GlobalWare

Version: 7.3

PA-DSS 3.2 Implementation Guide

Document Version: 1

Date: 02/14/2017

Document Owners

Julie Simon Ashcraft

Senior Business Analyst – GlobalWare BOS

Travelport

Redefining travel commerce

Confidential Information

The information contained in this document is Travelport confidential. Distribution of this document outside of Travelport is strictly prohibited. Do not copy or distribute without the permission of Travelport.

Table of Contents

Notice

THE INFORMATION IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. TRAVELPORT 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 TRAVELPORT 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 travel agency may undertake activities that may affect compliance. For this reason, Travelport 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 GlobalWare 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].

Travelport instructs and advises its customers to deploy Travelport 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 GlobalWare 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	Title	Date of Update	Summary of Changes
Julie Simon Ashcraft	Sr. Business Analyst	02/14/2017	Initial Version

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. Travelport will distribute the IG to new customers via:

- Ask Travelport secure web site (https://travelport-english.custhelp.com/)
- Distributed with the GlobalWare software
- PDF documentation (printed or e-mailed)

Executive Summary

GlobalWare v7.3 has been reviewed as part of a compliance review in accordance with the Payment Application - Data Security Standard (PA-DSS) Version 3.2. Due to the application's ineligibility to qualify as a payment application under the current PA-DSS guidelines, the application was reviewed for adherence with the PA-DSS standard but cannot be officially listed as a validated PA-DSS payment application. For this assessment, we worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PAQSA):

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 Travelport GlobalWare Version 7.3 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>GlobalWare</td><td><b>Payment Application Version</b></td><td>7.3.0.0100 General Release</td></tr>
<tr><td><b>Application Description</b></td><td colspan="3">GlobalWare is a back office system (BOS) that is used by U.S.-based travel agencies for accounting and reporting. The GlobalWare database is backed up regularly per individual agencies maintenance and business procedures. Purge and archive of data is available within the application.

GlobalWare is not used for any authorization or settlement of credit card payments. However, it can store the credit card number for agencies that have business need for the credit card number (PAN). This data is stored for reconciliation and reporting purposes.

The card holder data is fed into the application through GDS Interfaces, Credit Card Reconciliation Files, and through Invoice Import Files. Cardholder data is only retained for the extent of agencies business need and can be truncated to first 6 and last 4 digits when it is no longer needed. Secure deletion of this data is then facilitated via the application.</td></tr>
<tr><td><b>Typical Role of Application</b></td><td colspan="3">GlobalWare is used in Travel Agencies as a Back Office System (BOS). It is the receiver of payment information for travel records/invoices. It is not used for Point of Sale (POS). GlobalWare is an accounting system used for reporting and business accounting functions.</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></td><td>Retail</td><td></td><td>Processors</td><td></td><td>Gas/Oil</td></tr>
<tr><td></td><td>e-Commerce</td><td></td><td>Small/medium merchants</td><td></td><td></td></tr>
<tr><td>✓</td><td colspan="5">Others (please specify): Travel Agencies</td></tr>
</table>
</td></tr>
<tr><td><b>Stored Cardholder Data</b></td><td colspan="3">
<table>
<tr><td colspan="2">The following is a brief description of files and tables that store cardholder data:</td></tr>
<tr><td>File or Table Name</td><td>Description of Stored Cardholder Data</td></tr>
<tr><td>InvCreditCard</td><td>PAN and Expiry</td></tr>
<tr><td>CCRTransaction</td><td>PAN</td></tr>
<tr><td>CCRAccountCC</td><td>PAN</td></tr>
<tr><td>CustomerCreditCard</td><td>PAN and Expiry</td></tr>
<tr><td colspan="2"><b>Individual access to cardholder data is logged as follows:</b>

Whenever an Agency Employee who has Security rights to view the credit card information views it, a log entry is added to the Admin Access Log.</td></tr>
</table>
</td></tr>
</table>

Components of the Payment Application	The following are the application-vendor-developed components that comprise the payment application:
	Gblware Directory: Houses Sqlany16 folder, CrypKey copy protection files, and all executables and DLLs that are included in GlobalWare Application installation. These are installed in all 3 GlobalWare environments: Standalone, Client, and Server. However, the installation and files for Standalone is the same as for the Server environment. Components that are installed for the GlobalWare application in the *Gblware* directory are listed below in alphabetical order: *AAAQS5.exe:* Specialized report for AAA surveys. *Acctedit.exe:* Utility to clean up/rename/delete GlobalWare Account IDs. *AddDbCmt.exe:* Support Tool for updating comments in the database. *Amadeus.exe:* Interface for Amadeus GDS. *Apollo.exe:* Interface for Apollo GDS. *ChartVal.exe:* Validation with report for Processing Table combinations Sale/Settle/Revenue types. *ChgAcPer.exe:* Support tool to change accounting periods when incorrectly input at yearend close. *ChgDbVer.exe:* Support tool to change DB version number back, when the database upgrade did not go to completion. *CreateODBC.exe:* Utility used for adding ODBC configurations for 3rd Party Access to GlobalWare table views. *DeleteDupeIndexes.exe:* Support Tool used to delete duplicate indexes from 24 tables within the database. *EditUserView.exe:* Agency DBA utility for direct access to Database Table Views. *FixComDt.exe:* Support tool used to fix commission received date on invoices. *Fxcvduez.exe:* Support tool used to fix converted payment records. *Fxinvpmt.exe:* Support tool used to fix converted payment records. *FxProvPd.exe:* Support tool used to fix Imported items for commission overpayments to show that payment flag as received. *FxSegOX.exe:* Utility used to fix segment connection information. *Gblware.exe:* Main Application. *Gwdbupd.exe:* Database update utility during upgrades. *GwDbVal.exe:* Database Validation with Report for DB integrity. *GwRecovr.exe:* Utility for unloading and reloading the DB (re-indexing). *Gwrestore.exe:* Utility for restoring a Standalone zipped backup of the database and log file, interface files, and financial statements. *GWService.exe:* Used for Server configuration and database service creation. *GwSrvBkp.exe:* Server Backup Utility. *Gwstart.exe:* Starts Database Engine/GlobalWare. *GwUtils.exe:* Small application with customer definitions to utilities and shortcuts. *Gwword.exe:* GlobalWare word processor for mail merge. *MapAndDeleteBranch.exe:* Support tool to assist in deleting GL Branches and mapping financials to existing branch. *MulitDB.exe:* Utility used to configure clients or multi-database access to database service(s).

	Pyupdate.exe: Support tool for updating erroneous payment information. *RepCCnum.exe:* Utility that secure-deletes and replaces portions of the credit card number (PAN) from GlobalWare Database. *Sabreint.exe:* Interface for Sabre GDS. *Stmtbal.exe:* Support tool for correcting erroneous opening balance on customer statements. *Wrldspan.exe:* Interface for Worldspan GDS. *AuthenticateDBLib.dll:* Library for Sybase DB authentication. *Download.dll:* Used for interface download. *GblWebService.dll:* uR XML Feed Interface that is for future implementation. *GWFuncs.dll:* Used by GlobalWare service account. *XceedZip.dll:* Used for Standalone Backup Zip functionality.
Required Third Party Payment Application Software	The following are additional third party payment application components required by the payment application:
	No third-party payment applications are required by GlobalWare.
Database Software Supported	The following are database management systems supported by the payment application:
	Custom Licensed *Sybase SQL Anywhere 16.0.0.2322* installed with executables and DLLs for use with the GlobalWare DB and GlobalWare Application and associated utilities bundled with the software.
Other Required Third Party Software	The following are other required third party software components required by the payment application:
	CrypKey Copy Protection for Licensing and against reverse-engineering, installed with the following executables and DLLs in the Gblware directory: CKCONFIG.EXE, CKREFRESH.EXE, CKS.EXE, Cryserv.exe, CASPER.DLL, cki32k.dll, InetCli.dll, and SETUPEX.EXE.
Operating System(s) Supported	The following are Operating Systems supported or required by the payment application:
	Operating system(s) and versions supported for Clients and Standalone PCs: Windows 7, Windows 8, and Windows 10 The latest supported versions of for multi-user environment: Windows Server 2010 or 2012 and Windows Server 2010 or 2012 R2 (32 and 64 bit)
What about Application Authentication	Authentication for GlobalWare is on a user level (3 fold), the application authenticates at an application, database, and connection level.
Application Encryption	• Dynamic/Hybrid key generation for encrypted columns in the database and for GlobalWare processed interfaced files stored in the Gblware directory • 128 bit Sybase Encryption for database encrypted columns • AES 256 bit Encryption of AIR and 001-005 Interface flat files • TLS1.2 for Multi-users to insure secure traffic between server and workstation • Password and fields related to Passwords use Salt and Hash • Standards around Secure Delete, requires 3 passes at the data (2, Single Character and Last Pass, Random Character before truncate/delete)

<table>
<tr><th></th><th></th></tr>
<tr><td></td><td><ul><li>HTTPS secure websites for GlobalWare downloads and patch releases</li><li>Secure SFTP and other secure remote access tools for GlobalWare Support/GlobalWare Helpdesk</li><li>Copy protection through Crypkey to ensure against reverse engineering and VeriSign Code Signatures to ensure against code that could be injected into the installation or installed components</li></ul></td></tr>
<tr><td><b>Application Functionality Supported</b></td><td><b>Payment Application Functionality (check only one):</b>

N/A – GlobalWare does not perform payment processing.

<table>
<tr><th></th><th></th><th></th><th></th><th></th><th></th></tr>
<tr><td></td><td>Automated Fuel Dispenser</td><td></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 Processing Connections:</b></td><td>N/A</td></tr>
<tr><td><b>Description of Listing Versioning Methodology</b></td><td>GlobalWare software versioning has three levels, Major, Minor, and Build: X.X.X.XXX

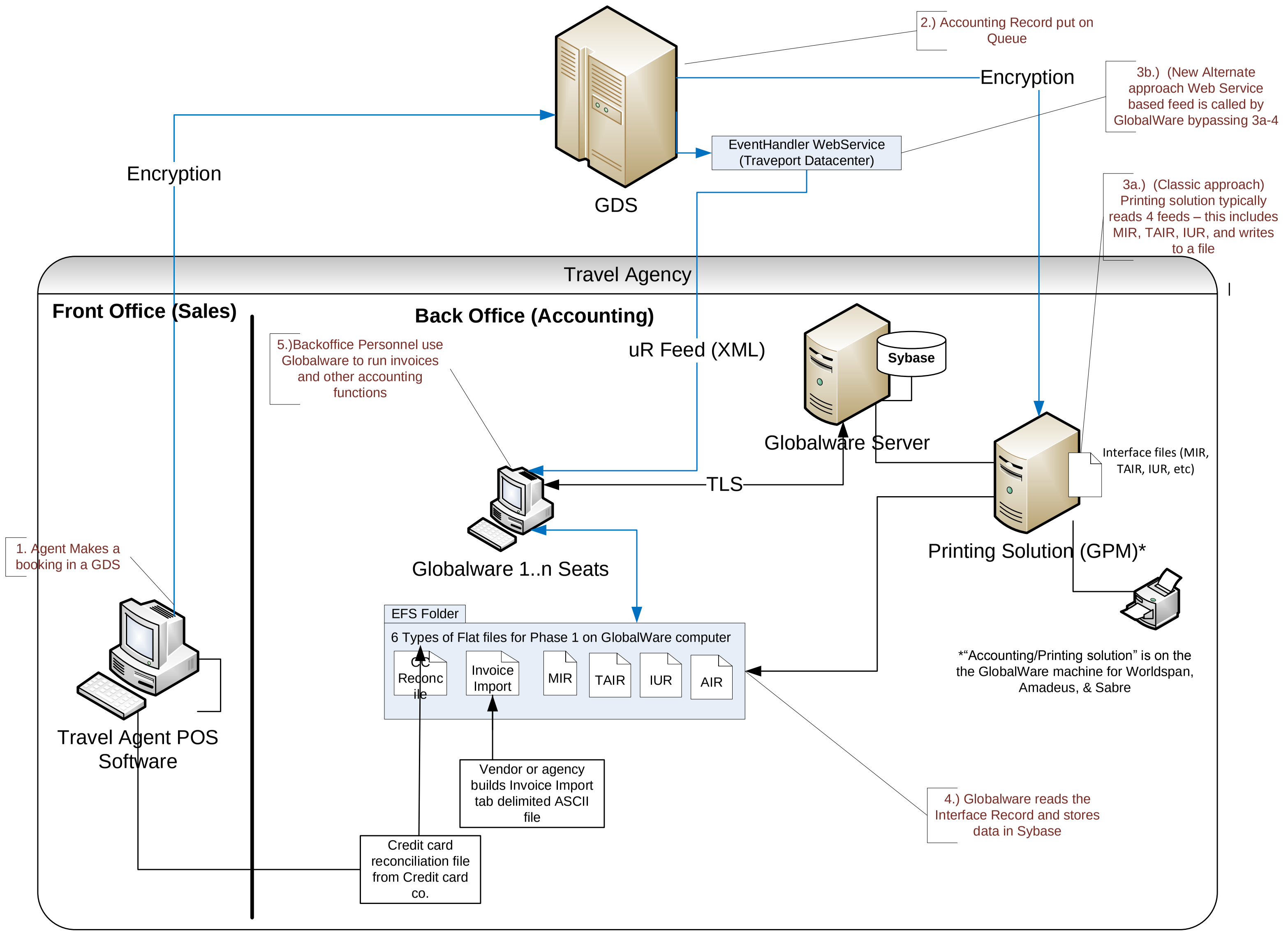
Major changes would have an incremental change in X position 1 and would include major Sybase upgrades. Ex: 7.X.X.XXXX

Minor changes would have an incremental change in X position 2 and would include bug fixes, GUI changes, and small enhancements. Ex: X.3.X.XXXX

An incremental change in X position 3 includes bug fixes and Patches. Ex:X.X.1.XXXX

Builds are signified by the XXXX in position 4 and reflect build numbers as fixes are incrementally implemented and tested. Ex: X.X.X.0100</td></tr>
</table>

Typical Network Implementation

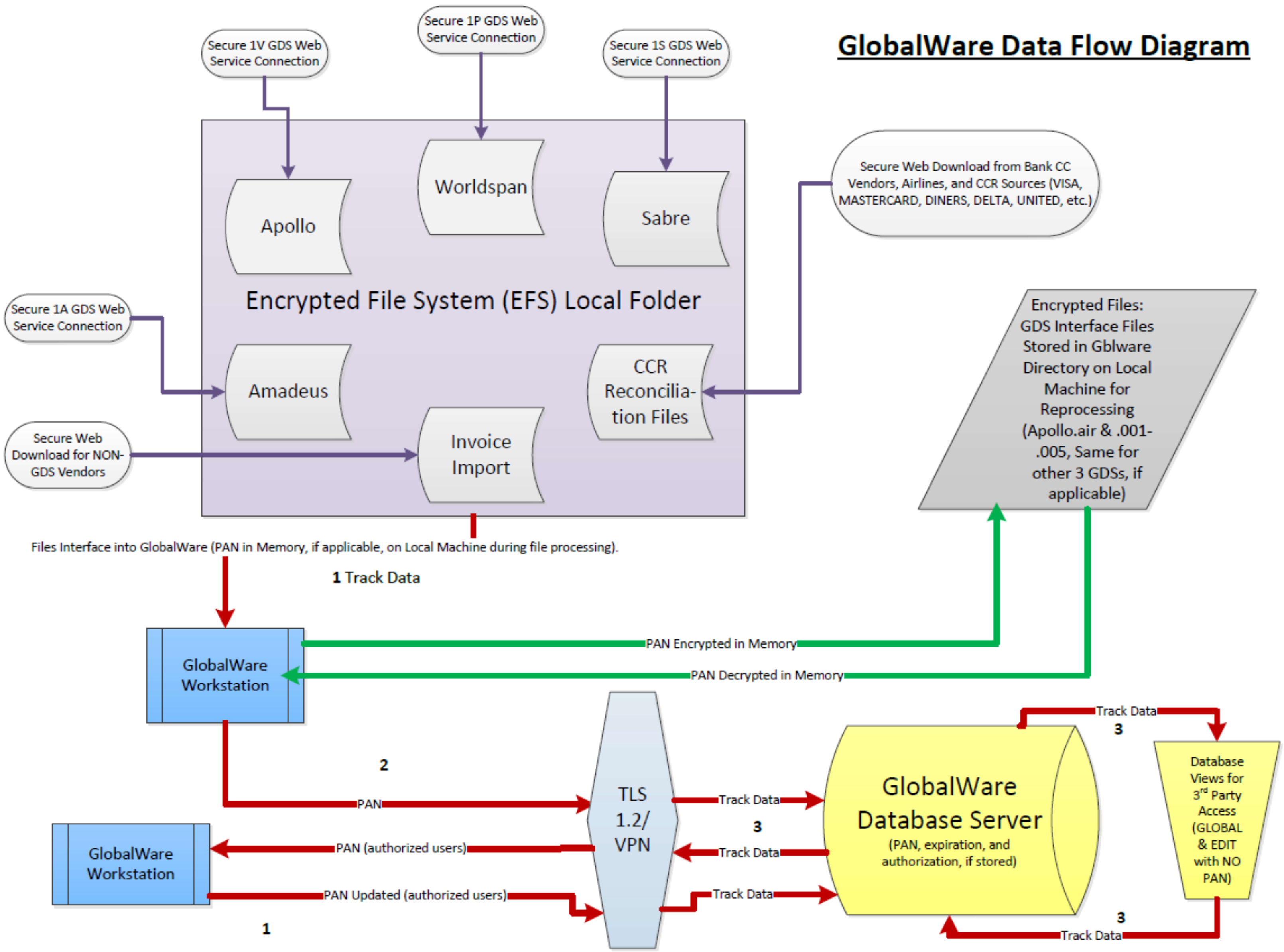

GDS
Encryption
Encryption
2.) Accounting Record put on Queue
3b.) (New Alternate approach Web Service based feed is called by GlobalWare bypassing 3a-4
EventHandler WebService (Traveport Datacenter)
3a.) (Classic approach) Printing solution typically reads 4 feeds – this includes MIR, TAIR, IUR, and writes to a file
Travel Agency
Front Office (Sales)
Back Office (Accounting)
uR Feed (XML)
5.)Backoffice Personnel use Globalware to run invoices and other accounting functions
Sybase
Globalware Server
Interface files (MIR, TAIR, IUR, etc)
TLS
Printing Solution (GPM)*
1. Agent Makes a booking in a GDS
Globalware 1..n Seats
EFS Folder
6 Types of Flat files for Phase 1 on GlobalWare computer
CC Reconc ile
Invoice Import
MIR
TAIR
IUR
AIR
*"Accounting/Printing solution" is on the the GlobalWare machine for Worldspan, Amadeus, & Sabre
Travel Agent POS Software
Vendor or agency builds Invoice Import tab delimited ASCII file
4.) Globalware reads the Interface Record and stores data in Sybase
Credit card reconciliation file from Credit card co.

