WashCard systems

PA-DSS

Secure Implementation Guide for Credit Card Acceptance

WashCard Systems Satellite Server v4.5.x
PA-DSS Implementation Guide

About the Payment Card Industry (PCI) Security Standards

The PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including: the **D**ata **S**ecurity **S**tandard (**DSS**), **P**ayment **A**pplication **D**ata **S**ecurity **S**tandard (**PA-DSS**), and PIN-Entry Device (PED) Requirements. All of the five founding credit card brands have agreed to incorporate the PCI DSS as the technical requirements of each of their data security compliance programs. Each founding member also recognizes the QSAs and ASVs certified by the PCI Security Standards Council as being qualified to validate compliance to the PCI DSS.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. All businesses handling credit and debit cards are required by the card brands to maintain PCI DSS compliance.

The PA-DSS is a security standard designed to help software vendors develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure their payment applications support compliance with the PCI Data Security Standard. All payment applications handling credit and debit cards are required by the card brands to maintain PA-DSS compliance.

For more information on the PCI standards, visit http://www.pcisecuritystandards.org

Notice

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

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

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

About this Document

This document describes the steps that must be followed for your Satellite Server installations to comply with Payment Application – Data Security Standards (PA-DSS). The information in this document is based on PCI Security Standards Council Payment Application - Data Security Standards program (version 3.2 dated June 2016)[1].

WashCard Systems instructs and advises its customers to deploy WashCard Systems 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.

A copy of this document is included with each new system shipped from WashCard Systems. Whenever a revised version of this document becomes available, the updated PDF document will be emailed to you for your records. Should an additional replacement copy be needed, contact WashCard Systems Technical Support for assistance.

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

The Difference between PCI Compliance and PA-DSS Validation

As a software vendor who develops payment applications, our responsibility is to be "PA-DSS Validated." We have performed an assessment and payment application validation review with our independent assessment firm (PAQSA), to ensure that our platform does conform to industry best practices when handling, managing and storing payment related information. PA-DSS Version 3.2 is the standard against which Satellite Server 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 Satellite Server will help you facilitate and maintain PCI Compliance with respect to how the payment application handles user accounts, passwords, encryption, and other payment data related information. The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the PCI Data Security Standard (DSS). The security requirements defined in the DSS apply to all members, merchants, and service providers that store, process, or transmit cardholder data.

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

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

The 12 Requirements of the PCI DSS

Build and Maintain a Secure Network and Systems

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

Protect Cardholder Data

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

Maintain a Vulnerability Management Program

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

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know
8. Identify and authenticate access to system components
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for all personnel

Implementing Satellite Server Securely

Of the PA-DSS and PCI-DSS criteria that determine the security level and ultimate compliance of WashCard Systems Satellite Server, six areas stand out as requiring particularly close attention: storing card data, user management, logging, network considerations, remote access and encryption over public networks.

Storing Sensitive Authentication Data

Satellite Server does not and will never store full magnetic stripe data, CVV2, and/or PIN data (Sensitive Authentication Data, or **SAD**). Satellite Server will also never store the Primary Account Number (**PAN**). There are no debugging or troubleshooting settings that permit SAD or PAN data to be stored. Therefore, neither encryption of cardholder data nor PAN display configuration instruction are required, as per PA-DSS v3.2.

NOTE: Storing Sensitive Authentication Data through alternate means is not allowed for any reason. If you store sensitive card data, your system will be rendered NON-COMPLIANT.

Storing the Primary Account Number

Storing the Primary Account Number (PAN) should also be avoided whenever possible to avoid risk of theft and to minimize PCI compliance requirements. SAD data such as full magnetic stripe, CVV2, or PIN data (SAD) should never be stored after authorization is complete.

If PAN data must be collected for troubleshooting purposes:

- Collect these data only when needed to solve a specific problem
- Store these data only in specific, known locations with limited access
- Collect as little of these data as necessary to solve the specific problem
- Encrypt these data when stored
- Securely delete these data immediately after use (see following section)

Securely Deleting Sensitive Card Data

After the specific problem is resolved, you must securely delete any sensitive data *immediately* using a secure removal tool such as Heidi Eraser. Heidi Eraser is available for download at:

http://www.heidi.ie/eraser/

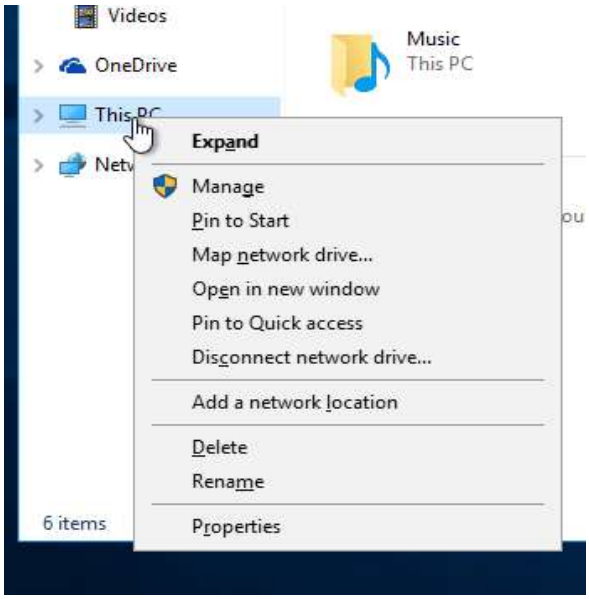
To use this tool to securely erase a file, the following procedure must be used:

1. Start Eraser.exe
2. Right click in the program window and select New Task
3. Under Task Properties, ensure that Run Manually is selected.
4. Click Add Data, this brings up the *Select Data to Erase* dialog.
5. Select US DoD 5520 as the Erasure Method, then select the file to be securely deleted.
6. Close all dialogs by clicking OK, then click on the Erase Schedule tab.
7. On the main Erase Schedule screen, right click the newly created task and select Run Now.
   - This task may take several hours to days to complete.
8. Ensure the status is now Completed.

Addressing Inadvertent Capture of PAN – Windows 10

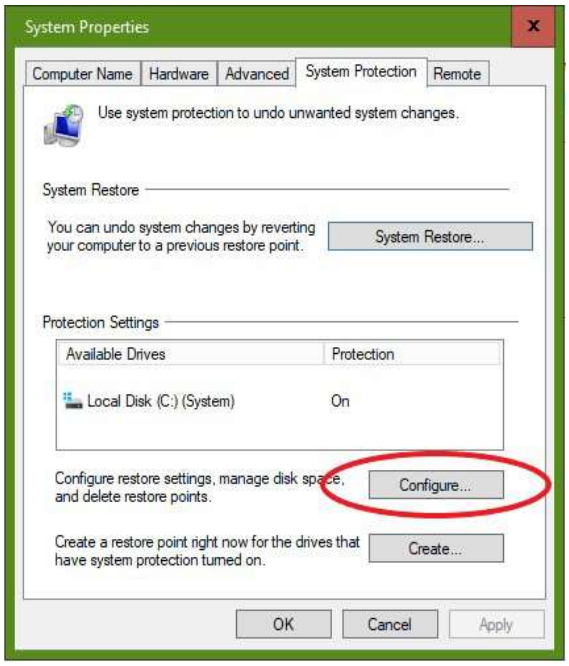
Disabling System Restore and System Management of the Windows Paging File

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

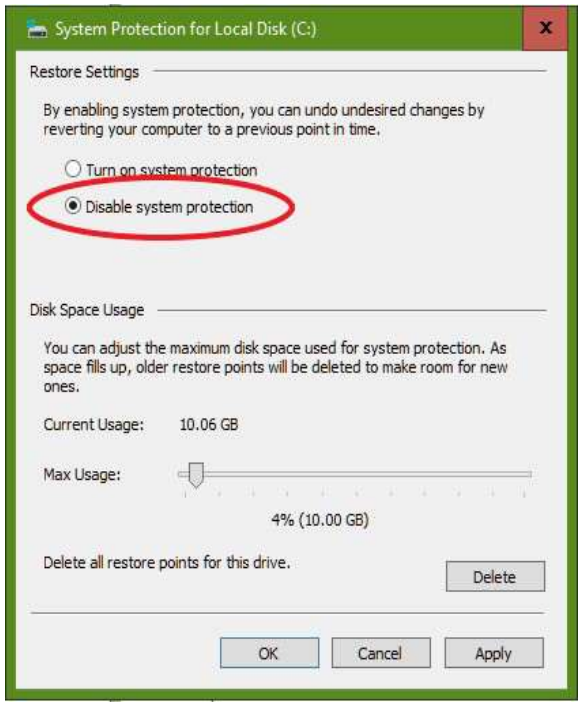


- Click “Advanced System Settings” from the System screen:

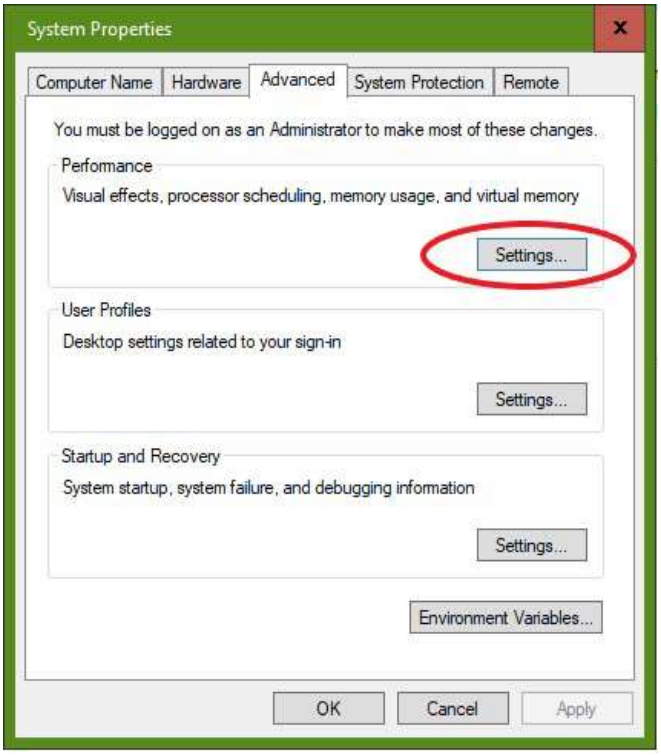
- Select the “System Protection” tab and click “Configure”



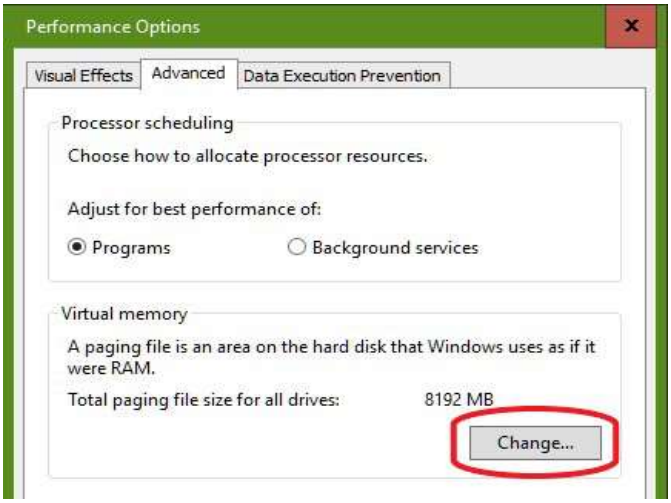
- Select “Disable system protection”



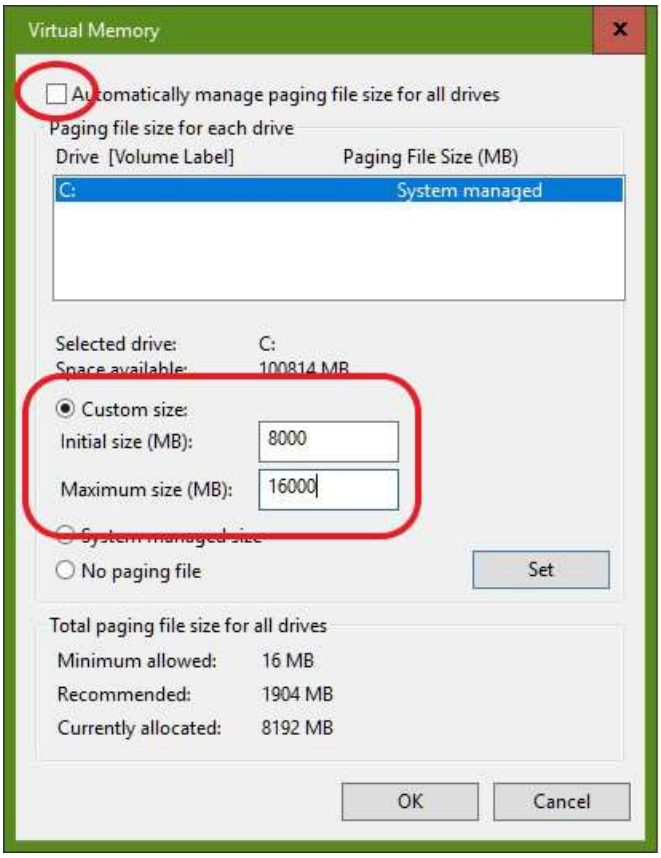
- Click OK to save and close the System Protection window
- Select the “Advanced” tab and in the Performance section click “Settings”



- Select the “Advanced” tab and in the Virtual memory section click “Change”



- Uncheck “Automatically manage paging file size for all drives”
- Select Custom Size
- Configure Initial Size to match the amount of RAM in the SMC, and Maximum Size to twice the amount of RAM in the SMC, as shown below:



- Click OK three times to save the Virtual Memory settings, close the Performance Options window, and close the System Properties window

- Reboot the computer

Encrypting the Windows Paging File (PageFile.sys)

The Windows paging file can allow data to propagate from memory onto the hard disk. Encrypting the paging file helps to prevent the inadvertent retention and capture of cardholder data.

To encrypt the paging file, the following procedure must be used:

- Open a command prompt
- Type in the command, “fsutil behavior set EncryptPagingFile 1” and press <Enter>
- Restart the computer
- Verify that the change occurred by opening a command prompt and typing in the command, “fsutil behavior query EncryptPagingFile” and pressing <Enter>
- This should return, “EncryptPagingFile = 1”

Clear the Windows Paging File on Shutdown

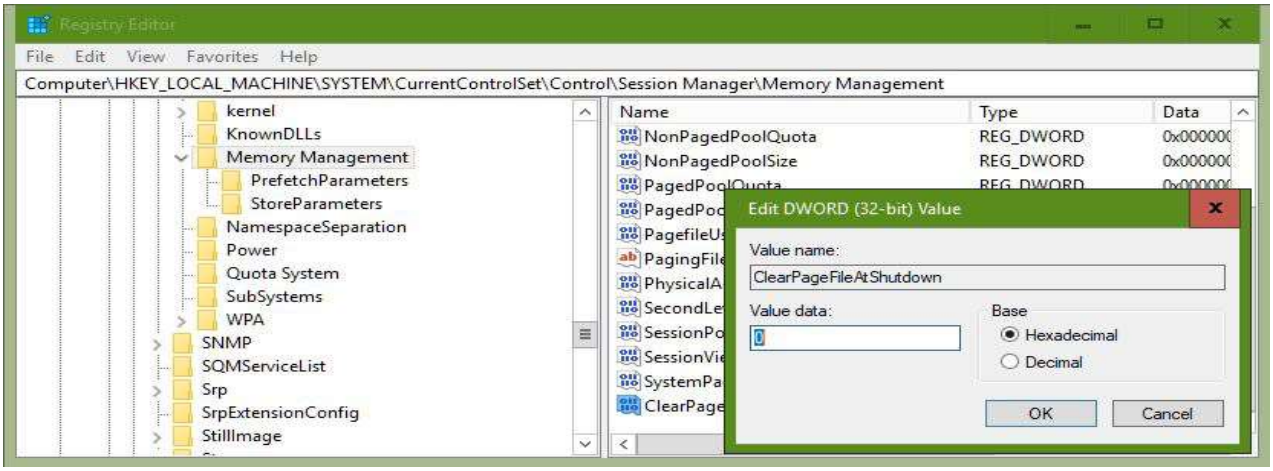
NOTE: Enabling this feature may increase windows shutdown time.

Windows has the ability to clear the paging file on system shutdown. This will purge all temporary data from pagefile.sys. (Temporary data includes system and application passwords, cardholder data (SAD/PAN), etc.)

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

If the value does not exist, add the following DWORD within the Memory Management key:

- Value Name: ClearPageFileAtShutdown
- Value Type: REG_DWORD
- Value: 1



Encrypt Sensitive Traffic over Public Networks

Satellite Server utilizes HTTPWebRequest and HTTPWebResponse functionality over HTTPS, utilizing TLS 1.2, for data security over public networks. This secured communication is used whenever sending Sensitive Authentication Data to your credit card processing gateway for credit card authorization. In this way, Satellite Server meets public network security requirements for PCI-DSS and keeps your customers' credit card data encrypted and safe from potential interception.

