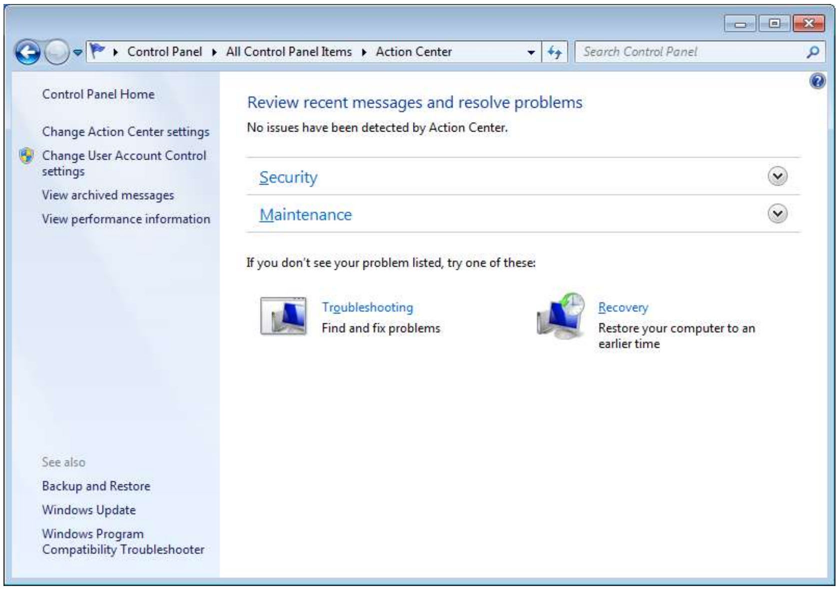
Minimum allowed:	16 MB
Recommended:	5935 MB
Currently allocated:	3957 MB

- Uncheck **Automatically manage page file size for all drives**
- Select **Custom Size**
- Enter the following for the size selections:
  - Initial Size – As a good rule of thumb, the size should be equivalent to the amount of memory in the system.
  - Maximum Size – As a good rule of thumb, the size should be equivalent to twice the amount of memory in the system.
- Click **OK**, **OK**, and **OK**
- You will be prompted to reboot your computer.

Disabling Windows Error Reporting

Win 7

- Open the Control Panel
- Open the Action Center
- Select **Change Action Center Settings**



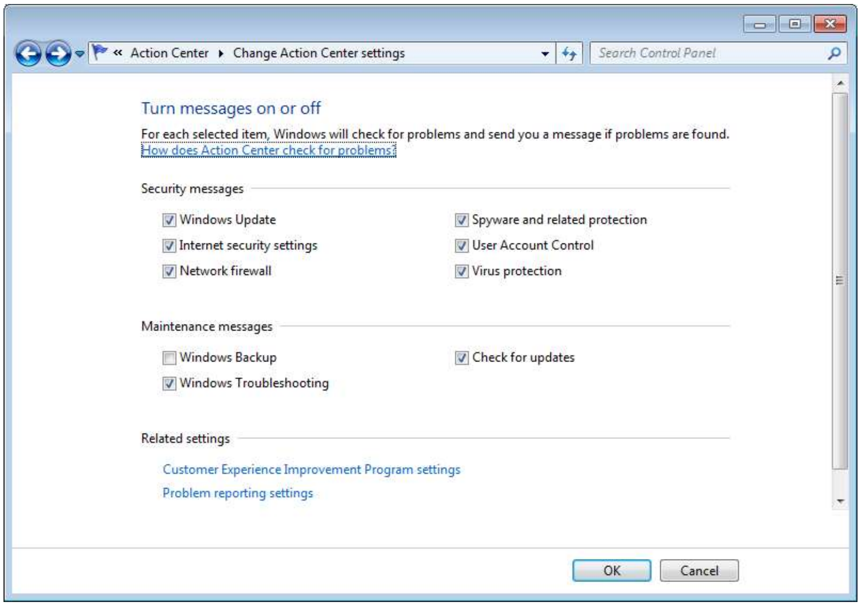
Control Panel ▸ All Control Panel Items ▸ Action Center
Search Control Panel
Control Panel Home
Change Action Center settings
Change User Account Control settings
View archived messages
View performance information
See also
Backup and Restore
Windows Update
Windows Program Compatibility Troubleshooter
Security
Maintenance
Troubleshooting
Find and fix problems
Recovery
Restore your computer to an earlier time

Review recent messages and resolve problems

No issues have been detected by Action Center.

If you don't see your problem listed, try one of these:

- Select **Problem Reporting Settings**



Turn messages on or off

For each selected item, Windows will check for problems and send you a message if problems are found.
How does Action Center check for problems?

Security messages

☑ Windows Update
☑ Internet security settings
☑ Network firewall
☑ Spyware and related protection
☑ User Account Control
☑ Virus protection