Credit/Debit Cardholder Dataflow Diagram

Please refer to the GlobalWare Dataflow Diagram on the next page. This is the index that explains how the PAN and expiry date (if applicable) flows through the GlobalWare application.

- Purple lines signify all the places that the PAN and expiry may be captured in the application via interface, import, or reconciliation. These files are securely downloaded from a secure Web Server and reside in an EFS folder or encrypted drive until they are processed by the application. At this entry point Agencies may decide to Truncate or not store Credit Card information in GlobalWare. There are user controls available to accomplish this.
- Green lines are used to show fallback process if interface files (AIR and 001-005) need to be reprocessed. They are encrypted with AES 256 bit encryption and are unique to each agency as the keys are generated and stored (encrypted) on the fly based on both static and variable data and are only unencrypted in memory if fallback is required.
- Red lines show all areas where data is tracked/logged or manually entered by authorized users. In these areas, if the PAN is viewed by an authorized user, an entry will be made in the Admin Access Log. During those times, PAN is decrypted/encrypted in memory and for multiusers, thus workstation client- server environments vs. standalone, TLS 1.2 is used to encrypt application information across the network. If the user does not have security rights to view the credit card information, then that information is masked to that user in the GUI where only the last 4 characters of the PAN are visible and manual input of CC# data is also disallowed. There are GlobalWare Database Views of applicable fields and tables in the Sybase DB that can be accessed by authorized DBA users via an ODBC connection for ad hock queries, but these views are devoid of full PAN—only a truncated view is available which has first 6 and last 4. A DBlog.txt file is stored in the DB directory that logs all database access to the Sybase database.

GlobalWare Data Flow Diagram


Secure 1V GDS Web Service Connection
Secure 1P GDS Web Service Connection
Secure 1S GDS Web Service Connection
Apollo
Worldspan
Sabre
Secure Web Download from Bank CC Vendors, Airlines, and CCR Sources (VISA, MASTERCARD, DINERS, DELTA, UNITED, etc.)
Encrypted File System (EFS) Local Folder
Secure 1A GDS Web Service Connection
Amadeus
CCR Reconcilia-tion Files
Secure Web Download for NON-GDS Vendors
Invoice Import
Encrypted Files: GDS Interface Files Stored in Gblware Directory on Local Machine for Reprocessing (Apollo.air & .001-.005, Same for other 3 GDSs, if applicable)
Files Interface into GlobalWare (PAN in Memory, if applicable, on Local Machine during file processing).
1 Track Data
GlobalWare Workstation
PAN Encrypted in Memory
PAN Decrypted in Memory
Track Data
3
Database Views for 3rd Party Access (GLOBAL & EDIT with NO PAN)
2
PAN
TLS 1.2/ VPN
Track Data
3
GlobalWare Database Server
(PAN, expiration, and authorization, if stored)
GlobalWare Workstation
PAN (authorized users)
Track Data
PAN Updated (authorized users)
Track Data
1
3
Track Data

Difference between PCI Compliance and PA-DSS Validation

As a software vendor who develops payment applications, our responsibility is to be "PA-DSS Validated." However, GlobalWare is out-of-scope of PA-DSS and is not considered a Payment Application, as it does not facilitate authorization or settlement on its own.

We have performed an assessment and certification compliance 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 GlobalWare v7.3 has been tested, assessed, and validated.

PCI Compliance is then later obtained by the Agency, 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 Agency 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 GlobalWare 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, Agencies, 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

Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4)

Previous versions of GlobalWare did not store sensitive authentication data. Therefore, there is no need for secure deletion of this historical data by the application as required by PA-DSS v3.2.

Handling of Sensitive Authentication Data (PA-DSS 1.1.5)

GlobalWare 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 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)

The GlobalWare application can be configured to either store cardholder data or not. Please see the appropriate section depending on how GlobalWare is configured for your environment.

If Cardholder Data Is Being Stored in GlobalWare

The following guidelines must be followed when dealing with cardholder data (Primary Account Number [PAN], Cardholder Name, Expiration Date, or Service Code):

- A customer defined retention period must be defined with a business justification.
- Cardholder data exceeding the customer-defined retention period or when no longer required for legal, regulatory, or business purposes must be securely deleted.
- Here are the locations of the cardholder data you must securely delete:

    - InvCreditCard.CCNumber
    - CCRTransaction.CCNumber
    - CCRAccountCC.CCNum
    - CustomerCreditCard.CCNumberCCNumber
- To securely delete cardholder data, you must do the following:
    - Outside of the application, you must address historically stored PANs by using the RepCCnum.exe utility, which is stored in the Gblware directory. This utility securely deletes any old credit card data that is no longer being used for a business need. You must be a system High user to run this utility. This application runs three swipes before it truncates the CCNumber, so use small data ranges so that you can become familiar with the amount of time it takes to run the utility in your environment. Truncate the CCNumber to the first six and the last four digits to satisfy PCI standards. Before purging CCRTransactions, securely delete PAN to ensure it is properly wiped off of your hard drive.
    - If you used the PCI Security tab to set up GlobalWare for Automated Secure Delete, the application securely deletes CCNumber automatically in the InvCreditCard table and other database fields based on user-controlled settings. After initial setup, this service runs automatically at user-specified intervals. The setup of these intervals is based on business need. Truncating CCNumber to the first six and the last four digits meets PCI standards and user controls when setting automation should be set to accommodate this setup. Automated Secure Delete, like the RepCCnum.exe manual tool, also takes three swipes at the data before truncating the PAN. Because of this, you should set it to run during quiet times in database processing so that you do not impact performance.

  For detailed instructions about the RepCCnum.exe utility and Automated Secure Delete, see the GlobalWare help system.

- 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**.

If Cardholder Data Is Not Being Stored in GlobalWare

GlobalWare does not store cardholder data unless the full PAN is interfaced through the GDSs or imported into the GlobalWare application. Therefore, there is no data to be purged by the application for current record maintenance of cardholder PAN as required by PA-DSS v3.2. However, because not storing full PAN only became an option in the last three years, and because there could be credit card data stored that you might not be aware of, when upgrading to GlobalWare v6.0 or v7.0, v7.20, or v7.3, you must run the Manual Secure Delete utility (RepCCnum.exe) to securely delete historical data that might remain in your database. By doing this for all stored dates within your database, you effectively take GlobalWare out of PCI scope. In doing so, your agency can use the controls on the PCI Security option in the GW menu to reduce the level of security. Because this pertains to columns encryption in your database, doing so will increase database performance related to these encrypted columns. Please consult with your PCI auditor to ensure you have indeed taken GlobalWare out of PCI scope before changing these PCI security settings.

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.

Disable Operating System (Windows OS) automatic restore points and do not manually create OS restore points on GlobalWare computers or servers. Database backups should be kept in secure locations, and they should be deleted or destroyed when they are no longer useful for disaster recovery.

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)

GlobalWare versions 6.0 and above mask all PANs by default in all locations that display PAN (screens, paper receipts, printouts, reports, etc.) by displaying only the last 4 digits of the credit card #. The payment application displays PAN in the following locations:

- Invoice Edit and Invoice Print
- Invoice/PRISM Export

GlobalWare does have the ability to display full PAN for users with legitimate business need. In order to configure the application to display full PAN for only personnel with a legitimate business need, you must have Mask CC unchecked in their employee security settings.

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

GlobalWare does not store encryption keys. Keys are agency specific and are generated dynamically on the fly per each individual record via a Hybrid key generation solution, which uses both variable and static data to generate strong cryptographic keys. No Key Custodian is needed as keys are generated dynamically and not stored outside GlobalWare or in the application code.

Removal of Historical Cryptographic Material (PA-DSS 2.6)

Previous versions of GlobalWare never stored encryption keys and therefore there is no cryptographic data to be securely deleted as required by PA-DSS v3.2.

Set Up Strong Access Controls (3.1 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.

- GlobalWare does not use any default accounts and the service account is used only by the application. All login information is unique to each individual users.

All authentication credentials are generated and managed by the application or bundled utility for Agency DBA access (*EditUserView.exe*). 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 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 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 Travelport for support purposes) (PCI DSS 2.1 / PA-DSS 3.1.2)
3. The application must assign unique IDs for all user accounts (PCI DSS 8.1.1 / PA-DSS 3.1.3)
4. The 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 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 application requires passwords must 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 application requires passwords to be changed at least every 90 days (PCI DSS 8.2.4 / PA-DSS 3.1.7)
8. The 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 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 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 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)

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, and never store passwords or authentication settings in ODBC settings.

These same account and password criteria from the above requirements must also be applied to any applications or databases included in payment processing to be PCI compliant. GlobalWare, as tested in our PA-DSS validation audit, meets, or exceeds these requirements for the following additional required applications or databases:

GlobalWare 6.0, 7.0, 7.1, 7.2, and 7.3 versions

[**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 systems with cardholder data, and for access controlled by the application.

The requirements apply to the application and all associated tools used to view or access cardholder data.]

PA-DSS 3.2: Control access, via unique username and PCI DSS-compliant complex passwords, to any PCs or servers with 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.

Log Settings Must Be Compliant (PA-DSS 4.1.b, 4.4.b)

4.1.b: GlobalWare has PCI DSS compliant logging enabled by default. This logging is not configurable and can only be disabled by system high, administrative user. Disabling or subverting the logging function of GlobalWare in any way will result in non-compliance with PCI DSS if your agency is in PCI scope and stores cardholder data in GlobalWare. Consult with your PCI auditor to determine whether you have taken GlobalWare out of PCI scope before making any changes to PCI Security.

GlobalWare has two logs: an Admin Access Log that can be accessed through PCI Security screen under the System menu and DBlog.txt that is stored in the DB Directory where ever the database resides and logs database access. Logs must be kept for a minimum of one year, but can be archived every 90 days. Admin access log within the GlobalWare application does not allow you to archive log data that is less than 90 days. The Sybase Dblog.txt will create a new log file every 100MB and will rename predecessor with date for easy archiving.

GlobalWare logging is enabled upon install of version 6.0, 7.0, 7.1, 7.2, and 7.3, and meets the following logging requirements in PCI DSS 10.2 and 10.3.

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

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:

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.

4.4.b: GlobalWare facilitates centralized logging through Sybase Syslog and through Proprietary Application logging into a database table (PCI DSS 10.5.3). This can be done within the application's "PCI Security" Screen under the System menu, by going to "Send to" and saving a log to a file in an exportable format.

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

GlobalWare does not support wireless technologies. However, should the Agency 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)

GlobalWare does not require the use of any insecure services or protocols. Here are the services and protocols that GlobalWare does require:

SSL - GlobalWare downloads and patches

SFTP – For transfer of files to the GlobalWare Helpdesk

HTTPS – For Secure downloads

TLS1.2 – For Multiuser data stream encryption between Client and Server

EFS – Encrypted Folder for sensitive data storage before it is interfaced to GlobalWare

Do not use insecure protocols with GlobalWare. Having insecure protocols enabled and configured (such as FTP, Telnet, Rlogin, rsh, rexec) would make your environment non-compliant with PCI DSS.

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).

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. This 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

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

GlobalWare delivers patches and updates in a secure manner:

- Timely development and deployment of patches and updates.

  Security patches are made available on a priority risk approach based on the CVSS ranking. High risks, would be delivered on an as soon as possible basis, or maximum of a month from the time of detection. Low and Medium risk security patches will be release quarterly. Product Marketing will advise customers of the need to download critical patches.

- Delivery in a secure manner with a known chain-of-trust.

  Patches and GlobalWare Downloads will be available on HTTPS secure website, and links are sent to agency/customer designated email addresses. Links to GlobalWare download sites are not posted to general public.

- Delivery in a manner that maintains the integrity of the deliverable.

  Security Patches will be delivered via HTTPS website connection.

- Integrity testing of patches or updates prior to installation.

  All Patches installations will have VeriSign certificates are in place before release and will be tested before they are posted on the website and the link is emailed.

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:

- Microsoft Advisories
- Red Hat Advisories
- McAfee Security Event Notifications
- SQL Anywhere 16 Notifications

Once we identify a relevant vulnerability, we work to develop and test a patch that helps protect GlobalWare against the specific, new vulnerability. We attempt to publish a patch within 10 days of the identification of the vulnerability. We will then contact Agencies to encourage them to install the patch. Typically, Agencies are expected to respond quickly to and install available patches within 30 days.

We do not deliver software and/or updates via remote access to customer networks. Instead, software and updates are e-mailed to agency-designated e-mail addresses and also posted on our GlobalWare General Release download site which is currently Travelport Marketplace.

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 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

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 TLS1.2 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).

PCI DSS requirement 4.1: Use strong cryptography and security protocols such as transport layer security (TLS1.1 / TLS1.2) 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 GlobalWare.

GlobalWare is not an internet-based application; however, we have implemented TLS1.0 with self-signed certificate in the multi-user (client/server) environment with RSA algorithms. GlobalWare must be installed on a private network.

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

GlobalWare 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 and Multi-Factor Authentication (PA-DSS 12.1, 12.2)

GlobalWare or server allows non-console administration, so you must use SSH, VPN, or TLS1.1 or higher for encryption of this non-console administrative access. Because GlobalWare allows such access, multi-factor authentication (at least 2 of something you know, something you have, and something you are) must be utilized when accessing GlobalWare over these technologies.

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 GlobalWare.

Maintain an Information Security Program

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

The following is a very basic plan every Agency 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 application level, all entities should complete annual self-assessments using the PCI Self-Assessment Questionnaire.
- Call in outside experts as needed.

GlobalWare System Configuration

Below are the operating systems and dependent application patch levels and configurations supported and tested for continued PCI DSS compliance.

Please see GlobalWare Hardware document for specified system configuration. Hardware and GPM for GlobalWare Installation documents can be accessed from the software download or ASK knowledgebase.

Payment Application Initial Setup & Configuration

The general releases of GlobalWare v6.0, v7.0, v7.1, v7.2, and v7.3 are PCI Compliant out-of-the-box. This means encryption will be enabled during installation, along with other PCI related options. Installation instructions and uninstall instructions are available from the software download menu.

