NetSuite POS

Version: 2017.1.X

PA-DSS 3.2 Implementation Guide

Document Version: 1.0

Date: 03/16/2017

Document Owner

Karel Kisza

Product Manager

Oracle Confidential Information

Table of Contents

Notice and Disclaimer

About this Document

This document describes the steps that must be followed in order for your NetSuite Point of Sale (hereafter NetSuite POS) 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)[1].

Oracle instructs and advises its customers to deploy Oracle 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 NetSuite POS installation to support your PCI DSS compliance efforts.

[1] PCI PA-DSS 3.2 can be downloaded from the PCI SSC Document Library (https://www.pcisecuritystandards.org/documents/PA-DSS_v3-2.pdf).

Revision Information

Name	Title	Date of Update	Summary of Changes
George Hanson	Director of Engineering, Retail Anywhere	Jan 6, 2012	Initial version 1.0 for PA-DSS v1.2
George Hanson	Director IT, NetSuite	Aug 26, 2013	Revision 2.0 for PA-DSS v2.0, Company context Retail Anywhere replaced with NetSuite
George Hanson	Director IT, NetSuite	Sep 24, 2013	Product name and version methodology changed from Retail Anywhere POS version 7.2.4 Major.Minor.Revision.Build to NetSuite POS version 2013.2 ReleaseYear.Major.Minor
George Hanson	Director IT, NetSuite	Oct 4, 2013	Removed sensitive authentication data removal instructions for integrated payment applications. Removed prior application references no longer required. Add information on Disabling System Restore Points.
Joshua Goodwin	Product Manager	Jun 1, 2014	Yearly reviewed
Joshua Goodwin	Product Manager	Jun 1, 2015	Updated to PA-DSS v3.0 requirements
Karel Kisza	Product Manager	Mar 1, 2016	Initial version 1.0 for PA-DSS v3.1
Karel Kisza	Product Manager	Aug 31, 2016	New product version revalidation.
Karel Kisza	Product Manager	March 10, 2017	Company name change
Karel Kisza	Product Manager	March 17, 2017	Initial version 1.0 for PA-DSS v3.2

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 accommodation should be made to distribute or make the updated guide available to users. Oracle Corporation will distribute the IG to new customers by email informing them to download it from our customer Help Center.

Summary

NetSuite POS 2017.1.X has been Payment Application Data Security Standard (PA-DSS) validated, in accordance with PA-DSS Version 3.1. For the PA-DSS assessment, Oracle worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PAQSA):

Coalfire Systems, Inc.
11000 Westmoor cir, Westminster CO 80021

This document 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 NetSuite POS Version 2017.1.X as a PA-DSS validated Application operating in a PCI DSS compliant environment.

PCI Security Standards Council Reference Documents

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

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

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

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

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

Application Summary

<table>
<tr><td><b>Payment Application Name</b></td><td>NetSuitePOS</td><td><b>Payment Application Version</b></td><td>2017.1.X</td></tr>
<tr><td><b>Application Description</b></td><td colspan="3">NetSuite POS is used as a point of sale sales terminal running on a dedicated Windows POS hardware setup or standard personal computer. It uses payment gateway applications coupled with PIN pads, signature capture devices and receipt printers to process credit, debit and gift card payments.</td></tr>
<tr><td><b>Typical Role of Application</b></td><td colspan="3">POS system used in various types of retail merchandising outlets.</td></tr>
<tr><td><b>Target Market for Payment Application</b></td><td colspan="3">
<table>
<tr><td colspan="6"><b>Target Market for Payment Application (check all that apply)</b>:</td></tr>
<tr><td>X</td><td><b>Retail</b></td><td></td><td>Processors</td><td></td><td>Gas/Oil</td></tr>
<tr><td></td><td>e-Commerce</td><td>X</td><td><b>Small/medium merchants</b></td><td></td><td></td></tr>
<tr><td></td><td colspan="5">Others (please specify):</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>N/A</td><td><ul><li>Cardholder Name</li><li>Truncated PAN</li><li>Expiration Date</li></ul></td></tr>
<tr><td colspan="2"><b>Individual access to cardholder data is logged as follows:</b><ul><li>Cardholder data from the above table is used only for receipt printing/reprinting purposes</li><li>There is no clear text PAN stored in the application DB.</li></ul></td></tr>
</table>
</td></tr>
<tr><td><b>Components of the Payment Application</b></td><td colspan="3">The following are the application-vendor-developed components which comprise the payment application:<ul><li>NSPOS_2017.1.0.msi<ul><li>Primary POS application, deployed on primary POS terminals</li></ul></li><li>ReplicationPushAgent_2017.1.0.msi<ul><li>Primary replication service for back office data synchronization</li></ul></li><li>AutoUpdater_2017.1.0.msi<ul><li>Primary service for patches/updates delivery</li></ul></li></ul></td></tr>
</table>

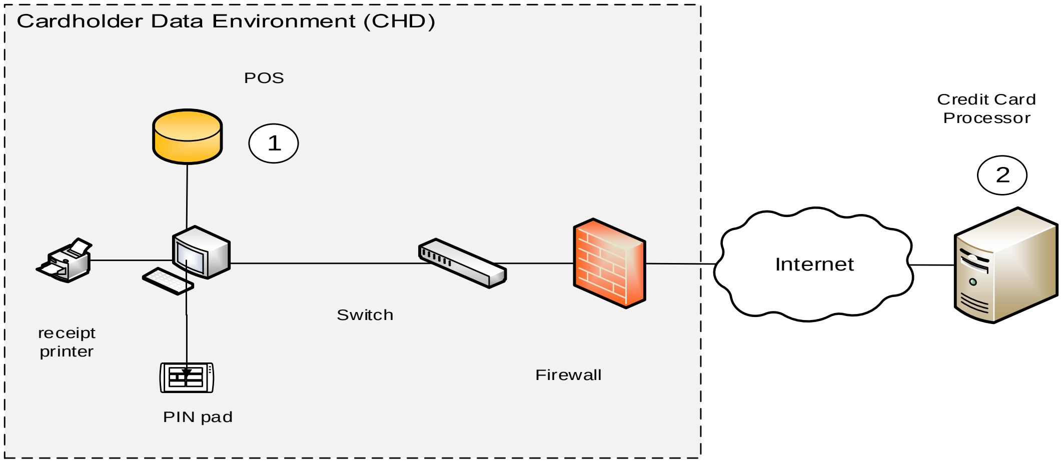
Required Third Party Payment Application Software	The following are additional third party payment application components required by the payment application:

<table>
<tr><td></td><td><ul><li>Shift4, UTG, version 4.7</li><li>NETePay 5, Version 5.06.XX</li></ul></td></tr>
<tr><td><b>Database Software Supported</b></td><td>The following are database management systems supported by the payment application:<ul><li>Microsoft SQL Server 2008 R2 Express</li></ul></td></tr>
<tr><td><b>Other Required Third Party Software</b></td><td>The following are other required third party software components required by the payment application:<ul><li>NONE</li></ul></td></tr>
<tr><td><b>Operating System(s) Supported</b></td><td>The following are Operating Systems supported or required by the payment application:<ul><li>Windows 8.1 (x86, x64)</li><li>Windows 7 Professional (x86, x64)</li><li>Windows Embedded POSReady 7 (x86, x64)</li><li>Windows 10 (x86, x64)</li></ul></td></tr>
<tr><td><b>Application Authentication</b></td><td><p>The administrator of NetSuite POS is allowed to manage users’ accounts and define their privileges. Each user is required to login to the application using a username/password at the beginning of work and has to logout at the end. After 15 minutes of inactivity, the user is automatically logged out.</p><p>Users’ NetSuite POS credentials are stored in the database. Passwords are hashed by SHA-1 with salt.</p></td></tr>
<tr><td><b>Application Encryption</b></td><td>NetSuite POS does not use any encryption; rather the PAN is truncated immediately as it is read from the pin pad prior to storing on the database.</td></tr>
<tr><td><b>Application Functionality Supported</b></td><td><b>Payment Application Functionality (check only one):</b>
<table>
<tr><td></td><td>Automated Fuel Dispenser</td><td></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>X</td><td><b>POS Suite/General</b></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><p><b>Shift4:</b></p><ol><li>The NetSuite POS initiates a transaction with the installed UTG<ol type="a"><li>UTG obtains MSR information without interacting with NetSuite POS</li></ol></li><li>The authorization transaction is encrypted and processed by UTG communicating with Shift4's processing center running DOLLARS ON THE NET.</li><li>The authorization response is encrypted and returned to the UTG over the Internet</li><li>The transaction response is returned to NetSuite POS.</li></ol><p><b>Vantiv Integrated Payments:</b></p></td></tr>
</table>

	1. Credit Card is read/swiped at the card reading device and according to configuration: a. NetSuite POS receives the MSR data and supplies it to DSIClientX 2. Track data is encrypted and sent by DSIClientX to the server running NETePay 5; transaction is processed. 3. NETePay sends encrypted response to DSIClientX 4. NetSuite POS receives response from DSIClientX
Description of Listing Versioning Methodology	NetSuite POS versioning has three levels, Year, Major, Minor: <Year>.<Major>.<Minor> • **Year** – determines the year of the release, may or may not have an impact on PA-DSS requirements. • **Major** – determines main release within given year containing new functionality including significant changes to the application; these may or may not have an impact on PA-DSS requirements. • **Minor** – changes include bug fixes or small non impacting enhancements; these would have no impact on PA-DSS requirements and are indicated by the WILDCARD (X). Based on the above versioning methodology the application version being listed with PCI SSC is: 2017.1.X.

Typical Network Implementation

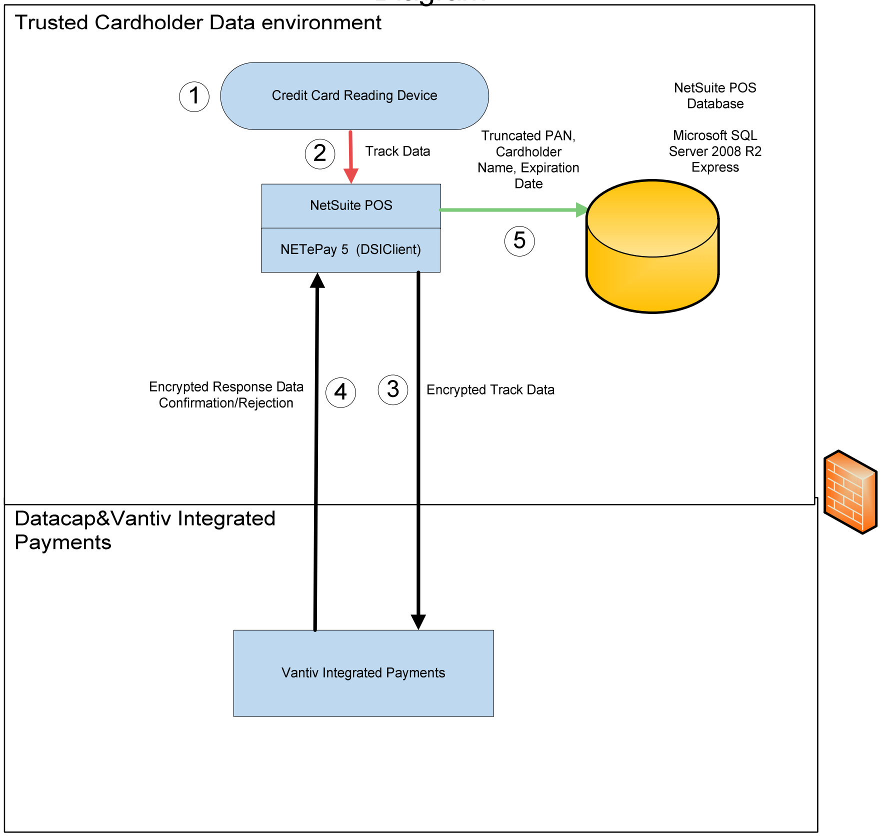
NetSuite POS Network Diagram



1. NetSuite POS (PC, or tablet) connected to locally installed database (database resides on sales terminal PC, or optionally on remote local server). Receipt printer and PIN pad or MSR could be connected to the NetSuite POS.
2. Payment Service Provider.

Credit/Debit Cardholder Dataflow Diagram

Vantiv Integrated Payments(NETePay 5) / NetSuite POS Data Flow Diagram

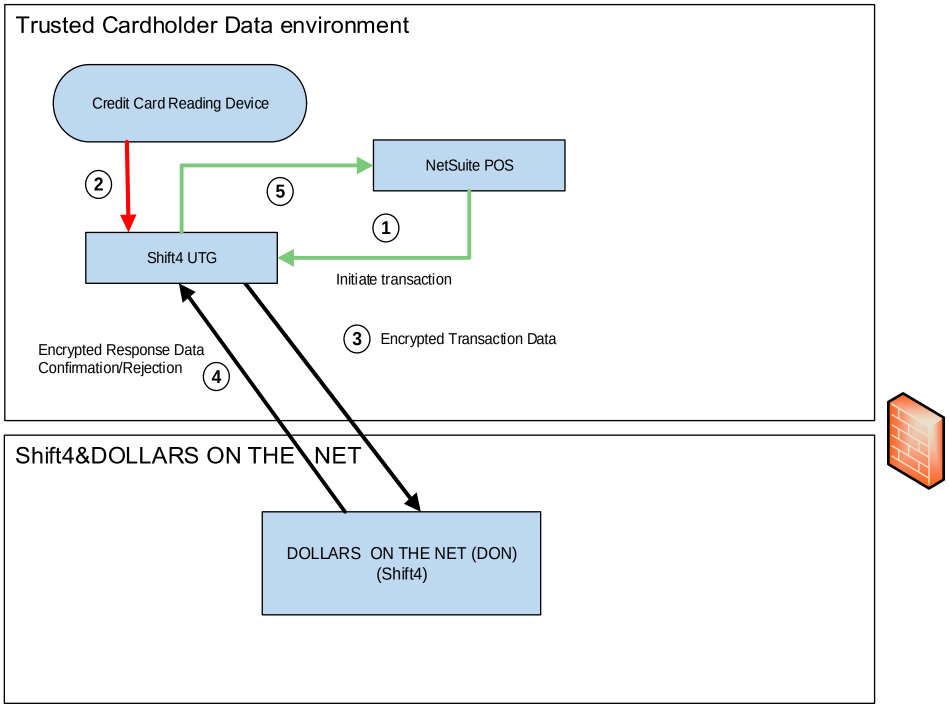

Trusted Cardholder Data environment
1
Credit Card Reading Device
2
Track Data
NetSuite POS
NETePay 5 (DSIClient)
Truncated PAN, Cardholder Name, Expiration Date
5
NetSuite POS Database
Microsoft SQL Server 2008 R2 Express
Encrypted Response Data Confirmation/Rejection
4
3
Encrypted Track Data
Datacap&Vantiv Integrated Payments
Vantiv Integrated Payments

1. Credit card is read / swiped at the card reading device.
2. NetSuite POS receives MSR data and supplies it to DSIClinet which is integrated with NtSuite POS.
3. Track data sent encrypted from POS Station PC by DSIClinet to Vantiv Integrated Payments for processing.
4. Authorization response from Vantiv Integrated Payments is returned to NETePay 5.
5. NetSuite POS stores Truncated PAN, Cardholder Name, and Expiration Date to DB running Microsoft SQL Server 2008 R2 E1xpress

NOTE: DSIClinet is an integrated part of NetSuite POS. Once response received, it is also available to NetSuite POS.

Lines represent type of data in transit as follows:
Red - encrypted or unencrypted sensitive authentication data or cardholder data in transit.
Green - data not considered cardholder or sensitive authentication data.
Black - data flowing from 3rd party software outside scope of NetSuite POS.

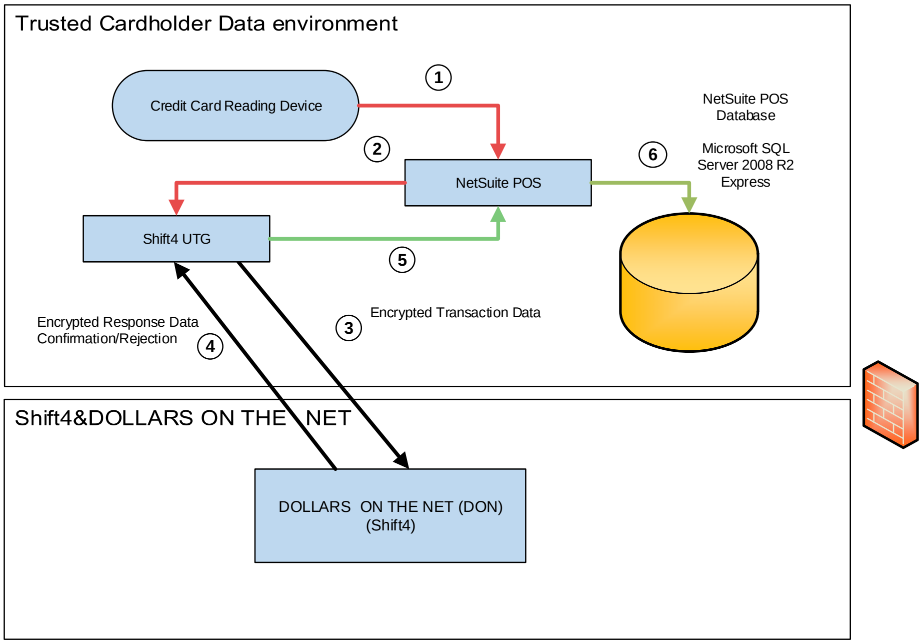
SHIFT4/NetSuite POS Data Flow Diagram



1. **NetSuite POS initiates transaction with UTG.**
2. **UTG sends request to Credit Card Reader Device and processes credit card information from NetSuite POS.**
3. **Authorization transaction is encrypted by UTG and sent to Shift4 processing center running DON.**
4. **Authorization response encrypted by DON and sent to UTG via Internet.**
5. **Transaction response returned to NetSuite POS (does not include any cardholder or sensitive data).**

Lines represent type of data in transit as follows:
Red - encrypted or unencrypted sensitive authentication data or cardholder data in transit.
Green - data not considered cardholder or sensitive authentication data.
Black - data flowing from 3rd party software outside scope of NetSuite POS.