Attempting to send Sensitive Authentication Data through alternate means should be avoided whenever possible to avoid risk of theft and to minimize PCI compliance requirements. *Never* send credit card account numbers (PAN) or other Sensitive Authentication Data (SAD) using email, chat, or other instant messaging services. These messages can easily be intercepted on internal and public networks. If you must send PAN data for a valid business reason, you must ensure you're sending it via secure protocols, encrypted using TLS 1.2 or greater, and utilizing trusted keys and certificates at all times. You must also securely delete all Sensitive Authentication Data once the business reason has been resolved. See the earlier section *Securely Deleting Sensitive Card Data* in this same document for complete details.

Truncating and Masking the Primary Account Number (PAN)

Satellite Server truncates primary account numbers (PAN) data, stores only the last four digits of PAN, and truncates all occurrences of displayed PAN data. There are no options available to change the way Satellite Server truncates or masks this critical data when being displayed during or after the sale. Therefore, there is no way to export full PAN data from the Satellite Server application, as only the last four digits of any primary account number are ever stored for historic reporting purposes. All truncated PAN data is generated from these last four digits of the account number, so that only the last four digits of the account number are visible, with the preceding account digits replaced with the "X" character; for example, XXXXXXXXXXXX9999.

Interfaces at which masked PAN data is printed or displayed include:

- Card Dispenser receipts
- Receipt Printing Station receipts
- The LCD on the self service device (washer, dyer, wash bay, etc.)
- Satellite Server transaction history tab of the application window on the Site Management Controller
- Satellite Server diagnostic event logs
- CSV transaction history backup files
    - See Implementation Guide section **Accessing Transaction History Locally on the Site Management Controller (SMC)**

CRITICAL NOTE: Again, Satellite Server stores no Sensitive Authentication Data (SAD) or full Primary Account Numbers (PAN). There are no options available to force Satellite Server to store critical data. As a result, management of application storage is simplified for the business owner and there are no encryption key-custodian requirements or processes in place to expire and manage encryption keys for the purpose of securely storing Primary Account Numbers (PAN).

If PAN data is gathered by the business through a method other than the Satellite Server application, you MUST encrypt and securely store this cardholder data per PCI-DSS requirement 3.6. Failure to comply with this requirement will render your location **NON-COMPLIANT**.

Remote Access

Satellite Server does not require the use of remote access.

If vendors, resellers/integrators, or customers can access customers' payment applications remotely, the remote access must be implemented securely. Remote access security requirements include:

- Do not use remote access solutions which require "port forwarding" such as VNC and PCAnywhere.
- Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer).
- Allow connections only from specific, known IP or MAC addresses.
- Require all users to have unique Logins and Passwords.
- Users can not use shared, group, or generic logins or passwords.
- All passwords must be changed at least every 90 days.
- You must not reuse a password used in the past 4 previous.
- Use strong authentication and complex passwords for logins. Passwords must be at least 7 characters in length, have alpha and numeric characters, and at least 1 upper case alpha character.
- Multi-Factor authentication is required for remote access sessions.
- Enable encrypted data transmission using TLS 1.2 or newer.
- Enable account lockout after 6 failed login attempts for at least 30 minutes.
- If account is idle for 10 minutes, remote session is automatically logged off.
- Activate remote-access technologies only when needed with immediate deactivation after use.
- Configure the system so a remote user must establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed.
- Your system must be configured with your personal firewall turned on before you can remotely access your WashCard System Satellite Server.
- You must enable logging functions and review logs regularly.
- Restrict access to customer passwords to authorized reseller/integrator personnel.
- Establish customer passwords according to PCI-DSS requirements 8.1, 8.2, 8.4, and 8.5.

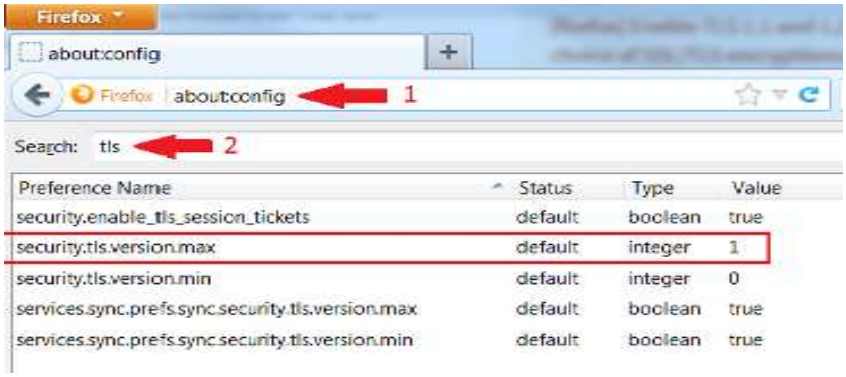
WashCard Systems has evaluated several remote access solutions; comparing cost, convenience and security features that meet PCI compliance requirements for remote access. WashCard Systems recommends the use of LogMeIn Central with free or professional client packages. LogMeIn accounts must be configured for multi-factor authentication. As stated above, remote access must only be activated when needed and deactivated immediately after use. See page 10 of the LogMeIn Security Whitepaper for additional information:

https://secure.logmein.com/welcome/documentation/EN/pdf/common/LogMeIn_SecurityWhitepaper.pdf
NOTE: LogMeIn refers to Multi-factor Authentication as Two-Step Verification.

Remote Access (Continued)

The web browser being used to remotely access the Site Management Controller via LogMeIn must be updated to support the TLS 1.2 standard. This level of support is available on all current releases of web browsers running on up to date operating systems. Ensure you are running the current version of your preferred browser. Further, if using Mozilla Firefox, additional steps are required to enable this support level. If running Mozilla Firefox, the following steps must be completed to maintain PCI compliance:

- Open the Firefox browser
- Type “about:config” (without the quotes) into the navigation bar and press <enter>.
- Type “tls” (without the quotes) into the Search bar.
- Security.tls.version.max is the variable we are interested in. It should be set to 1, by default.



- Double-click security.tls.version.max.
- Change the value from 1 to 3.
- Click OK.
- Close and restart Firefox for the change to take effect.

Non-Console Administrative Access

Satellite Server does not ship with any options for Non-Console Administration of the application. If you use an alternate administration interface over the network (*e.g.* administrative web page, telnet) to access your payment processing environment, this traffic must be encrypted with a secure encryption technology such as SSH, VPN, or TLS 1.2 or newer, and Multi-Factor Authentication must be enabled.

Non-Console Administration security requirements include:

- Do not use solutions which require "port forwarding" such as VNC and PCAnywhere.
- Change default settings in the administraion software (for example, change default passwords and use unique passwords for each customer).
- Allow connections only from specific, known IP or MAC addresses.
- Require all users to have unique Logins and Passwords.
- Users can not use shared, group, or generic logins or passwords.
- All passwords must be changed at least every 90 days.
- You must not reuse a password used in the past 4 previous.
- Use strong authentication and complex passwords for logins. Passwords must be at least 7 characters in length, have alpha and numeric characters, and at least 1 upper case alpha character.
- Multi-Factor authentication is required for all non-console administration solutions.
- Enable encrypted data transmission using TLS 1.2 or newer.
- Enable account lockout after 6 failed login attempts for at least 30 minutes.
- If account is idle for 10 minutes, remote session is automatically logged off.
- Your system must be configured with your personal firewall turned on before you can remotely access your WashCard System Satellite Server.
- You must enable logging functions and review logs regularly.
- Establish customer passwords according to PCI-DSS requirements 8.1, 8.2, 8.4, and 8.5.

Wireless Networks

WashCard Systems Satellite Server does not ship with or come delivered with a wireless option. Should merchants choose to implement wireless connectivity, they must perform the following to insure PCI-DSS compliance:

- Do not use WEP encryption. WashCard Systems recommends WPA2 encryption.
- Existing wireless setups must use WPA2 encryption when it's an available option. Some older wireless equipment may lack WPA2 support. Almost all can be updated through firmware and driver updates available on the manufacture's web site.
- In the rare case when there are no available updates from the manufacturer that add WPA2 support, those devices must be replaced with newer equipment and the encryption set to WPA2 encryption.
- The default WPA2 encryption key must be changed to a unique strong key.
- The default password for accessing the Wireless Access Point's settings must be changed to a unique strong password.
- Change default SNMP (Smart Network Management Protocol) community strings on Wireless Access Points if SNMP is supported or disable SNMP altogether on installation.
- Change default SNMP community strings on Wireless Access Points if SNMP is supported or disable SNMP altogether whenever anyone with knowledge of the keys/passwords leaves the company or changes positions.
- Install a firewall between any wireless networks and systems that store cardholder data. Configure firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.
- Use industry best practices (for example, IEEE 802.11.i) to provide strong encryption for authentication and transmission.
- Synchronize the access point clocks to be the same as your computers to ensure logged timestamps match.
- It is HIGHLY RECOMMENDED that wireless networks attached to your payment processing network enable the following additional security:
    1. Use wireless keys of 13 random characters containing letters, numbers, and symbols.
        - Keys comprised of words or names are quickly found by criminals using readily available, easy to use tools.
    2. Disable SSID Broadcast to make your wireless network less visible to unauthorized users.
    3. Use MAC address filtering so that only authorized computers are allowed access to the wireless network.
    4. When configuring WPA2, use the AES option. Only use TKIP when AES is not an available option. Although not severe, there are known weaknesses in TKIP.

More information on network segmentation can be found in the section, *Network Basics and Segmentation*. Recommended network configuration diagrams are available in Appendix A, *Recommended Network Configurations*. For a more thorough explanation regarding setting up wireless networks, review the PCI DSS Wireless Guidelines document listed on the PCI Security Council's website:

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

Network Basics and Segmentation

Switches are network devices that allow you to connect together multiple computers, routers, firewalls, etc. Switches have multiple network ports, one for each item connected using a network cable. All devices connected to the same switch can communicate with each other unobstructed.

Firewalls are network devices that allow you to protect a network segment on the LAN side from the network segment on the WAN side. Although they can be very costly, there are inexpensive ($40-$100) small routers containing firewall functionality that can be found at any store containing computer equipment. These inexpensive routers will work sufficiently, so long as they support Stateful Packet Inspection (SPI).

Network segmentation is a strategy intended to simplify PCI compliance of your network and to help you protect your business from hackers. At the most basic level, there are three zones representing three levels of risk.

Untrusted Environment – Network connections that anonymous people have access to are considered "untrusted." They should have no network access to your business computers and POS equipment. Business computers should never be connected directly to this zone. Common, untrusted networks are the internet connection itself, customer wireless internet access, and visitor network connections. This is the highest risk zone because anybody can connect to it anonymously. Systems connected to this zone are commonly hacked or get infected with malware and viruses.

Non Card Data Business Environment – Systems not used for payment processing, but still business owned, fit into this segment. These are systems that can be used for email, web browsing, and other higher risk activity that you would never want to perform on your payment processing systems. On occasion, these systems may become infected with malware and viruses. Once a computer in this zone is infected, the hacker or infection will spread to other systems if they're not protected by a firewall. Note that if any systems in this zone handle credit card data, that data is being put at risk. This is a medium risk zone due to the likelihood of occasional infection. By segmenting these systems into their own zone, the breach is contained. The hacker, malware, or virus doesn't reach your firewall protected payment processing zone.

Card Data Business Environment – Systems used for payment processing fit into this segment. These systems should only be used for POS activity and should NEVER be used for any other reason. Should these computers become infected with malware or viruses, sophisticated hacking tools can potentially steal sensitive data such as credit cards. The average cost of a breach for a small merchant is $36,000. This is a low risk zone because it's protected from the other two zones, and because high risk activities such as web browsing and email do not occur inside it.

In summary, to segment your network for security you should:

- Protect both business environments from the untrusted environment
- Protect your card data business environment from the non card data business environment

For a simple network diagram to help guide your network configuration, see Appendix A, *Recommended Network Configurations*.

Required Components and Protocols

Components	Additional Details	Function
aiOne Controller	IRCB v0.2	Wash Bay Interface Unit w/ Integrated Reader
Laundry Controller	V1.1.15.0	Washer/Dryer Interface Unit w/ Integrated Reader
G2 Terminal Controller	V1.39	Wash Bay Interface Unit
Neuron Card Reader	Model: SCR-933SF-4R-6003	Used in conjunction with G2 Terminal Controller
Site Controller	V1.1	controller network. Communicates with Satellite Server over crossover ethernet cable and the TCP/IP Protocol.

Protocols	Additional Details	Function
TCP/IP	Port 33601	Communications between controller network and Satellite Server
TLS 1.2	HTTPS Port 443	Negotiated secure communications for credit card processing, and synchronization with Business Management Center.

Software	Additional Details	Function
Windows 10	64-Bit Professional	Operating System
Satellite Server	V4.5.x	Payment Management Application
.Net Framework	V4.6.1	Required by Payment Management Application
SQL Compact Edition	V4.0	Required by Payment Management Application

Hardware	Additional Details	Function
Motherboard	Asus – Socket LGA1155	Required for Operating System
Processor	Intel Pentium Dual Core 3.2 GHz	Required for Operating System
500 GB Hard Drive	Western Digital	Required for Operating System
8 GB RAM	Kingston DDR3	Required for Operating System

Required TCP/IP Ports

Port Number	Additional Details	Function
33601	Site Controller Listener Port	Local Area Network: Satellite Server network connectivity to the laundromat and car wash devices.
443	HTTPS	Wide Area Network: Negotiated secure communications with credit card processing gateways and the BMC.
465	SMTP	Outgoing TLS secured email.
53	DNS	Domain Name Services.
547	DHCP	Local Area Network IP Address Allocation.

Satellite Server User Management

The Satellite Server program, when first installed, contains only a single default administrative user and password:

User: WashCardAdmin
Password: S@tS3rver$

It is highly recommended that you create a new User and Password for your use and disable the default account during system configuration. As a minimum requirement, the Satellite Server User Management system will require a password change for the default user account on initial login and each 90 days following.

It is highly recommended to disable inactive or terminated user accounts immediately to prevent access. Although immediate action is recommended, for PCI compliance, this absolutely must be done within 90 days.

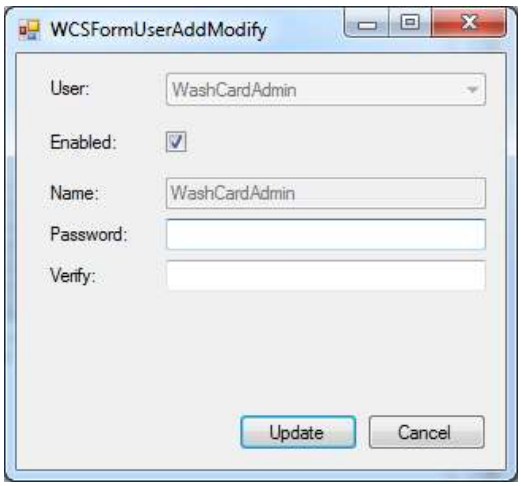
Satellite Server utilizes a 10 position unique salt and the SHA-2 (SHA-256) hash functionality to encode user passwords before storage in the user repository. Additionally, the following requirements for PA-DSS compliance are enforced programmatically across the WashCard Systems platform and cannot be changed. They apply to all user types and roles.

- Passwords must be at least seven characters
- Passwords must contain at least one upper case, one lower case, and one special character
- Passwords must be changed every 90 days
- Passwords must not be the same as the last four used
- After a user idle time of no more than 15 minutes, the password must be re-entered.

Each user must have a unique user ID and password. Do not use group, shared or generic accounts or passwords. Users should never share their passwords. User IDs are case insensitive. The account management system checks each new creation request against the existing user list and returns an exception if a duplicate User ID is specified on the creation request.

To open the user management interface, follow the steps below:

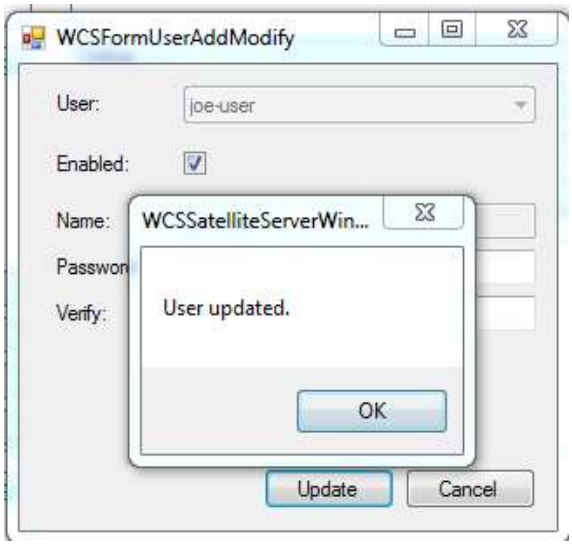
- From the Satellite Server menu bar, click View
- Click Users in the resulting drop down list
- Enter the default credentials: WashCardAdmin/S@tS3rver$
- Click <OK>
- The following form will now be displayed.