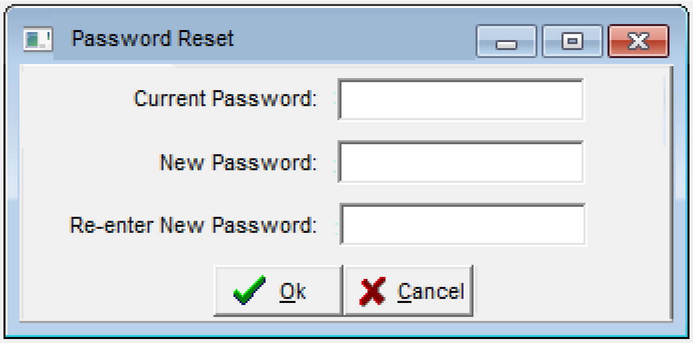
PCI options enabled at installation:

- Password must be changed to 8-12 alphanumeric characters, and GlobalWare will store the last 4 passwords, so they cannot be reused at password reset. Password and historical password information is encrypted using Hash and Salt and is not accessible to GlobalWare users.
- User will be locked out after 6 invalid password attempts, but can try again in 30 minutes. See Password Reset section for more information.
- User will need to sign into GlobalWare after 15 minutes of computer idle time (not application idle time).
- Password will expire every 90 days.
- Admin Access log will be stored and can only be archived for data greater than 90 days. Sybase Syslog will be available at DB Directory, Dblog.txt, where ever the database resides and will rename and create a new log for easy archiving with date every 100MB.
- CCNumber fields within the database will be encrypted with dynamically generated keys that are unique to every GlobalWare database and each individual record.
- TLS 1.2 with self-signed certificate implemented with RSA algorithm for Multiusers.

Options that have to be initiated or enabled for use:

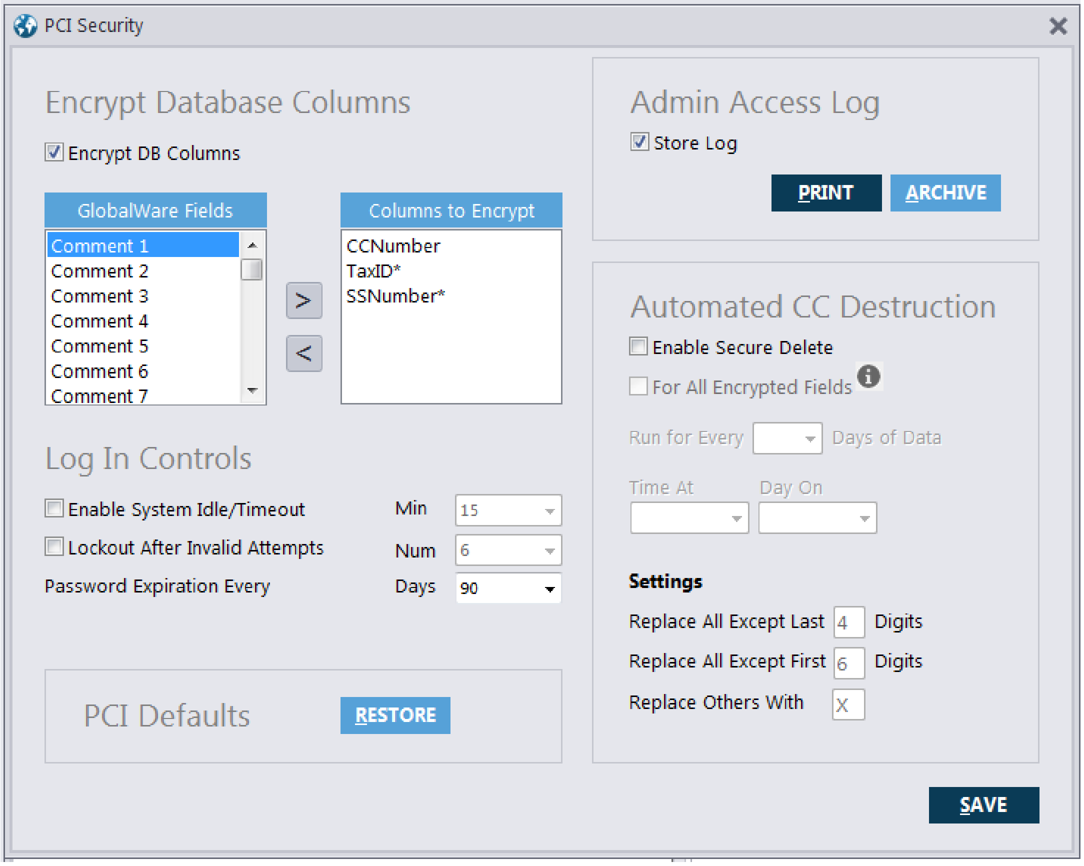
- Manual or Automated CC Destruction.
- “Global” or “Edit” access securities to the GlobalWare database, for agency DBA users only.
- SMTP Messaging for password reset via email.

Password Screen to create alphanumeric password will be initiated at login to GlobalWare v6.0, v7.0, v7.1, v7.2, and v7.3, or during password expiration:



All passwords must have at least 1 alpha character and 1 numeric character. Validations are in place to ensure that New Password meets both requirements before accepted. Passwords must be a minimum of 8 characters long and a maximum of 12.

PCI Security screen in System Menu:



Encrypt Database Columns

☑ Encrypt DB Columns

GlobalWare Fields: Comment 1, Comment 2, Comment 3, Comment 4, Comment 5, Comment 6, Comment 7

Columns to Encrypt: CCNumber, TaxID*, SSNumber*

Log In Controls

□ Enable System Idle/Timeout	Min	15
□ Lockout After Invalid Attempts	Num	6
Password Expiration Every	Days	90

PCI Defaults

Admin Access Log

☑ Store Log

Automated CC Destruction

□ Enable Secure Delete

□ For All Encrypted Fields

Run for Every Days of Data

Time At Day On

Settings

Replace All Except Last 4 Digits

Replace All Except First 6 Digits

Replace Others With X

In the case of GlobalWare agencies that have taken measures to take GlobalWare out-of-scope of PCI (truncating the PAN where only first 6 and last 4 characters of the CC# are visible), we have added user controls, which allow changes to PCI Security Options. These options can only be accessed by Employee, System High users, and should be limited at the agency to include DBAs and GlobalWare password administrators. Even for agencies that have taken GlobalWare out-of-scope, it is recommended that the RepCCNum.exe is used to securely deleting PAN (3 passes over data prior to deletion) for all historical data.

Although, we strongly recommend that agencies do not store any PANs or other sensitive cardholder data outside of standard CCNumber designated areas in GlobalWare, we have secured comment fields with dynamic encryption per individual record to meet PCI encryption requirements for agencies that have business needs to store sensitive data outside the standard database fields.

User Controls:
Column Encryption: Choices to encrypt CC Number Fields, Comment Fields and SS Number (PII).
System Idle Time: Choice to change the time-out for computer idle time settings.
Lockout Attempts: Choice to change the number of invalid login attempts before lockout.
Password Expiration: Choice to change the duration of time until password expiration.
Admin Access Log Storage: Choice to store log or not.
Automated Secure Delete: Settings to enable Secure Delete of sensitive data in encrypted fields.
Credit Card Number Security: Choice to truncate PAN before it is stored in the GlobalWare database.

With the GlobalWare v6.0, v7.0, v7.1, v7.2, and v7.3 installation, all user controls will be set to the minimum PCI standards. There is a message that will appear if they are set to less than requirements, but will allow users to continue.

If the GlobalWare agency stores sensitive cardholder data in their GlobalWare database, do not change these controls to less than PCI standards.

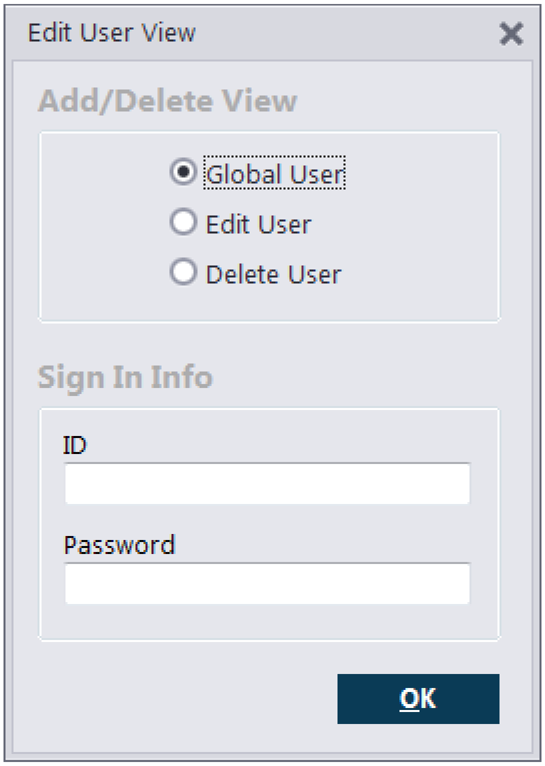
If the GlobalWare agency truncates the PAN/CCNumber to a minimum of 6 first and 4 last characters of the CC#, and has taken GlobalWare out-of-scope of PCI, the agency can make changes to these controls.

If a GlobalWare agency was out-of-scope prior to GlobalWare v6.0, v7.0, v7.1, v7.2, and v7.3 and changes user controls, but would like to start storing PAN for business need at a later date, clicking the Restore button under PCI Defaults on PCI Security Tab in System Control File makes restoring PCI settings easy.

Note: *Encryption and Logging for PCI Security will take both memory and storage resources, so if the full CCNumber (PAN) is not required for business need, it should not be stored in the GlobalWare database. Every connection, disconnection, and invalid attempt to the GlobalWare database with any type of user will be logged in location DB Directory, DBlog.txt, in addition to the Admin Access Log. This database log must be kept for a minimum of 90 days unless GlobalWare was taken out-of-scope.*

Also, for all users, the interface files (GDSname.air and .001-.005) located in the Gblware Directory are now dynamically encrypted, so an agency can reprocess only these 6 files for each corresponding GDS. Any backups of older GlobalWare interface files will not work. For GlobalWare Support only Pre-interfaced file(s) can be transmitted to the GlobalWare Helpdesk via secure methods as the encryption of these files is agency specific and has a limited file fallback duration.

Creating DBA database connections with the ***New EditUserView.exe utility***:



● Global User
○ Edit User
○ Delete User

All connections to the GlobalWare Application and GlobalWare Database have unique passwords that will expire according to agency PCI Security settings. Global and Edit user securities must be added through this new utility. Only Employee “System High” users will have the ability to create the Global User. For Edit User (edit non-accounting data), as currently, a password from the GlobalWare Helpdesk is required. This password is reset only when logging into the GlobalWare application.

Password Reset Options:

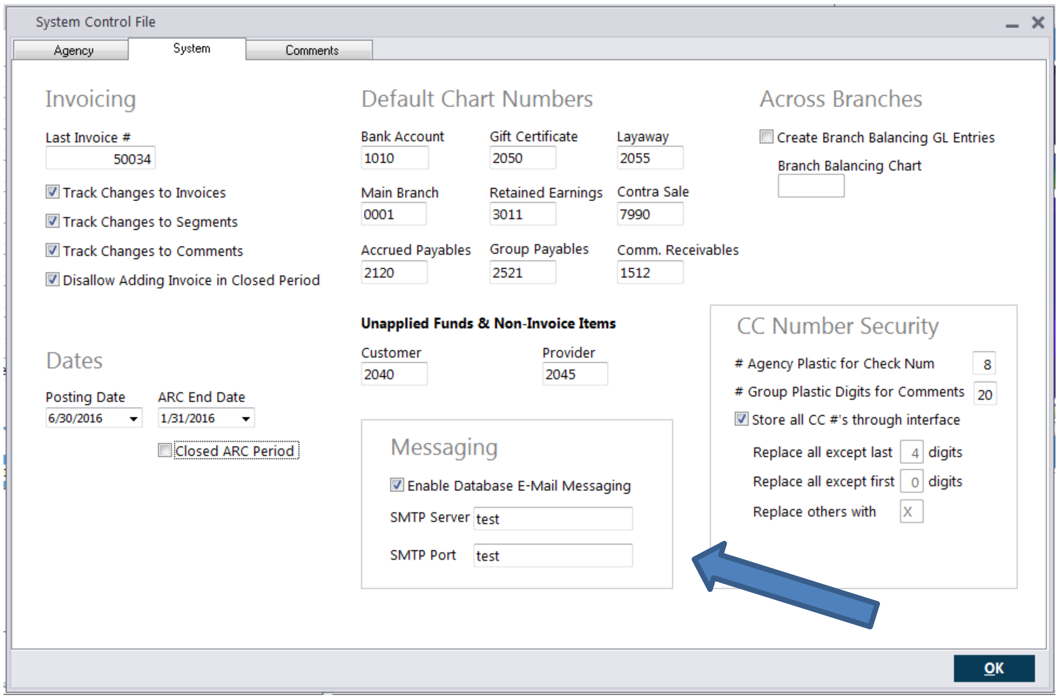
- *30 Minute Lockout and Retry:* After 30 min the application will let you try again to attempt the password. However, if “Enable E-Mail Password Reset” is set for that Employee, then they will get an SMTP email message after the last invalid attempt.

- *Reset via GlobalWare Agency Administrator:* Reset in Employee Account ID by Employee "System High" user that has "Empl Security" checked in their Account ID Security options.

- *Temporary Password via SMTP Messaging thru Email:* With SMTP information in place, sends a TEMP password thru email, then asks security question and verifies answer.

- *Through GlobalWare Helpdesk:* If GlobalWare Agency Administrator(s) is locked out, then with security questions and documentation, the GlobalWare Helpdesk can allow temporary GlobalWare access to Reset Password.

Enabling SMTP Messaging:



Invoicing

Last Invoice # 50034

☑ Track Changes to Invoices
☑ Track Changes to Segments
☑ Track Changes to Comments
☑ Disallow Adding Invoice in Closed Period

Default Chart Numbers

Bank Account 1010 | Gift Certificate 2050 | Layaway 2055
Main Branch 0001 | Retained Earnings 3011 | Contra Sale 7990
Accrued Payables 2120 | Group Payables 2521 | Comm. Receivables 1512

Across Branches

□ Create Branch Balancing GL Entries
Branch Balancing Chart

Unapplied Funds & Non-Invoice Items

Customer 2040 | Provider 2045

Dates

Posting Date 6/30/2016
ARC End Date 1/31/2016
□ Closed ARC Period

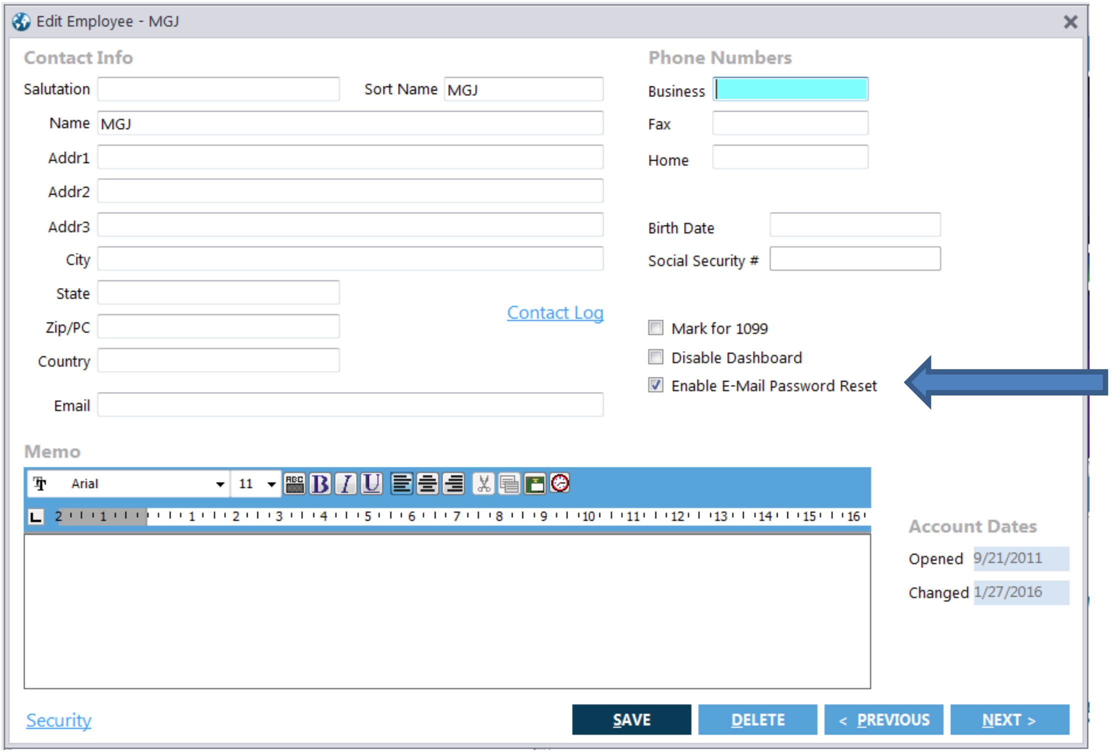
Messaging

☑ Enable Database E-Mail Messaging
SMTP Server test
SMTP Port test

CC Number Security

Agency Plastic for Check Num 8
Group Plastic Digits for Comments 20
☑ Store all CC #'s through interface
Replace all except last 4 digits
Replace all except first 0 digits
Replace others with X

Enable Database E-Mail Messaging must be checked and SMTP Server and SMTP Port must be filled in before individual Employees can Enable E-Mail Password Reset: illustration below.