SHIFT4/NetSuite POS Data Flow Diagram


Trusted Cardholder Data environment
Credit Card Reading Device
1
2
NetSuite POS
NetSuite POS Database
Microsoft SQL Server 2008 R2 Express
6
Shift4 UTG
5
Encrypted Transaction Data
3
Encrypted Response Data Confirmation/Rejection
4
Shift4&DOLLARS ON THE NET
DOLLARS ON THE NET (DON) (Shift4)

1. Credit card is read / swiped at the card reading device.
2. NetSuite POS receives MSR data and supplies to UTG application.
3. Authorization transaction is encrypted by UTG and sent to Shift4 processing center running DON.
4. Response encrypted by DON and sent to UTG via Internet.
5. Transaction response returned to NetSuite POS (does not include any cardholder or sensitive data).
6. NetSuite POS stores Truncated PAN, Cardholder Name, and Expiration Date to DB running Microsoft SQL Server 2008 R2 Express

Lines represent type of data in transit as follows:
Red - encrypted or unencrypted sensitive authentication data or cardholder data in transit.
Green - data not considered cardholder or sensitive authentication data.
Black - data flowing from 3rd party software outside scope of NetSuite POS.

Difference between PCI Compliance and PA-DSS Validation

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

PA-DSS Version 3.2 is the standard against which our Payment Application has been tested, assessed, and validated.

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

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

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

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

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

The 12 Requirements of 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 the business on a need-to-know basis*
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 PANs are 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 NetSuite POS did not store sensitive authentication data. Consequently, there is no need for a secure deletion of historical data by the application as required by PA-DSS v3.2.

Handling of Sensitive Authentication Data (PA-DSS 1.1.5)

NetSuite POS 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 required to solve a specific problem.
- Store data only in specific, known locations with limited access.
- Only collect the minimum amount of data needed to solve a specific problem.
- Encrypt sensitive authentication data while stored.
- Securely delete data immediately after use.

Secure Deletion of Cardholder Data (PA-DSS 2.1)

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

All PANs are Masked by Default (PA-DSS 2.2)

By default, NetSuite POS masks all PANs immediately upon receipt from the pin pad/gateway application; in some cases, PANs are received by NetSuite POS in a pre-masked format. PANs are stored in the database as first 6 digits and last four digits unmasked e.g. 123456 XXX XXX 1234. The payment application displays PANs in the following locations:

- On printed receipts in the same format as stored in the DB, or according to country-specific legislation (e.g. only the last four digits are left unmasked in USA).

NetSuite POS does not have the ability to display full PANs for whatever reason. No configuration details therefore need be provided as required by PA-DSS v3.2.

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

NetSuite POS does not store cardholder data in a way that may allow merchants to store cardholder data, therefore no encryption of cardholder data is required under PA-DSS v3.2.

Removal of Historical Cryptographic Material (PA-DSS 2.6)

Previous versions of NetSuite POS did not use encryption, therefore there is no legacy cryptographic data requiring secure deletion as required by PA-DSS v3.2.

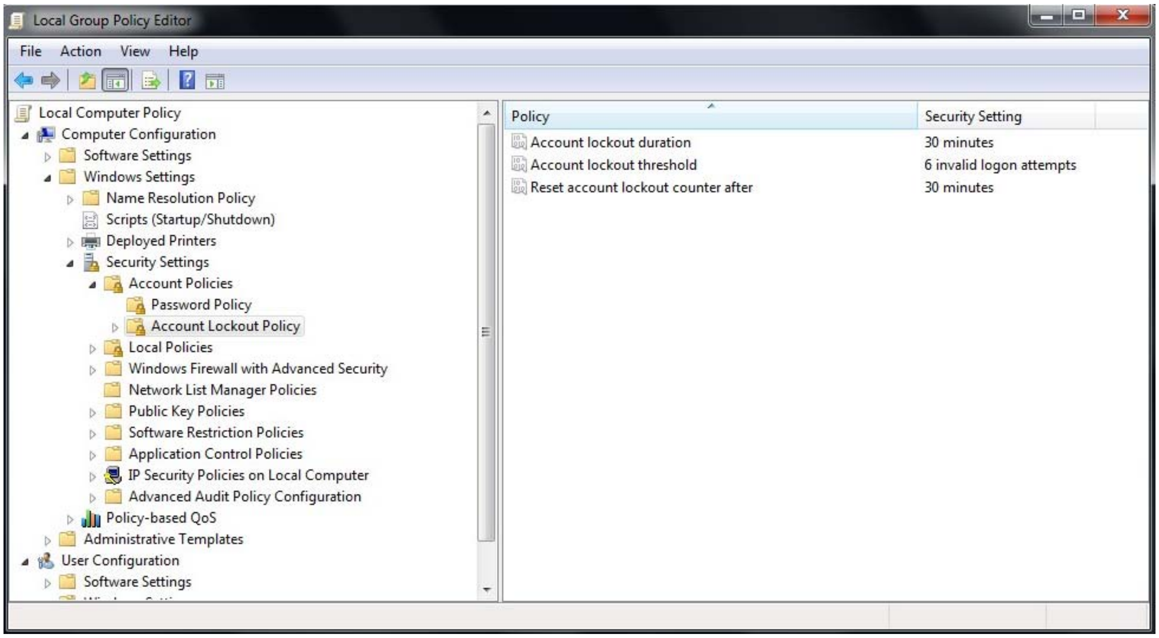
Set up Strong Access Controls (3.1 and 3.2)

PCI DSS requires that access to all systems in the payment processing environment be protected through the 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.

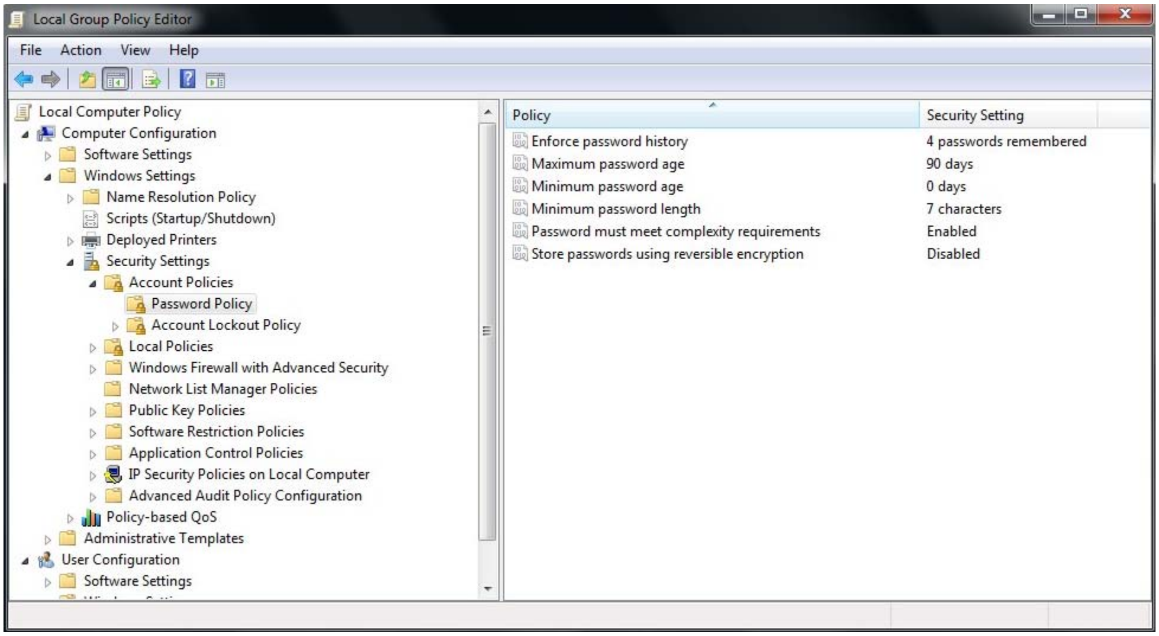
All authentication credentials are generated and managed by the application. Secure authentication is enforced automatically by the payment application for all credentials by the completion of the initial installation and for any subsequent changes (for example, any changes that result in user accounts reverting to default settings, any changes to existing account settings, or changes that generate new accounts or recreate existing accounts). To maintain PCI DSS compliance the following 11 points must be followed:

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

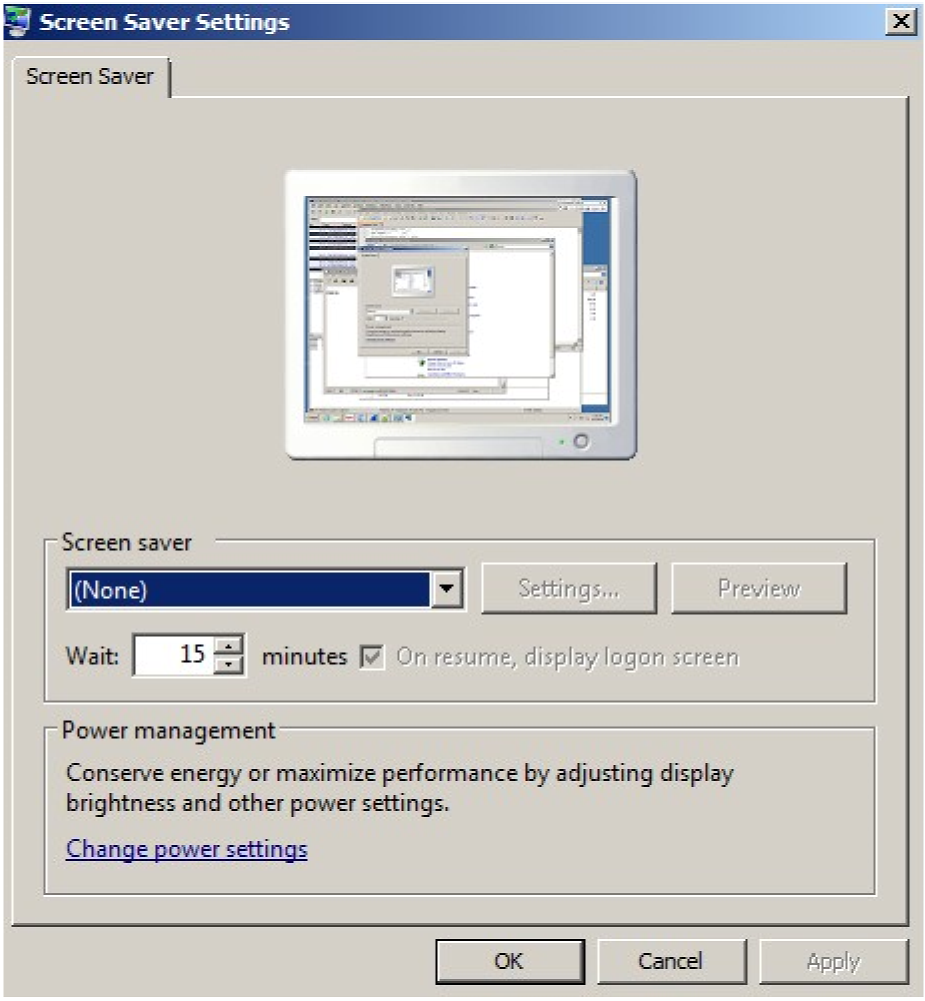
NetSuite POS uses Windows accounts and integrated Windows authentication for accessing the database. To increase account security, set your Windows group policies as depicted:



Policy	Security Setting
Account lockout duration	30 minutes
Account lockout threshold	6 invalid logon attempts
Reset account lockout counter after	30 minutes



Policy	Security Setting
Enforce password history	4 passwords remembered
Maximum password age	90 days
Minimum password age	0 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled



Screen saver: (None)

Wait: 15 minutes ☑ On resume, display logon screen

Conserve energy or maximize performance by adjusting display brightness and other power settings.

Passwords for Windows service account (RARS) used by NetSuite POS should be changed by customers after installation. Users must also change the password on the “RA replication agent” service and restart it otherwise replication will not work.

Configuration of the database should also follow the following rules:

- Windows Authentication mode is more secure than SQL Authentication; Windows authentication is therefore only recommended.
  - If there is still a need to use SQL Authentication – enforce a strong password policy.
- Disable default accounts (e.g. SA account) and rename them. Do not use them for SQL server management.

PA-DSS 3.2 states you must control access, via unique username and PCI DSS-compliant complex passwords, to any PCs or servers with payment applications and to databases storing cardholder data.

Properly Train and Monitor Admin Personnel

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

In most systems, a security breach is the result of unethical personnel. Pay special attention to those entrusted with administrative access and whom you allow to view fully decrypted and unmasked payment information.

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

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

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.

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

4.4.b: NetSuite POS facilitates centralized logging and stores logged events in the SQL Server database table RAPOS.dbo.EventLog. A database trigger may be added to facilitate exporting this table's contents to a standard event log format for centralized logging with a standard logging tool.

Services and Protocols (PA-DSS 8.2)

NetSuite POS does not require the use of any insecure services or protocols. It requires:

- TLS 1.1 and higher
- HTTPS

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

NetSuite POS supports wireless technologies. The following guidelines for secure wireless settings must be followed as per PCI Data Security Standards 1.2.3, 2.1.1 and 4.1.1:

2.1.1: Change wireless vendor defaults as per the following 5 points:

1. Encryption keys must be changed from the default at installation, and must be changed anytime anyone with knowledge of the keys leaves the company or changes positions or their role changes within the company to one that does not include access to the keys.
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 (for example WPA2)
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.

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

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

PCI-Compliant Remote Access (10.2)

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

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

PCI-Compliant Delivery of Updates (PA-DSS 10.2.1)

NetSuite POS delivers patches and updates in a secure manner. As a development company, we keep abreast of the relevant security concerns and vulnerabilities in our area of development and expertise.

We do not deliver software and/or updates via remote access to customer networks. Instead, updates and patches are automatically installed on the sales terminal through a dedicated auto-updater. When an update or patch is ready for delivery to customers, it is automatically pushed over an HTTPS using TLS to the sales terminal and installed. The packages are signed and their integrity is checked before the installation is initiated.

PCI-Compliant Remote Access (10.2.3.)

NetSuite POS does not access user environments by remote access by default. The following instructions are provided to inform the user to operate in a PCI compliant environment.

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

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

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

In order to be compliant, each 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 3.1.1–3.1.11 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 3.1.9 through 3.1.10 and PCI DSS 8.5.13
- Require that remote access takes 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.)

The PCI DSS requires the use of strong cryptography and encryption techniques with at least a 128bit encryption strength (either at the transport layer with TLS 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 (TLS 1.1 or higher) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

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

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

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

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

NetSuite POS does not allow or facilitate the sending of PANs via any end user messaging technology (for example, email, instant messaging, and chat).

Non-console administration (PA-DSS 12.1)

NetSuite POS allows non-console administration — use SSH, VPN, or TLS 1.1 or higher for encryption of this non-console administrative access.

Network Segmentation

PCI DSS requires that firewalls are 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 is 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 NetSuite POS.

Maintain an Information Security Program

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

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

- Read the entire PCI DSS and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.
- Once gaps are identified, determine the steps to close them and protect cardholder data. Changes could mean adding new technologies to strengthen 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 the merchant or service provider level, all entities should complete annual self-assessments using the PCI Self-Assessment Questionnaire.
- Call in outside experts as needed.

Application System Configuration

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

Any of the following Windows operating systems. In all cases, all latest updates and hot-fixes should be applied and tested.

- Windows 8.1 (x86, x64)
- Windows 7 Professional (x86, x64)
- Windows Embedded POSReady 7
- Windows 10 (x86, x64)

- 4 GB or higher recommended for Payment Application
- 30 GB of available hard-disk space
- TCP/IP network connectivity
- SQL Server 2008 R2 Express. All latest updates and hot-fixes should be applied

Disable System Restore Points

If you use a Microsoft Windows system that supports System Restore Points, they must be disabled. System Restore creates and uses restore points to track changes in Windows, and recovers to a previous configuration. It is possible these restore points may retain cardholder data. When you turn off System Restore, the operating system automatically removes existing restore points and stops the creation of new restore points. Instructions on how to do this are also available from Microsoft.

To turn off System Restore

1. Click **Start**, right-click **My Computer**.
2. Click **Properties**.
3. In the **System Properties** dialog box, click the **System Restore** tab.

4. Check the **Turn off System Restore** box.
5. Alternatively, check the **Turn off System Restore on all drives** box.
6. Click **OK**.
7. When you receive the following message, click **Yes** to confirm that you want to turn off System Restore:

> You have chosen to turn off System Restore. If you continue, all existing restore points will be deleted, and you will not be able to track or undo changes to your computer.
>
> Do you want to turn off System Restore?

After a few moments, the System Properties dialog box closes.

Payment Application Initial Setup & Configuration

This process consists of three steps:

- Installing NetSuite POS
- Installing the Payment Gateway Application
- Defining the Payment Gateway within NetSuite POS

Installing NetSuite POS

1. Installation of SQL server, and its configuration at the customer environment, is done by Oracle Professional Services or customer following recommended setting
2. The provisioning/installation process consists of two stages:
   a. Initiation of staging process — generating the terminal-specific URL required for the prepared terminal system environment.
   b. Running generated URL — implementing URL in the terminal system environment and following installation procedures.