NOTE: If the password for the active user is over 90 days old, or if this is the initial login utilizing the default credentials, a "Password is Expired" dialog appears. The user must click <OK> and immediately change their password per the *Editing an existing user* instructions below.

Editing an existing user:

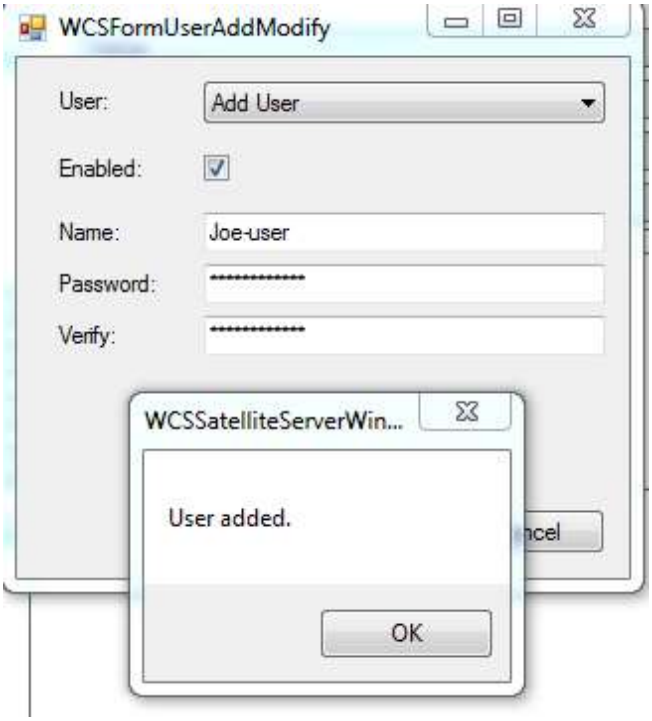
- Select the user in question from the User drop down list
- Enable or disable the user as required
- If changing the password, provide an updated password and verify the password as required
  - Requirements: 7+ characters including 1 uppercase, 1 lowercase, and 1 special character.
  - Satellite Server will verify that the password meets the above requirements and that it does not match one of the 4 previously used passwords.
- Click <Update>
- On success, a confirmation dialog box will appear showing "User updated."



- Click <OK>
- The user has now been updated. Close the WCSFormUserAddModify form to return to Satellite Server's main program window.

Adding a new user:

- Select “Add User” from the User drop down list
- Enable or disable the user as required
- Provide a unique Name for the user
- Provide a password and verify the password
  - Password requirements: 7+ characters including 1 uppercase, 1 lowercase, and 1 special character.
- Click <Update>
- On failure, a message will be displayed indicating cause of failure. In this case, click OK and take corrective action by repeating steps 2 – 4 above
- On success, a confirmation dialog box will appear showing “User added.”



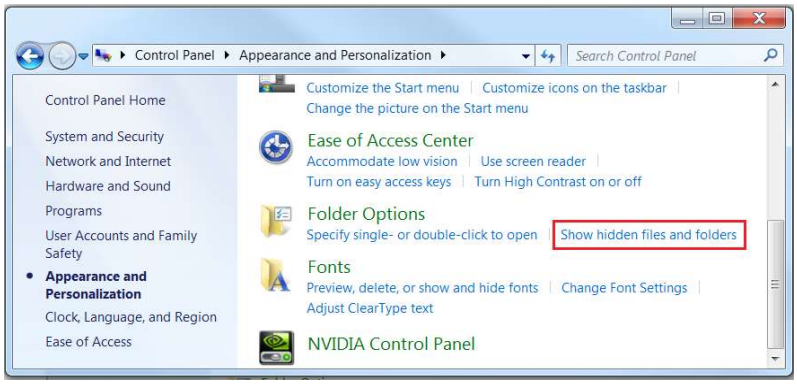
- Click <OK>
- The new user has now been added. Close the WCSFormUserAddModify form to return to Satellite Server's main program window.

NOTE: Security in user management is a major component of PCI compliance. To protect your system configuration and ensure compliance, Satellite Server utilizes SHA256 encryption with unique salts and one way hash algorithms for each user password being stored.

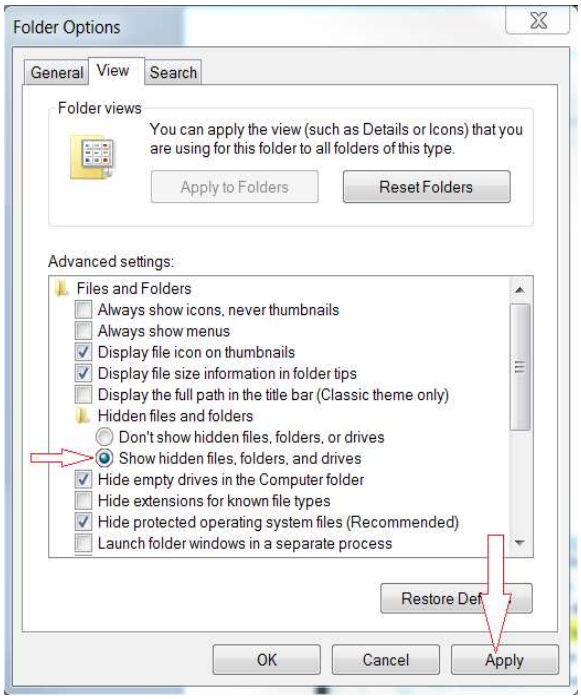
Recovering From Forgotten Satellite Server User Credentials

If a single user or password is forgotten, it can be recovered and reset by any other valid configured administrative user in the local user repository utilizing the steps detailed above, in the section titled *Satellite Server User Management*. However, if all administrative user account passwords have been lost or forgotten, the local configuration database must be cleared and rebuilt from default with the following steps:

- Log into Windows on the Site Management Controller with an administrator account
- By Default, this administrator account is: WashCardAdmin
- Click *START* and Select *Windows System*
- Click *Control Panel*
- Click *Appearance and Personalization*
- Under the File Explorer Options section, click *Show hidden files and folders*



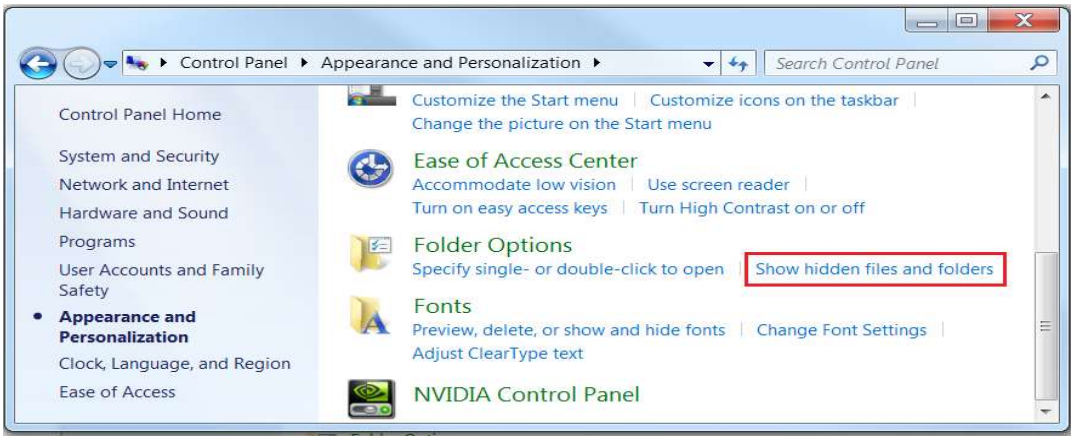
- Select *Show hidden files, folders, and drives*
- Click <Apply>



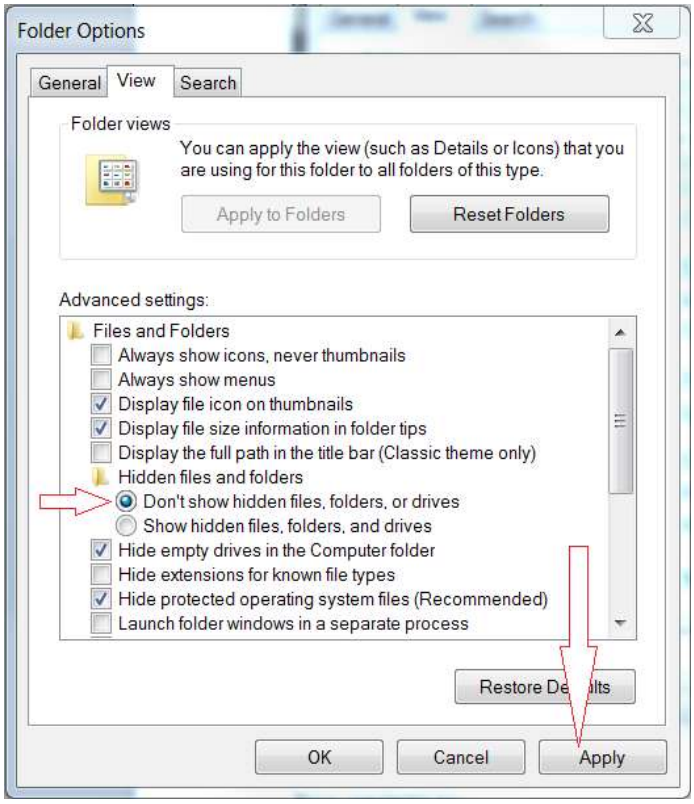
- Open windows File Explorer (//START/Windows System/File Explorer)
- On the left side of the File Explorer window expand *This PC*
- Expand *Local Disk (C:)*
- Expand *Users*
- Expand *WashCardUser*
- Expand *AppData*
- Expand *Local*
- Expand *WashCard Systems*
- Note that there may be a second folder named WashCard_Systems. Make sure to expand the folder name with a space between the words, NOT the underscore.
- Ensure the Satellite Server program has been closed and is not running.
- Delete the file WCSDatabaseAuthorizer.sdf
- Restart Satellite Server

Restore hidden status to hidden files, folders, and drives:

- Log in to Windows on the Site Management Controller with an administrator account
- By Default, this administrator account is: WashCardAdmin
- Click *START* and Select *Windows System*
- Click *Control Panel*
- Click *Appearance and Personalization*
- Under the File Explorer Options section, click *Show hidden files and folders*



- Select *Don't show hidden files, folders, or drives*
- Click <Apply>



When Satellite Server restarts, a new user credential and credit card authorizer database is created with the as-shipped default settings. See above section *Satellite Server User Management* for the default user, password and all user configuration instructions.

CRITICAL NOTE: Restoring user and credit card authorizer settings to default with the above detailed steps means that Credit Card Processing will not function until the credit card processing gateway has been reconfigured. See the following section for instructions on reconfiguring your processing gateway: *Credit Card Processor Configuration and Management.*

If you have any questions or concerns regarding this reconfiguration process, please contact WashCard Systems Technical Support for assistance:

888-439-5740 x: 200
support@washcard.com

Auditing User Activity

Auditing of user activity in Satellite Server is on by default. Audit functionality cannot be disabled. All activity relating to adding or editing users and all activity relating to setting or editing credit card processing gateway configuration options is logged to the Satellite Server diagnostic history records.

Diagnostic history records can be viewed within the Satellite Server application by selecting VIEW from the application menu bar and then selecting History. User audit records are flagged with a TerminalControllersID of -1000, and a HistoryName of WCSFormAuthorizerModify.

Each type of audit record is detailed below for reference: Invalid Login, Add Login, Reset Password, Enable Login, Disable Login, Edit Location CC Authorizer, and Successful Login.

Invalid Login

AuditsTypesID [Invalid Login (20)] AuditsLocationsID [571] AuditsClientsID [411] AuditsLogin [administrator] AuditsDateTime [20141119093951], WCSFormAuthorizerModify, -1000

Details:

- AuditsTypesID - Indicates the type of audit log being viewed. In this case, this is recording an Invalid Login event.
- AuditsLocationsID and AuditsClientsID – These fields can be ignored at this time. The location and client associated with this event will always be the physical location and client at which the Satellite Server application is running. This information is required only if further assistance is requested from WashCard Systems Technical Support.
- AuditsLogin - Indicates the user account which is performing the audited login attempt.
- AuditsDateTime – Records the date and time when user *administrator* attempted login.
- WCSFormAuthorizerModify and -1000 both flag this history record as an audit entry

Add Login

AuditsTypesID [Add Login (27)] AuditsLocationsID [571] AuditsClientsID [411] AuditsLogin [administrator] AuditsTextBox1 [Tim] AuditsDateTime [20141119093951], WCSFormAuthorizerModify, -1000

Details:

- AuditsTypesID - Indicates the type of audit log being viewed. In this case, this is recording an Add Login event.
- AuditsLocationsID and AuditsClientsID – These fields can be ignored at this time. The location and client associated with this event will always be the physical location and client at which the Satellite Server application is running. This information is required only if further assistance is requested from WashCard Systems Technical Support.
- AuditsLogin - Indicates the currently logged in user account which is performing the audited action.
- AuditsTextBox1 - Logs the User which is being added during the audited Add Login event.
- AuditsDateTime – Records the date and time when user *Tim* was added to the system by user *administrator*
- WCSFormAuthorizerModify and -1000 both flag this history record as an audit entry

Reset Password
AuditsTypesID [Reset Password (26)] AuditsLocationsID [571] AuditsClientsID [411] AuditsLogin [administrator] AuditsTextBox1 [Tim] AuditsDateTime [20141119093951], WCSFormAuthorizerModify, -1000

- Details:
- AuditsTypesID - Indicates the type of audit log being viewed. In this case, this is recording a Reset Password event.
- AuditsLocationsID and AuditsClientsID – These fields can be ignored at this time. The location and client associated with this event will always be the physical location and client at which the Satellite Server application is running. This information is required only if further assistance is requested from WashCard Systems Technical Support.
- AuditsLogin - Indicates the currently logged in user account which is performing the audited action.
- AuditsTextBox1 - Logs the User which is being modified during the audited Add Login event.
- AuditsDateTime – Records the date and time when user *Tim's* password was changed by user *administrator*
- WCSFormAuthorizerModify and -1000 both flag this history record as an audit entry

Enable Login
AuditsTypesID [Enable Login (29)] AuditsLocationsID [571] AuditsClientsID [411] AuditsLogin [administrator] AuditsTextBox1 [Tim] AuditsDateTime [20141119093951], WCSFormAuthorizerModify, -1000

Details:
- AuditsTypesID - Indicates the type of audit log being viewed. In this case, this is recording an Enable Login event.
- AuditsLocationsID and AuditsClientsID – These fields can be ignored at this time. The location and client associated with this event will always be the physical location and client at which the Satellite Server application is running. This information is required only if further assistance is requested from WashCard Systems Technical Support.
- AuditsLogin - Indicates the currently logged in user account which is performing the audited action.
- AuditsTextBox1 - Logs the User which is being modified during the audited Enable Login event.
- AuditsDateTime – Records the date and time when user *Tim* was enabled by user *administrator*
- WCSFormAuthorizerModify and -1000 both flag this history record as an audit entry

Disable Login
AuditsTypesID [Disable Login (30)] AuditsLocationsID [571] AuditsClientsID [411] AuditsLogin [administrator] AuditsTextBox1 [Tim] AuditsDateTime [20141119093953], WCSFormAuthorizerModify, -1000

Details:
- AuditsTypesID - Indicates the type of audit log being viewed. In this case, this is recording an Disable Login event.
- AuditsLocationsID and AuditsClientsID – These fields can be ignored at this time. The location and client associated with this event will always be the physical location and client at which the Satellite Server application is running. This information is required only if further assistance is requested from WashCard Systems Technical Support.
- AuditsLogin - Indicates the currently logged in user account which is performing the audited action.
- AuditsTextBox1 - Logs the User which is being modified during the audited Disable Login event.
- AuditsDateTime – Records the date and time when user *Tim* was disabled by user *administrator*
- WCSFormAuthorizerModify and -1000 both flag this history record as an audit entry

Edit Location Credit Card Authorizer
AuditsTypesID [Edit Location CC Authorizer (23)] AuditsLocationsID [571] AuditsClientsID [411] AuditsLogin [administrator] AuditsDateTime [20141119093921], WCSFormAuthorizerModify, -1000

Details:

- AuditsTypesID - Indicates the type of audit log being viewed. In this case, this is recording an Edit Location Credit Card Authorizer event.
- AuditsLocationsID and AuditsClientsID – These fields can be ignored at this time. The location and client associated with this event will always be the physical location and client at which the Satellite Server application is running. This information is required only if further assistance is requested from WashCard Systems Technical Support.
- AuditsLogin - Indicates the currently logged in user account which is performing the audited action.
- AuditsDateTime – Records the date and time when the credit card authorizer was modified
- WCSFormAuthorizerModify and -1000 both flag this history record as an audit entry

Successful Login
AuditsTypesID [Successful Login (21)] AuditsLocationsID [571] AuditsClientsID [411] AuditsLogin [administrator] AuditsDateTime [20141119093951], WCSFormAuthorizerModify, -1000

Details:

- AuditsTypesID - Indicates the type of audit log being viewed. In this case, this is recording a Successful Login event.
- AuditsLocationsID and AuditsClientsID – These fields can be ignored at this time. The location and client associated with this event will always be the physical location and client at which the Satellite Server application is running. This information is required only if further assistance is requested from WashCard Systems Technical Support.
- AuditsLogin - Indicates the user account which is performing the audited login attempt.
- AuditsDateTime – Records the date and time when user *administrator* successfully logged in.
- WCSFormAuthorizerModify and -1000 both flag this history record as an audit entry

Windows Account Management

In order to meet secure authentication requirements for PCI DSS compliance, your Microsoft Windows Admin account , when first installed, uses our default temporary Admin Username and Password.