Edit Employee - MGJ

Contact Info

Salutation

Sort Name MGJ

Name MGJ

Addr1

Addr2

Addr3

City

State

Zip/PC

Country

Email

Contact Log

Phone Numbers

Business

Fax

Home

Birth Date

Social Security #

□ Mark for 1099

□ Disable Dashboard

☑ Enable E-Mail Password Reset

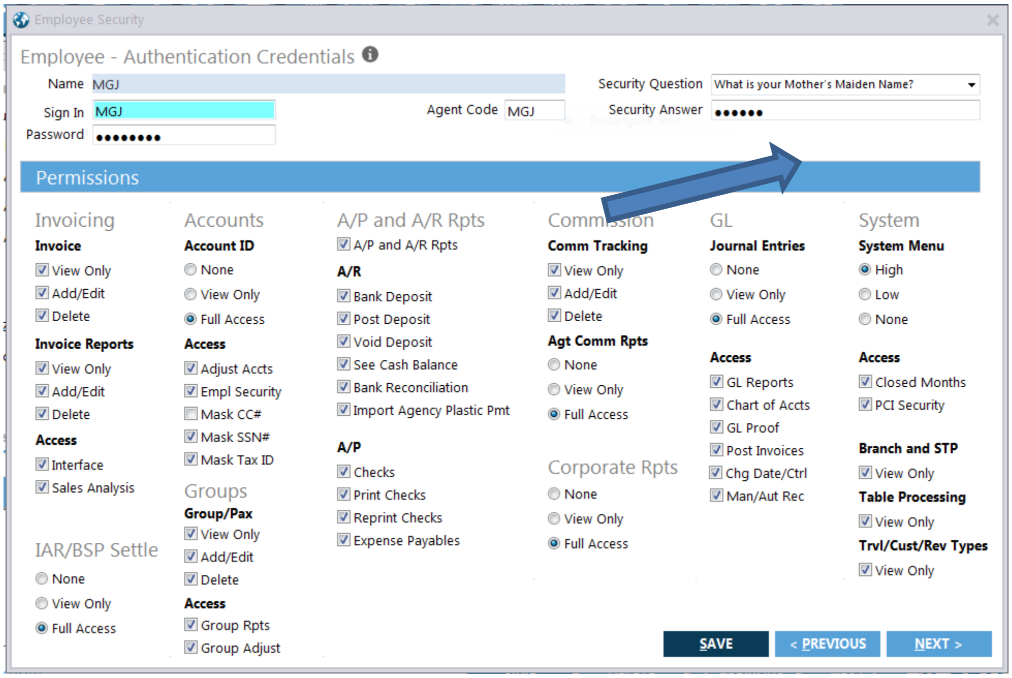
Memo

Account Dates

Opened 9/21/2011

Changed 1/27/2016

Security Question and Answer must also be filled in for E-Mail password reset via SMTP messaging (print screen below).



Employee Security

Employee - Authentication Credentials

Name MGJ

Sign In MGJ

Password ●●●●●●●●

Agent Code MGJ

Security Question What is your Mother's Maiden Name?

Security Answer ●●●●●●

Permissions

Invoicing

Invoice

☑ View Only

☑ Add/Edit

☑ Delete

Invoice Reports

☑ View Only

☑ Add/Edit

☑ Delete

Access

☑ Interface

☑ Sales Analysis

IAR/BSP Settle

○ None

○ View Only

● Full Access

Accounts

Account ID

○ None

○ View Only

● Full Access

Access

☑ Adjust Accts

☑ Empl Security

□ Mask CC#

☑ Mask SSN#

☑ Mask Tax ID

Groups

Group/Pax

☑ View Only

☑ Add/Edit

☑ Delete

Access

☑ Group Rpts

☑ Group Adjust

A/P and A/R Rpts

☑ A/P and A/R Rpts

A/R

☑ Bank Deposit

☑ Post Deposit

☑ Void Deposit

☑ See Cash Balance

☑ Bank Reconciliation

☑ Import Agency Plastic Pmt

A/P

☑ Checks

☑ Print Checks

☑ Reprint Checks

☑ Expense Payables

Commission

Comm Tracking

☑ View Only

☑ Add/Edit

☑ Delete

Agt Comm Rpts

○ None

○ View Only

● Full Access

Corporate Rpts

○ None

○ View Only

● Full Access

GL

Journal Entries

○ None

○ View Only

● Full Access

Access

☑ GL Reports

☑ Chart of Accts

☑ GL Proof

☑ Post Invoices

☑ Chg Date/Ctrl

☑ Man/Aut Rec

System

System Menu

● High

○ Low

○ None

Access

☑ Closed Months

☑ PCI Security

Branch and STP

☑ View Only

Table Processing

☑ View Only

Trvl/Cust/Rev Types

☑ View Only

Automated Secure Delete:

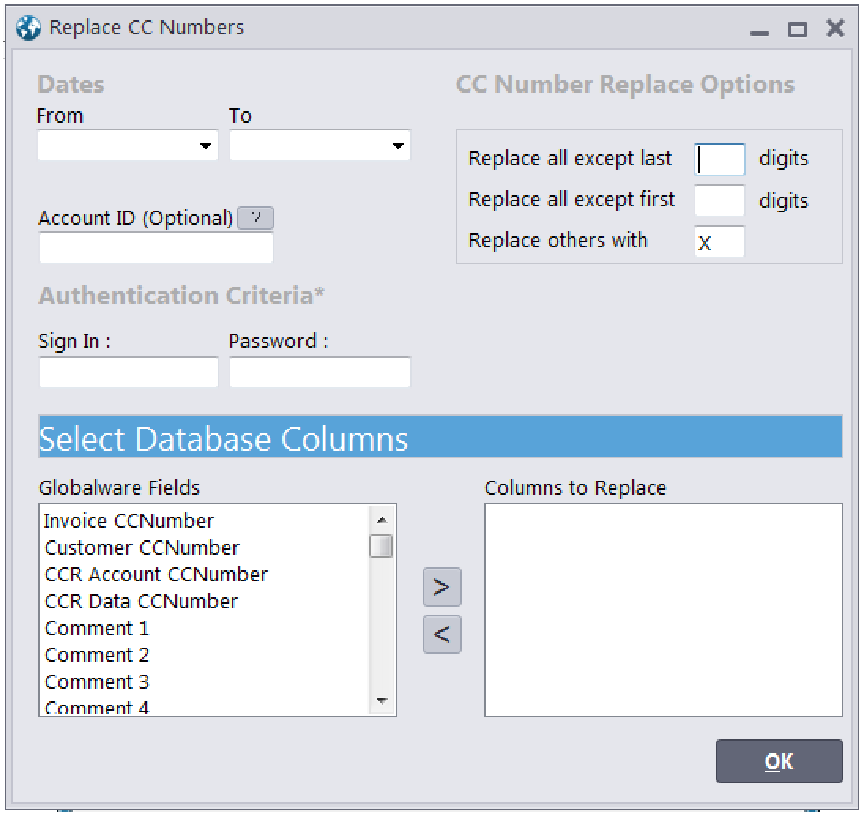
If enabled, this is a Sybase database service that runs in conjunction with the current database service. It automates the secure deletion (3 passes over data, before replace/delete) of Invoice CCNumber (PAN) and/or Comment lines. Employee SSNumber* (Social Security # for PII) is not included in either the automated or manual secure delete processes, and Customer CCNumber, CCR Account CCNumber, and CCR Data CCNumber must be Secure Deleted Manually using the RepCCNum.exe utility.

When enabling this automated service, there will be a message to re-start the database service for the settings to take effect.

These automated and/or manual secure deletion methods should be used for maintenance of cardholder data once there is no longer a business need for it, thus they should be run periodically. This will reduce liability if there is a breach in the agency environment.

Manual Secure Delete:

The RepCCNum.exe utility has been expanded to replace (truncate) all CCNumber fields to user Credit Card Security specifications. Secure deleting an individual comment line is possible with this manual utility. Only users with System High security can use the utility. See illustration below.



Replace CC Numbers

Dates

From

To

Account ID (Optional)

CC Number Replace Options

Replace all except last digits

Replace all except first digits

Replace others with X

Authentication Criteria*

Sign In :

Password :

Select Database Columns

Globalware Fields

- Invoice CCNumber
- Customer CCNumber
- CCR Account CCNumber
- CCR Data CCNumber
- Comment 1
- Comment 2
- Comment 3
- Comment 4

Columns to Replace

Note: *Due to the 3 required passes at the data before secure deletion or truncation, both the automated and manual methods will take some time to run. The amount of time they take will* *vary based on the size of GlobalWare database, the date range, the amount of cardholder data stored, and the speed of the hardware it is being run on in the agency environment. Once this data is secure deleted it is no longer retrievable in its entirety.*

Misc. PCI Items:

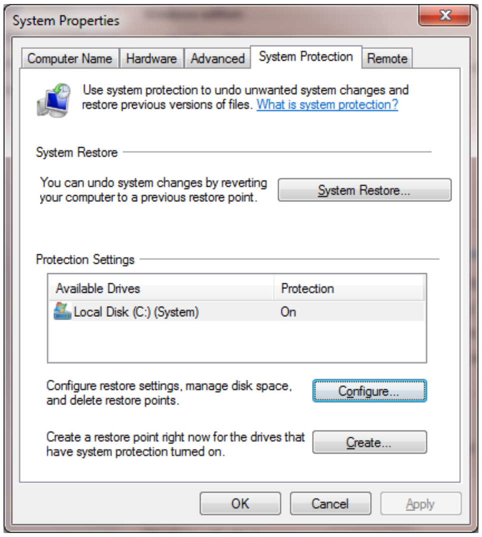
- Dynamic/Hybrid key generation for encrypted columns in the database and for GlobalWare processed interfaced files stored in the Gblware directory
- 128 bit Sybase Encryption for database encrypted columns
- AES 256 bit Encryption of AIR and 001-005 Interface flat files
- TLS1.2 for Multi-users to insure secure traffic between server and workstation
- Idle Time is not Application Idle, but Computer Idle (no keyboard or cursor activity)
- Password History Stored for Last 4 Passwords and those cannot be re-used at Password Reset
- New CC Customer and CC Invoice look-up Tables to separate CCNumber from the Name and Address for added security
- No emailing of CC Number (full PAN) is facilitated
- No Invoice Change Log Entries around CCNumber as CCNumber is no longer in the Invoice Table
- Due to PCI Logging Requirements, Create and Modified Date will be incorporated for Interfaced Records
- Standards around Secure Delete, requires 3 passes at the data (2, Single Character and Last Pass, Random Character before truncate/delete)
- 3 Types of Authentication (Database Level, Application Level, and Connection Level)
- HTTPS secure websites for GlobalWare downloads and patch releases
- Secure SFTP and other secure remote access tools for GlobalWare Support/GlobalWare Helpdesk
- Copy protection through Crypkey to insure against reverse engineering
- VeriSign Code Signatures to insure against code that could be injected into the installation or installed components
- SDLC written processes in place for GlobalWare
- Secure coding practices (OWASP)
- PCI Implementation Guide (link will be available in ASK and in Software Download Menu)
- Secure Coding Practices (OWASP)
- PCI Implementation Guide

Appendix A: Addressing Inadvertent Capture of PAN

Addressing Inadvertent Capture of PAN on WINDOWS 7

Disabling System Restore – Windows 7

- Right Click on Computer > Select “Properties”
- Select “System Protection” on the top left list, the following screen will appear:



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.

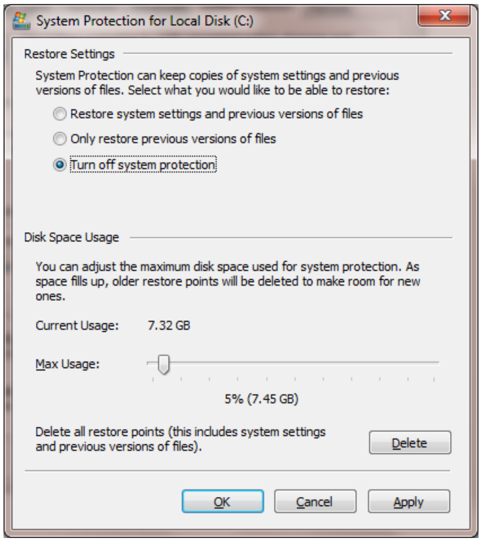
Protection Settings

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 will appear:



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)

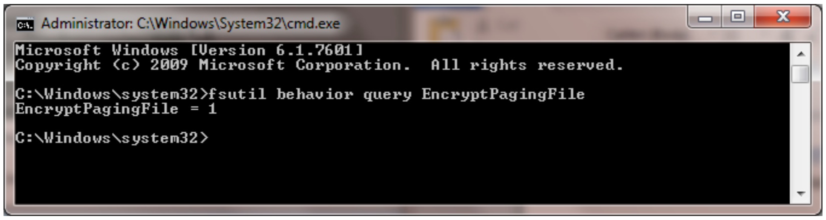
Delete all restore points (this includes system settings and previous versions of files).

- Select “Turn off system protection”
- Click apply, and OK to shut the System Protection window
- Click OK again to shut the System Properties window
- Reboot the computer

Encrypting PageFile.sys – Windows 7

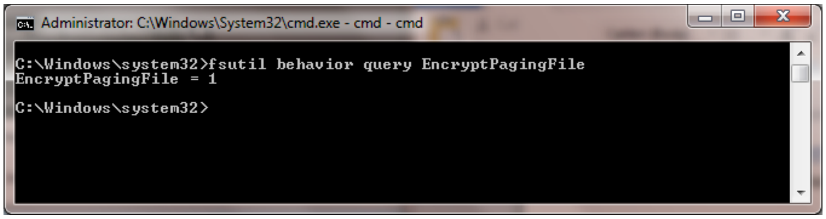
* Please note that in order to perform this operation the hard disk must be formatted using NTFS.

- Click on the Windows “Orb” and in the search box 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



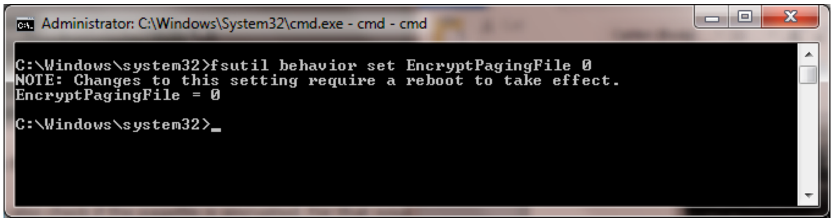
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

C:\Windows\system32>
```

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



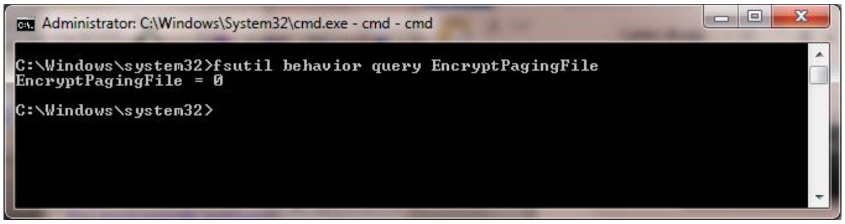
```
C:\Windows\system32>fsutil behavior query EncryptPagingFile
EncryptPagingFile = 1