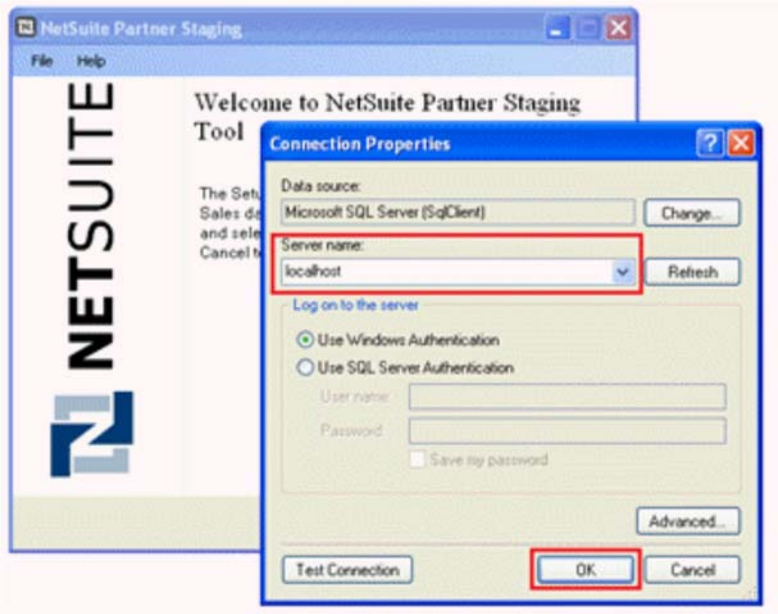
Ad 2.a) To initiate terminal staging in NetSuite:

1. Log in to NetSuite as an administrator.
2. Go to Customization > Lists, Records, & Fields > Record Types.
3. Locate the RA-Workstation record.
4. Click Lists.
5. Click Edit on the required workstation.
6. Check the Provision box.

7. Click Save.
8. In the Installation URL field, right click on the click here link and copy the URL by selecting Copy shortcut.
9. Use this link on a register to initiate the staging process.
10. **Important**: Important: For security reasons the URL expires within next 24 hours. You can generate a new one by repeating the process described above.

Ad 2.b) To install NetSuite POS database and application itself:

1. Go to the register system environment.
2. Open Internet Explorer
   a. **Important**: Only Internet Explorer (8 or higher) is supported. Do not use other types of browsers for this procedure.
3. Paste the copied URL from NetSuite into the Address bar.
4. After opening the page, the staging process is initiated.
5. Click Run to download the installation packages.
6. Proceed through the Windows security dialogues.
   a. Windows 8 — click on More info.
7. Click Run anyway.
8. The Partner Staging Tool will begin downloading.
9. Click Next to continue.
10. In the connection dialog box, complete the sql server name and sql server instancefields.



Welcome to NetSuite Partner Staging Tool

The Setu
Sales da
and sele
Cancel t

Data source: Microsoft SQL Server (SqlClient)

Server name: localhost

Log on to the server

● Use Windows Authentication

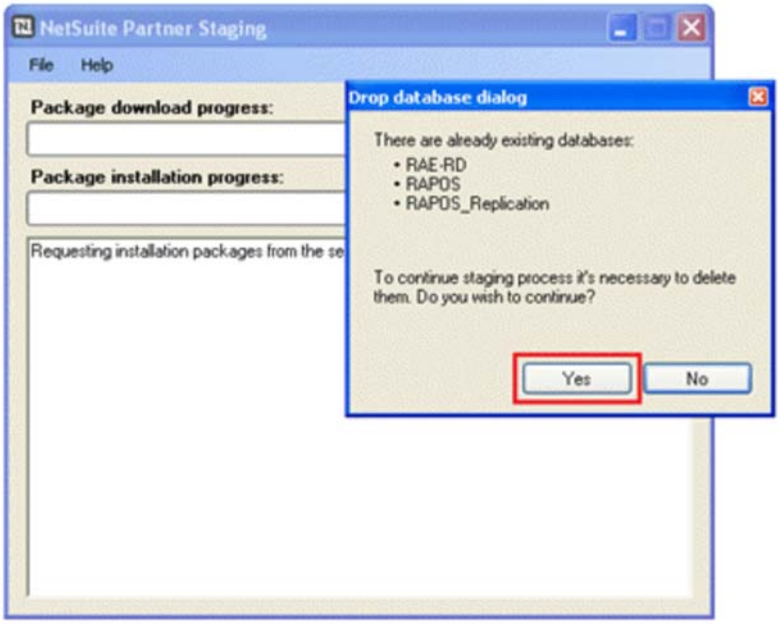
○ Use SQL Server Authentication

User name:

Password:

□ Save my password

11. Test the server connection by clicking Test Connection.
12. Click OK.
    a. **Note**: In instances where a NetSuite POS application already exists, you may be asked to drop the existing databases. If such a dialog window appears, confirm by clicking Yes for dropping the database including data and proceed to the next step. Alternatively, press No to cancel the entire staging process.

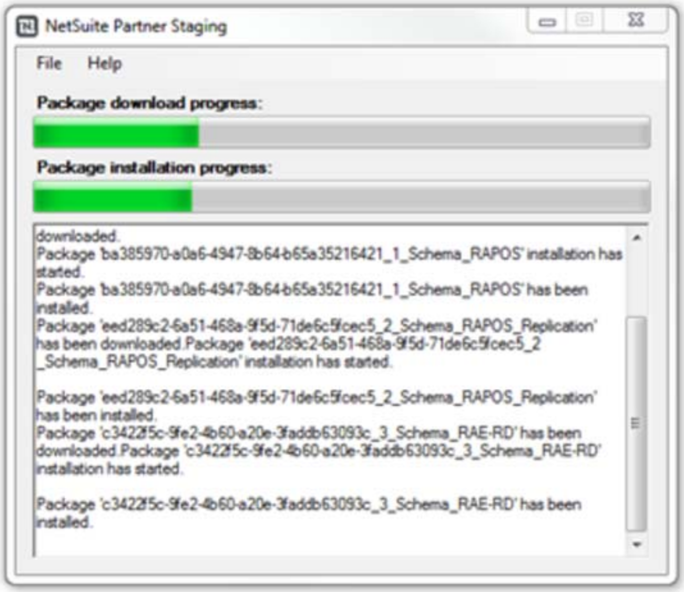


Requesting installation packages from the se

There are already existing databases:
- RAE-RD
- RAPOS
- RAPOS_Replication

To continue staging process it's necessary to delete them. Do you wish to continue?

13. The staging process will start and installation packages processed

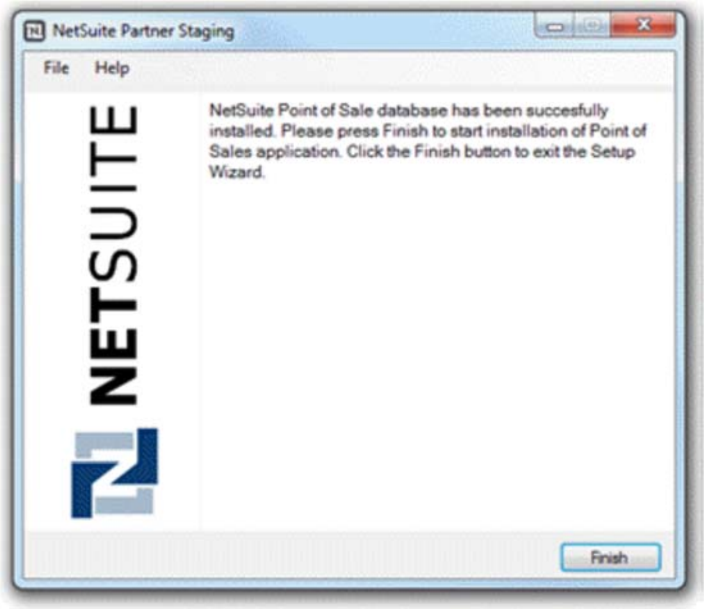


```
downloaded.
Package 'ba385970-a0a6-4947-8b64-b65a35216421_1_Schema_RAPOS' installation has
started.
Package 'ba385970-a0a6-4947-8b64-b65a35216421_1_Schema_RAPOS' has been
installed.
Package 'eed289c2-6a51-468a-9f5d-71de6c5fcec5_2_Schema_RAPOS_Replication'
has been downloaded.Package 'eed289c2-6a51-468a-9f5d-71de6c5fcec5_2
_Schema_RAPOS_Replication' installation has started.

Package 'eed289c2-6a51-468a-9f5d-71de6c5fcec5_2_Schema_RAPOS_Replication'
has been installed.
Package 'c3422f5c-9fe2-4b60-a20e-3faddb63093c_3_Schema_RAE-RD' has been
downloaded.Package 'c3422f5c-9fe2-4b60-a20e-3faddb63093c_3_Schema_RAE-RD'
installation has started.

Package 'c3422f5c-9fe2-4b60-a20e-3faddb63093c_3_Schema_RAE-RD' has been
installed.
```

14. The following dialog window will appear to confirm the package was installed successfully.

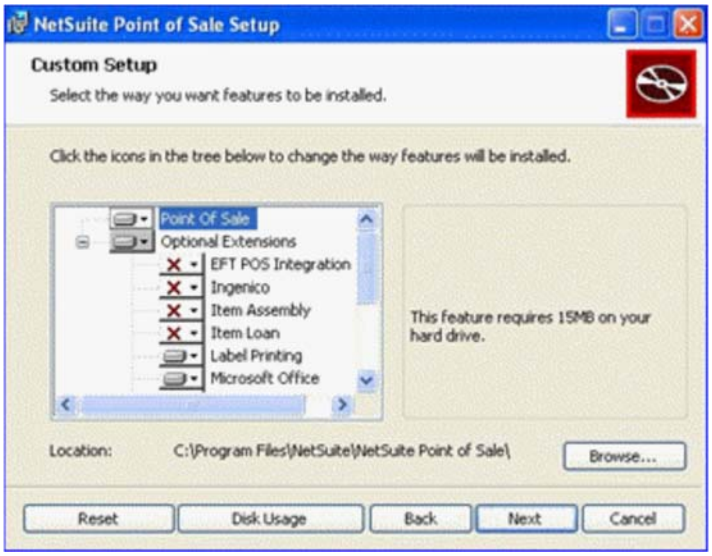


NetSuite Point of Sale database has been succesfully installed. Please press Finish to start installation of Point of Sales application. Click the Finish button to exit the Setup Wizard.

a. **Important**: If provisioning fails, a different dialog window will appear. Attempt the installation again; if the problem persists, please contact Oracle Professional Services.

After the database has been successfully staged, the installation process for the NetSuite POS Application begins automatically. To complete the installation of NetSuite POS following a successful database staging:

1. Click Next on the Setup Wizard dialog window.
2. Select the required features to install.



Custom Setup

Select the way you want features to be installed.

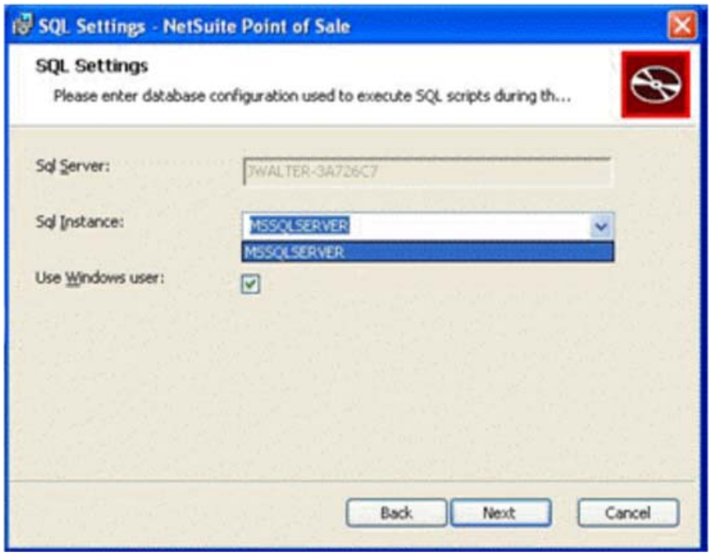
Click the icons in the tree below to change the way features will be installed.

This feature requires 15MB on your hard drive.

Location: C:\Program Files\NetSuite\NetSuite Point of Sale\

a. Note: If you are unsure how to proceed, please contact Oracle Professional Services.

3. Click Next.
4. Select the sql server instance from the sql Instance dropdown list.



SQL Settings - NetSuite Point of Sale

SQL Settings

Please enter database configuration used to execute SQL scripts during th...

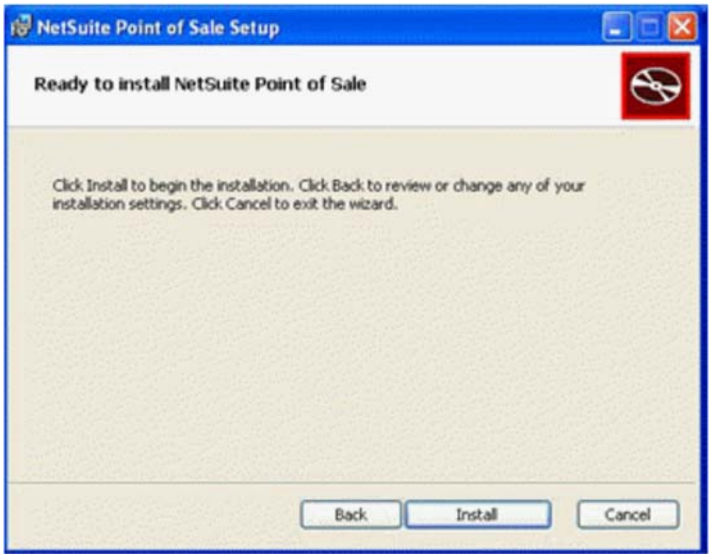
Sql Server: JWALTER-3A726C7

Sql Instance: MSSQLSERVER

Use Windows user: ☑

a. **Note**: If there are multiple options available in the sql instance field, select the instance that performs NetSuite POS data operations. If you are unsure how to proceed, please contact Oracle Professional Services.

5. Click Next.
6. Click Install.

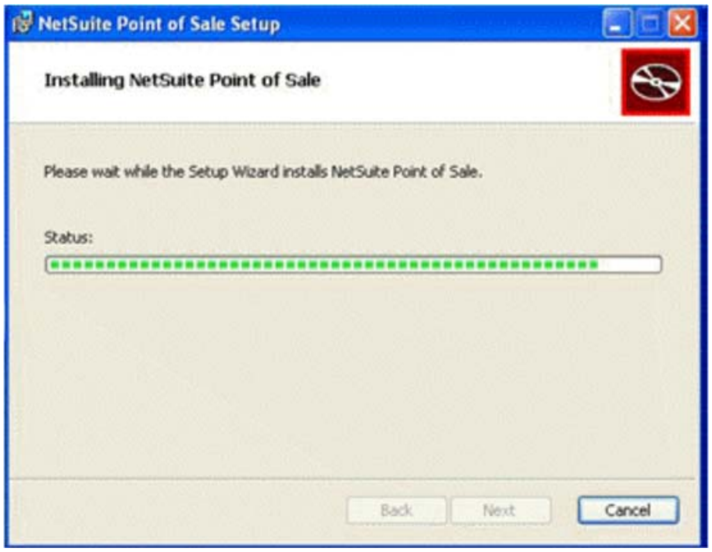


NetSuite Point of Sale Setup

Ready to install NetSuite Point of Sale

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

7. Click Next.



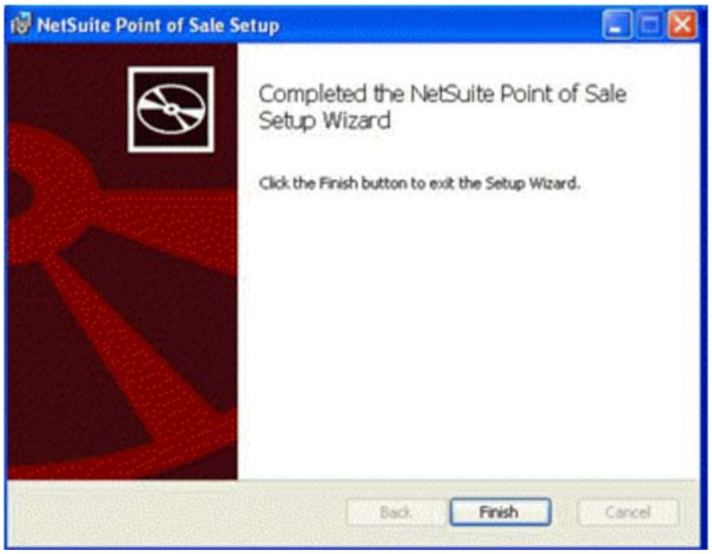
NetSuite Point of Sale Setup

Installing NetSuite Point of Sale

Please wait while the Setup Wizard installs NetSuite Point of Sale.

Status:

8. A dialog window will confirm the application has been successfully installed.



NetSuite Point of Sale Setup

Completed the NetSuite Point of Sale Setup Wizard

Click the Finish button to exit the Setup Wizard.

9. Click Finish to complete the installation process.

Complete the entire installation process by installing the payment gateway application and configuring external devices.

Once the installation is completed, there could be a default admin account with the user name “9999” available. You should change the password for this account immediately or disable it completely.

Installing the Payment Gateway Application

NetSuite POS supports the following payment applications:

- Vantiv Integrated Payments via Datacap Systems DSIClientX control
- Shift4 UTG Dollars on the Net

After installation of the payment application is finished, conduct a test transaction as described further.

Vantiv Integrated Payments#

No installation is required. DSIClientX control is embedded within the NetSuite POS application.

Shift4 Dollars on the Net#

Follow the installation instructions provided with the third-party software.

Conducting Test Transaction

Upon installation and configuration of the Payment Application and Gateway, perform basic credit and debit card transactions. Contact your payment processor or bank for information on test cards and testing practices.

Defining the Payment Gateway within NetSuite POS

When you have installed the payment gateway software, you will need to configure the payment gateway for processing payment cards in NetSuite POS.

By default, this is done by Oracle Professional Services or customer himself by accessing the customer's NetSuite account and setting configuration there).