Default Username:	WashCardAdmin
Default Password:	Admin1!

When a user first logs in, the user will utilize the temporary password and should change the temporary password immediately. Users are advised to change the default user IDs and passwords since they're easily guessed and are, like here, often documented in product manuals.

Additional users can be added and each user must have a unique user ID and password. Do not use group, shared or generic accounts or passwords. Users should never share their passwords. It is highly recommended to disable or delete inactive or terminated user accounts immediately to prevent unauthorized access. Although immediate action is recommended, for PCI compliance this absolutely must be done within 90 days.

The following PCI compliant requirements apply to all user passwords.

- Passwords must be at least seven characters
- Passwords must contain at least one upper case and one lower case letter
- Passwords must be changed at least every 90 days
- Passwords must not be the same as the last four used
- After a user idle time of 15 minutes, the password must be re-entered.

Configuring the Local Security Policy to Ensure Secure Passwords

WashCard Systems ships all Site Management Controllers loaded with Windows 10 Professional 64-bit. System security depends on password strength at the Windows platform level itself as well as the application (See section *Satellite Server User Management*, above). As shipped, Local Security Policies are configured to enforce the following requirements.

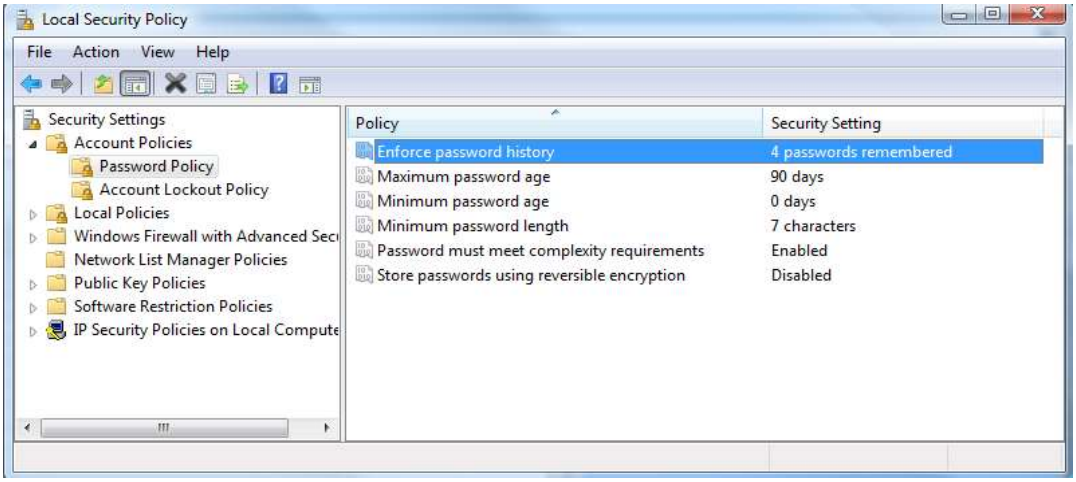
These requirements must remain in place for PCI compliance:

- No reuse of the previous four passwords
- Password changes required every 90 days
- 7 character minimum w/ both numeric and alphabetic characters
- Lockout after six failed login attempts
- Lockout to last at least 30 minutes
- Timeout, and repeat login required after 15 minutes

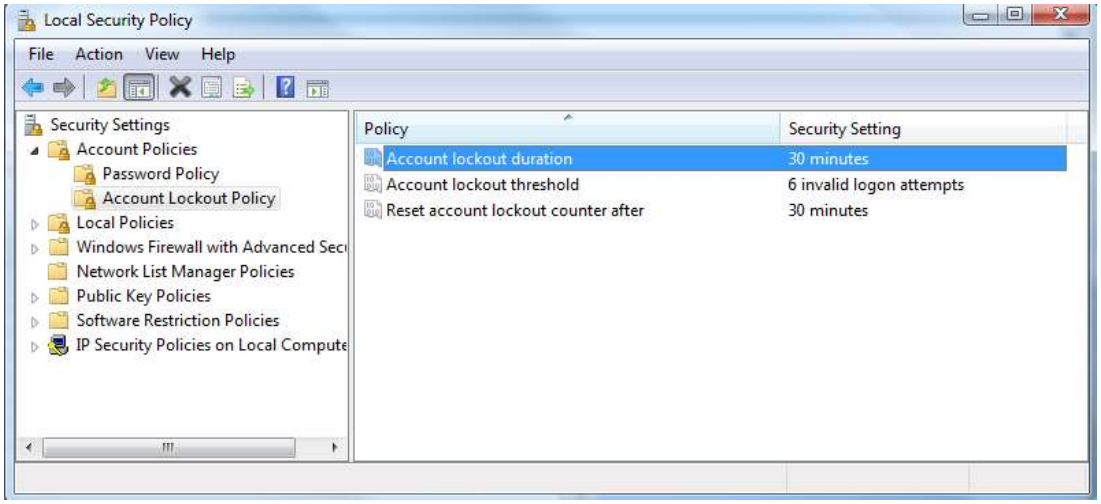
Configuring the Local Security Policy to Ensure Secure Passwords (Continued)

Below are the implementation instructions:

1. Click the SEARCH icon
2. On the search bar, type: "Local Security Policy" and press <ENTER>
3. Expand Account Policies
4. Set **Password Policy** per the following image:



5. Set **Account Lockout Policy** per the following image:

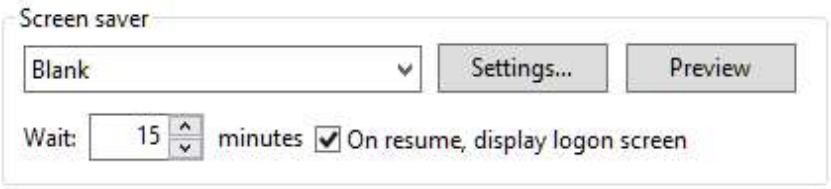


6. Close the Local Security Policy window.

Configuring the Screen Saver to Require Password Re-Entry on Idle

Below are the implementation instructions:

1. Right click the desktop and select *Personalize*
2. Click the *Lock Screen* link on the left side of the window
3. Click *Screen saver settings*
4. Set **Screen Saver** properties per the following image:



5. Click <OK>

Configuring the Local Security Policy for Auditing Compliance

WashCard Systems ships all Site Management Controllers loaded with Windows 10 Professional 64-bit. As shipped, Local Security Policies are configured to audit the following events. These requirements must remain in place for PCI compliance:

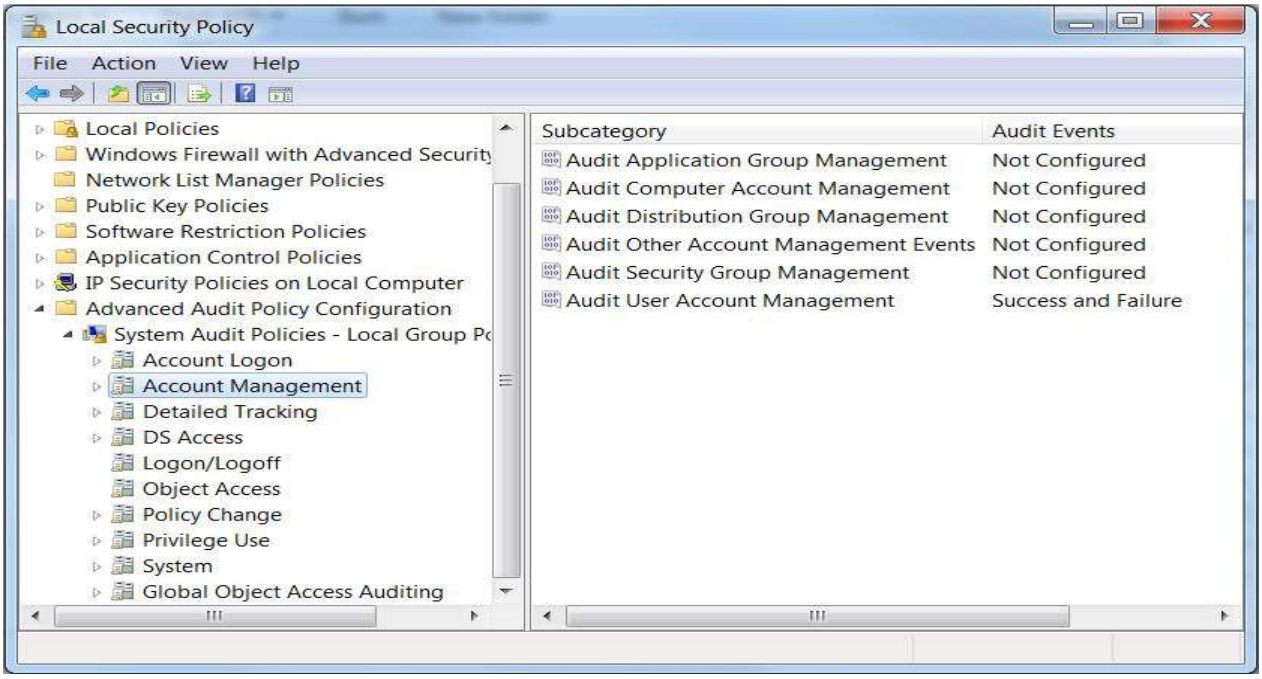
- Actions taken by administrative users
- Access of audit logs
- Successful and failed logon attempts
- Account creation, edit, and removal
- Audit logging being started
- Audit logging being stopped
- System-level object creation and removal

Below are the implementation instructions:

1. Click the START button
2. On the search bar, type: "Local Security Policy" and press <ENTER>
3. Expand Advanced Audit Policy Configuration
4. Expand System Audit Policies – Local Group Policy Object
5. Click Account Management
6. In the right pane of the Local Security Policy window, double-click Audit User Account Management
7. Check the box for Configure the following audit events.
8. Check both Success and Failure
9. Click the Apply button and then click OK

Configuring the Local Security Policy for Auditing Compliance (Continued)

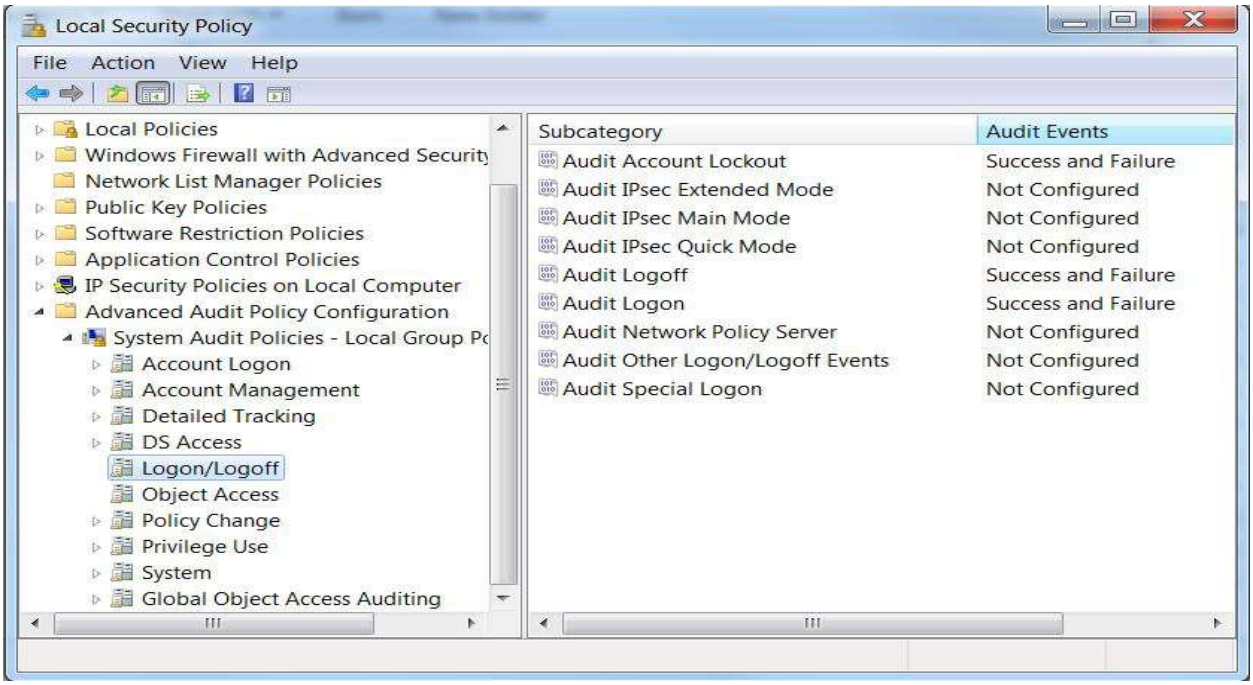
10. The configuration window should now match the following image:



11. In the left pane of the Local Security Policy window, Click Logon/Logoff
12. In the right pane of the Local Security Policy window, double-click Audit Account Lockout
13. Check the box for Configure the following audit events.
14. Check both Success and Failure
15. Click the Apply button and then click OK
16. In the right pane of the Local Security Policy window, double-click Audit Logoff
17. Check the box for Configure the following audit events.
18. Check both Success and Failure
19. Click the Apply button and then click OK
20. In the right pane of the Local Security Policy window, double-click Audit Logon
21. Check the box for Configure the following audit events.
22. Check both Success and Failure
23. Click the Apply button and then click OK

Configuring the Local Security Policy for Auditing Compliance (Continued)

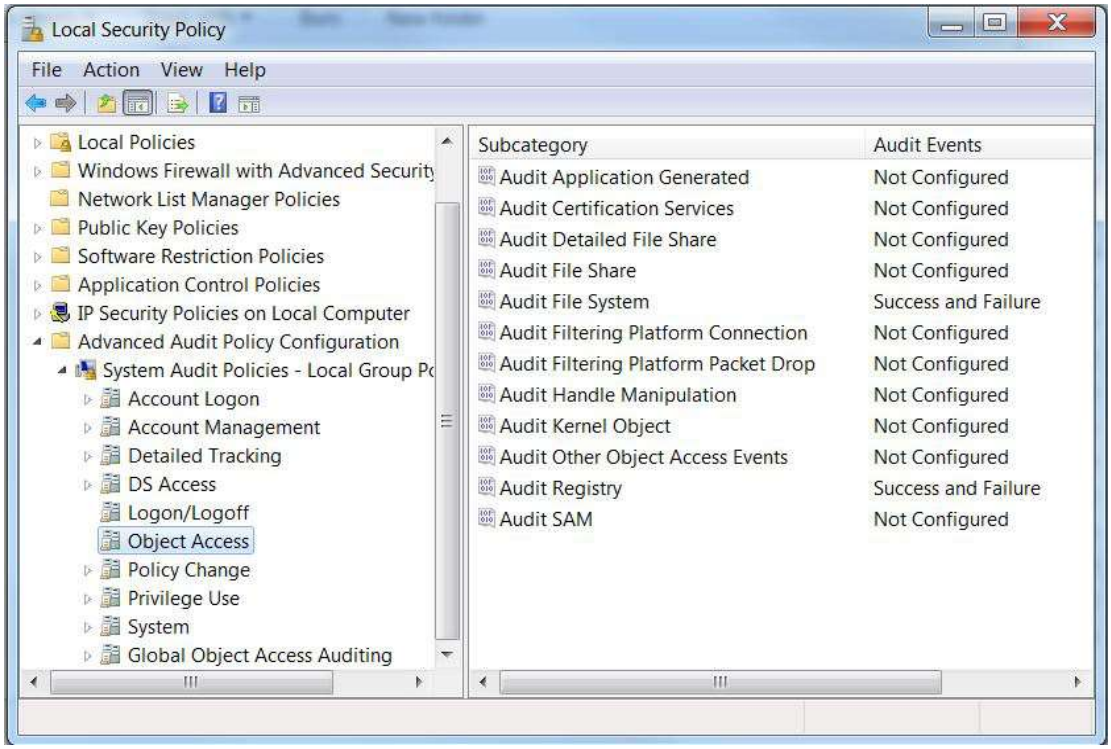
24. The configuration window should now match the following image:



25. In the left pane of the Local Security Policy window, Click Object Access
26. In the right pane of the Local Security Policy window, double-click Audit File System
27. Check the box for Configure the following audit events.
28. Check both Success and Failure
29. Click the Apply button and then click OK
30. In the right pane of the Local Security Policy window, double-click Audit Registry
31. Check the box for Configure the following audit events.
32. Check both Success and Failure
33. Click the Apply button and then click OK

Configuring the Local Security Policy for Auditing Compliance (Continued)

34. The configuration window should now match the following image:



35. Local Security Policy configuration is complete.
36. Close the Local Security Policy window.

Creating System Access Control Lists for Auditing Compliance

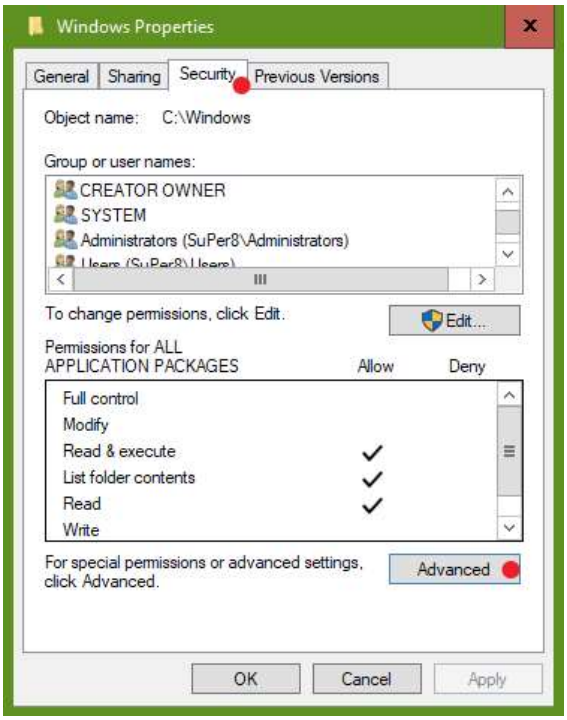
The policy configuration competed above relies on control lists configured on the underlying file system. Three System Access Control Lists (SACLs) are required.

Below are the implementation instructions:

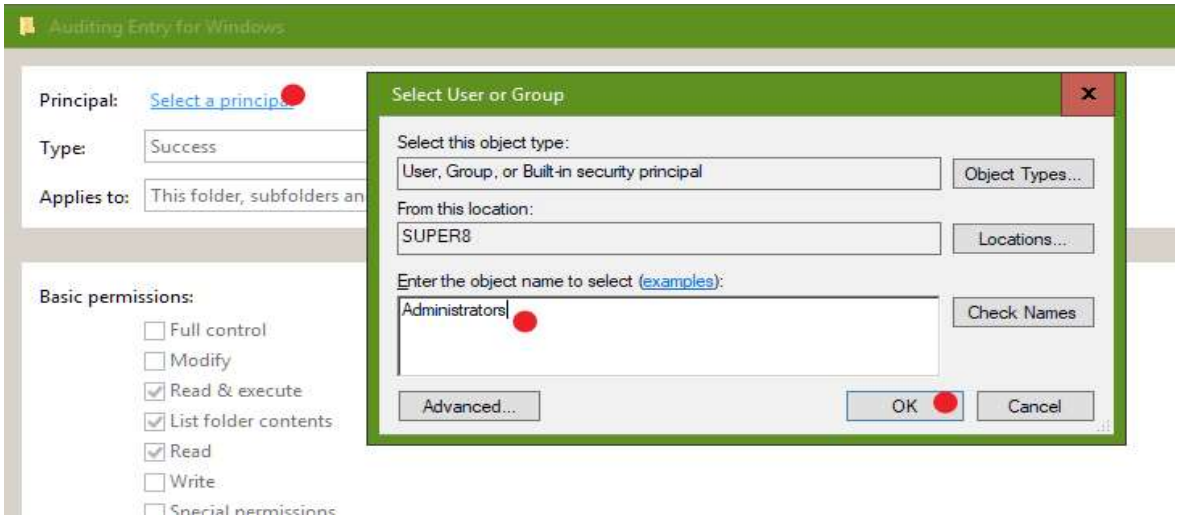
1. Login to Windows as an Administrative user.
2. Click *Start* and select *Windows System*
3. Click *File Explorer*
4. Expand *This PC*
5. Expand *Local Disk (C:)*
6. Right-click the Windows folder and select Properties

Creating System Access Control Lists for Auditing Compliance (Continued)

7. Click the Security tab, then click the Advanced button

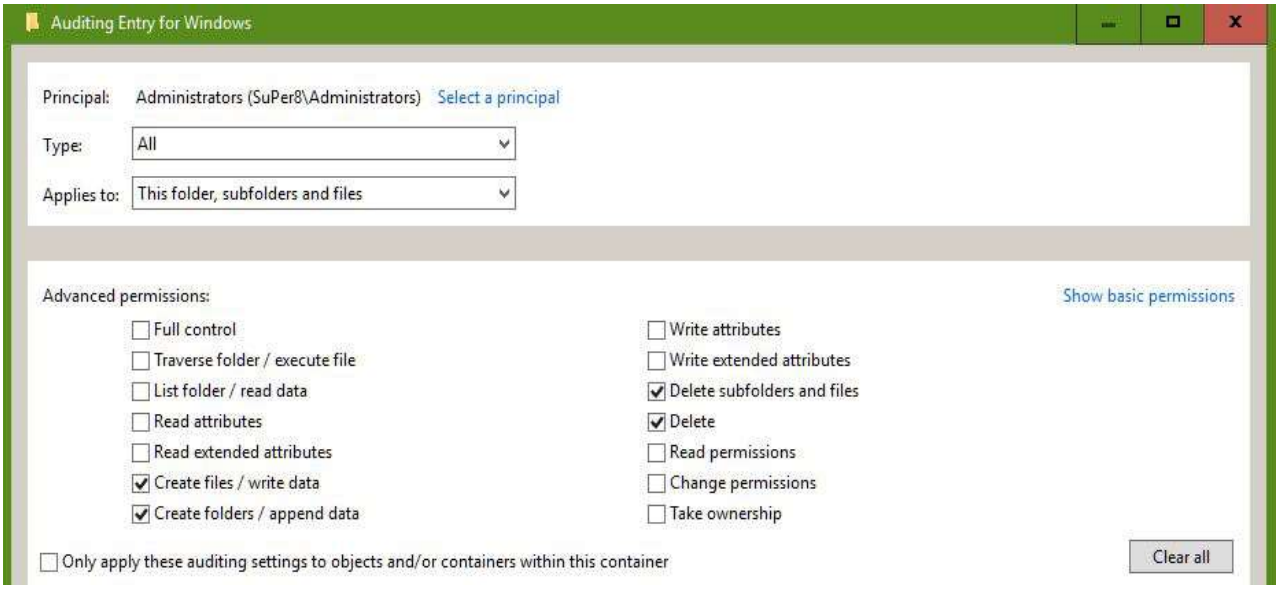


8. Click the Auditing tab on the newly displayed window
9. Click *Continue*
10. Click *Add* on the newly displayed window
11. Click *Select a principal* at the top of the window
12. As pictured below, enter “Administrators” in the object name section and click OK

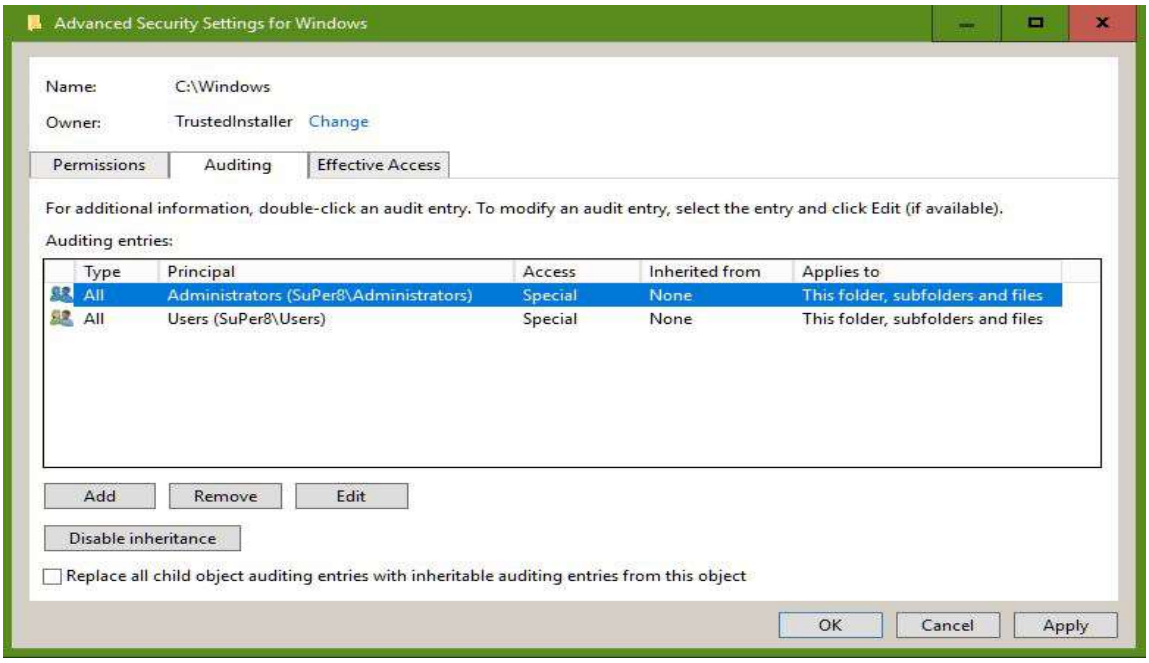


Creating System Access Control Lists for Auditing Compliance (Continued)

13. Set Type to All
14. Click *Show advanced permissions*
15. Select the Create and Delete options as shown in the image below, then click *OK*



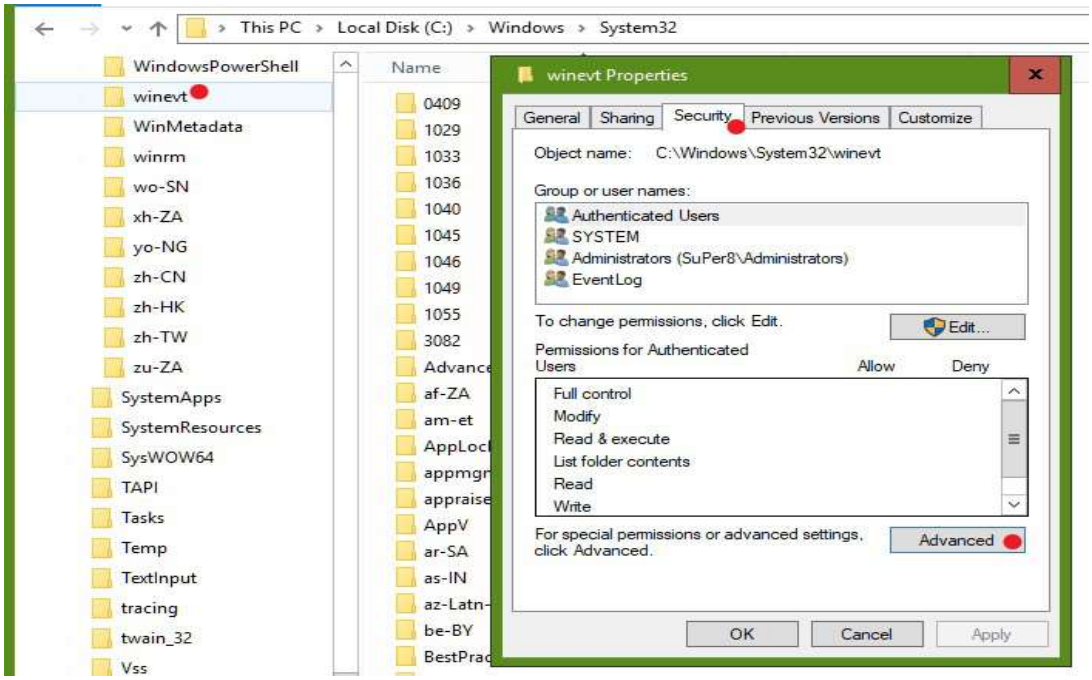
16. Repeat steps 11 – 14 for the Users group account.
17. Your Advanced Security Settings for Windows form should now appear as shown below:



18. Click *OK* (This may process for several minutes)

Creating System Access Control Lists for Auditing Compliance (Continued)

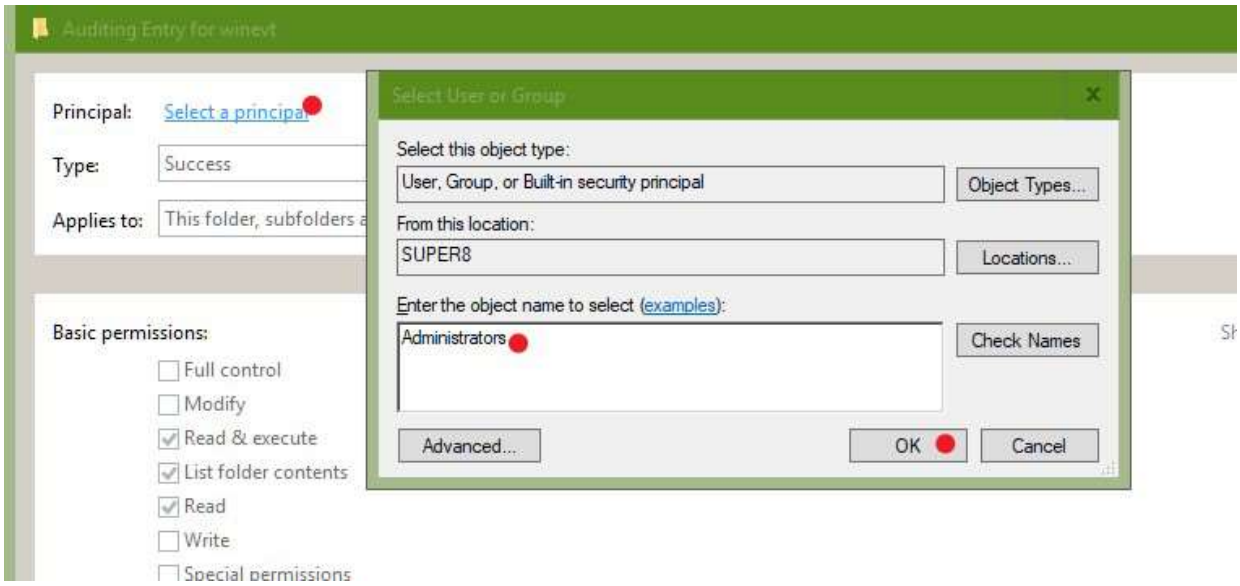
19. Click OK on the Advanced Security Settings for Windows form
20. Click OK on the Windows Properties form
21. In File Explorer, expand This PC, expand Local Disk (C:), expand Windows, expand System32
22. Right-click the winevt folder and select Properties
23. Click the Security tab, then click the Advanced button



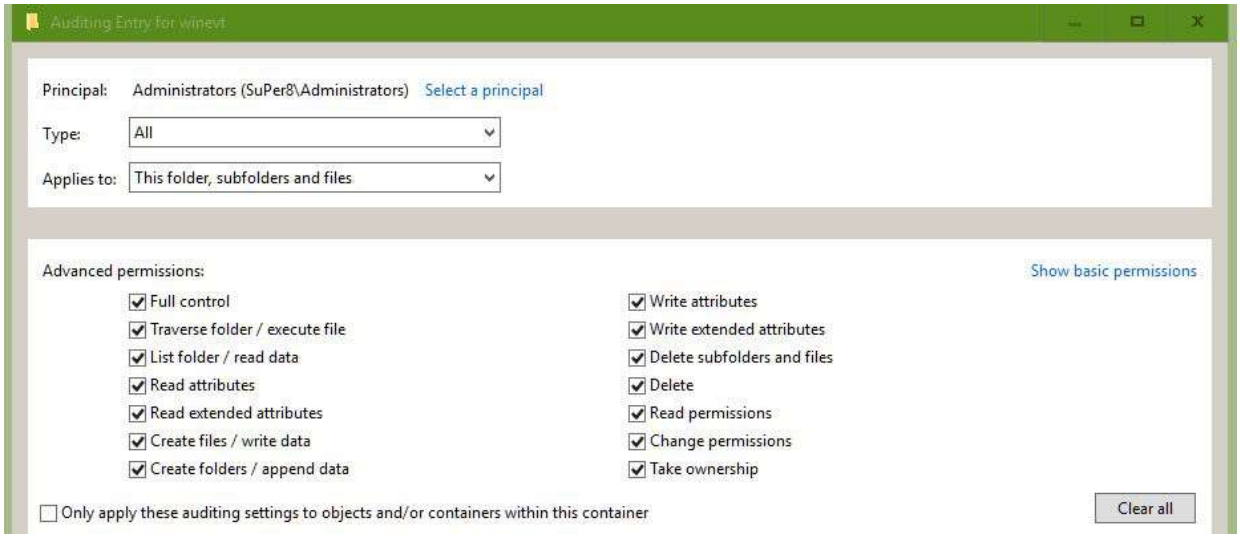
24. Click the *Auditing* tab and click *Continue* if required.
25. There will be two entries inherited from the entries created previously as shown below.