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>
```

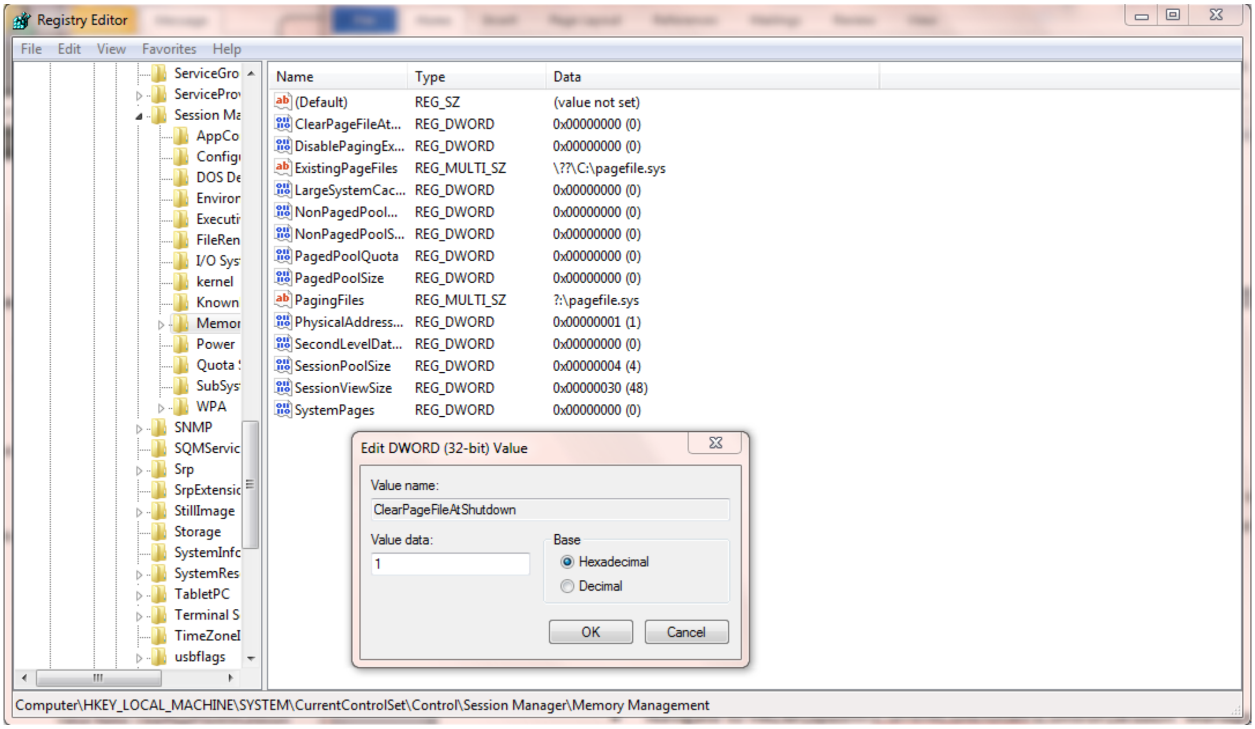
- If encryption is disabled EncryptPagingFile = 0 should appear

Clear the System Pagefile.sys on shutdown

Windows has the ability to 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.

- Click on the Windows “Orb” and in the search box type in “regedit”.
- Right click on regedit.exe and select “Run as Administrator”
- Navigate to HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management
- 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

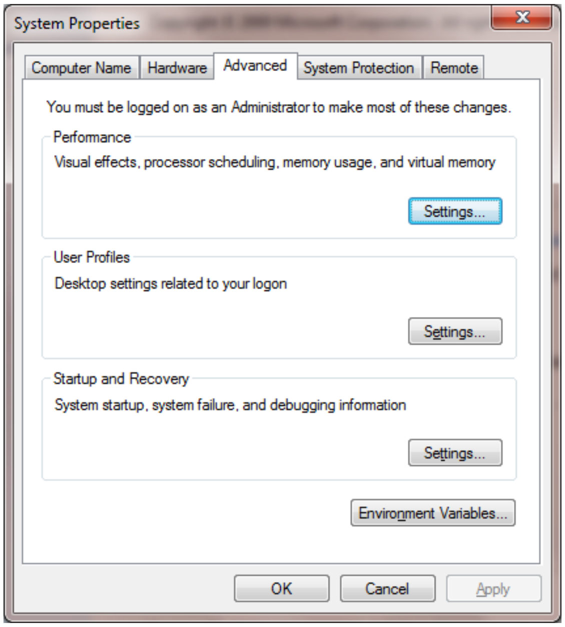
Base: ● Hexadecimal ○ Decimal

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 – Windows 7

- Right Click on Computer > Select “Properties”
- Select “Advanced System Settings” on the top left list, the following screen will appear:



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

Performance

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

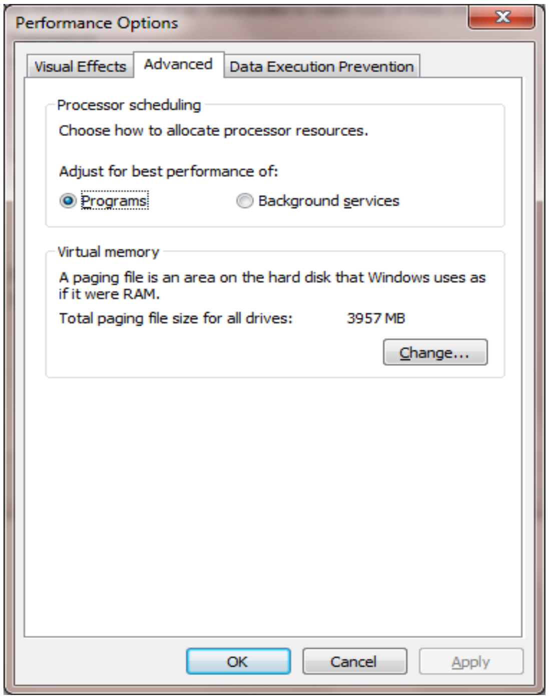
User Profiles

Desktop settings related to your logon

Startup and Recovery

System startup, system failure, and debugging information

- Under performance select “Settings” and go to the “Advanced” tab, the following screen will appear:


Performance Options

Processor scheduling

Choose how to allocate processor resources.

Adjust for best performance of:

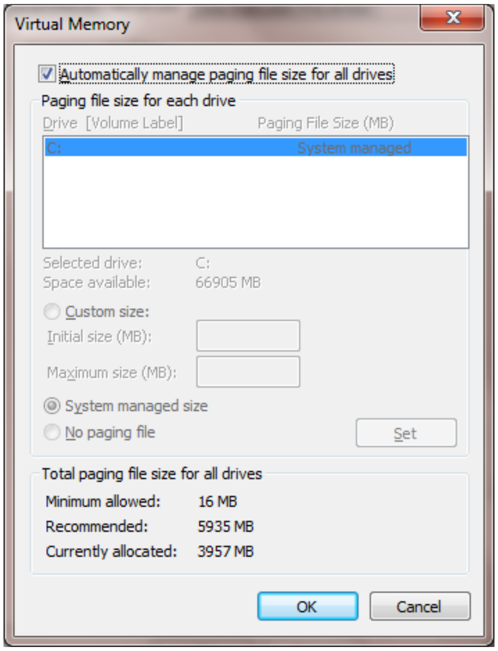
● Programs ○ Background services

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 will appear:


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

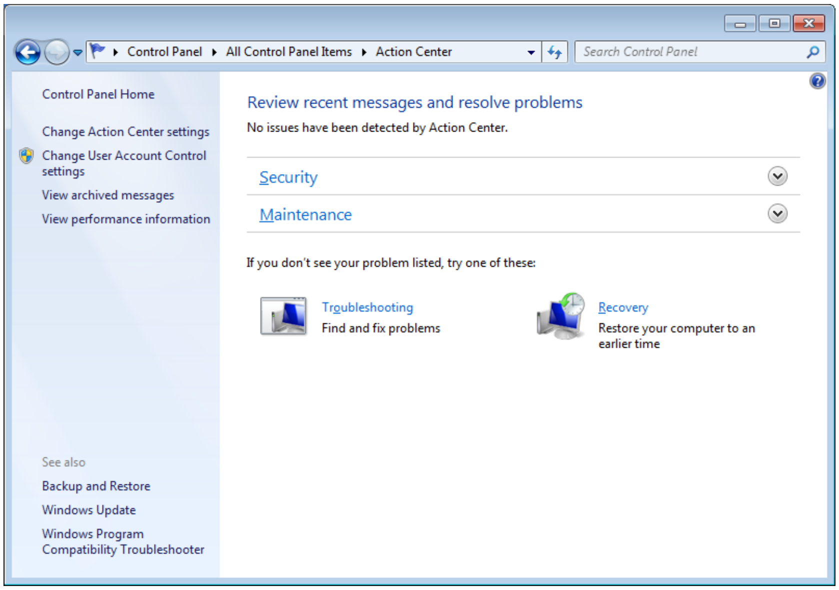
Currently allocated: 3957 MB

- 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 2x the amount of memory in the system.
- Click “Ok”, “OK”, and “OK”
- You will be prompted to reboot your computer.

Disabling Windows Error Reporting – Windows 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

Review recent messages and resolve problems

No issues have been detected by Action Center.

Security

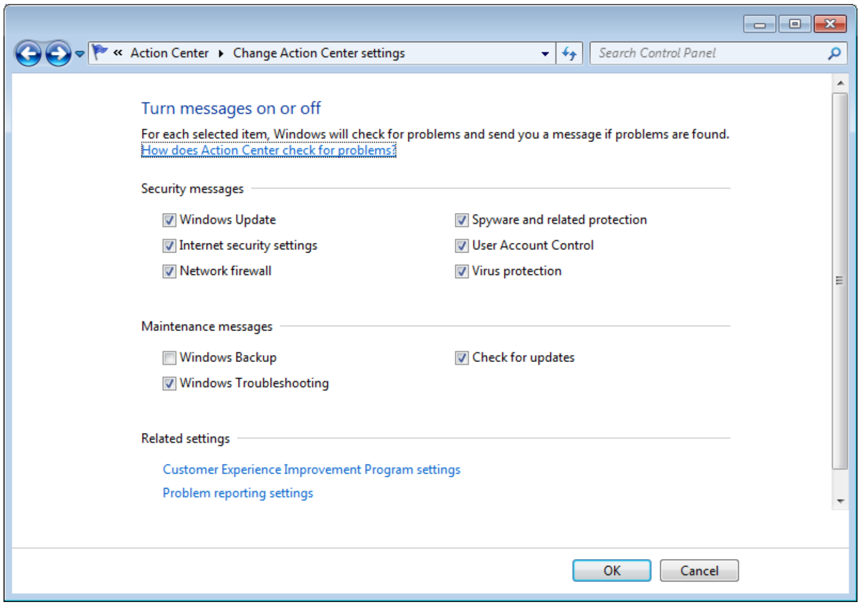
Maintenance

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

Troubleshooting
Find and fix problems

Recovery
Restore your computer to an earlier time

- 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

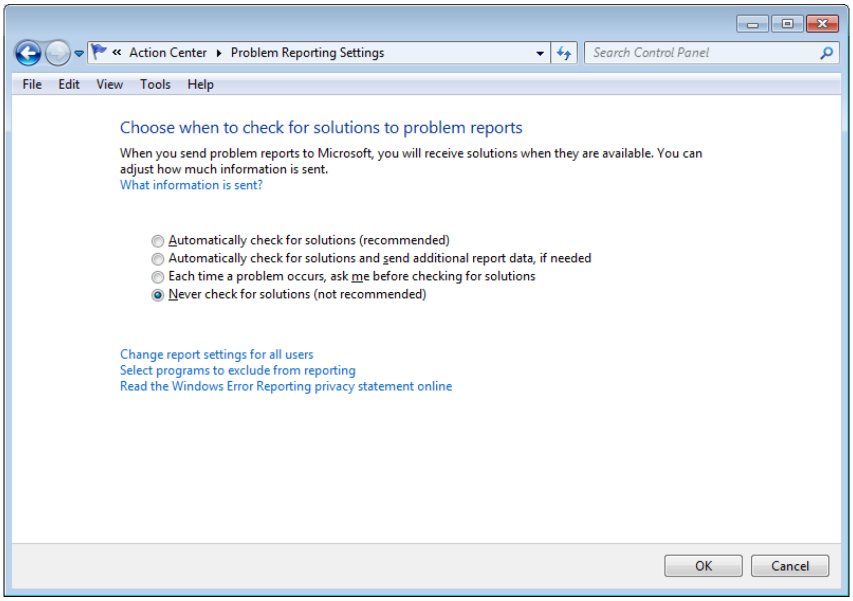
Maintenance messages

□ 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?

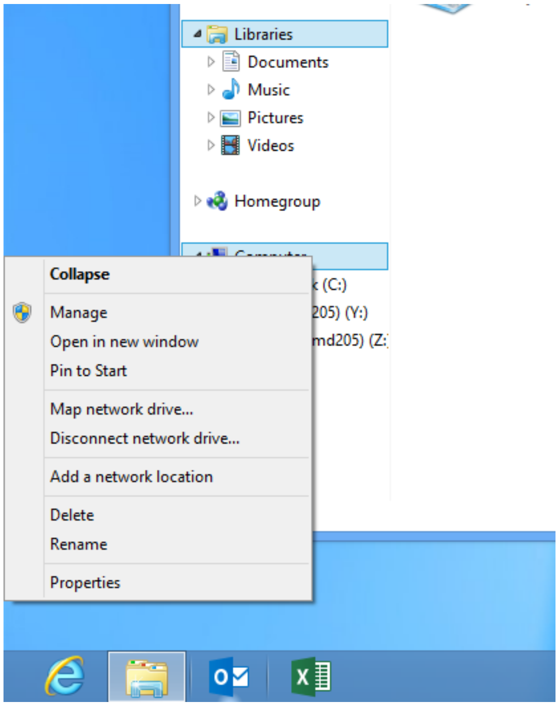
○ Automatically check for solutions (recommended)
○ Automatically check for solutions and send additional report data, if needed
○ Each time a problem occurs, ask me before checking for solutions
● Never check for solutions (not recommended)

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

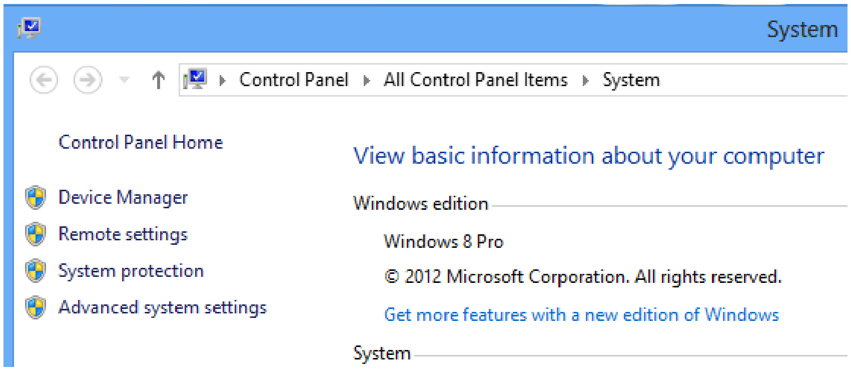
Addressing Inadvertent Capture of PAN on WINDOWS 8

Disabling System Restore – Windows 8

- Right Click on Computer > Select “Properties”:



- Select “Advanced System Settings” from the System screen:



View basic information about your computer

Windows edition

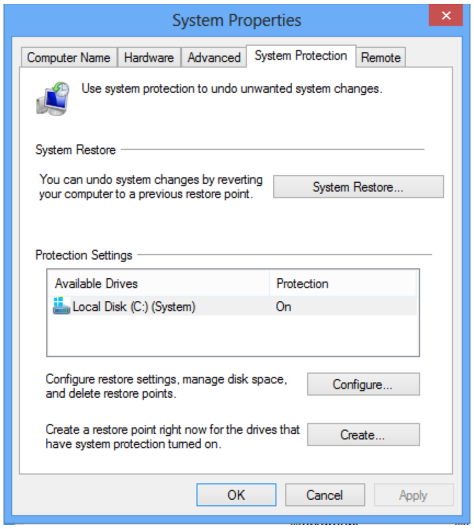
Windows 8 Pro

© 2012 Microsoft Corporation. All rights reserved.

Get more features with a new edition of Windows

System

- Select “System Protection” on the top left list, the following screen will appear:



Use system protection to undo unwanted system changes.

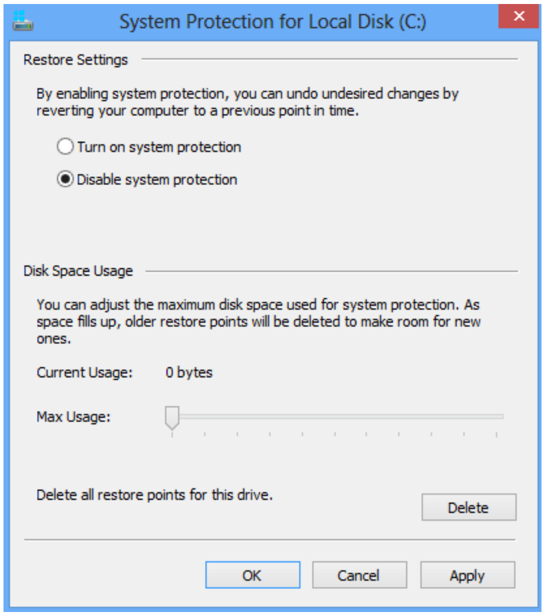
You can undo system changes by reverting your computer to a previous restore point.

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 will appear:



By enabling system protection, you can undo undesired changes by reverting your computer to a previous point in time.

○ Turn on system protection

● Disable system protection

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: 0 bytes

Delete all restore points for this drive.

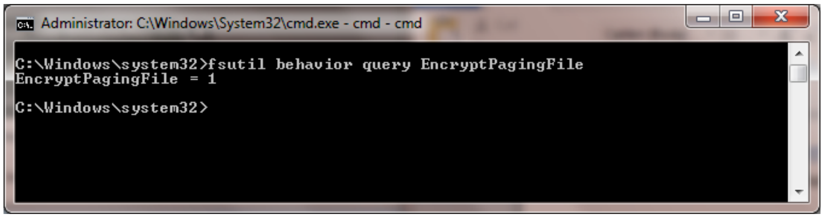
- Select “Disable system protection”
- Click apply, and OK to shut the System Protection window
- Click OK again to shut the System Properties window
- Reboot the computer

Encrypting PageFile.sys – Windows 8

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

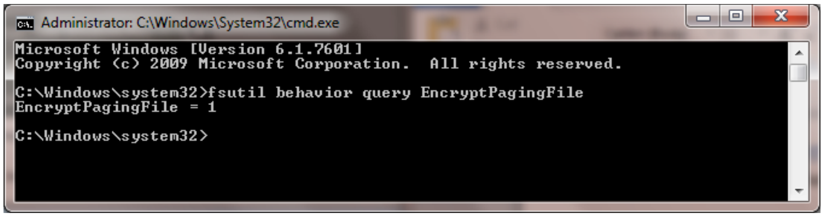
- From the desktop hold down the “Windows” key and type “F” to bring up the “Search” charm, select “Apps” in the “Apps” box type in “cmd”.

- Right click on “Command Prompt” icon located on the left side of your screen, a selection bar will appear at the bottom of the screen, select “Run as Administrator”
- To verify configuration type the following command: fsutil behavior query EncryptPagingFile”



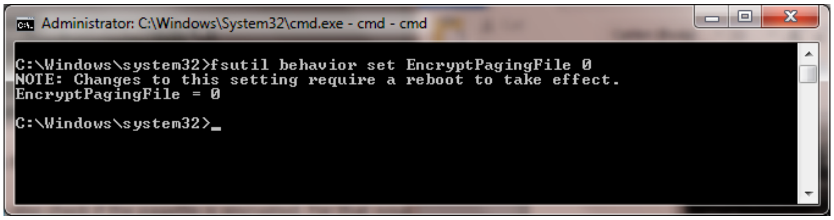
```
C:\Windows\system32>fsutil behavior query EncryptPagingFile
EncryptPagingFile = 1