Warning: It is possible to configure EMV support on any supported gateway. The setting is disabled by default. Please ensure EMV support remains disabled on unsupported gateways to prevent incorrect configuration which may cause a security risk for your application. EMV support must remain disabled for:

- Vantiv Integrated Payments DSIClientX (see p.9 *Vantiv Integrated Payments (DSIClientX)/NetSuite POS Data Flow* diagram)

- Shift4 UTG, where pin pads are configured through NetSuite POS (see p.10 *SHIFT4/NetSuite POS Data Flow* diagram)

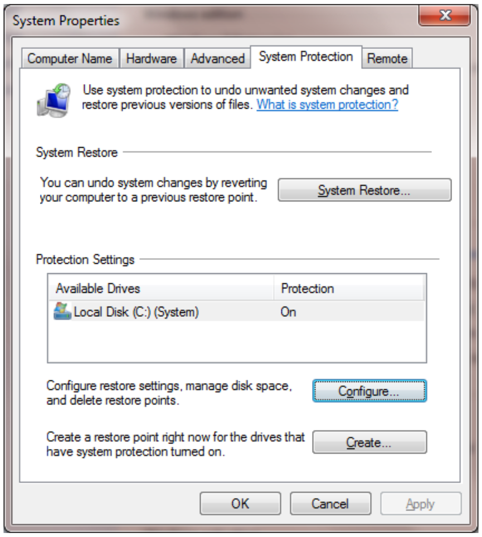
Appendix A: Addressing Inadvertent Capture of PAN

You can find instructions for all supported operating systems below

Addressing Inadvertent Capture of PAN on WINDOWS 7 and Windows Embedded POSReady 7

To disable System Restore:

1. Right Click on Computer > Select **Properties.**
2. Select **System Protection**.



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.

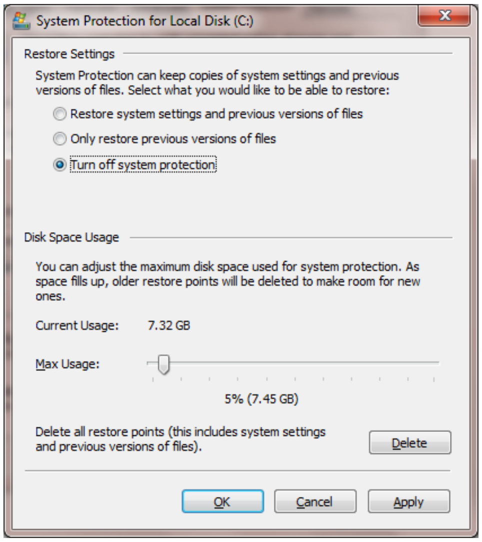
Protection Settings

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.

3. Select **Configure**.



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)

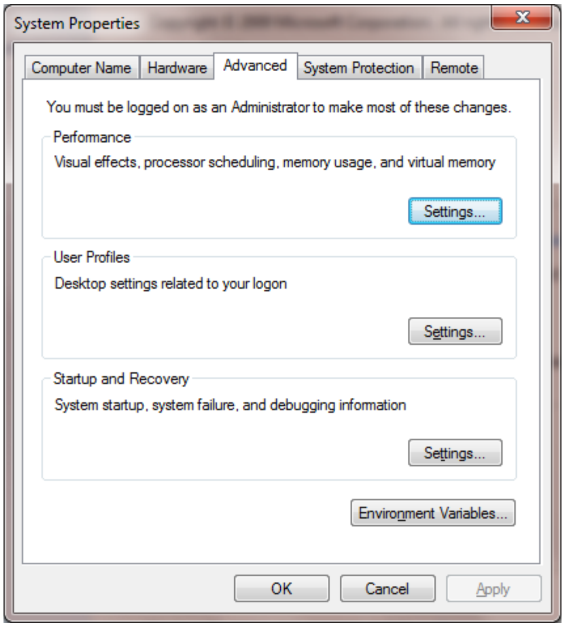
Delete all restore points (this includes system settings and previous versions of files).

4. Select **Turn off system protection**.
5. Click **Apply**.
6. Click **OK.**
7. Reboot PC.

Managing PageFile.sys

Important: If you are using SSD disk you should have **No paging file** turned on as recommended by HW instructions. To turn on “No paging file” follow these instructions:

1. Right Click on Computer > Select **Properties**.
2. Select **Advanced System Settings**.



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

Performance

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

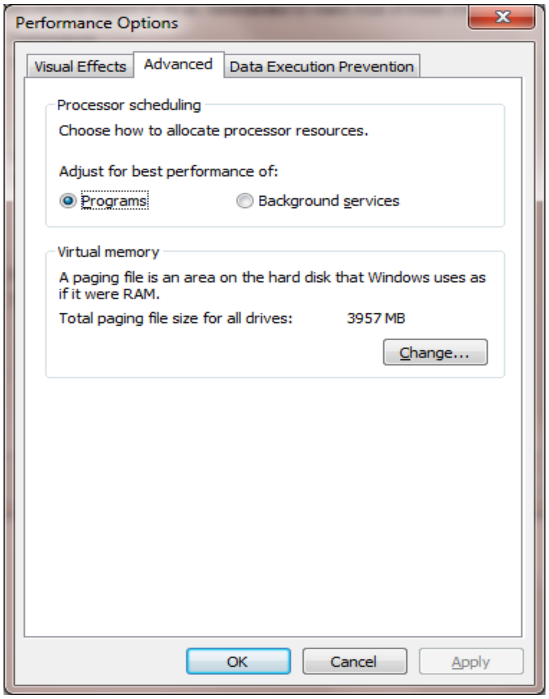
User Profiles

Desktop settings related to your logon

Startup and Recovery

System startup, system failure, and debugging information

3. Under Performance, select **Settings**
4. Click the **Advanced** tab.



Processor scheduling

Choose how to allocate processor resources.

Adjust for best performance of:

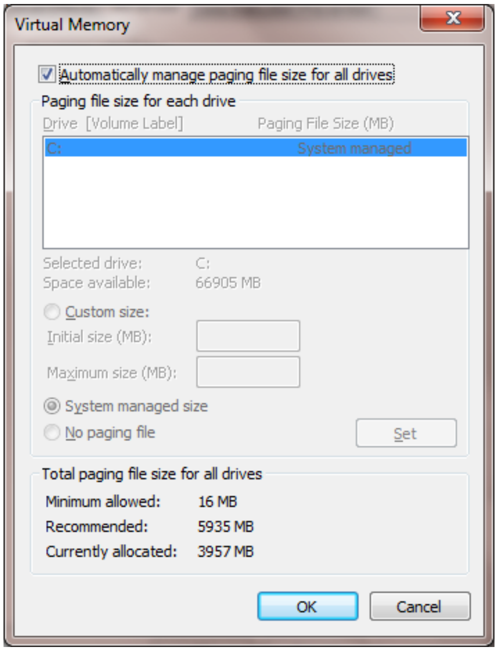
● Programs ○ Background services

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

5. Under Virtual Memory, select **Change**.



☑ 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

6. Uncheck **Automatically manage paging file size for all drives** and set **No paging file** option and confirm

Once **No paging file** is set you should skip chapters:

- "To encrypt PageFile.sys"
- "Clearing the System Pagefile.sys on shutdown"
- "To disable system management of PageFile.sys"

And continue with chapter:

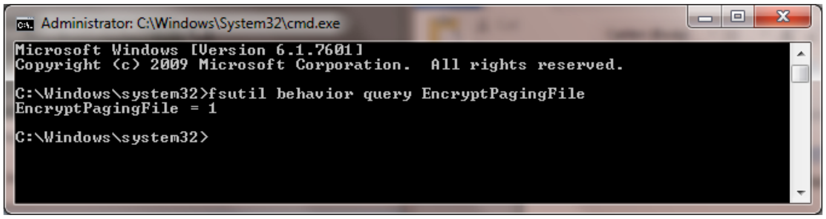
- “To disable Windows Error Reporting”

To encrypt PageFile.sys:

Important: If you are using SSD disk you should have **No paging file** turned on as recommended by HW instructions following instructions in “Managing PageFile.sys” chapter. If **No paging file** is set, you should skip this chapter!

NOTE: the hard disk must be formatted using NTFS to perform this operation.

1. Click **Start**.
2. Type **cmd** in the search box.
3. Right click on **cmd.exe**.
4. Select **Run as Administrator**.
5. To Encrypt the Pagefile type the following command:
   `fsutil behavior set EncryptPagingFile 1`

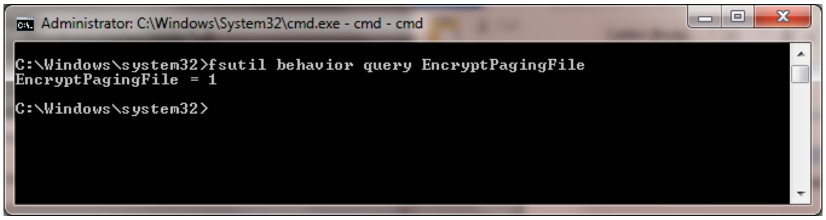


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

C:\Windows\system32>
```

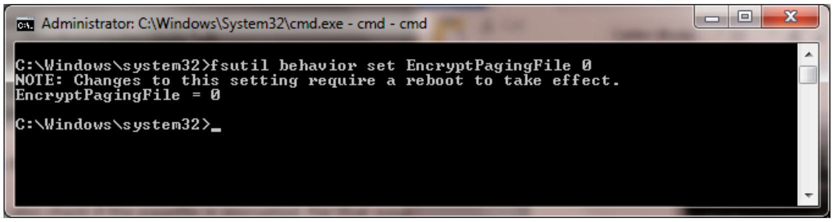
6. To verify configuration type the following command:
   `fsutil behavior query EncryptPagingFile`



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

C:\Windows\system32>
```

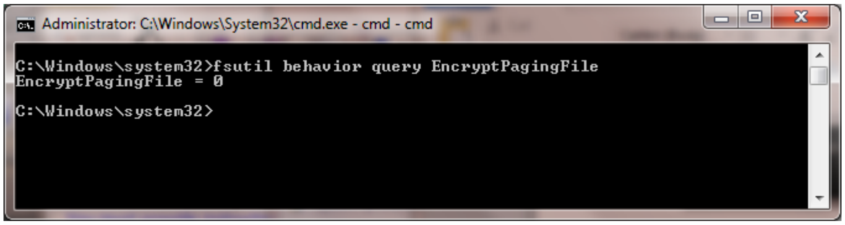
7. If encryption is enabled **EncryptPagingFile = 1** should appear
8. Reboot PC.
9. To disable PageFile encryption type the following command:
   `fsutil behavior set EncryptPagingFile 0`



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

C:\Windows\system32>_
```

10. To verify configuration type the following command:
    `fsutil behavior query EncryptPagingFile`



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

C:\Windows\system32>
```

11. If encryption is disabled, **EncryptPagingFile = 0** should appear.

Clearing the System Pagefile.sys on shutdown

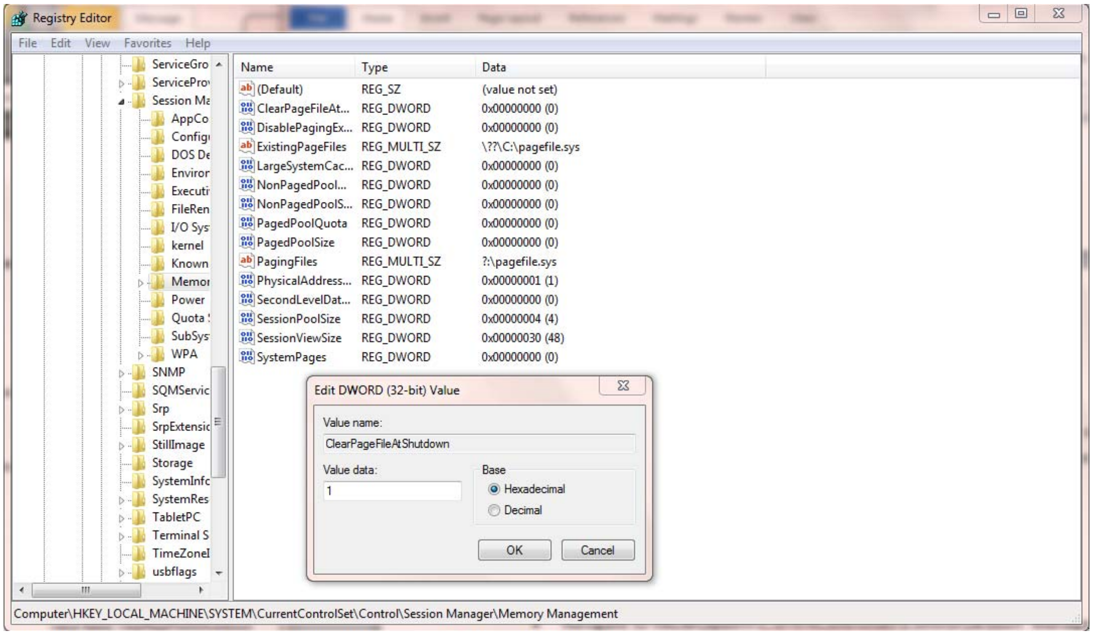
Important: If you are using SSD disk you should have **No paging file** turned on as recommended by HW instructions following instructions in “Managing PageFile.sys” chapter. If **No paging file** is set, you should skip this chapter!

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

NOTE: Enabling this feature may increase Windows shutdown time.

To clear the System Pagefile.sys on shutdown:

1. Click **Start**.
2. Type **regedit** in the search box.
3. Right click on **regedit.exe**.
4. Select **Run as Administrator**.
5. Navigate to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management
6. Change the value from 0 to 1
7. Click **OK**.
8. 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)

Value name: ClearPageFileAtShutdown

Value data: 1

Base
● Hexadecimal
○ Decimal

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

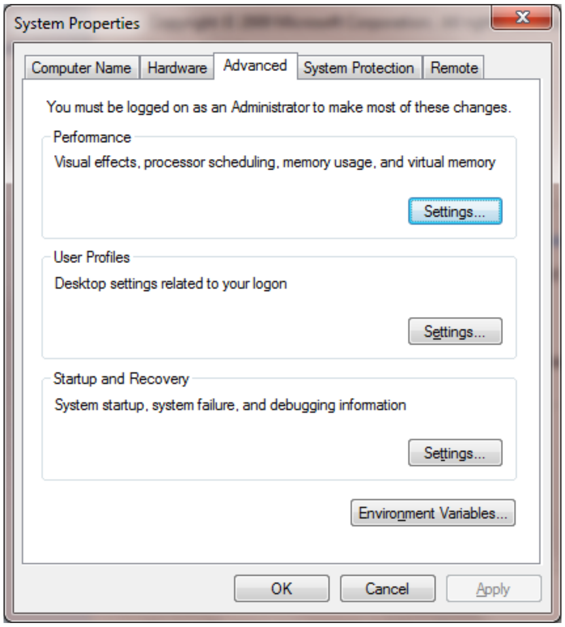
9. If the value does not exist, add the following:
   a. Value Name: **ClearPageFileAtShutdown**
   b. Value Type: **REG_DWORD**

c. Value: 1

To disable system management of PageFile.sys:

Important: If you are using SSD disk you should have **No paging file** turned on as recommended by HW instructions following instructions in “Managing PageFile.sys” chapter. If **No paging file** is set, you should skip this chapter!

1. Right Click on Computer > Select **Properties**.
2. Select **Advanced System Settings**.



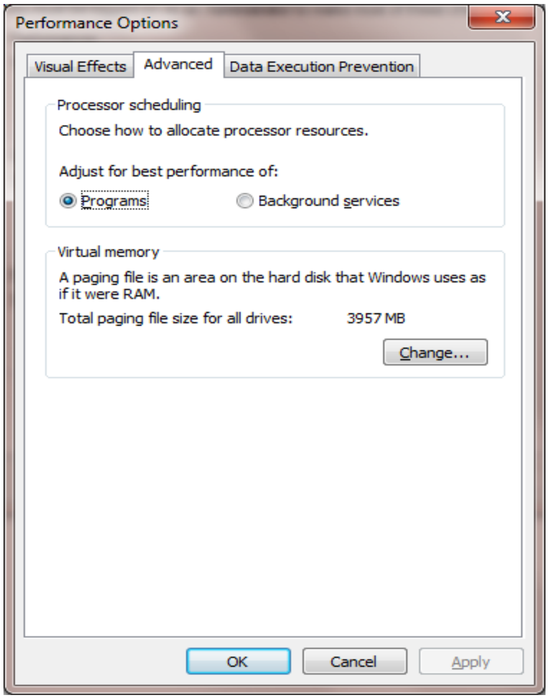
You must be logged on as an Administrator to make most of these changes.

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

3. Under Performance, select **Settings**
4. Click the **Advanced** tab.



Processor scheduling

Choose how to allocate processor resources.

Adjust for best performance of:

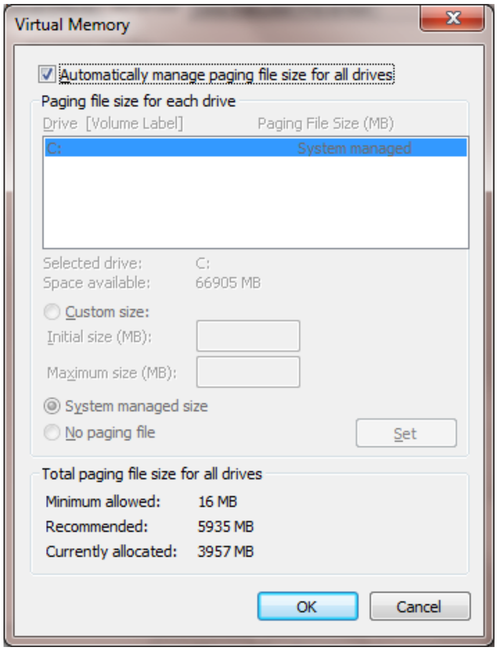
● Programs ○ Background services

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

5. Under Virtual Memory, select **Change**.



☑ 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

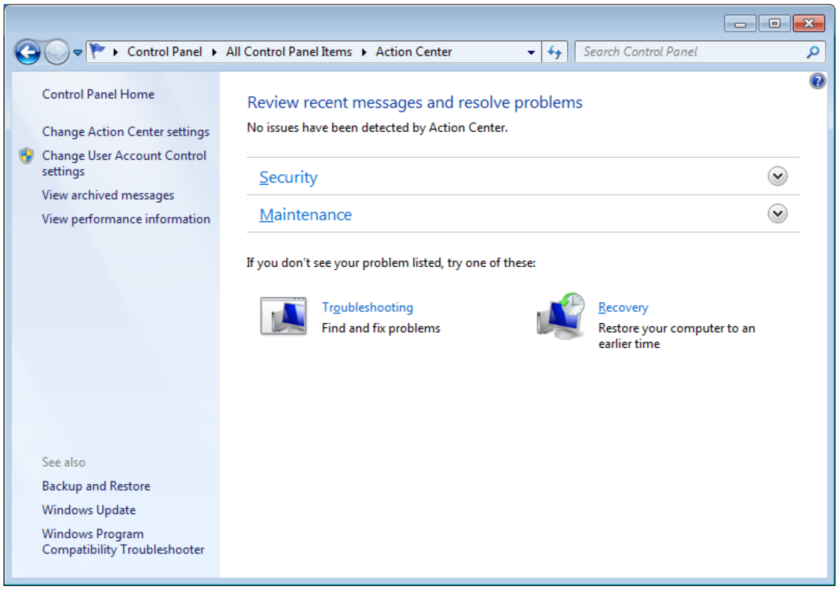
Minimum allowed:	16 MB
Recommended:	5935 MB
Currently allocated:	3957 MB

6. Uncheck **Automatically manage paging file size for all drives**.
7. Select **Custom Size**.
8. Enter the following:
   - Initial Size – enter the amount of installed system memory.
   - Maximum Size – enter 2x the amount of installed memory.
9. Click **OK**.