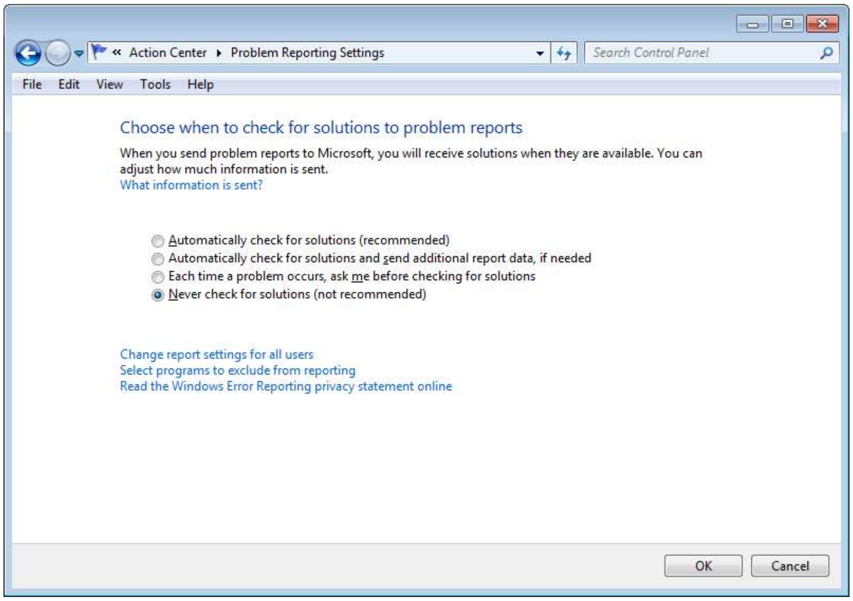
Maintenance messages

☐ Windows Backup
☑ Windows Troubleshooting
☑ Check for updates

Related settings

Customer Experience Improvement Program settings
Problem reporting settings

- Select **Never Check for Solutions**



Choose when to check for solutions to problem reports

When you send problem reports to Microsoft, you will receive solutions when they are available. You can adjust how much information is sent.
What information is sent?

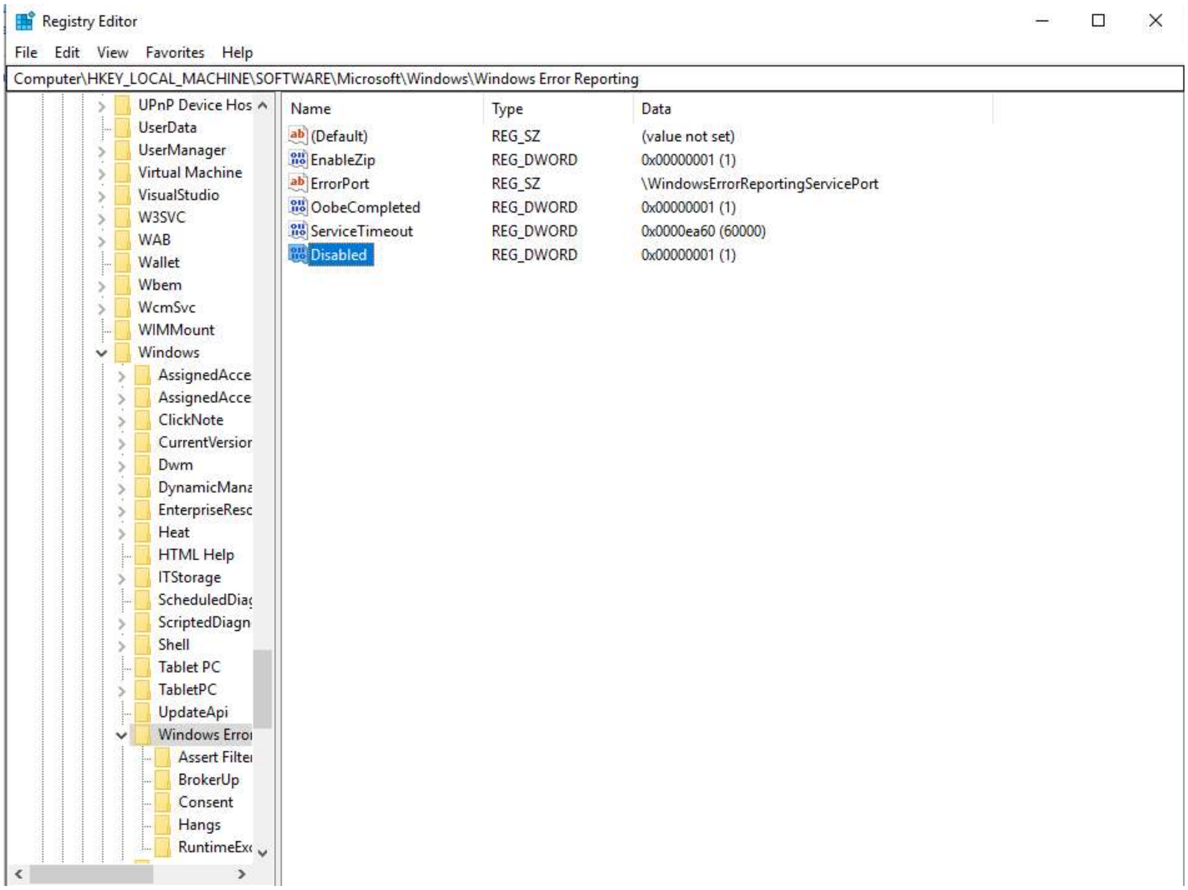
○ Automatically check for solutions (recommended)
○ Automatically check for solutions and send additional report data, if needed
○ Each time a problem occurs, ask me before checking for solutions
● Never check for solutions (not recommended)

Change report settings for all users
Select programs to exclude from reporting
Read the Windows Error Reporting privacy statement online

Win 10

- Open Windows Registry
- Click on the search icon located on the task bar and type in **regedit**
- Right-click on **regedit.exe** and select **Run as Administrator**
- Navigate to **HKLM\Software\Microsoft\Windows\Windows Error Reporting**
- Select **Disabled**
- Change the value from **0** to **1**

- Click **OK** and close Regedit



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting

Name	Type	Data
(Default)	REG_SZ	(value not set)
EnableZip	REG_DWORD	0x00000001 (1)
ErrorPort	REG_SZ	\WindowsErrorReportingServicePort
OobeCompleted	REG_DWORD	0x00000001 (1)
ServiceTimeout	REG_DWORD	0x0000ea60 (60000)
Disabled	REG_DWORD	0x00000001 (1)

- If the value does not exist, add the following:
  - Value Name: **Disabled**
  - Value Type: **REG_DWORD**
  - Value: **1**