C:\Windows\system32>
```

- If encryption is enabled EncryptPagingFile = 1 should appear
- If encryption is disabled EncryptPagingFile = 0 should appear
- 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>
```

- 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>_
```

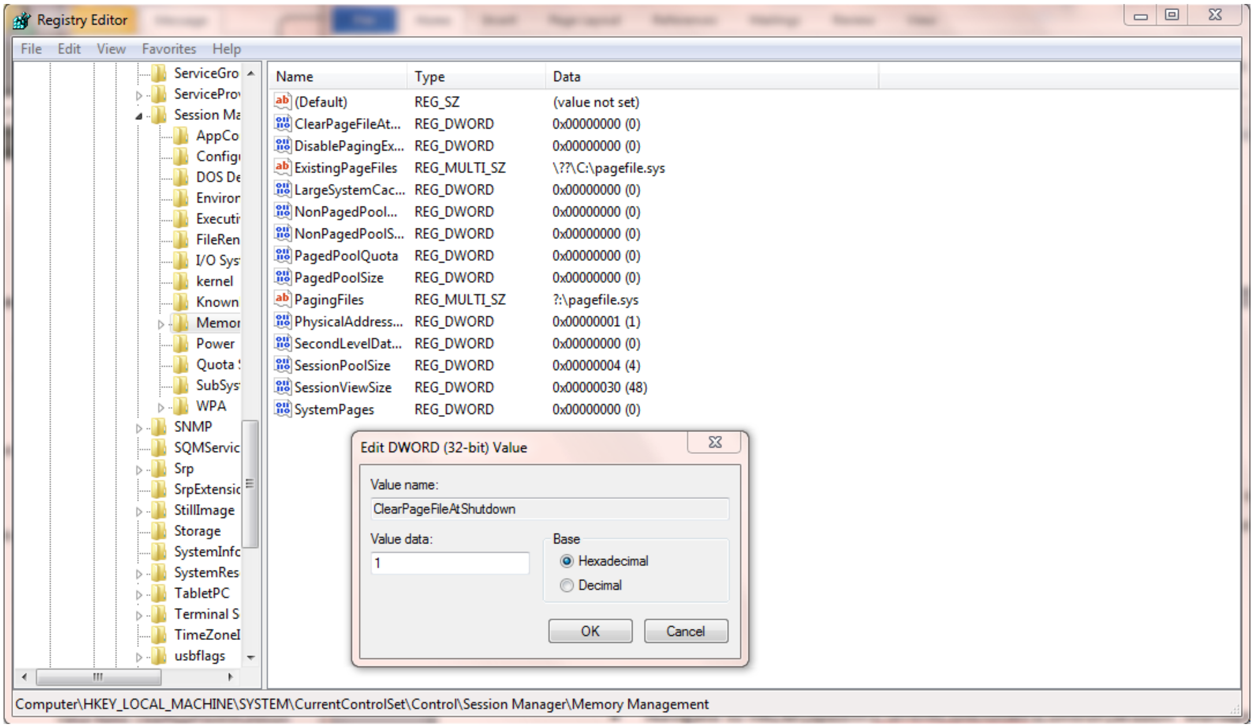
Clear the System Pagefile.sys on shutdown

Windows has the ability to 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.

- From the desktop hold down the “Windows” key and type “F” to bring up the “Search” charm, select “Apps” in the “Apps” box type in “regedit”.
- Right click on regedit.exe and select “Run as Administrator”
- Navigate to HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management
- Change the value from 0 to 1 on the “ClearPageFileAtShutdown” DWORD.

- 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

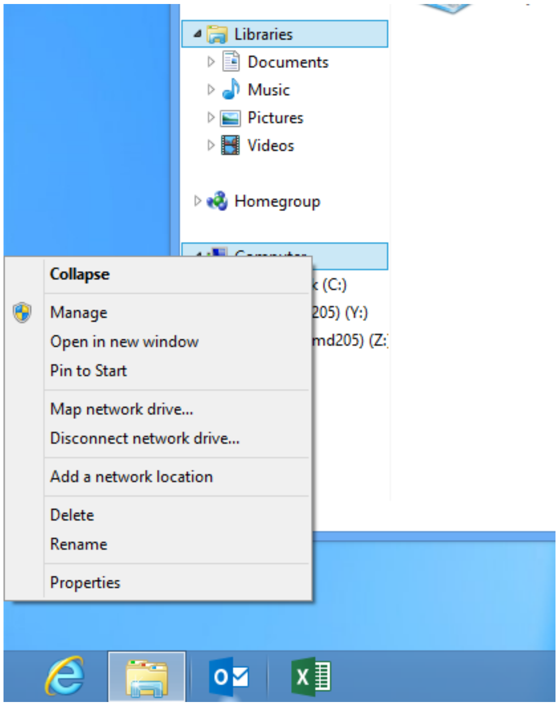
Base: ● Hexadecimal ○ Decimal

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

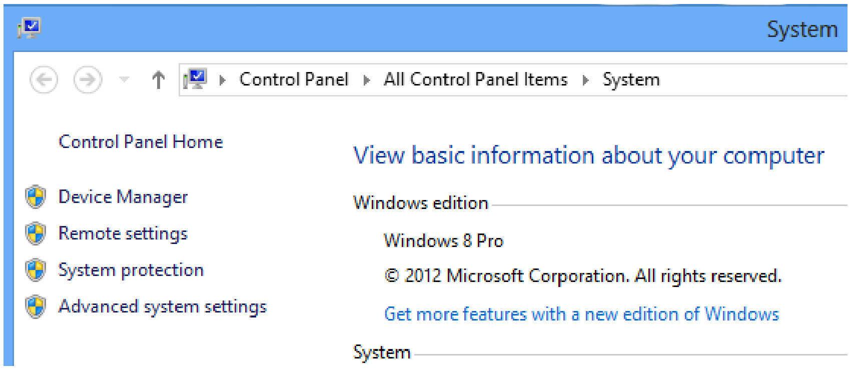
- If the value does not exist, add the following:
  - Value Name: ClearPageFileAtShutdown
  - Value Type: REG_DWORD
  - Value: 1

Disabling System Management of PageFile.sys – Windows 8

- Right Click on Computer > Select “Properties”:



- Select “Advanced System Settings” from the System screen:



View basic information about your computer

Windows edition

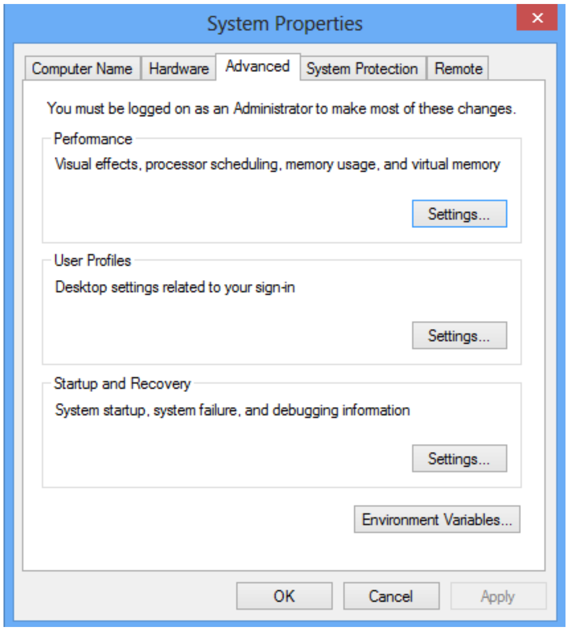
Windows 8 Pro

© 2012 Microsoft Corporation. All rights reserved.

Get more features with a new edition of Windows

System

- Select the “Advanced” tab:



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

Performance

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

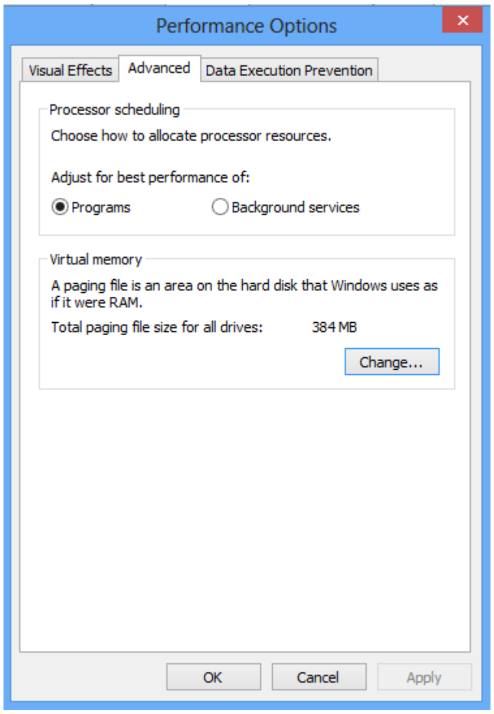
User Profiles

Desktop settings related to your sign-in

Startup and Recovery

System startup, system failure, and debugging information

- Under performance select “Settings” and go to the “Advanced” tab, the following screen will appear:



Processor scheduling

Choose how to allocate processor resources.

Adjust for best performance of:

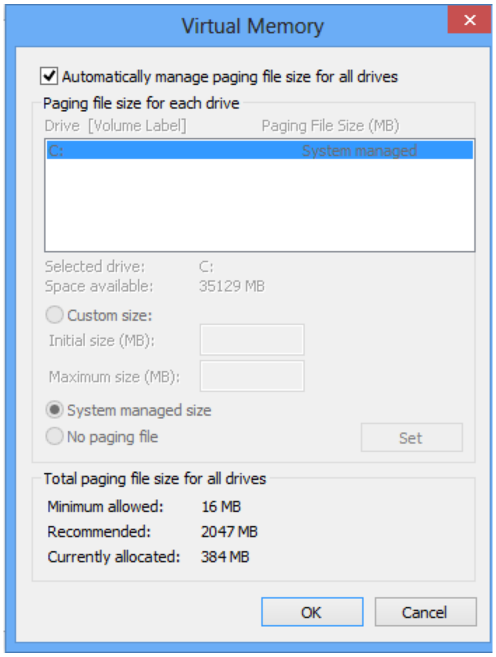
● Programs ○ Background services

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: 384 MB

- Select “Change” under Virtual Memory, the following screen will appear:



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: 35129 MB

○ Custom size:
Initial size (MB):
Maximum size (MB):
● System managed size
○ No paging file

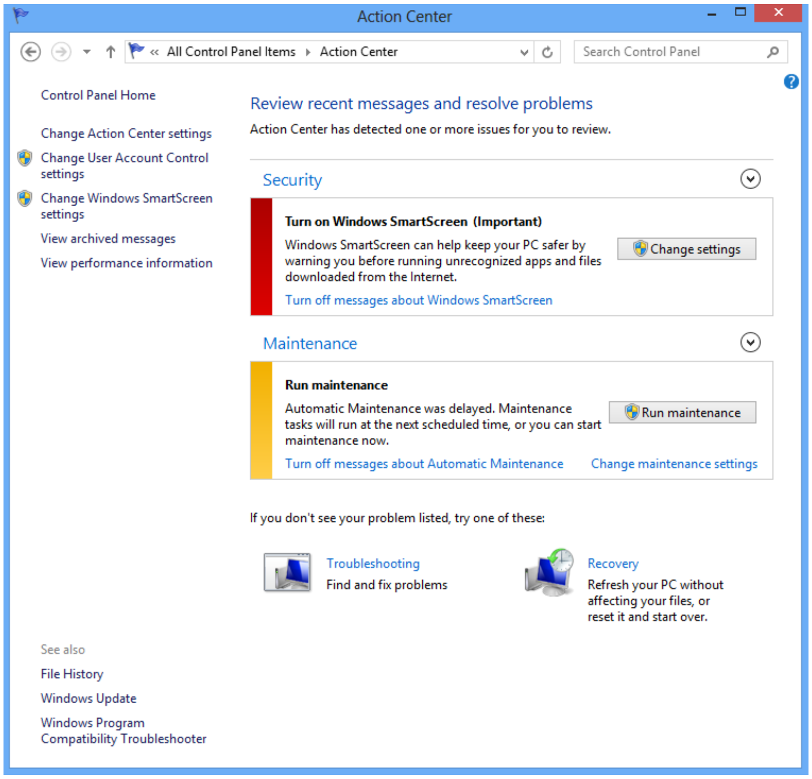
Total paging file size for all drives

Minimum allowed:	16 MB
Recommended:	2047 MB
Currently allocated:	384 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 2x the amount of memory in the system.
- Click "Ok", "OK", and "OK"
- You will be prompted to reboot your computer.

Disabling Windows Error Reporting – Windows 8

- From the desktop hold down the "Windows" key and type "I" to bring up the "Settings" charm, select "Control Panel".
- Open the Action Center
- Select "Change Action Center Settings":


Action Center
« All Control Panel Items ▸ Action Center
Search Control Panel
Control Panel Home
Change Action Center settings
Change User Account Control settings
Change Windows SmartScreen settings
View archived messages
View performance information

Review recent messages and resolve problems

Action Center has detected one or more issues for you to review.

Security

Turn on Windows SmartScreen (Important)

Windows SmartScreen can help keep your PC safer by warning you before running unrecognized apps and files downloaded from the Internet.

Change settings
Turn off messages about Windows SmartScreen

Maintenance

Run maintenance

Automatic Maintenance was delayed. Maintenance tasks will run at the next scheduled time, or you can start maintenance now.

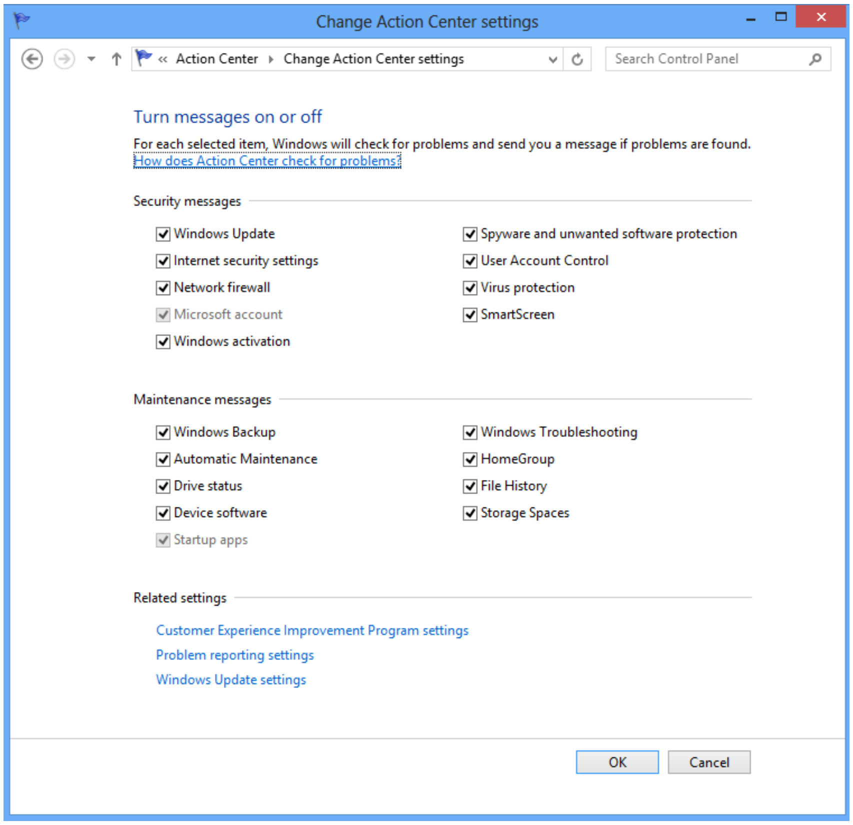
Run maintenance
Turn off messages about Automatic Maintenance
Change maintenance settings

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

Troubleshooting
Find and fix problems

Recovery
Refresh your PC without affecting your files, or reset it and start over.

- Select "Problem Reporting Settings":


Change Action Center settings
« Action Center ▸ Change Action Center settings
Search Control Panel

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
☑ Microsoft account
☑ Windows activation
☑ Spyware and unwanted software protection
☑ User Account Control
☑ Virus protection
☑ SmartScreen

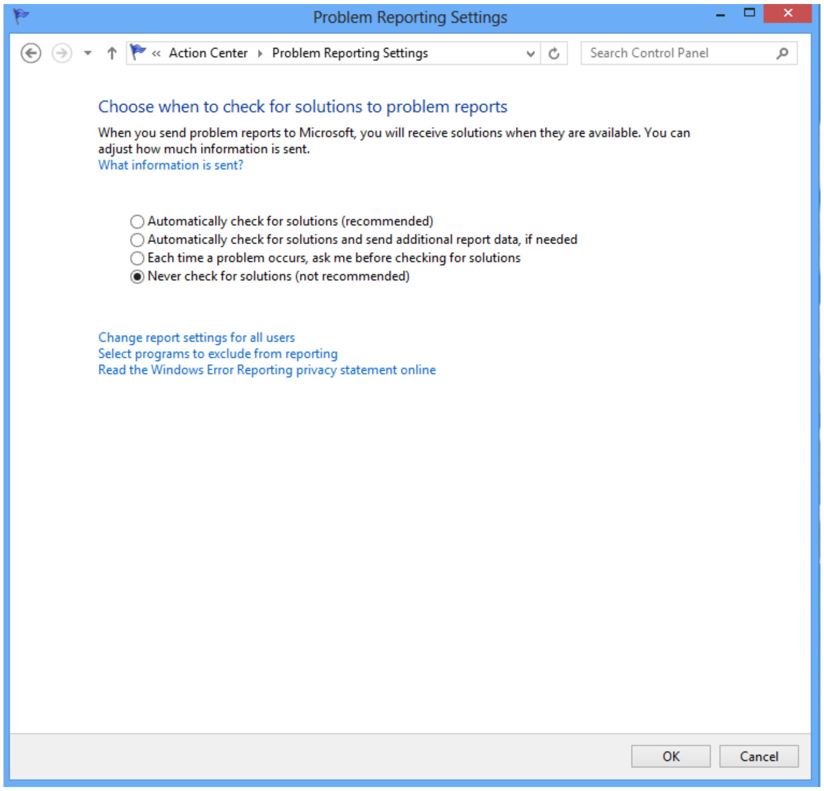
Maintenance messages

☑ Windows Backup
☑ Automatic Maintenance
☑ Drive status
☑ Device software
☑ Startup apps
☑ Windows Troubleshooting
☑ HomeGroup
☑ File History
☑ Storage Spaces

Related settings

Customer Experience Improvement Program settings
Problem reporting settings
Windows Update 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

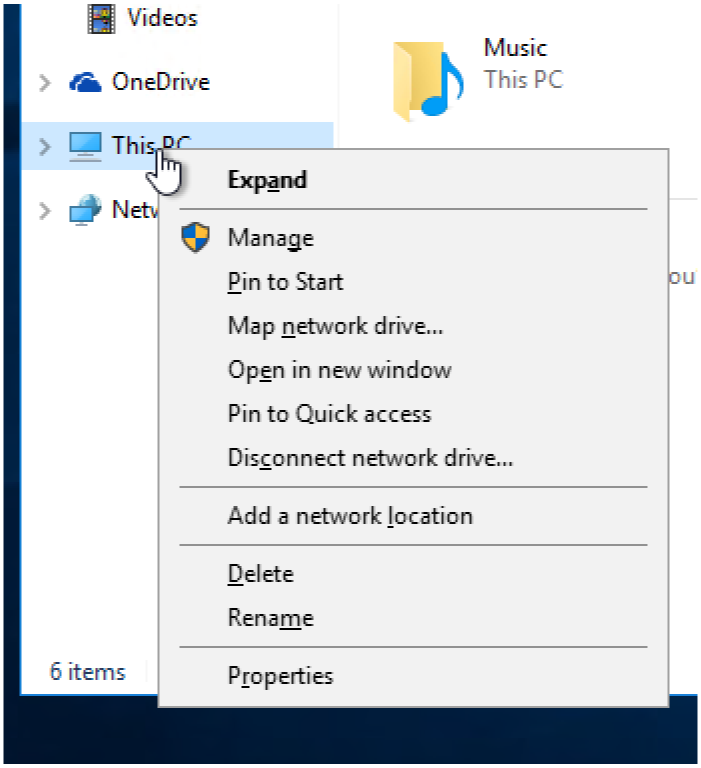
Problem Reporting Settings
« Action Center ▸ Problem Reporting Settings
Search Control Panel
OK
Cancel

- Select “OK” twice and then close Action Center.

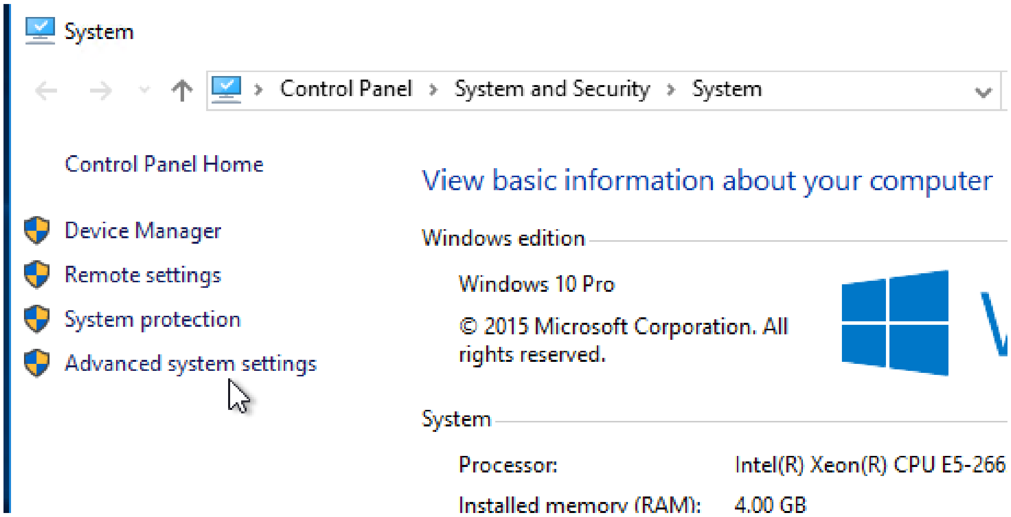
Addressing Inadvertent Capture of PAN on WINDOWS 10

Disabling System Restore – Windows 10

- Right Click on This PC > Select “Properties”:



- Select “Advanced System Settings” from the System screen:



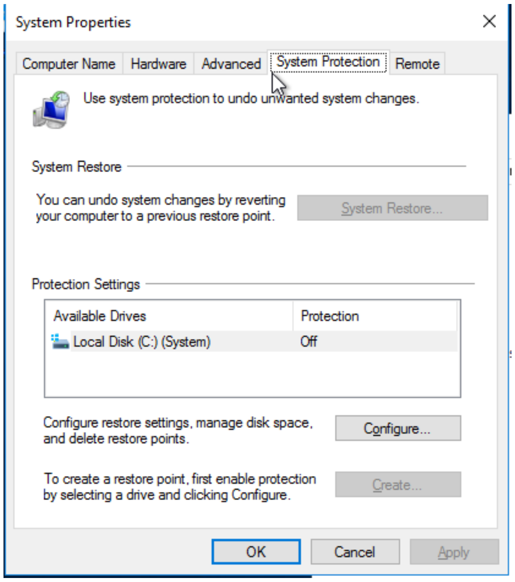
Windows 10 Pro

© 2015 Microsoft Corporation. All rights reserved.

Processor: Intel(R) Xeon(R) CPU E5-266

Installed memory (RAM): 4.00 GB

- Select “System Protection” tab, the following screen will appear:



Use system protection to undo unwanted system changes.

System Restore

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

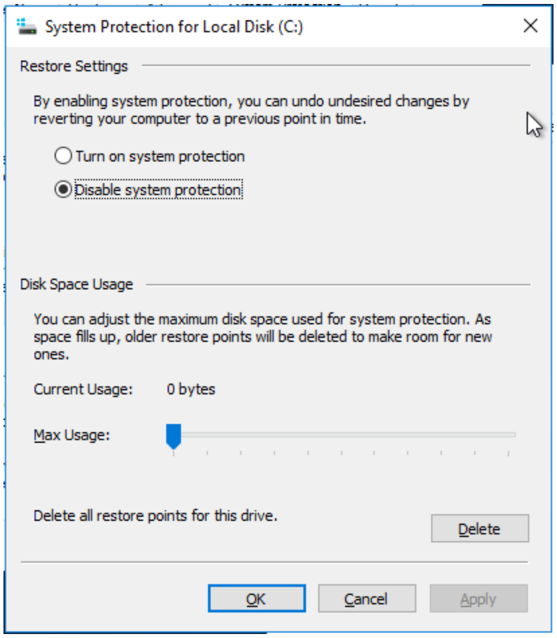
Protection Settings

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

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

To create a restore point, first enable protection by selecting a drive and clicking Configure.

- Select Configure, the following screen will appear:



Restore Settings

By enabling system protection, you can undo undesired changes by reverting your computer to a previous point in time.

○ Turn on system protection

● Disable 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: 0 bytes

Max Usage:

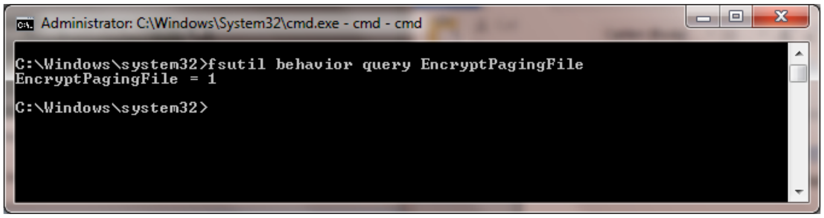
Delete all restore points for this drive.

- Select “Disable system protection”
- Click apply, and OK to shut the System Protection window
- Click OK again to shut the System Properties window
- Reboot the computer

Encrypting PageFile.sys – Windows 10

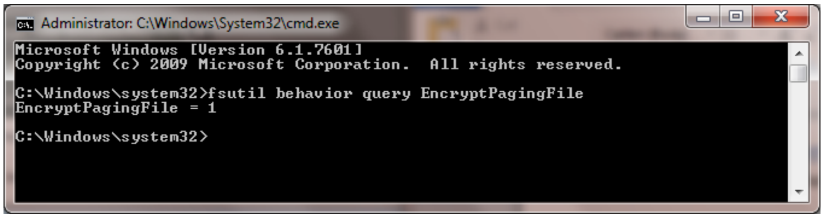
* Please note that in order to perform this operation the hard disk must be formatted using NTFS.

- From the start menu, type in “cmd”.
- Right click on “Command Prompt” icon located on the left side of your screen, a selection bar will appear at the bottom of the screen, select “Run as Administrator”
- To verify configuration type the following command: fsutil behavior query EncryptPagingFile



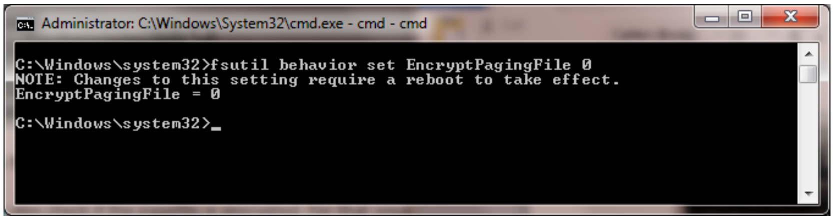
```
C:\Windows\system32>fsutil behavior query EncryptPagingFile
EncryptPagingFile = 1