Creating System Access Control Lists for Auditing Compliance (Continued)

26. Click *Add*
27. Click *Select a principal* at the top of the window
28. As pictured below, enter “Administrators” in the object name section and click OK



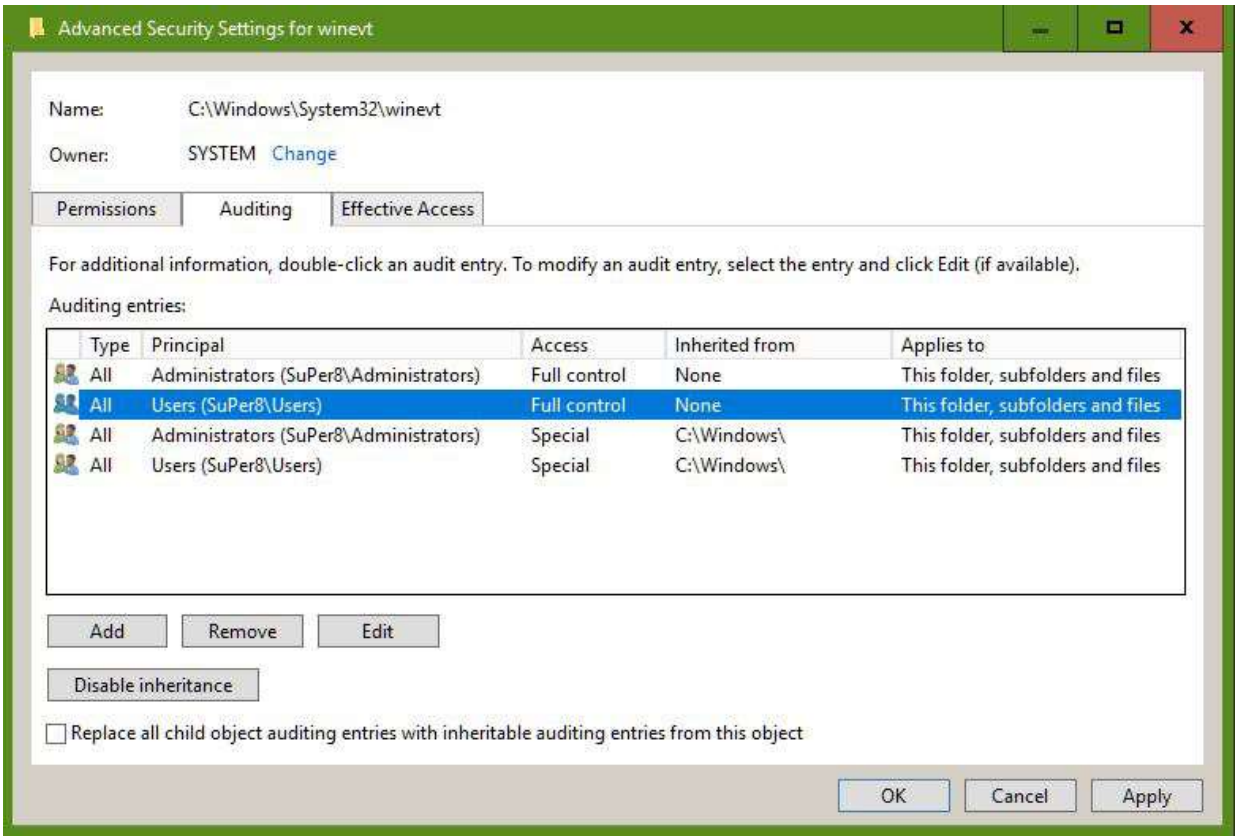
29. Set Type to All
30. Click *Show advanced permissions*
31. Select the *Full control* option as shown in the image below, then click *OK*



32. Repeat steps 26 – 31 for the “Users” group account.

Creating System Access Control Lists for Auditing Compliance (Continued)

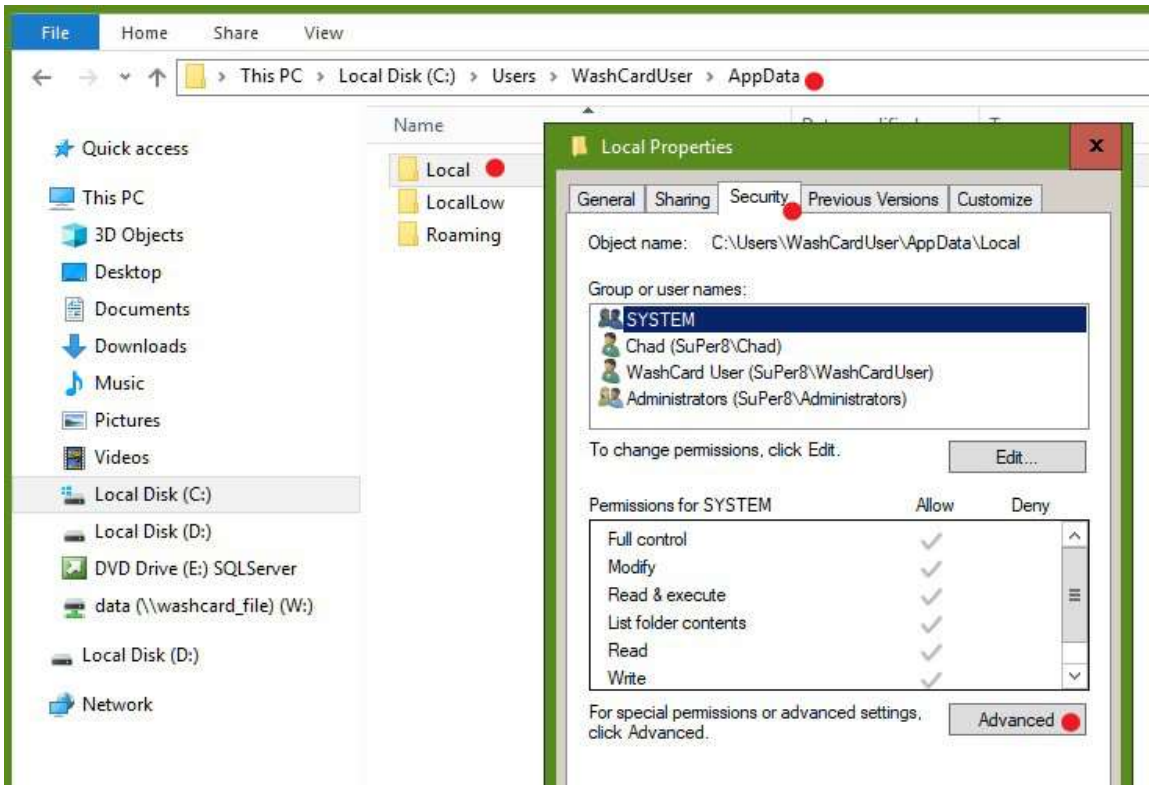
33. Your Advanced Security Settings for winevt form should now appear as shown below:



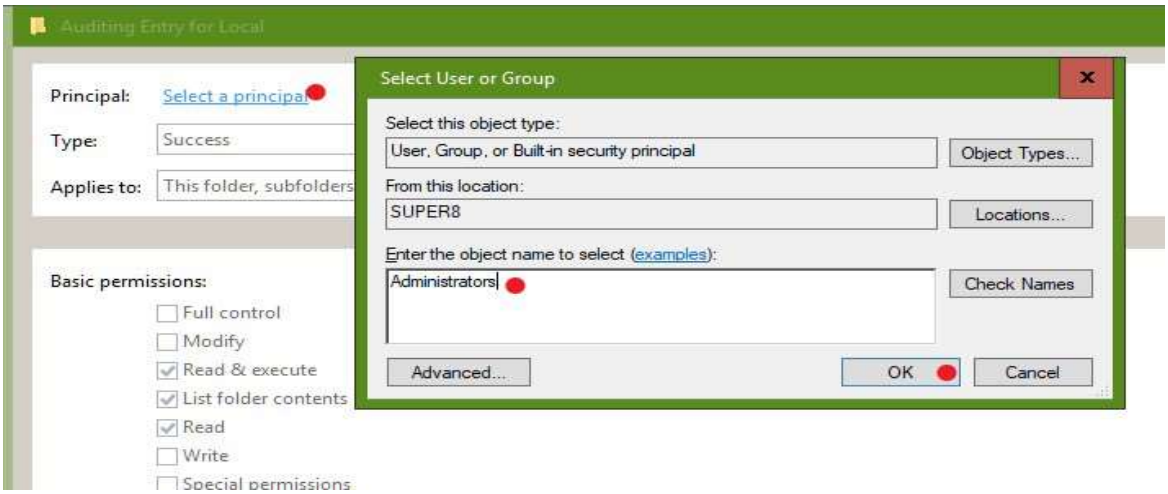
34. Click *OK* on the Advanced Security Settings for winevt form
35. Click *OK* on the winevt Properties form
36. In the File Explorer navigation bar, type: c:\Users\WashCardUser\AppData\
37. Press <ENTER>

Creating System Access Control Lists for Auditing Compliance (Continued)

38. Right-click the *Local* folder and select Properties
39. Click the Security tab, then click the Advanced button

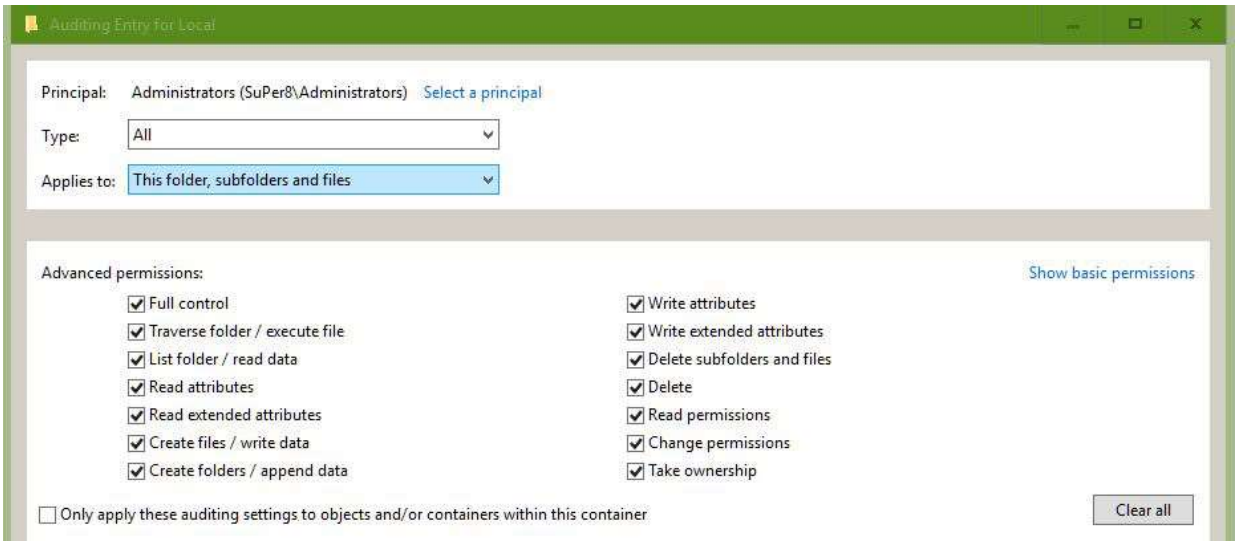


40. Click the *Auditing* tab and click *Continue* if required
41. Click *Add*
42. Click *Select a principal* at the tip of the window
43. As pictured below, enter “Administrators” in the object name section and click *OK*

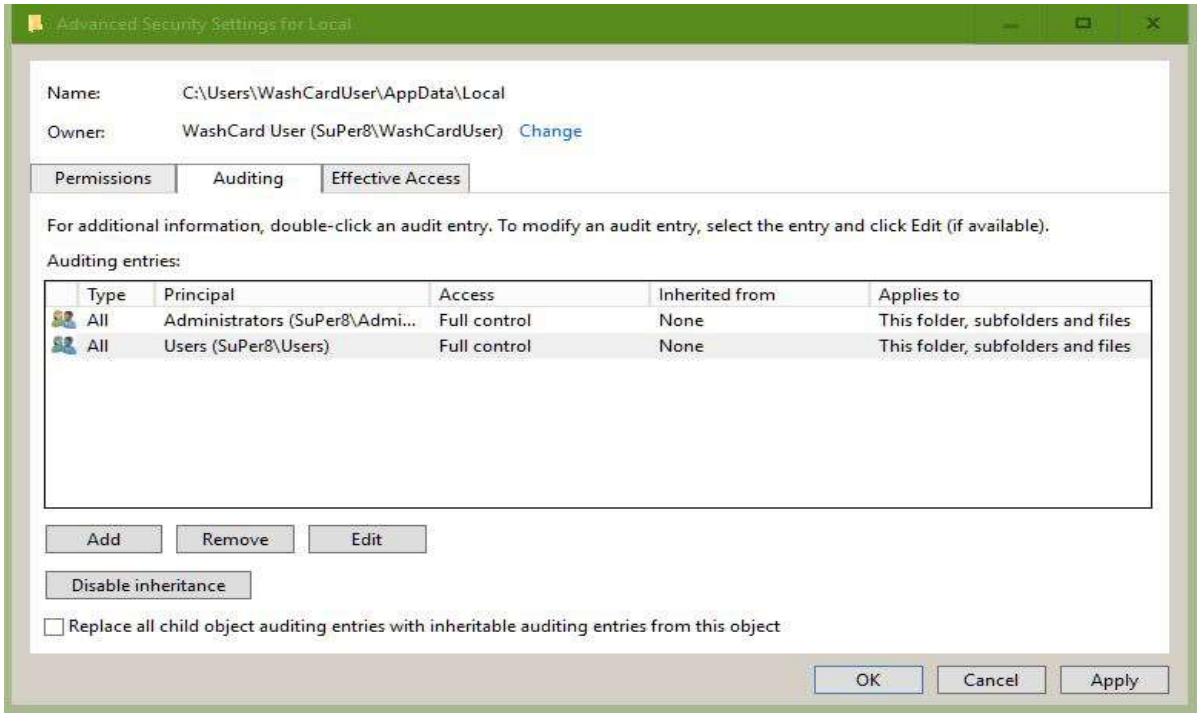


Creating System Access Control Lists for Auditing Compliance (Continued)

44. Set Type to *All*
45. Click Show advanced permissions
46. Select the *Full control* option as shown in the image below, then click *OK*



47. Repeat steps 41 – 46 for the "Users" group account.
48. Your Advanced Security Settings for Local form should now appear as shown below:



Creating System Access Control Lists for Auditing Compliance (Continued)

49. Click *OK* on the Advanced Security Settings for Local form
50. Click *OK* on the Local Properties form
51. System Access Control List configuration is complete. Close File Explorer.