10. Reboot PC.

To disable Windows Error Reporting:

1. Open **Control Panel**.
2. Open **Action Center**.
3. Select **Change Action Center Settings**.



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

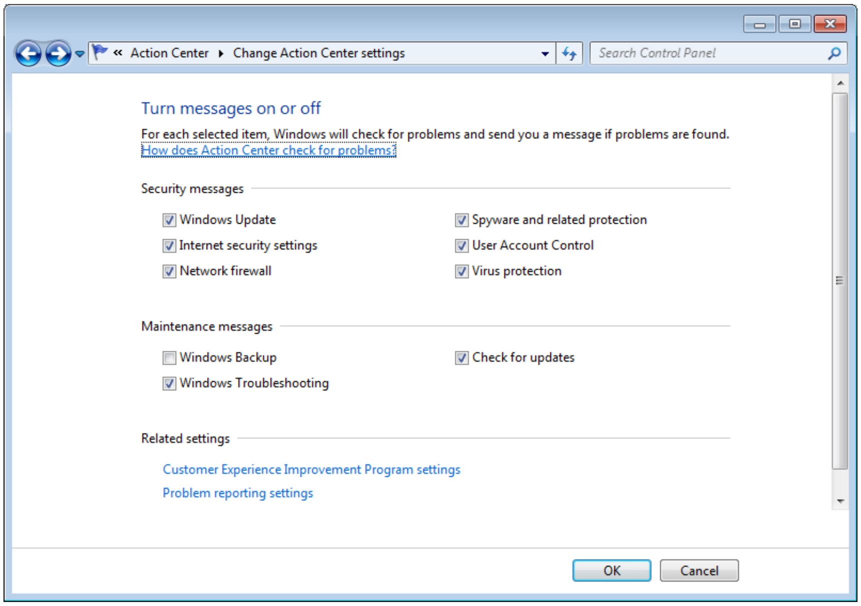
Maintenance

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

4. 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 ☑ Spyware and related protection
☑ Internet security settings ☑ User Account Control
☑ Network firewall ☑ Virus protection

Maintenance messages

□ Windows Backup ☑ Check for updates
☑ Windows Troubleshooting

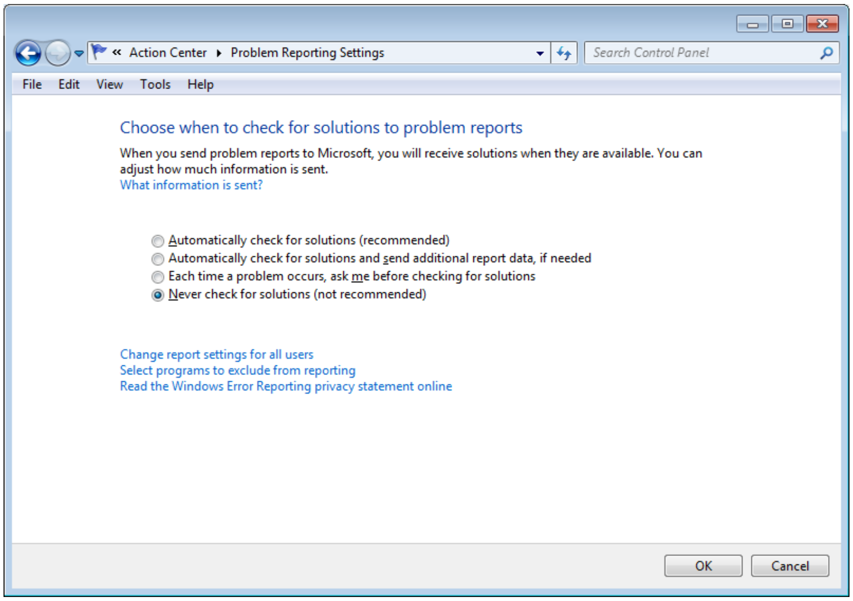
Related settings

Customer Experience Improvement Program settings

Problem reporting settings

OK Cancel

5. Select **Never Check for Solutions**.


« Action Center ▸ Problem Reporting Settings
Search Control Panel
File Edit View Tools Help
OK
Cancel

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

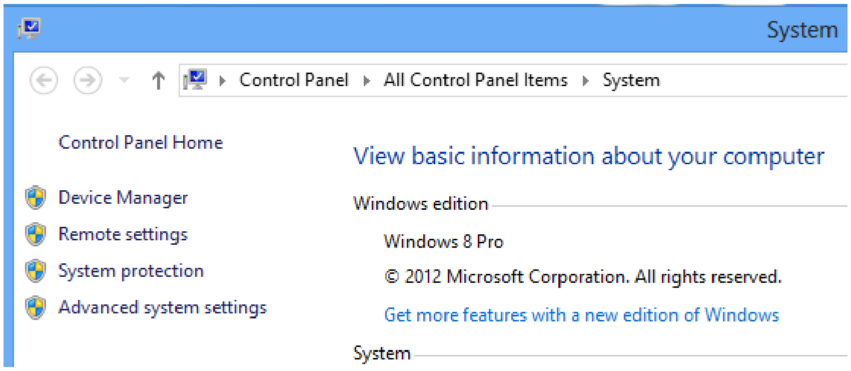
6. Select **OK.**

7. Close **Action Center**.

Addressing Inadvertent Capture of PAN on WINDOWS 8.1

To disable System Restore:

1. Right Click on Computer > Select **Properties**.
2. Select **Advanced System Settings**.



System

Control Panel ▸ All Control Panel Items ▸ System

Control Panel Home

Device Manager

Remote settings

System protection

Advanced system settings

View basic information about your computer

Windows edition

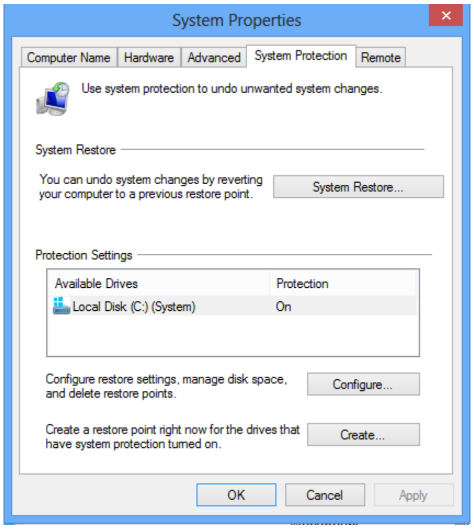
Windows 8 Pro

© 2012 Microsoft Corporation. All rights reserved.

Get more features with a new edition of Windows

System

3. Select the **System Protection** tab.



System Properties

Computer Name | Hardware | Advanced | System Protection | Remote

Use system protection to undo unwanted system changes.

System Restore

You can undo system changes by reverting your computer to a previous restore point. [System Restore...]

Protection Settings

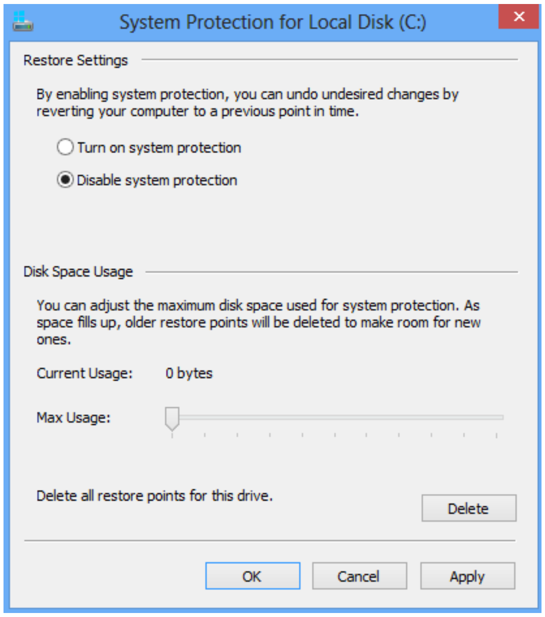
Available Drives	Protection
Local Disk (C:) (System)	On

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

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

[OK] [Cancel] [Apply]

4. Select **Configure**.



System Protection for Local Disk (C:)

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:

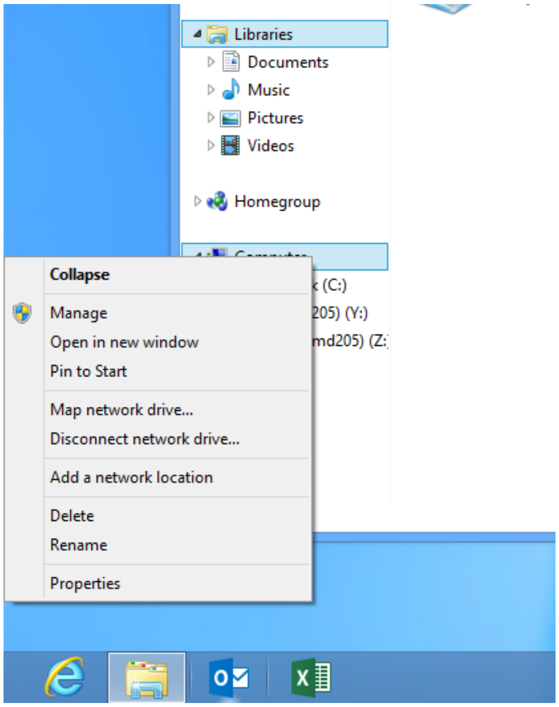
Delete all restore points for this drive.

5. Select **Disable system protection**.
6. Click **Apply**.
7. Click **OK** to shut the **System Protection window**.
8. Click **OK** to shut the **System Properties window**.
9. Reboot PC.

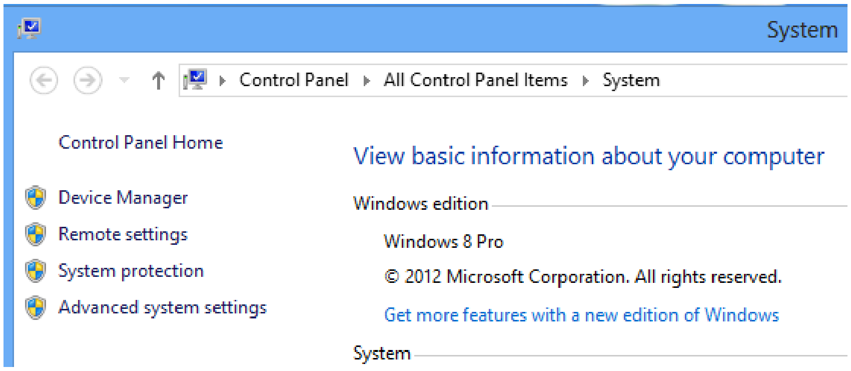
Managing PageFile.sys

Important: If you are using SSD disk you should have **No paging file** turned on as recommended by HW instructions. To turn on “No paging file” follow these instructions:

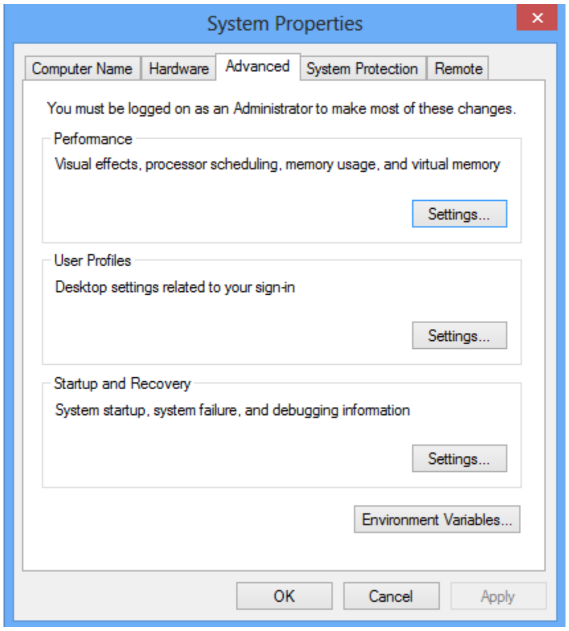
1. Right Click on Computer > Select **Properties**.



2. Select **Advanced System Settings** from the System screen.


System
Control Panel ▸ All Control Panel Items ▸ System
Control Panel Home
Device Manager
Remote settings
System protection
Advanced system settings
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

3. Click the **Advanced** tab.



System Properties

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

Performance

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

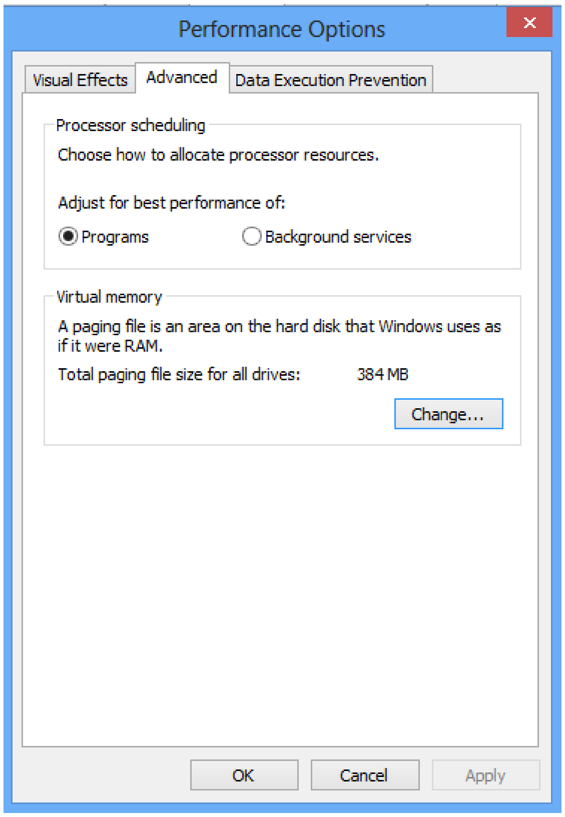
User Profiles

Desktop settings related to your sign-in

Startup and Recovery

System startup, system failure, and debugging information

4. Under Performance, select **Settings**.
5. Click the **Advanced** tab.



Performance Options

Processor scheduling

Choose how to allocate processor resources.

Adjust for best performance of:

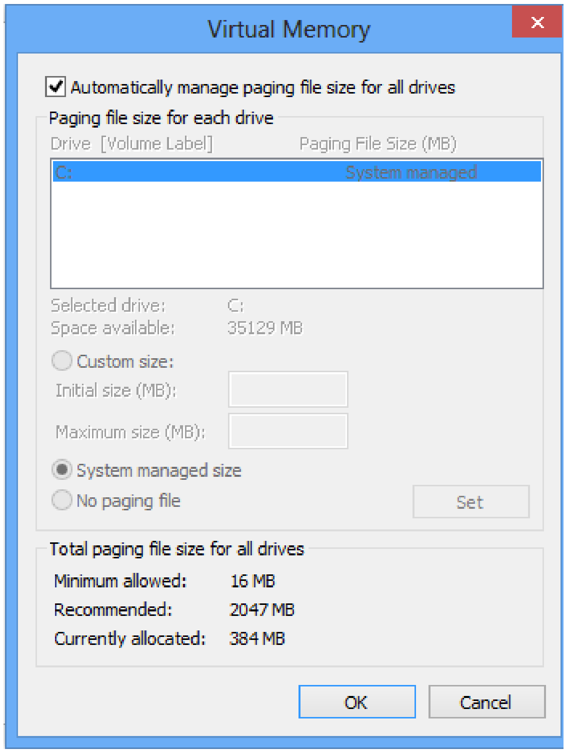
● Programs ○ Background services

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: 384 MB

6. Under Virtual Memory, select **Change**.



☑ 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

7. Uncheck **Automatically manage paging file size for all drives** and set **No paging file** option and confirm

Once **No paging file** is set you should skip chapters:

- "To encrypt PageFile.sys"
- "Clearing the System Pagefile.sys on shutdown"
- "To disable system management of PageFile.sys"

And continue with chapter:

- “To disable Windows Error Reporting”

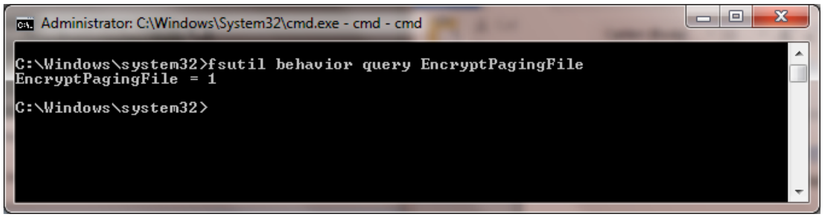
To encrypt PageFile.sys:

Important: If you are using SSD disk you should have **No paging file** turned on as recommended by HW instructions following instructions in “Managing PageFile.sys” chapter. If **No paging file** is set, you should skip this chapter!