C:\Windows\system32>
```

- If encryption is enabled EncryptPagingFile = 1 should appear
- If encryption is disabled EncryptPagingFile = 0 should appear
- 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>
```

- In the event you need to disable PageFile encryption type the following command: fsutil behavior set EncryptPagingFile 0



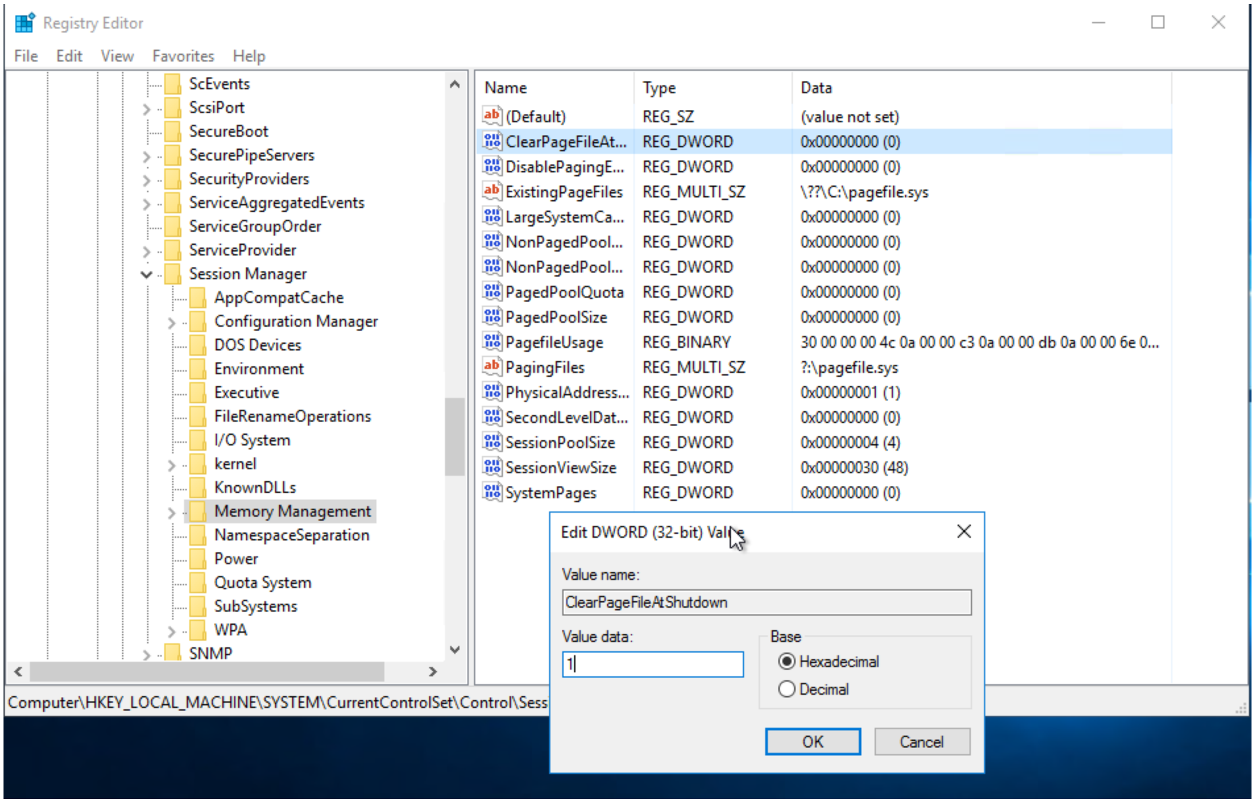
```
C:\Windows\system32>fsutil behavior set EncryptPagingFile 0
NOTE: Changes to this setting require a reboot to take effect.
EncryptPagingFile = 0

C:\Windows\system32>_
```

Clear the System Pagefile.sys on shutdown

Windows has the ability to 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.