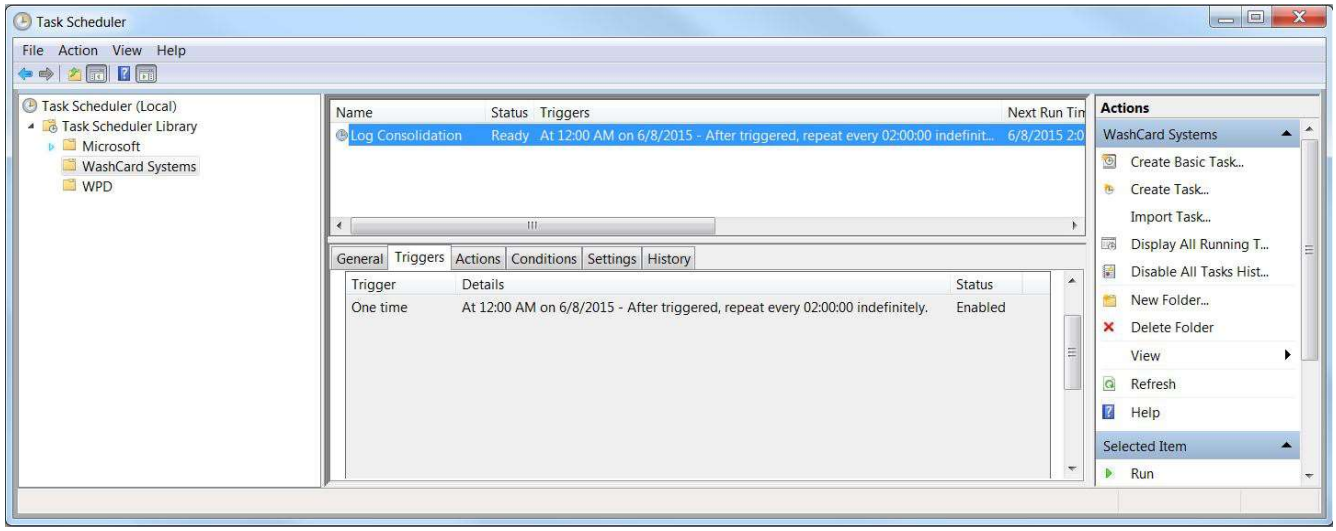
Centralized Logging for PCI-DSS Compliance

As shipped, the Site Management Controller (SMC) is configured to consolidate all applicable audit logs in support of the PCI-DSS Centralized Logging requirement. Windows Audit Logs and Satellite Server Audit Logs are converted to .CSV format and copied to the following folder: c:\SysLogs. This consolidation occurs every 2 hours. For immediate access to audit records, see sections *Auditing User Activity* and *Logging Windows Events* on page 23 and page 60 of this document, respectively.

Consolidated audit logs must be moved or copied from the c:\Syslogs folder on the SMC to your centralized syslog server via secure transfer (for example, SFTP or HTTPS). These centralized logs from the SMC, along with all logs generated by the remainder of your business, must be reviewed daily for suspicious activity in order to maintain PCI-DSS compliance.

Automated log consolidation is accomplished by a powershell script scheduled to run every 2 hours within the Windows Task Scheduler. To access the Windows Task Scheduler and review script related configuration and history, proceed as follows:

- Log in as WashCardAdmin
- Click the Search button
- On the search bar, type: “Task Scheduler” and press <ENTER>
- Expand Task Scheduler Library
- Click WashCard Systems in the left pane of the Task Scheduler window
- A Log Consolidation task should appear as shown in the following image
  - Confirm the Last Run Result and History subtab indicate successful completion of the task



Please contact WashCard Systems Technical Support with any further questions:

888-439-5740 x:200

support@washcard.com

Recovering From a Lost Consolidation Script

1. Confirm the following folder structure exists on the C: drive of the Site Management Controller (SMC), creating any missing folders as necessary.
   - C:\Syslogs\Bin\

2. Copy/Paste or Type the following script into a new Notepad editor window:

```
<#
The ConsolidateLogs script will export and consolidate Event Log data and Satellite Server history log data.

For event logs, the previous two hours worth of events from each of the following will be exported:
        Application, Security, Setup, System

        File Names of the resulting CSV files:
                ApplicationYYYYMMDDHHMMSS.csv
                SecurityYYYYMMDDHHMMSS.csv
                SetupYYYYMMDDHHMMSS.csv
                SystemYYYYMMDDHHMMSS.csv

For Satellite Server, any new audit files available in the application output directory (C:\Temp\WCSDatabase) will be copied.
#>

[string]$strProcessTime = get-date -format yyyyMMddHHmmss
[string]$strPathDir = 'c:\Syslogs\'
[string]$strLogName = ''

# Export Application EventLog Records
try
{
        $strLogName = 'Application'
        Get-WinEvent -ErrorAction SilentlyContinue -FilterHashTable @{LogName=$strLogName;StartTime=(Get-
Date).AddHours(-2)} | Export-Csv -path ($strPathDir + $strLogName + $strProcessTime + '.csv')
}
catch
{
        $error | out-file -filepath c:\syslogs\history\errorlog.txt -append -noclobber
        $error.clear()
}

# Export Security EventLog Records
try
{
        $strLogName = 'Security'
        Get-WinEvent -ErrorAction SilentlyContinue -FilterHashTable @{LogName=$strLogName;StartTime=(Get-
Date).AddHours(-2)} | Export-Csv -path ($strPathDir + $strLogName + $strProcessTime + '.csv')
}
catch
{
        $error | out-file -filepath c:\syslogs\history\errorlog.txt -append -noclobber
        $error.clear()
}
```

Recovering From a Lost Consolidation Script (Continued)

```
# Export Setup EventLog Records
try
{
        $strLogName = 'Setup'
        Get-WinEvent -ErrorAction SilentlyContinue -FilterHashTable @{LogName=$strLogName;StartTime=(Get-
Date).AddHours(-2)} | Export-Csv -path ($strPathDir + $strLogName + $strProcessTime + '.csv')
}
catch
{
        $error | out-file -filepath c:\syslogs\history\errorlog.txt -append -noclobber
        $error.clear()
}

# Export System EventLog Records
try
{
        $strLogName = 'System'
        Get-WinEvent -ErrorAction SilentlyContinue -FilterHashTable @{LogName=$strLogName;StartTime=(Get-
Date).AddHours(-2)} | Export-Csv -path ($strPathDir + $strLogName + $strProcessTime + '.csv')
}
catch
{
        $error | out-file -filepath c:\syslogs\history\errorlog.txt -append -noclobber
        $error.clear()
}

# Copy Satellite Server history logs
try
{
        XCOPY "c:\Temp\WCSDatabase\*.*" "c:\Syslogs\*.*" /D /Y /F >> "c:\syslogs\history\CopyResults.txt" 2>&1
}
catch
{
        $error | out-file -filepath c:\syslogs\history\errorlog.txt -append -noclobber
        $error.clear()
}
```

3. Save this new text file as: C:\Syslogs\Bin\ConsolidateLogs.ps1
4. Confirm a scheduled task is in place to run this script every 2 hours
5. See section *Centralized Logging for PCI-DSS Compliance*, above for details

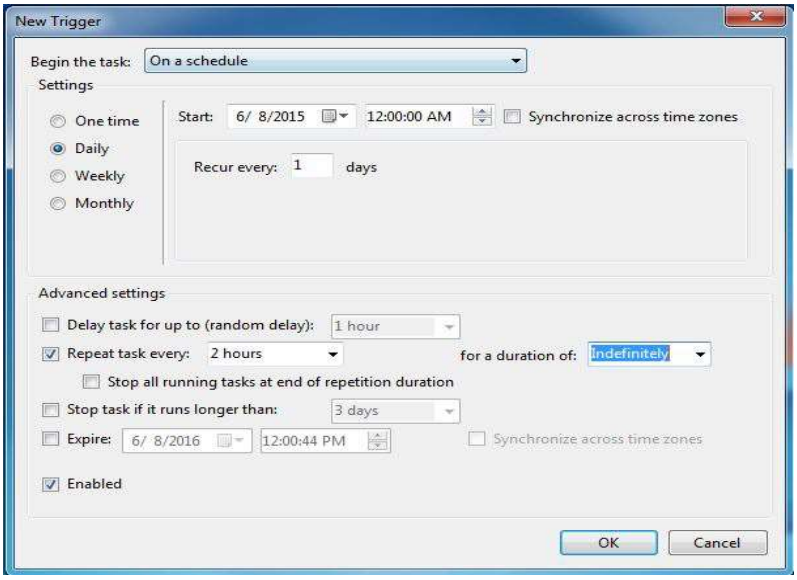
If a scheduled task does not exist, create one utilizing the following steps:

- Log in as WashCardAdmin
- Click the Search button
- On the search bar, type: “Task Scheduler” and press <Enter>
- Expand the Task Scheduler Library folder
- Right-click Task Scheduler Library and select *New Folder*
- For Name, type: “WashCard Systems” and click *OK*
- Right-click the WashCard Systems folder and select *Create Task*

Recovering From a Lost Consolidation Script (Continued)

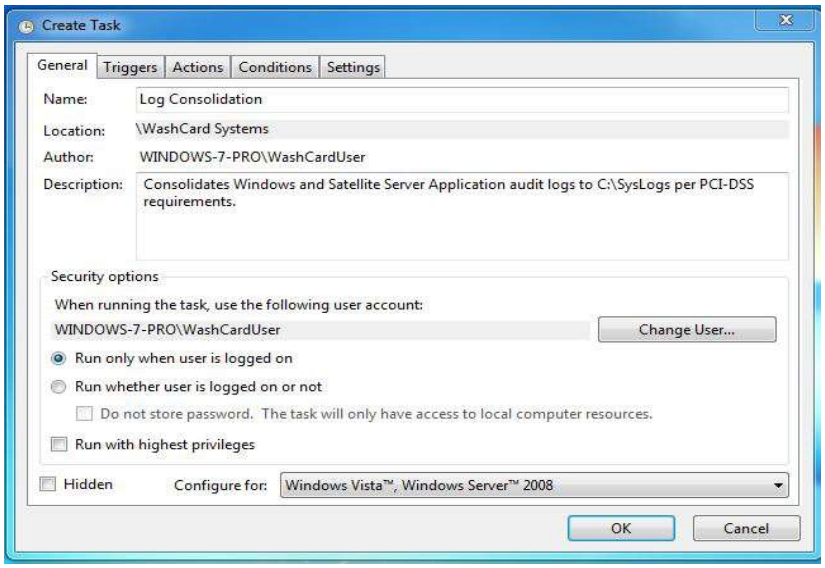
- Match the General tab configuration as shown below:

- Select the *Triggers* tab
- Click *New...*
- Configure the new Trigger as shown in the following image and click *OK*



Recovering From a Lost Consolidation Script (Continued)

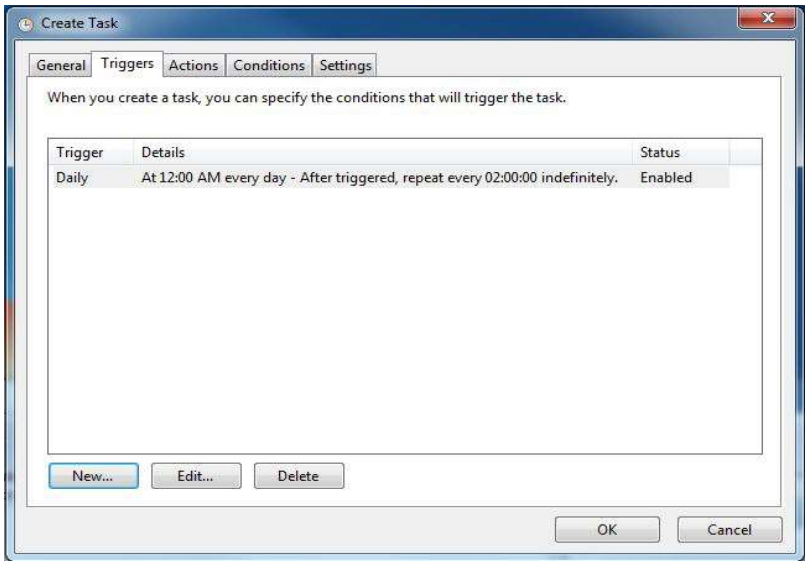
- Confirm the Triggers tab now appears as shown below:



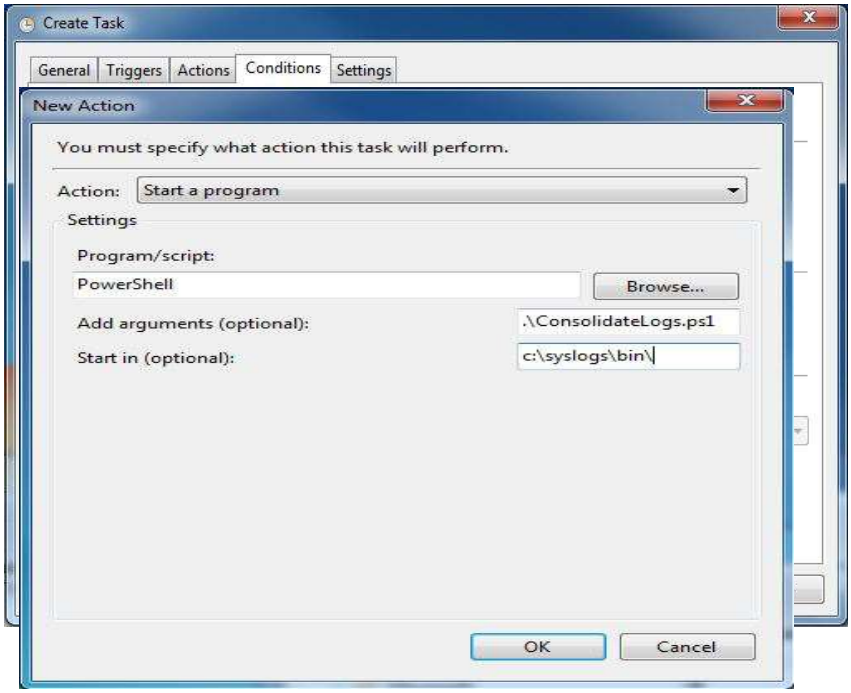
- Select the *Actions* tab
- Click *New...*
- Configure the new Action as shown in the following image and click OK

Recovering From a Lost Consolidation Script (Continued)

- Confirm the Actions tab now appears as shown below:

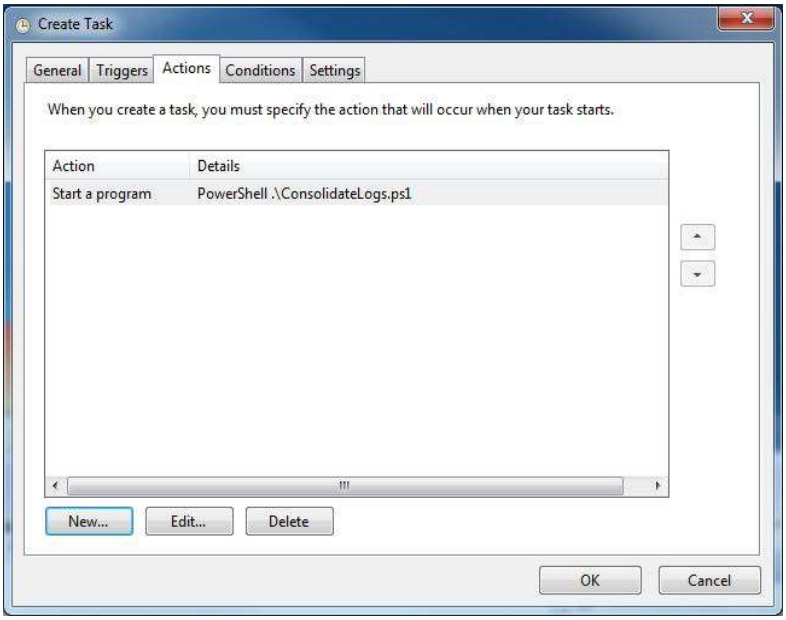


- Select the *Conditions* tab
- Configure the Conditions tab as shown below:

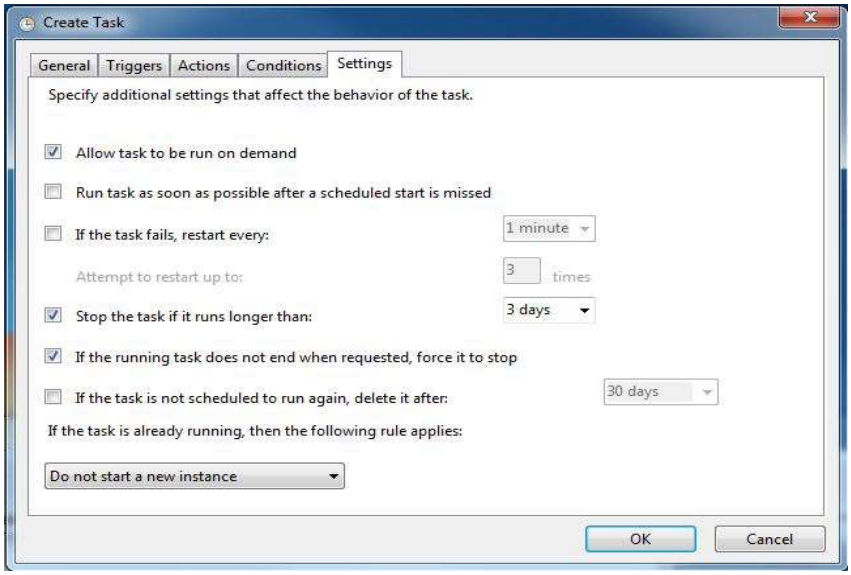


Recovering From a Lost Consolidation Script (Continued)