NOTE: the hard disk must be formatted using NTFS to perform this operation

1. From the desktop hold down the Windows key and type **F**.
2. Select **Apps**.

3. Type **cmd** in the box.
4. Right click the **Command Prompt**.
5. Select **Run as Administrator**.
6. To verify configuration, type the following command:
   `fsutil behavior query EncryptPagingFile`

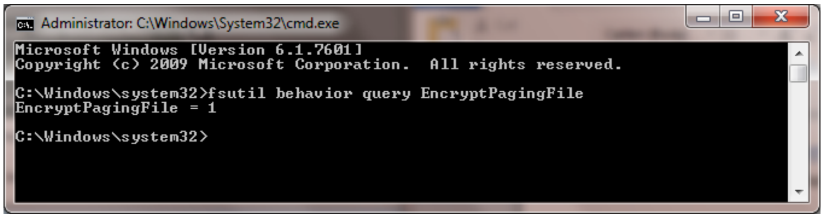


Administrator: C:\Windows\System32\cmd.exe - cmd - cmd

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

C:\Windows\system32>
```

7. If encryption is enabled **EncryptPagingFile = 1** should appear.
8. If encryption is disabled **EncryptPagingFile = 0** should appear.
9. To Encrypt the Paging file, type the following command:
   `fsutil behavior set EncryptPagingFile 1`



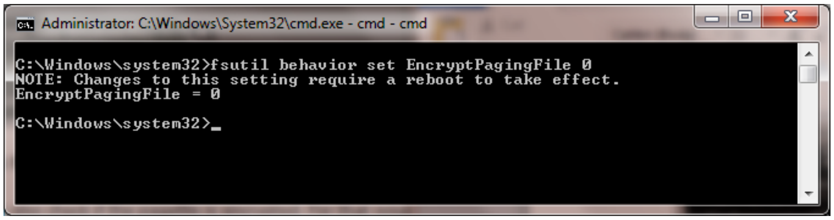
Administrator: C:\Windows\System32\cmd.exe

```
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>
```

10. To disable Paging file encryption, type the following command:
    `fsutil behavior set EncryptPagingFile 0`



Administrator: C:\Windows\System32\cmd.exe - cmd - cmd

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

C:\Windows\system32>_
```

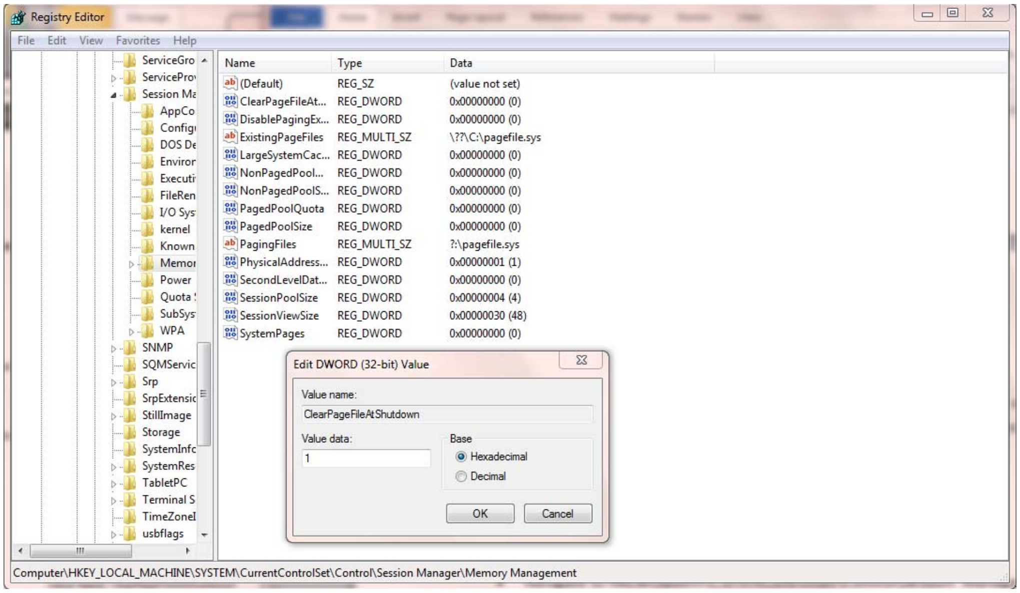
Clearing the System Pagefile.sys on shutdown

Important: If you are using SSD disk you should have **No paging file** turned on as recommended by HW instructions following instructions in “Managing PageFile.sys” chapter. If **No paging file** is set, you should skip this chapter!

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

NOTE: Enabling this feature may increase Windows shutdown time.

1. From the desktop hold down the Windows key and type **F**.
2. Select **Apps**.
3. Type **regedit** in the box.
4. Right click on **regedit.exe**.
5. Select **Run as Administrator**.
6. Navigate to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management
7. Change the value from 0 to 1 on the **ClearPageFileAtShutdown** DWORD.
8. Click **OK**.
9. 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

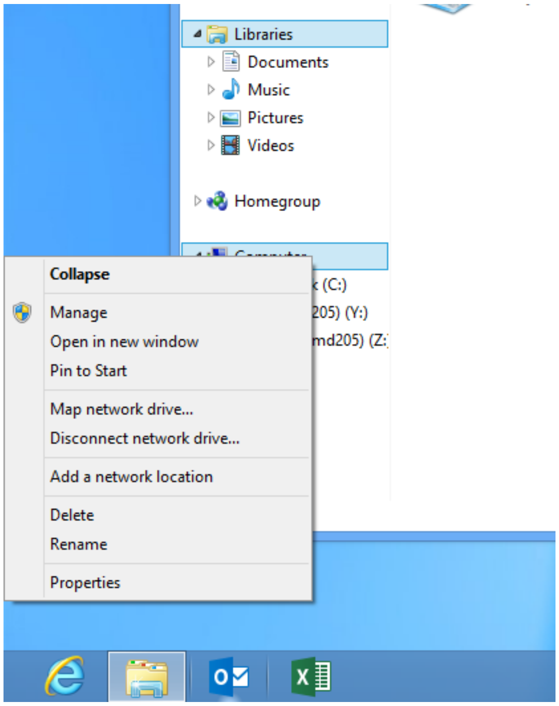
10. If the value does not exist, add the following:

d. Value Name: **ClearPageFileAtShutdown**
e. Value Type: **REG_DWORD**
f. Value: 1

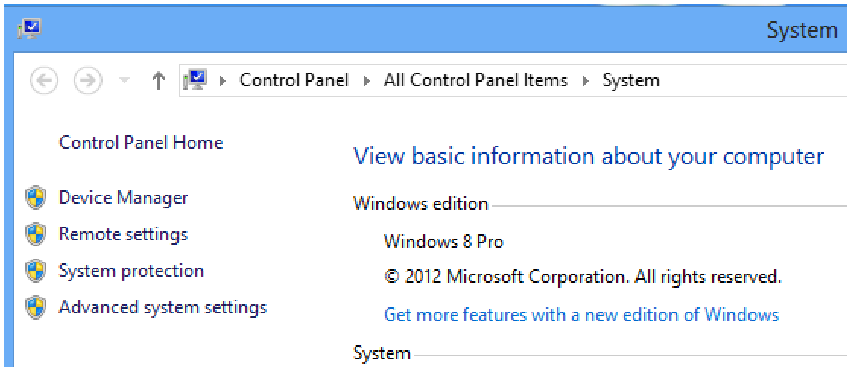
To disable system management of PageFile.sys:

Important: If you are using SSD disk you should have **No paging file** turned on as recommended by HW instructions following instructions in “Managing PageFile.sys” chapter. If **No paging file** is set, you should skip this chapter!

1. Right Click on Computer > Select **Properties**.



2. Select **Advanced System Settings** from the System screen.


System
Control Panel ▸ All Control Panel Items ▸ System
Control Panel Home
Device Manager
Remote settings
System protection
Advanced system settings
Get more features with a new edition of Windows

View basic information about your computer

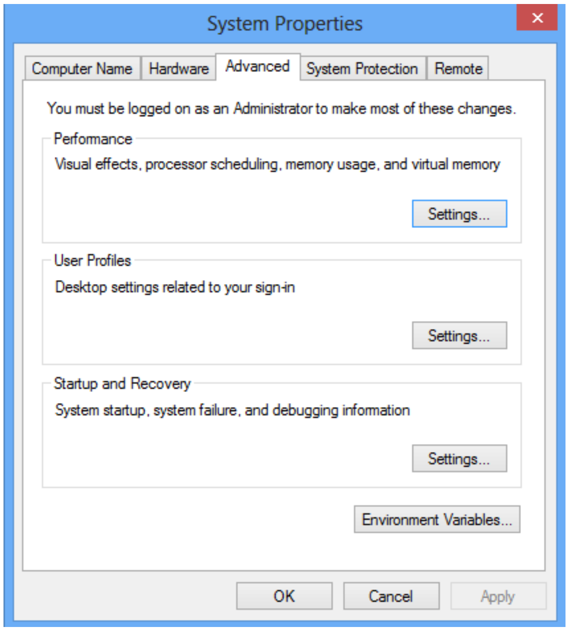
Windows edition

Windows 8 Pro

© 2012 Microsoft Corporation. All rights reserved.

System

3. Click 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

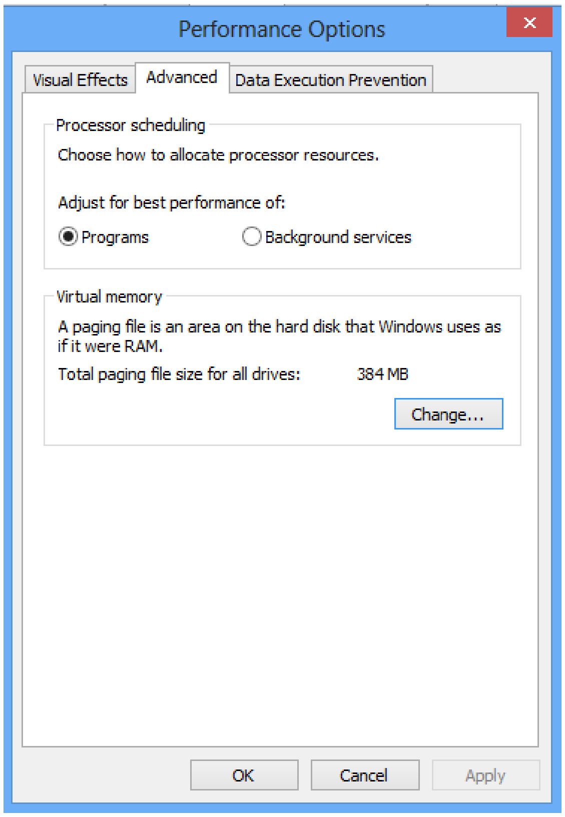
User Profiles

Desktop settings related to your sign-in

Startup and Recovery

System startup, system failure, and debugging information

4. Under Performance, select **Settings**.
5. Click the **Advanced** tab.



Processor scheduling

Choose how to allocate processor resources.

Adjust for best performance of:

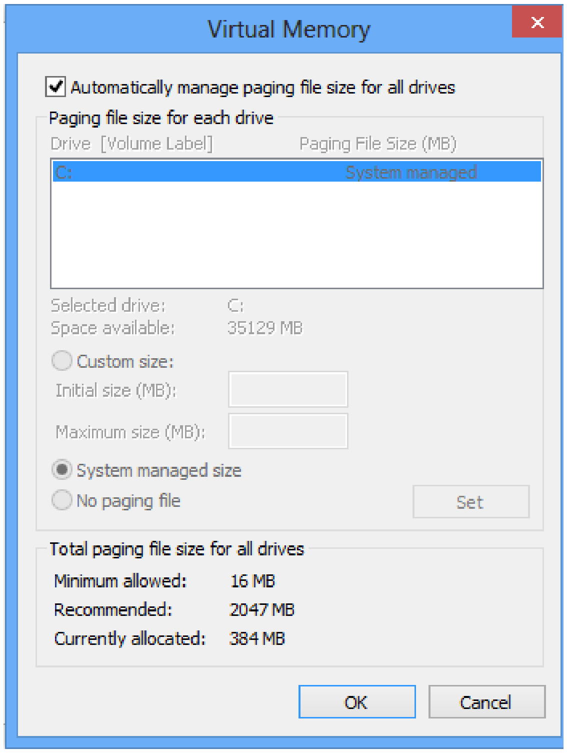
● Programs ○ Background services

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

6. Under Virtual Memory, select **Change**.



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

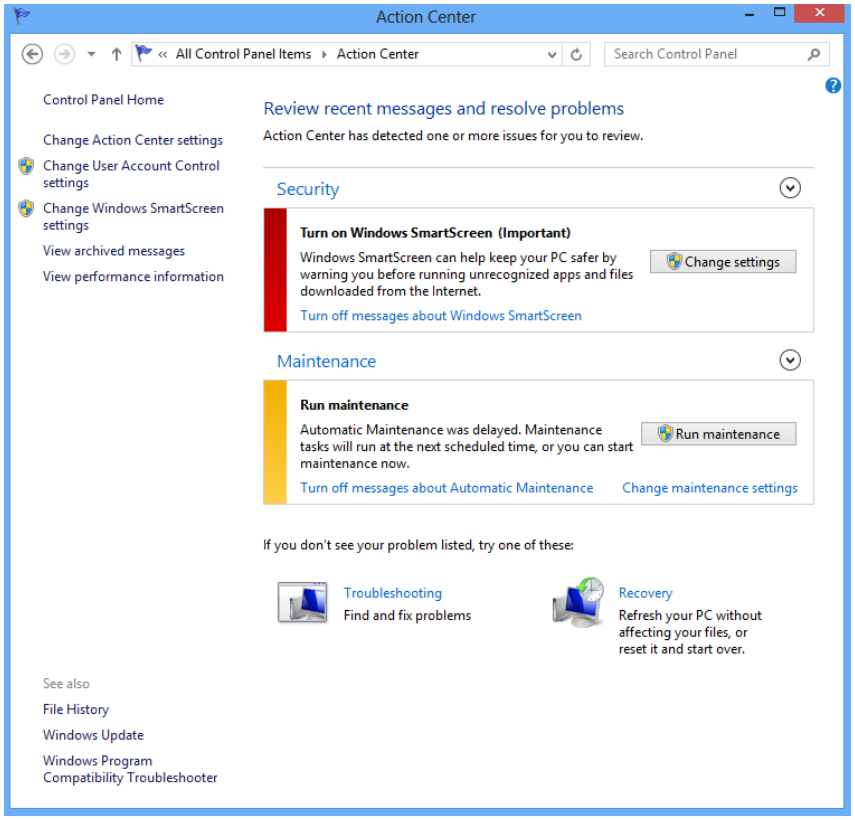
Total paging file size for all drives

Minimum allowed:	16 MB
Recommended:	2047 MB
Currently allocated:	384 MB

7. Uncheck **Automatically manage paging file size for all drives**.
8. Select **Custom Size**.
9. Enter the following:
   - Initial Size – enter the amount of installed system memory.
   - Maximum Size – enter 2x the amount of installed system memory.
10. Click **OK**.
11. Reboot PC.

To disable Windows error reporting:

8. From the desktop, hold down the Windows key and type **I**.
9. Select **Control Panel**.
10. Open the **Action Center.**
11. 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.

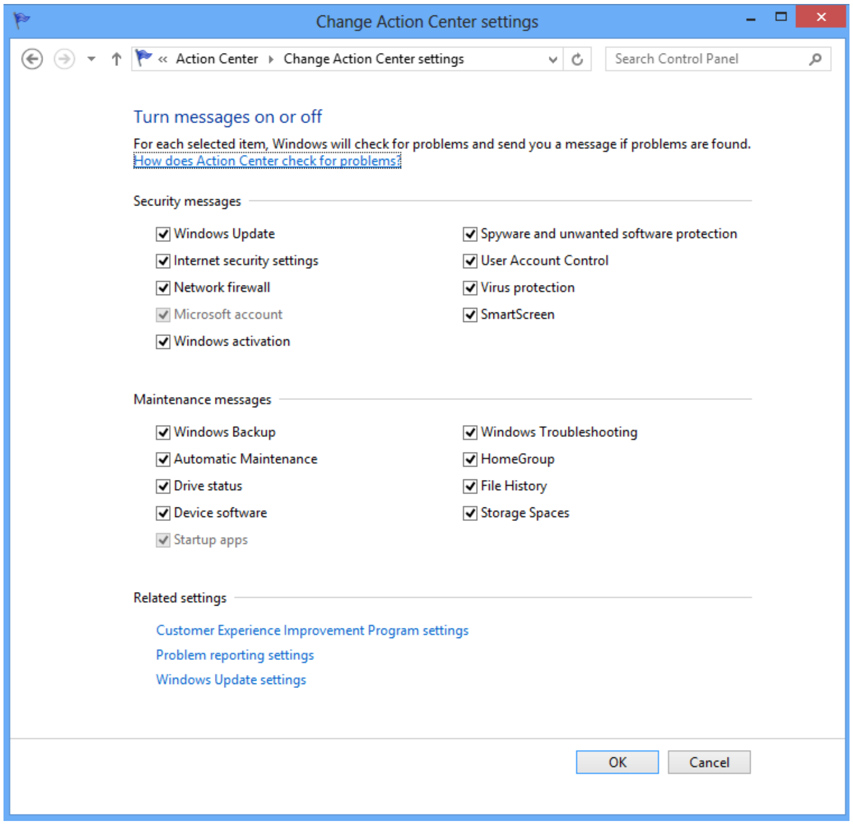
See also

File History

Windows Update

Windows Program Compatibility Troubleshooter

12. 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

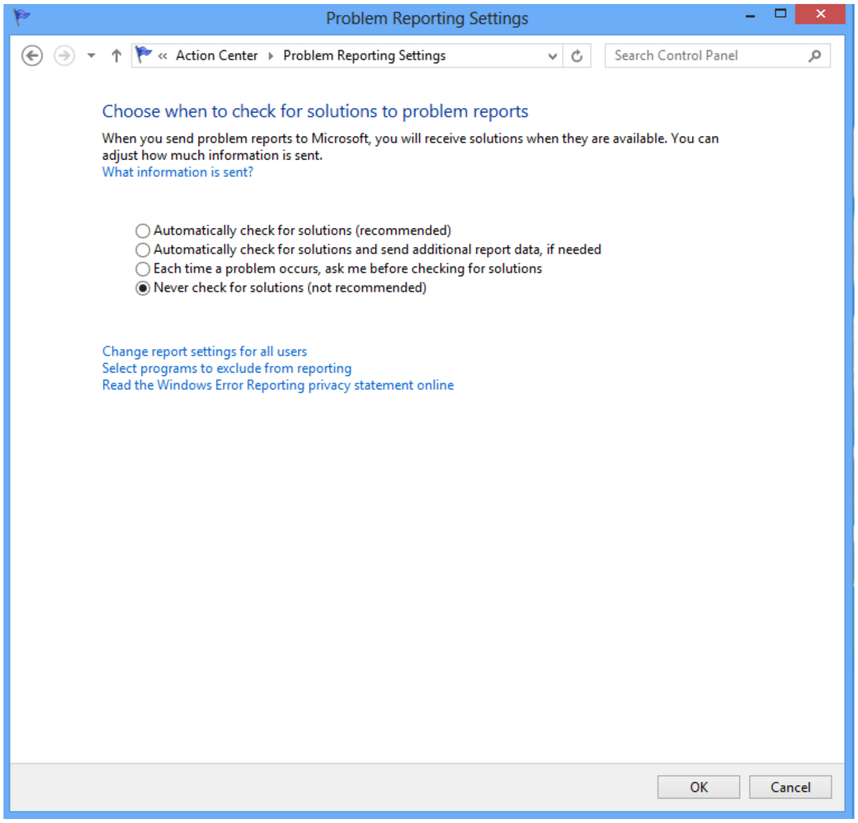
Customer Experience Improvement Program settings