- From the start menu, type in "regedit".
- Right click on regedit.exe and select "Run as Administrator"
- Navigate to HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management
- Change the value from 0 to 1 on the "ClearPageFileAtShutdown" DWORD.
- Click OK and close Regedit



Name	Type	Data
(Default)	REG_SZ	(value not set)
ClearPageFileAt...	REG_DWORD	0x00000000 (0)
DisablePagingE...	REG_DWORD	0x00000000 (0)
ExistingPageFiles	REG_MULTI_SZ	\??\C:\pagefile.sys
LargeSystemCa...	REG_DWORD	0x00000000 (0)
NonPagedPool...	REG_DWORD	0x00000000 (0)
NonPagedPool...	REG_DWORD	0x00000000 (0)
PagedPoolQuota	REG_DWORD	0x00000000 (0)
PagedPoolSize	REG_DWORD	0x00000000 (0)
PagefileUsage	REG_BINARY	30 00 00 00 4c 0a 00 00 c3 0a 00 00 db 0a 00 00 6e 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)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Sess

Edit DWORD (32-bit) Value

Value name: ClearPageFileAtShutdown

Value data: 1

Base

● Hexadecimal

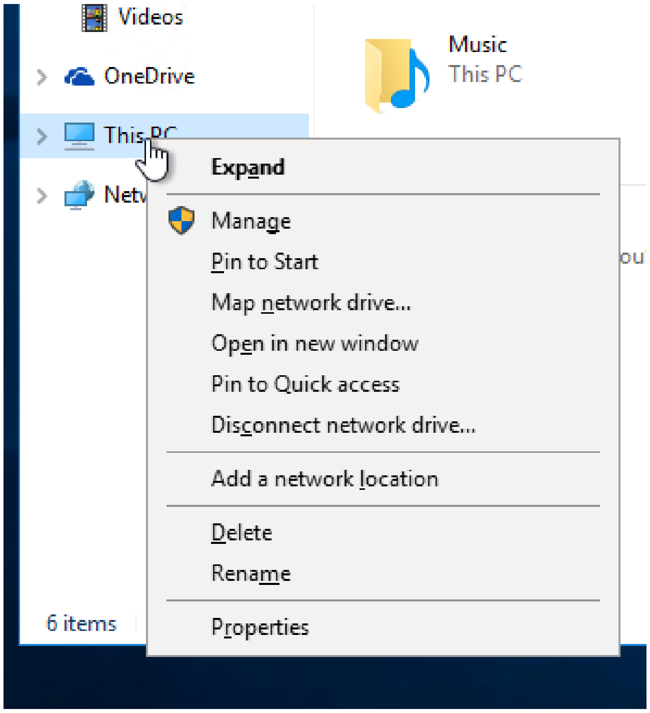
○ Decimal

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

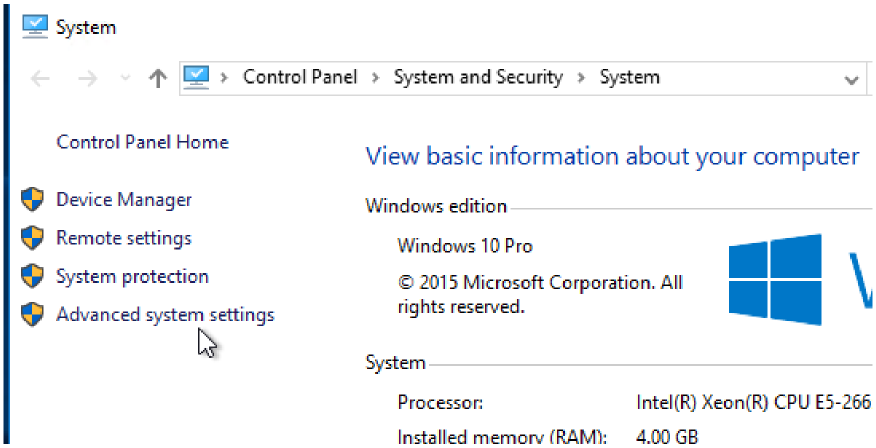
    - Value: 1

Disabling System Management of PageFile.sys – Windows 10

- Right Click on This PC > Select “Properties”:



- Select “Advanced System Settings” from the System screen:



View basic information about your computer

Windows edition

Windows 10 Pro

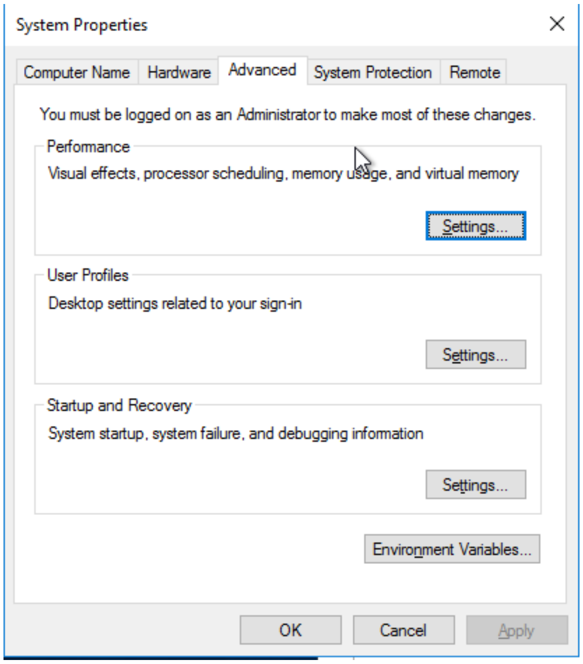
© 2015 Microsoft Corporation. All rights reserved.

System

Processor: Intel(R) Xeon(R) CPU E5-266

Installed memory (RAM): 4.00 GB

- Select the “Advanced” tab:



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

Performance

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

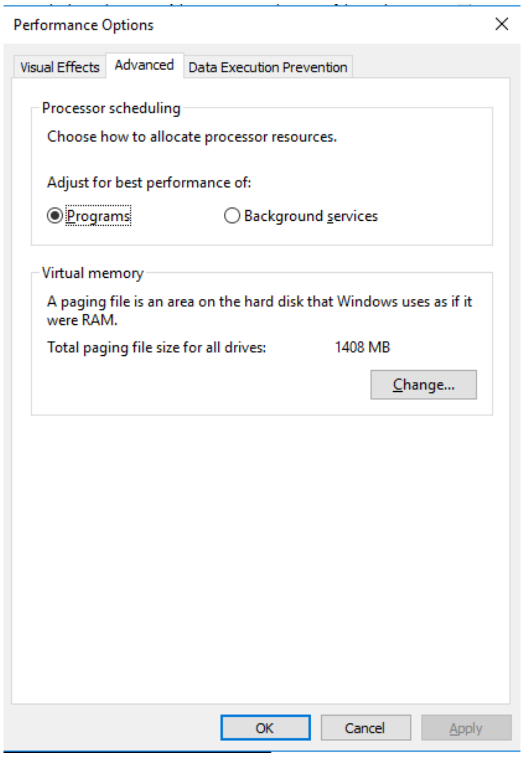
User Profiles

Desktop settings related to your sign-in

Startup and Recovery

System startup, system failure, and debugging information

- Under performance select “Settings” and go to the “Advanced” tab, the following screen will appear:



Performance Options

Processor scheduling

Choose how to allocate processor resources.

Adjust for best performance of:

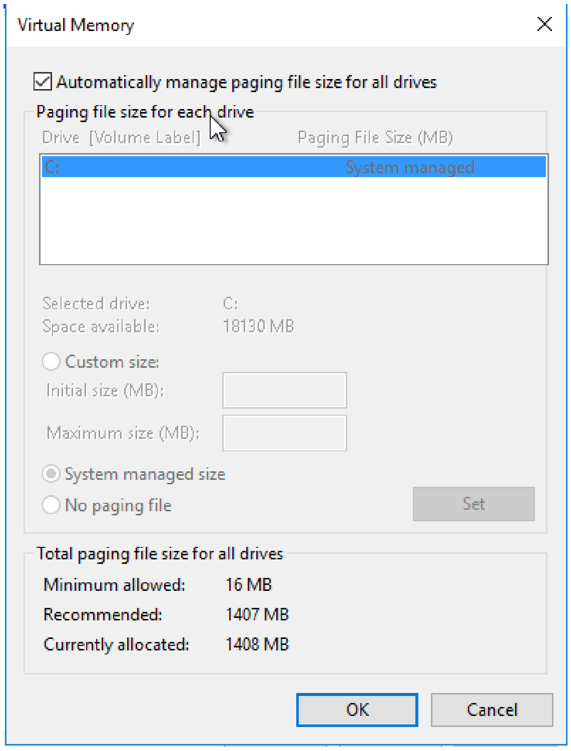
● Programs ○ Background services

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: 1408 MB

- Select “Change” under Virtual Memory, the following screen will appear:



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: 18130 MB

○ Custom size:

Initial size (MB):

Maximum size (MB):

● System managed size

○ No paging file

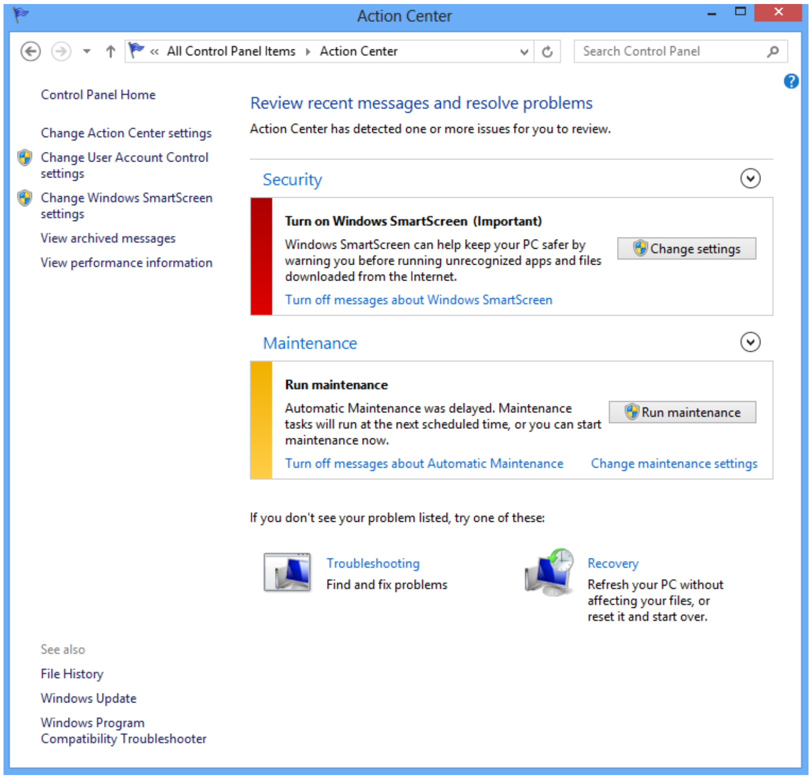
Total paging file size for all drives

Minimum allowed:	16 MB
Recommended:	1407 MB
Currently allocated:	1408 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 2x the amount of memory in the system.
- Click “Ok”, “OK”, and “OK”
- You will be prompted to reboot your computer.

Disabling Windows Error Reporting – Windows 10

- From the start menu, type “control panel”, then enter.
- Open Troubleshooting
- Select ne:


Action Center
« All Control Panel Items ▸ Action Center
Search Control Panel
Control Panel Home
Change Action Center settings
Change User Account Control settings
Change Windows SmartScreen settings
View archived messages
View performance information
Security
Change settings
Maintenance
Run maintenance
Troubleshooting
Recovery
See also
File History
Windows Update
Windows Program Compatibility Troubleshooter

Review recent messages and resolve problems

Action Center has detected one or more issues for you to review.

Turn on Windows SmartScreen (Important)

Windows SmartScreen can help keep your PC safer by warning you before running unrecognized apps and files downloaded from the Internet.

Turn off messages about Windows SmartScreen

Run maintenance

Automatic Maintenance was delayed. Maintenance tasks will run at the next scheduled time, or you can start maintenance now.

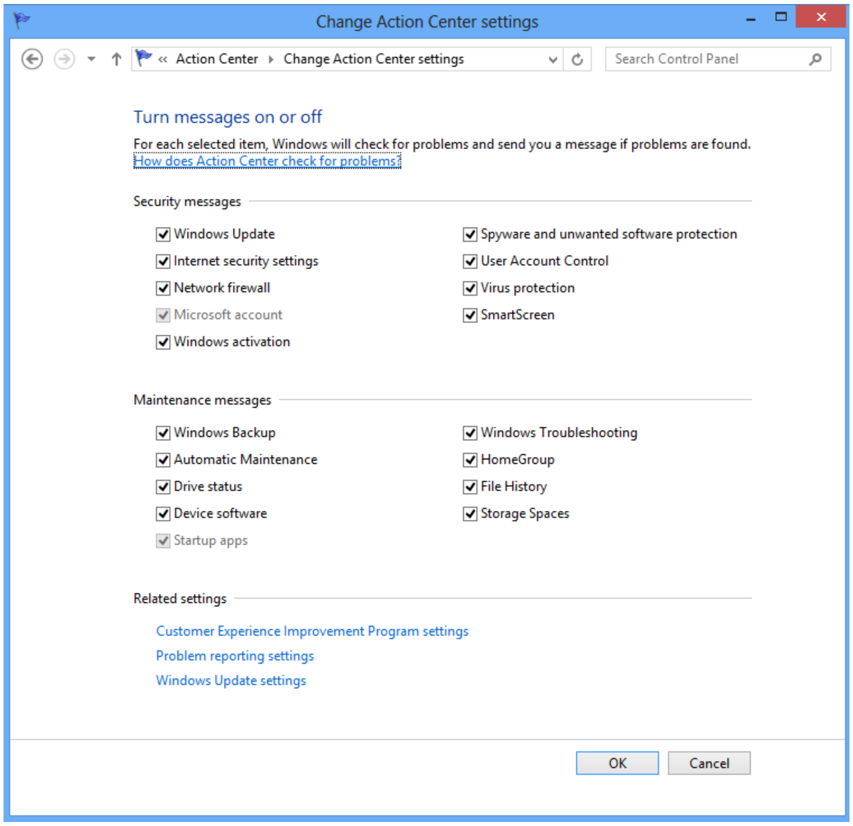
Turn off messages about Automatic Maintenance Change maintenance settings

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

Troubleshooting
Find and fix problems

Recovery
Refresh your PC without affecting your files, or reset it and start over.

- Select “Problem Reporting Settings”:



Change Action Center settings

« Action Center ▸ Change Action Center settings

Search Control Panel

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
☑ Microsoft account
☑ Windows activation
☑ Spyware and unwanted software protection
☑ User Account Control
☑ Virus protection
☑ SmartScreen

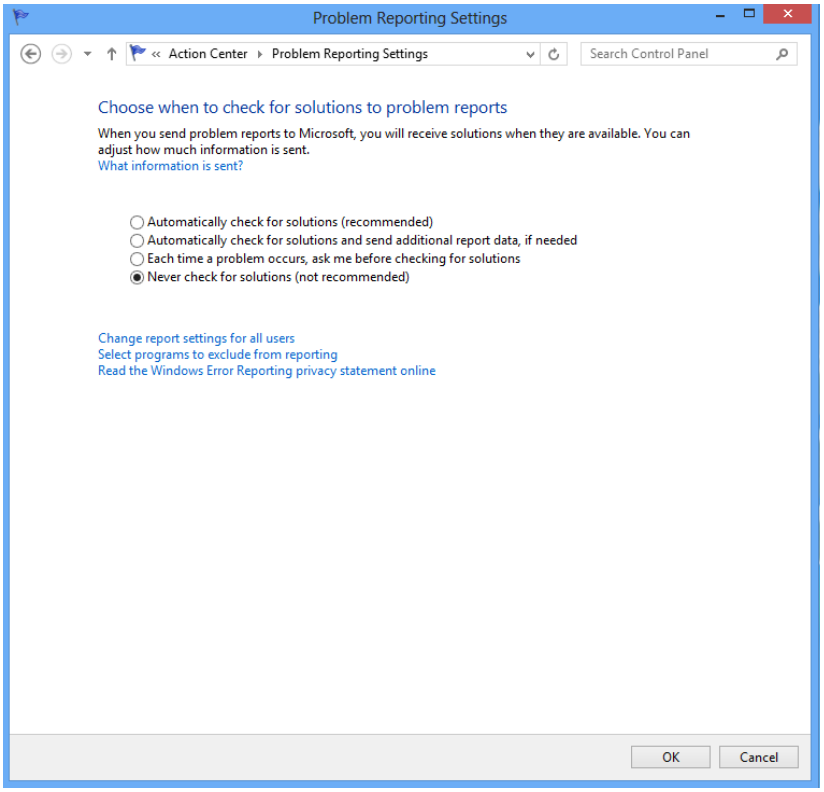
Maintenance messages

☑ Windows Backup
☑ Automatic Maintenance
☑ Drive status
☑ Device software
☑ Startup apps
☑ Windows Troubleshooting
☑ HomeGroup
☑ File History
☑ Storage Spaces

Related settings

Customer Experience Improvement Program settings
Problem reporting settings
Windows Update settings

- Select “Never Check for Solutions”:



Problem Reporting Settings
« Action Center ▸ Problem Reporting Settings
Search Control Panel

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

Select “OK” twice and then close Action Center.