Problem reporting settings

Windows Update settings

OK Cancel

13. Check the **Never Check for Solutions** box.



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

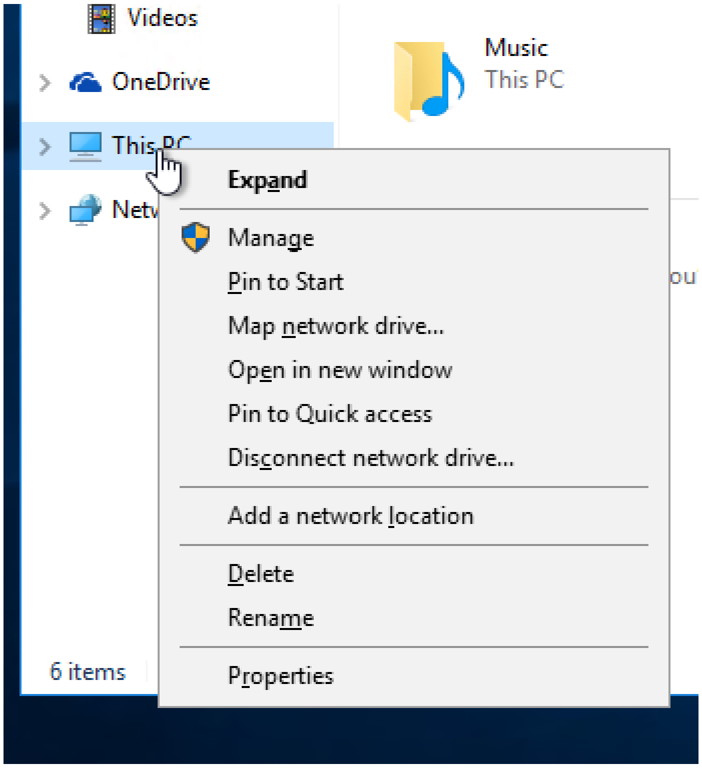
14. Click **OK**.

15. Close the **Action Center**.

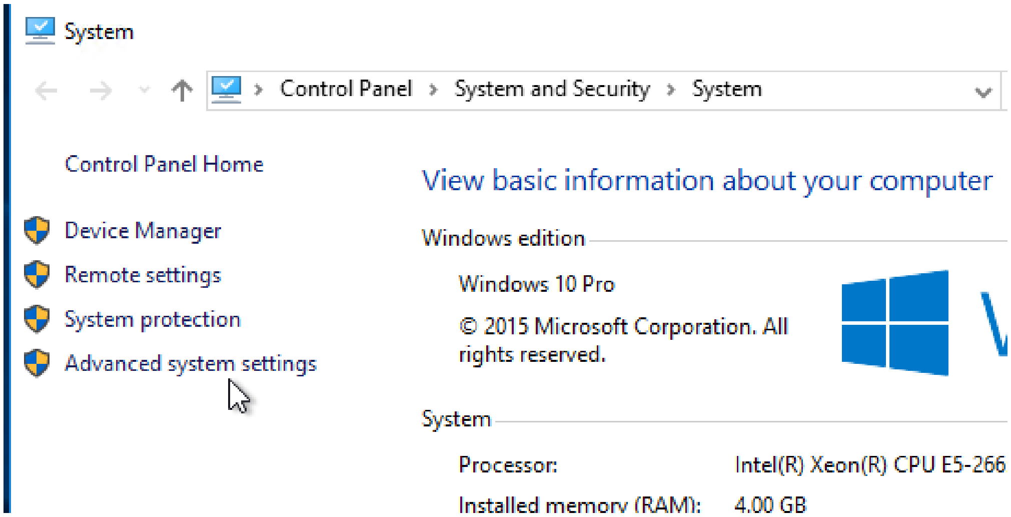
Addressing Inadvertent Capture of PAN on WINDOWS 10

Disabling System Restore – Windows 10

1. Right Click on This PC > Select “Properties”:



2. Select “Advanced System Settings” from the System screen:



View basic information about your computer

Windows edition

Windows 10 Pro

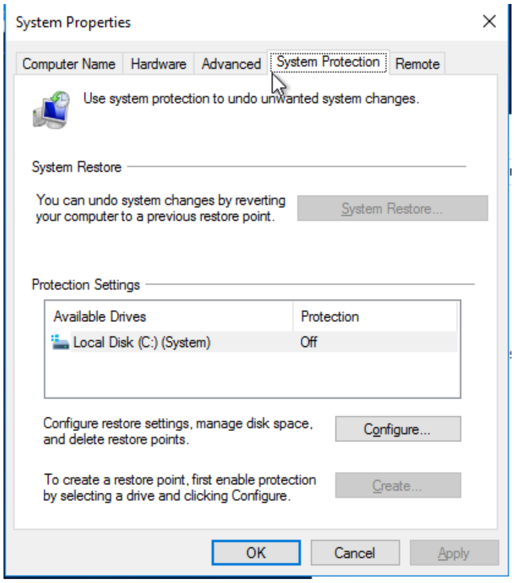
© 2015 Microsoft Corporation. All rights reserved.

System

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

Installed memory (RAM): 4.00 GB

3. 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.

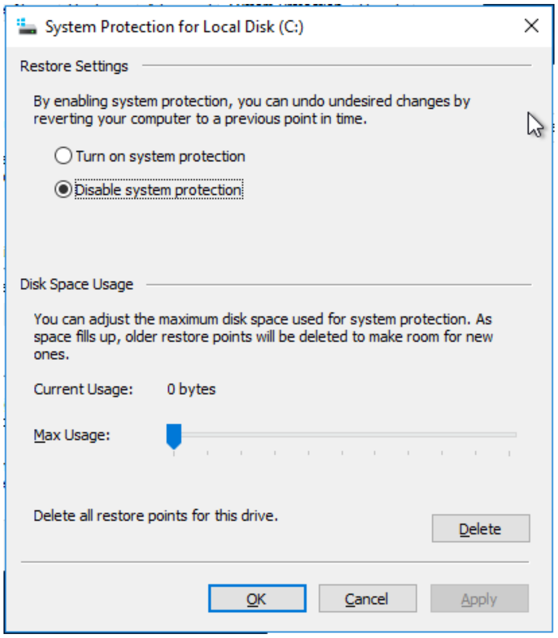
Protection Settings

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:

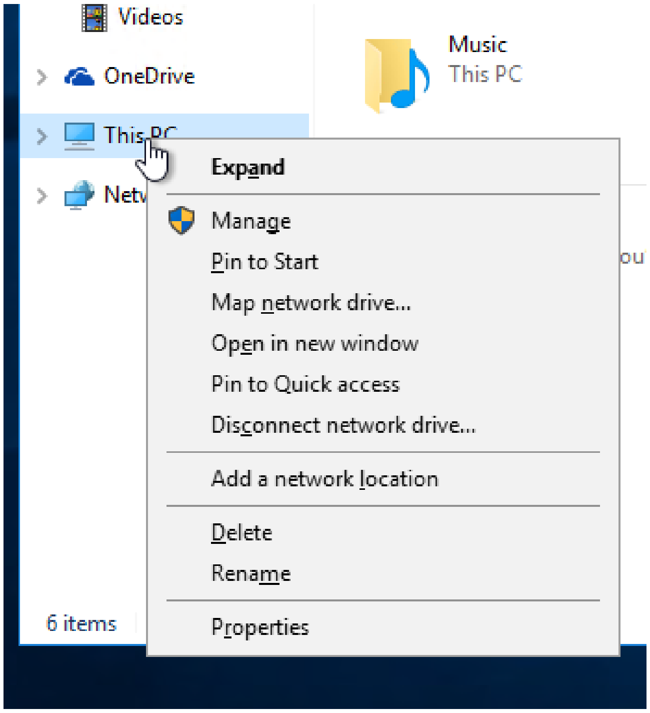
Delete all restore points for this drive.

- 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

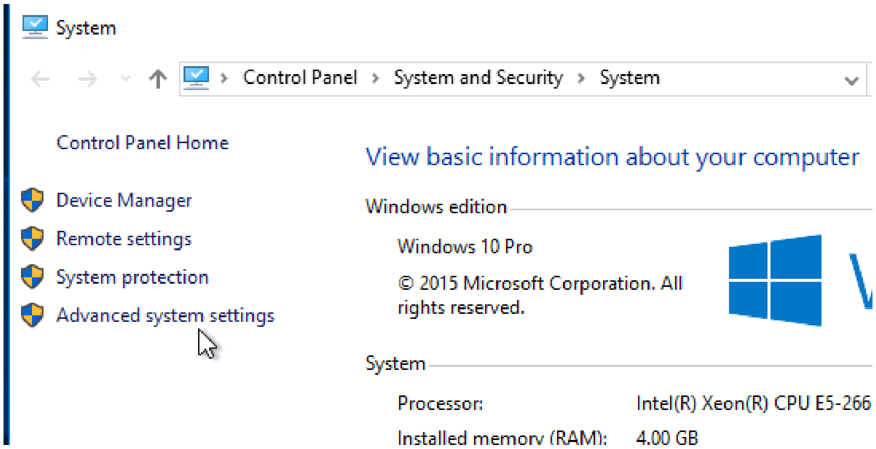
Managing PageFile.sys

Important: If you are using SSD disk you should have **No paging file** turned on as recommended by HW instructions. To turn on "No paging file" follow these instructions:

1. Right Click on This PC > Select "Properties":



2. Select "Advanced System Settings" from the System screen:



View basic information about your computer

Windows edition

Windows 10 Pro

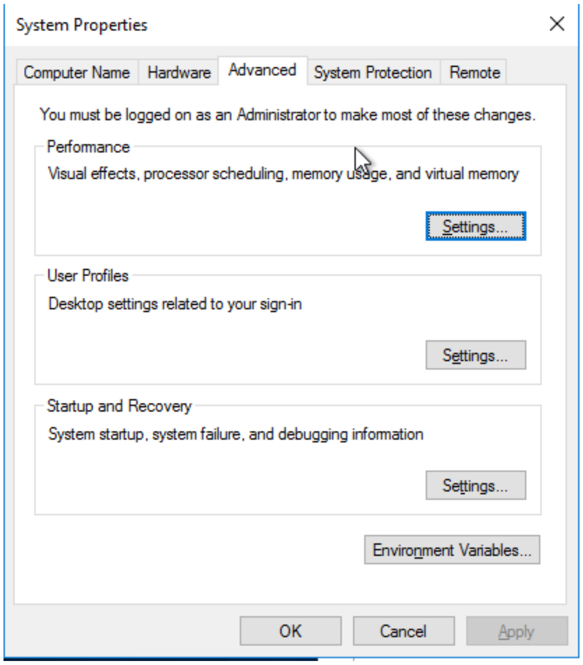
© 2015 Microsoft Corporation. All rights reserved.

System

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

Installed memory (RAM): 4.00 GB

3. 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

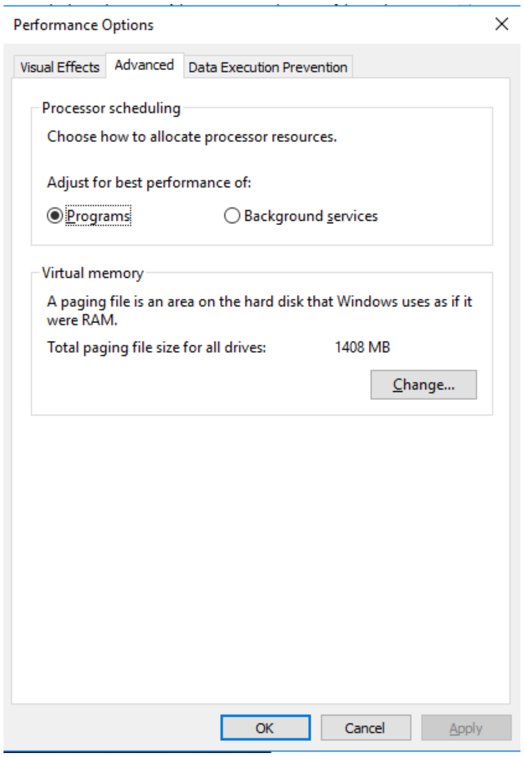
User Profiles

Desktop settings related to your sign-in

Startup and Recovery

System startup, system failure, and debugging information

4. 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:

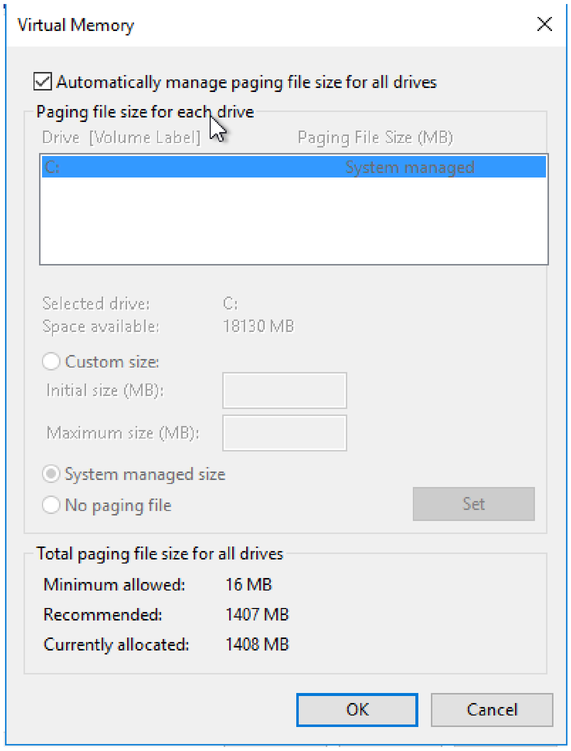
● Programs ○ Background services

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: 1408 MB

5. Select "Change" under Virtual Memory, the following screen will appear:



☑ 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

6. Uncheck **Automatically manage paging file size for all drives** and set **No paging file** option and confirm

Once **No paging file** is set you should skip chapters:

- "To encrypt PageFile.sys"
- "Clearing the System Pagefile.sys on shutdown"
- "To disable system management of PageFile.sys"

And continue with chapter:

- “To disable Windows Error Reporting”

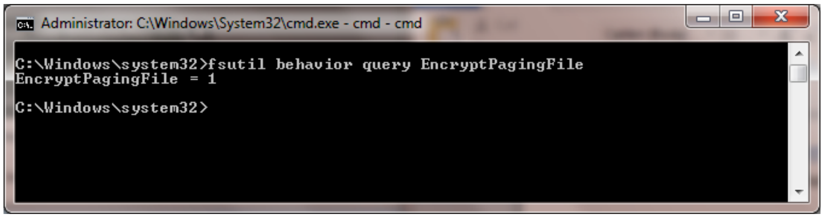
Encrypting PageFile.sys – Windows 10

Important: If you are using SSD disk you should have **No paging file** turned on as recommended by HW instructions following instructions in “Managing PageFile.sys” chapter. If **No paging file** is set, you should skip this chapter!

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

1. From the start menu, type in “cmd”.

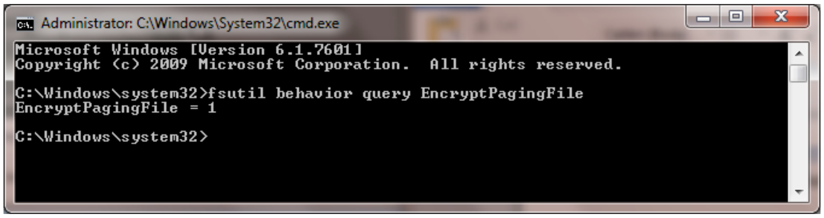
2. Right click on “Command Prompt” icon located on the left side of your screen, a selection bar will appear at the bottom of the screen, select “Run as Administrator”
3. To verify configuration type the following command: fsutil behavior query EncryptPagingFile



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

C:\Windows\system32>
```

4. If encryption is enabled EncryptPagingFile = 1 should appear
5. If encryption is disabled EncryptPagingFile = 0 should appear
6. To Encrypt the Pagefile type the following command: fsutil behavior set EncryptPagingFile 1

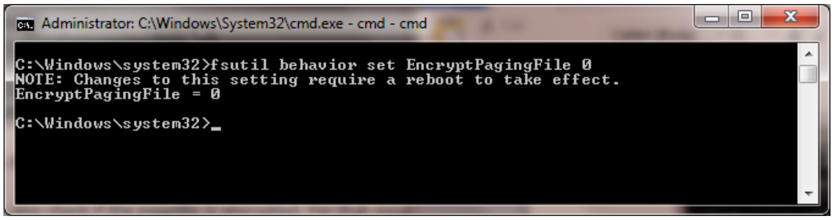


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

C:\Windows\system32>
```

7. 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>_
```

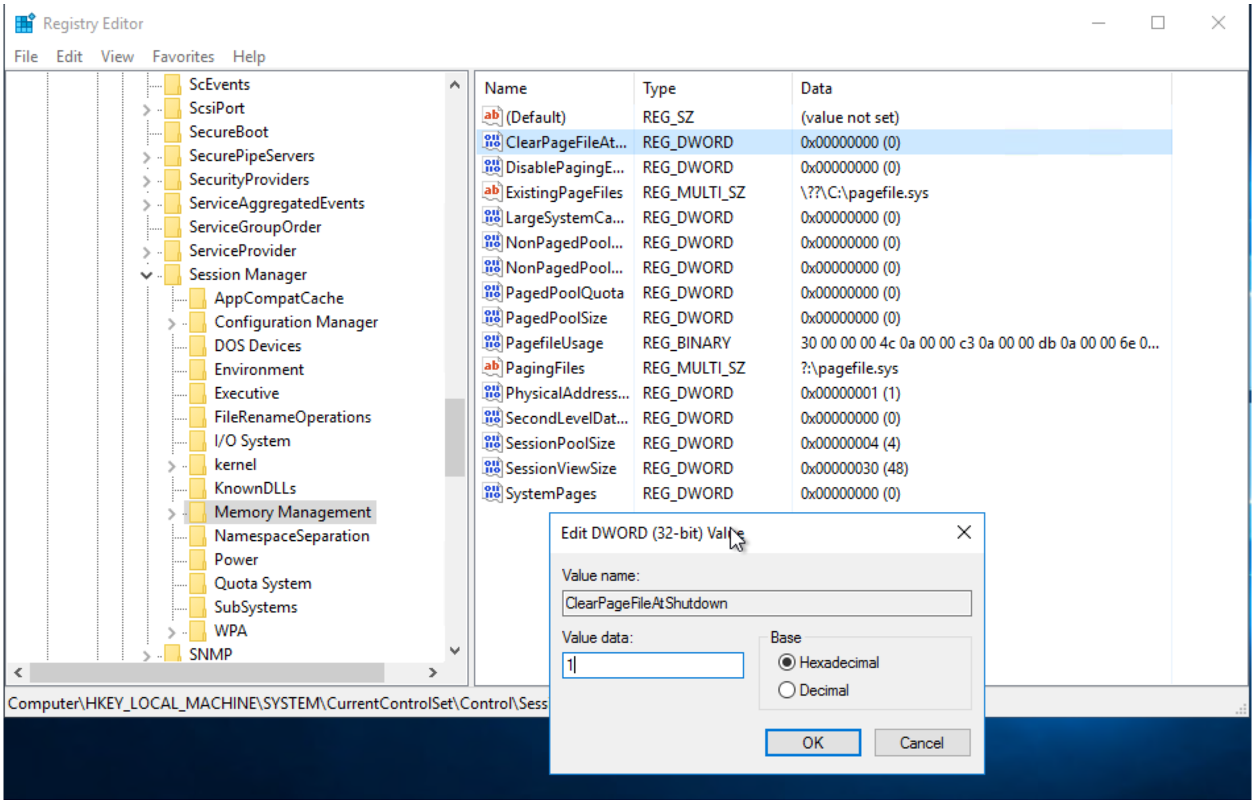
Clear the System Pagefile.sys on shutdown

Important: If you are using SSD disk you should have **No paging file** turned on as recommended by HW instructions following instructions in “Managing PageFile.sys” chapter. If **No paging file** is set, you should skip this chapter!

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.

1. From the start menu, type in “regedit”.
2. Right click on regedit.exe and select “Run as Administrator”
3. Navigate to HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management
4. Change the value from 0 to 1 on the “ClearPageFileAtShutdown” DWORD.
5. 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)

Edit DWORD (32-bit) Value

Value name: ClearPageFileAtShutdown

Value data: 1

Base: ● Hexadecimal ○ Decimal

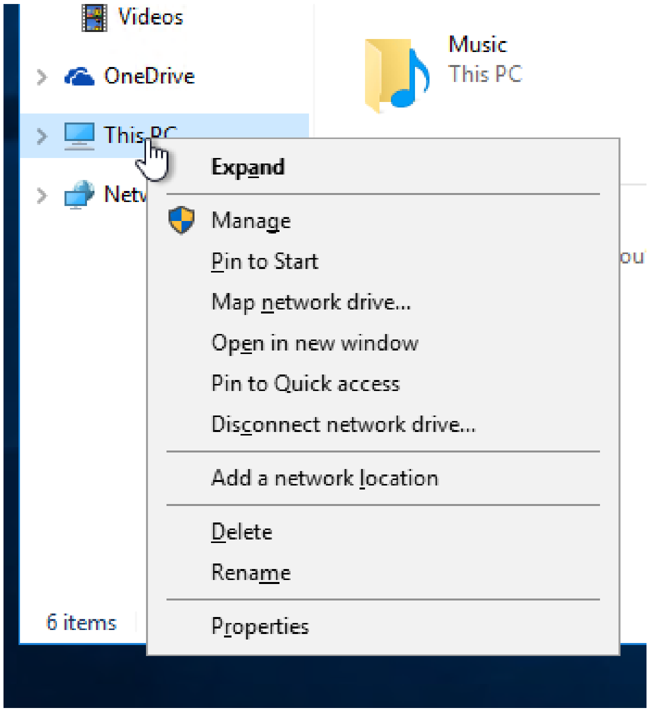
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Sess

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

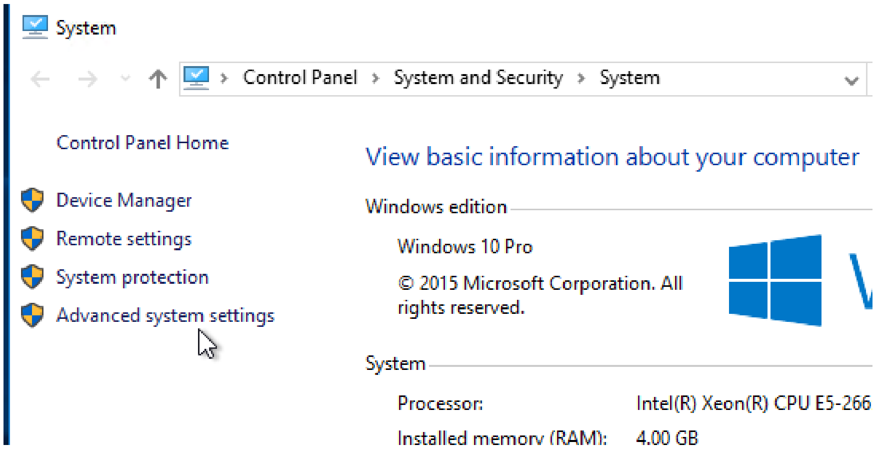
Disabling System Management of PageFile.sys – Windows 10

Important: If you are using SSD disk you should have **No paging file** turned on as recommended by HW instructions following instructions in “Managing PageFile.sys” chapter. If **No paging file** is set, you should skip this chapter!

1. Right Click on This PC > Select “Properties”:



2. Select “Advanced System Settings” from the System screen:



View basic information about your computer

Windows edition

Windows 10 Pro

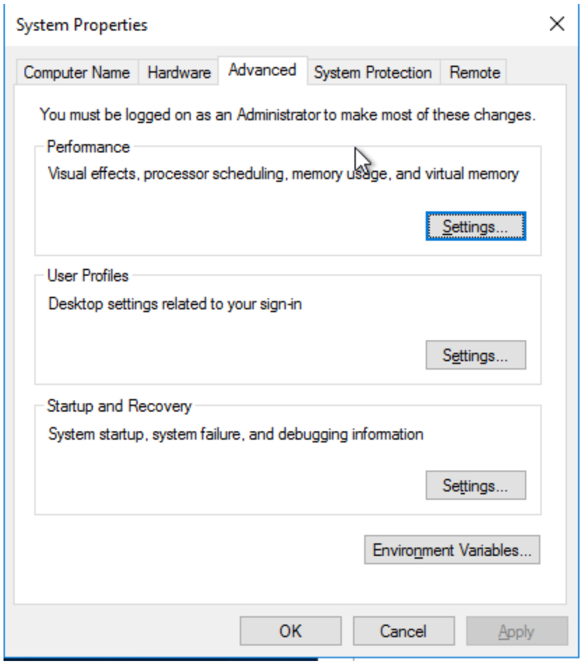
© 2015 Microsoft Corporation. All rights reserved.

System

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

Installed memory (RAM): 4.00 GB

3. 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

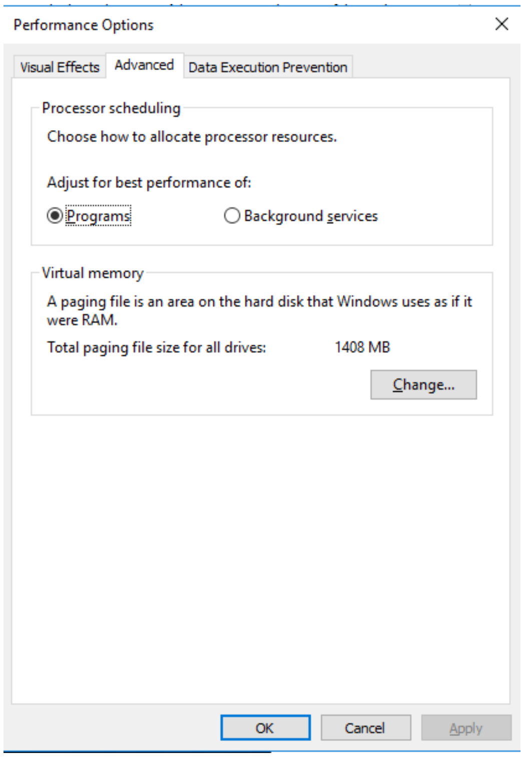
User Profiles

Desktop settings related to your sign-in

Startup and Recovery

System startup, system failure, and debugging information

4. 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:

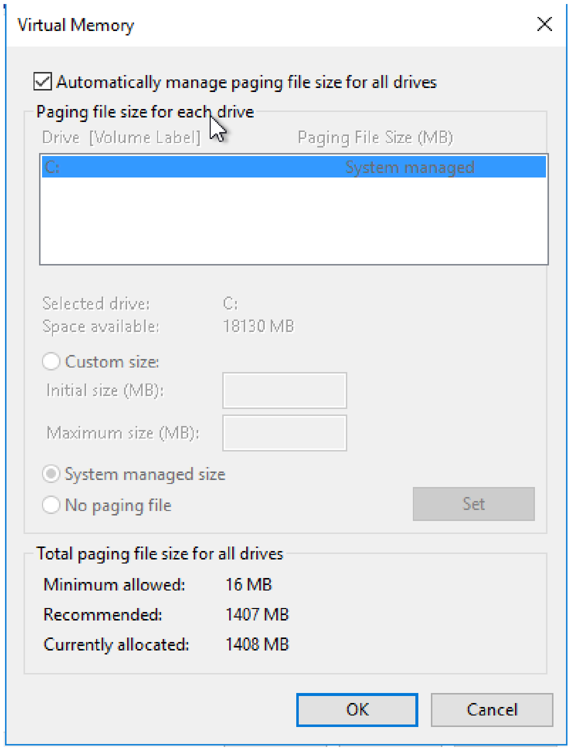
● Programs ○ Background services

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: 1408 MB

5. 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

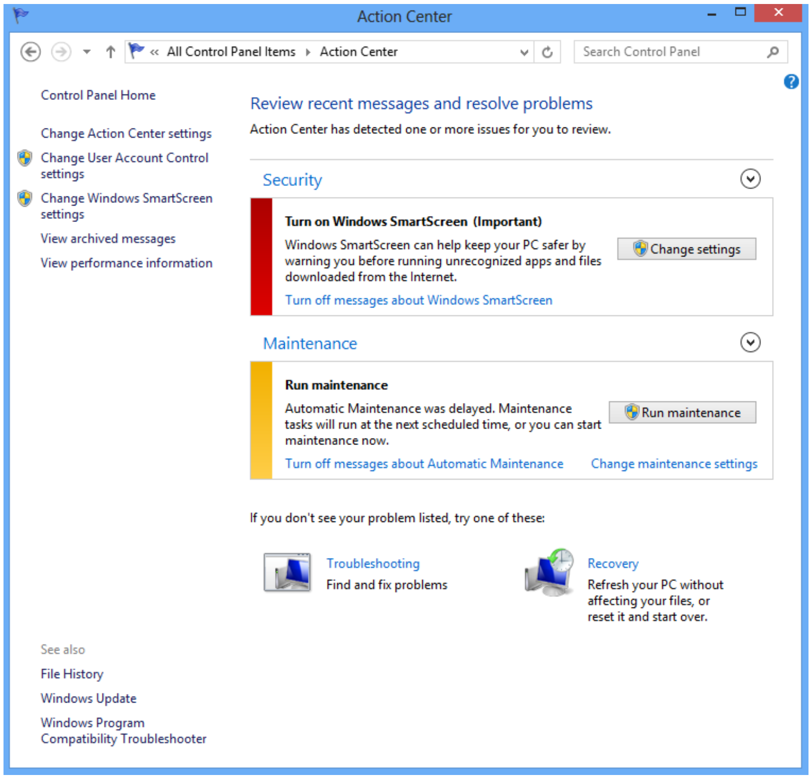
Recommended: 1407 MB

Currently allocated: 1408 MB

6. Uncheck “Automatically manage page file size for all drives”
7. Select “Custom Size”
8. 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.
9. Click “Ok”, “OK”, and “OK”
10. You will be prompted to reboot your computer.

Disabling Windows Error Reporting – Windows 10

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



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.

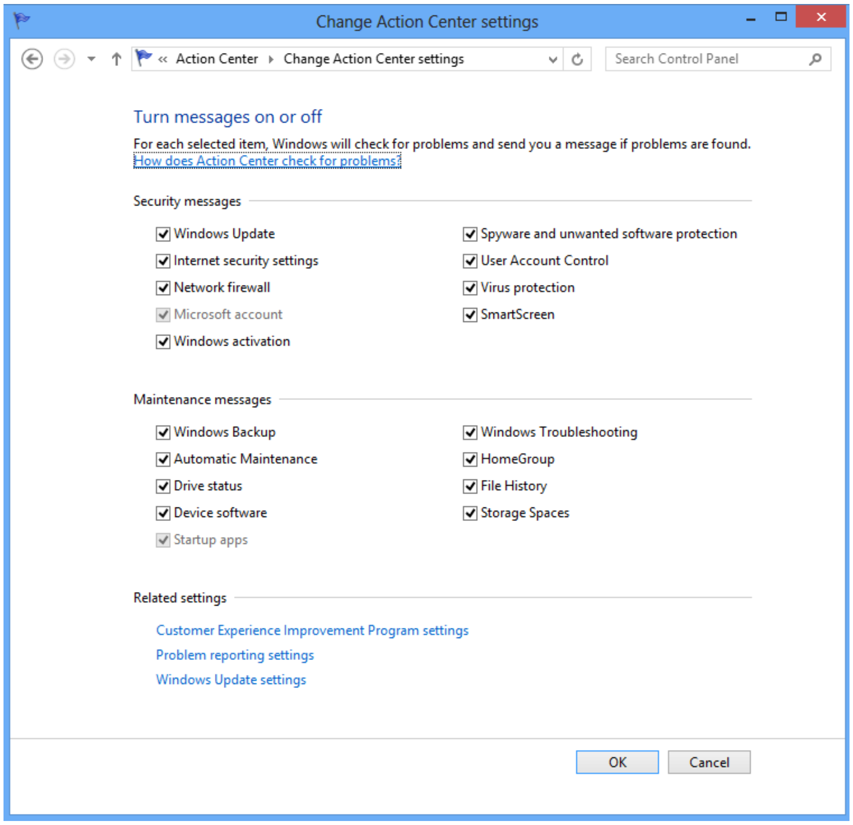
See also

File History

Windows Update

Windows Program Compatibility Troubleshooter

4. 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

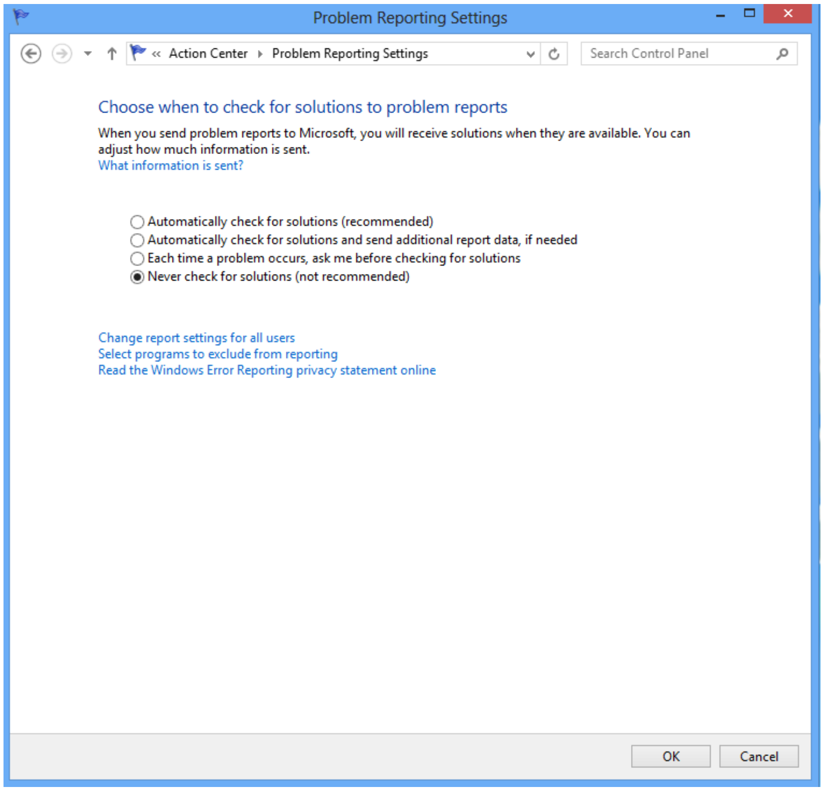
Customer Experience Improvement Program settings

Problem reporting settings

Windows Update settings

OK Cancel

5. 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.