- Select the *Settings* tab

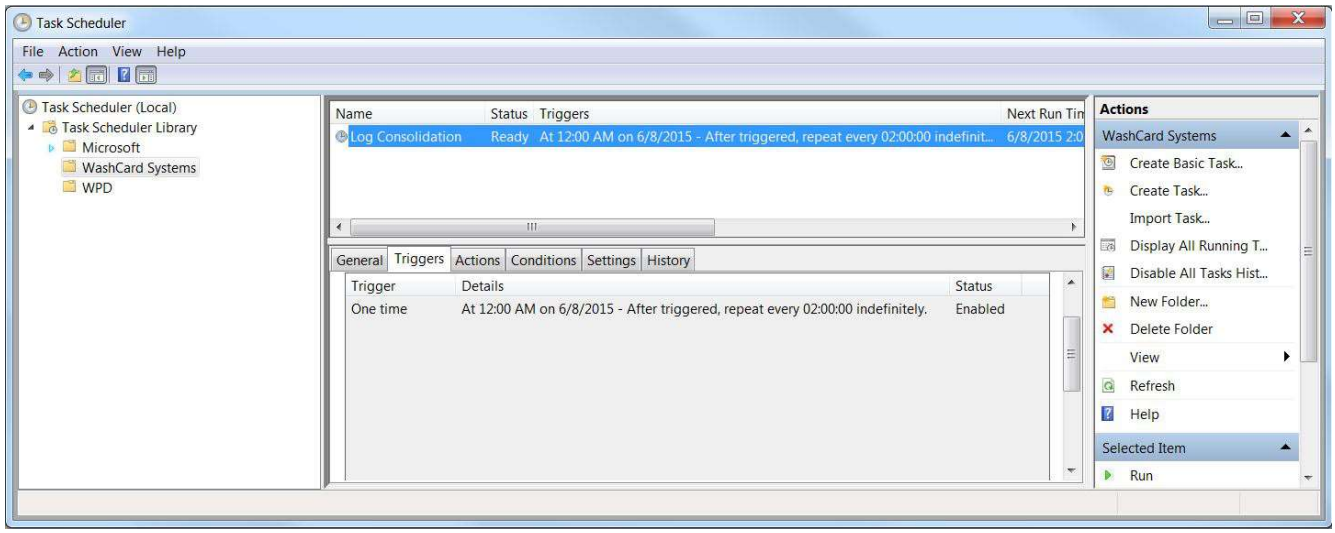


- Configure the Settings tab as shown below:



- Click *OK* to save the new task
- Enter the password for WashCardUser, if prompted

- The Task Scheduler should now appear as shown below:



- Log Consolidation configuration is complete. Close Task Scheduler.

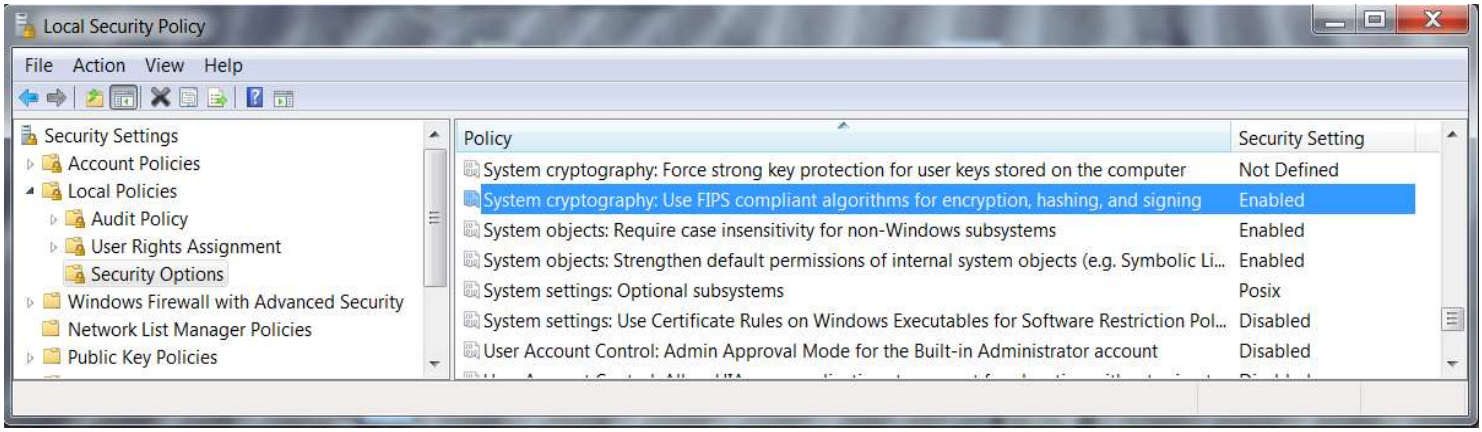
Please contact WashCard Systems Technical Support with any questions regarding these requirements:
888-439-5740 x:200
Support@washcard.com

Require TLS 1.2 Usage for HTTPS Communication

WashCard Systems ships all Site Management Controllers loaded with Windows 10 Professional 64-bit. As shipped, the Local Security Policy is configured to require TLS 1.2 or greater for HTTPS communication. This policy restriction must remain in effect in order to maintain PCI-DSS compliance.

Shown below is the correct setting as well as the process to verify or set the Local Security Policy to the required state:

1. Click the Search button
2. On the search bar, type: "Local Security Policy" and press <ENTER>
3. Expand Local Policies
4. Left click Security Options to highlight this policy type
5. In the right pane, find Use FIPS compliant algorithms for encryption, hashing, and signing
6. Double left click this Policy
7. Select ENABLED, click Apply, click OK.
8. Your Local Security Policy window should now match the following image.



9. Close the Local Security Policy interface

Disabling the SERVER Service

WashCard Systems ships all Site Management Controllers loaded with Windows 10 Professional 64-bit. As shipped, the SERVER service is stopped. The SERVER service must remain stopped according to PA-DSS requirements.

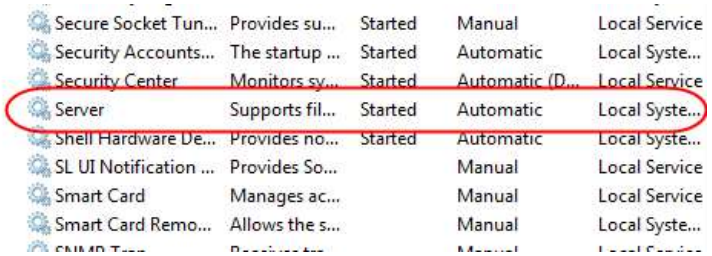
If this service is started manually for any reason, your system will not be PCI compliant.

Shown below is the correct setting as well as the process to verify or set the service to a stopped state.

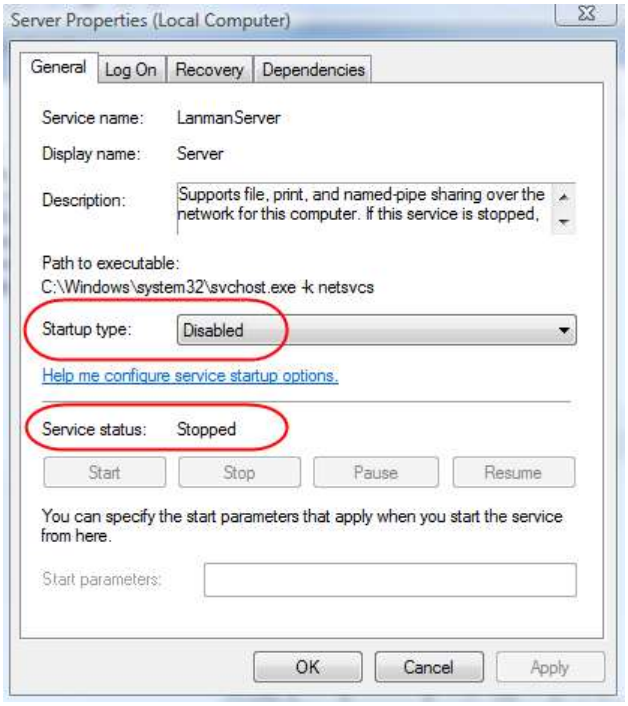
1. Click the *Start* Button and select *Windows System*
2. Click *Control Panel*
3. Click *System and Security*
4. Click *Administrative Tools*
5. Double-click *Services*

Disabling the SERVER Service (Continued)

6. Scroll down through the list of services until the service named SERVER is located



7. Double –click the SERVER service
8. Change the Startup type to “Disabled”
9. Click the STOP button, if necessary, to place the service in a stopped state
10. If prompted with a warning that other services will be stopped, click the YES button to stop these services as well
11. The properties for the service should now show as follows:



12. Click the OK button
13. Close the Services window, then close the Windows Control Panel.

Configuring the Default LogMeIn Remote Access Behavior - "Reject Request":

In order to abide by PCI Compliance standards, LogMeIn remote access must be user initiated. In other words, someone must be on site to allow remote access to the Site Management Controller running the WashCard Systems Satellite Server application. Following are instructions to set LogMeIn remote access preferences in a compliant manner:

1. Click the Windows START button.
2. Click the LogMeIn Control Panel icon
3. Click OPTIONS on the left side of the program window
4. Click the PREFERENCES button under the heading "Preferences and Security"
5. Scroll down to the Host Side User's Consent section

Set the following two options:

6. Check "Request Consent from Host Side User"
7. Check "Reject Request" for the option: If User Does Not Respond
8. Click OK
9. Close the LogMeIn program window

NOTE: These preferences are requirements of the PA-DSS PCI Compliance Standard. Changing the above detailed preferences will render your location NON-COMPLIANT. Please contact WashCard Systems Technical Support with any questions regarding these requirements:
888-439-5740 x:200
Support@washcard.com

Logging Transaction History

Satellite Server transaction history is enabled upon startup and cannot be disabled. Transaction history does **NOT** store any sensitive card data or full 16 digit PAN. It logs the following information, in read only format, for every credit or debit transaction:

- Date and time
- Type of transaction
- Location of transaction
- Last 4 digits of card number
- Card holder's name
- Success or failure indication
- Value of transaction

Satellite Server also creates debug files. These files contain no sensitive card data of any sort. These files are generated in order to perform problem determination on device communication and system failures. Communication exceptions with the connected devices, non sensitive client/server communication and application exceptions are logged to these debug files. The location of the Satellite Server debug directory is: "C:\TEMP\WCSDATABASE". Log files are non configurable and created using the following naming convention: wcnet_History20100218020021.csv Log files only contain the most current 365 days of history and files are automatically removed on a first in first out basis. Log files show event date and time. Again, **no** sensitive data, including any card holder data or card numbers, are stored in any of these debug files.

If you would like to remove files, you should securely delete any sensitive data using a secure removal tool such as Heidi Eraser using the procedure described above in the sections *Securely Deleting Sensitive Card Data* and *Addressing Inadvertent Capture of PAN – Windows 10*.

For PA-DSS compliance, log files have access controls applied so that they can not be modified and are set up as "READ ONLY" files. Log files are also backed up to the Business Management Center during regularly occurring synchronization.

Accessing Transaction History Locally on the Site Management Controller

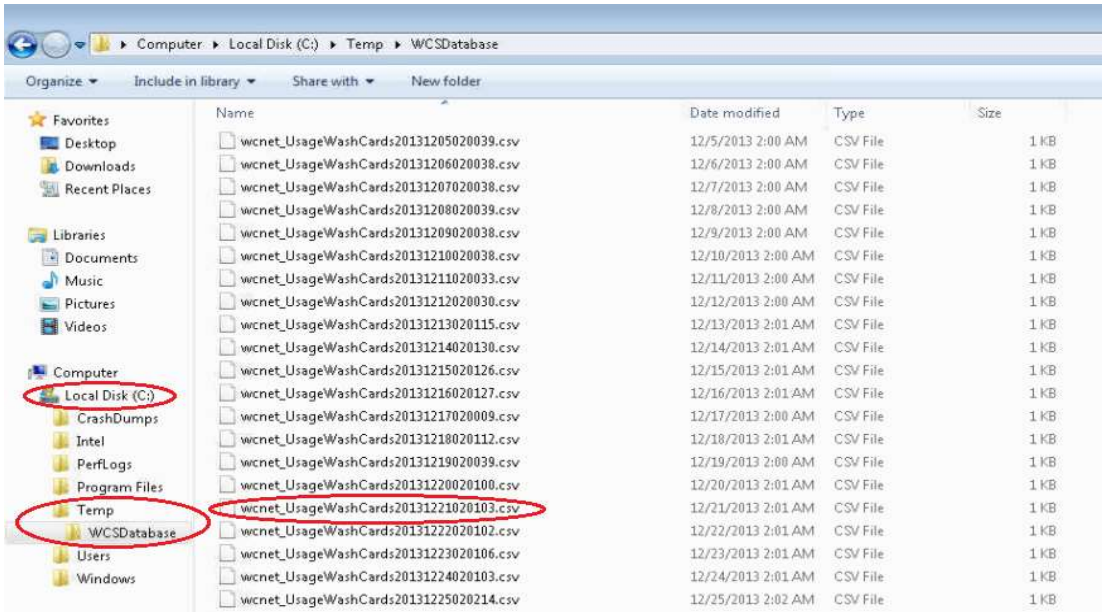
Transaction data is synchronized from each local SMC to the WashCard Systems centralized server throughout the day, on a regularly scheduled basis (default = every 60 minutes). This usage data is stored for reporting on our central server, backed up regularly to local drives and additionally backed up to secondary drives in a separate availability zone in case of critical hardware failure or site wide emergency.

However, usage history is also available locally should the Business Management Center become unavailable for any reason. In order to access local usage history backup data, proceed through the following steps:

- Log in to Windows as the Administrative User
- Click the Windows *START* button
- Select *Windows System*
- Click *File Explorer*
- In the left pane of the File Explorer application
  - Expand *This PC*
  - Expand *Local Disk (C:)*
  - Expand *Temp*
  - Left Click *WCSDatabase*

Accessing Transaction History Locally on the Site Management Controller (Continued)

- Folder contents similar to the following should now be visible:



- In the example image above, loyalty card usage files are shown. Scrolling through the C:\Temp\WCSDatabase directory content will show all historic usage data across payment methods. Locally stored historic usage data files will follow a naming convention of:
    - WashCard Filename Header: wcnet_
    - Content Data Type: UsageWashCards
    - Date the Content Data was stored to this file: 20131210 (December 10, 2013)
    - Time the Content Data was stored to this file: 20103 (2:01:03 AM)

Note: The history data stored is transaction information from the preceding day. Usage history from 12/09/2013 is stored in the above example file, which was created in the early morning hours of 12/10/2013. **NO** sensitive card data is stored in any backup file generated by WashCard Systems.

Please contact WashCard Systems technical support with any questions or concerns regarding these backup files or content.

888-439-5740 x:200
Support@washcard.com

Logging Windows Events

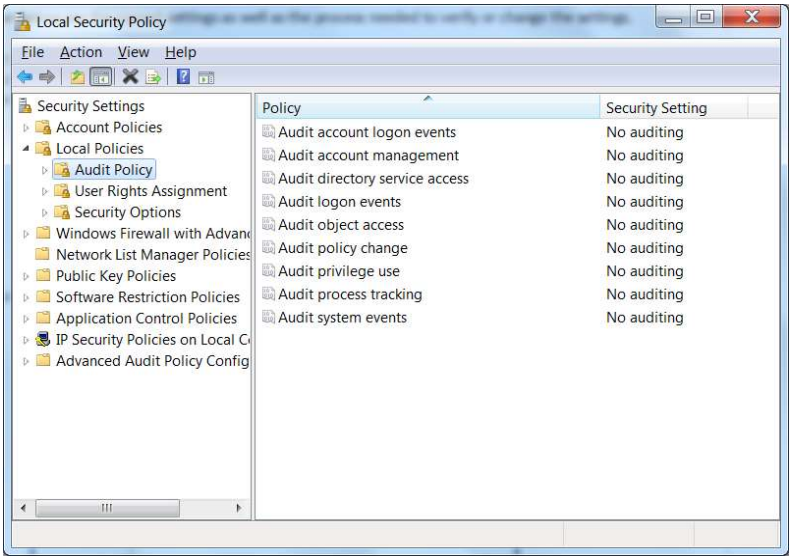
WashCard Systems ships all Site Management Controllers loaded with Windows 10 Professional 64-bit. As shipped, Windows Logging has been enabled and configured according to PA-DSS requirements. These logs provide a complete audit trail of user access to the system in the event of a security breach.

CRITICAL NOTE: If you disable or alter the logging configuration in any way, your system will **NOT** be PCI compliant.

Shown below are the correct settings as well as the process needed to verify or change the settings.

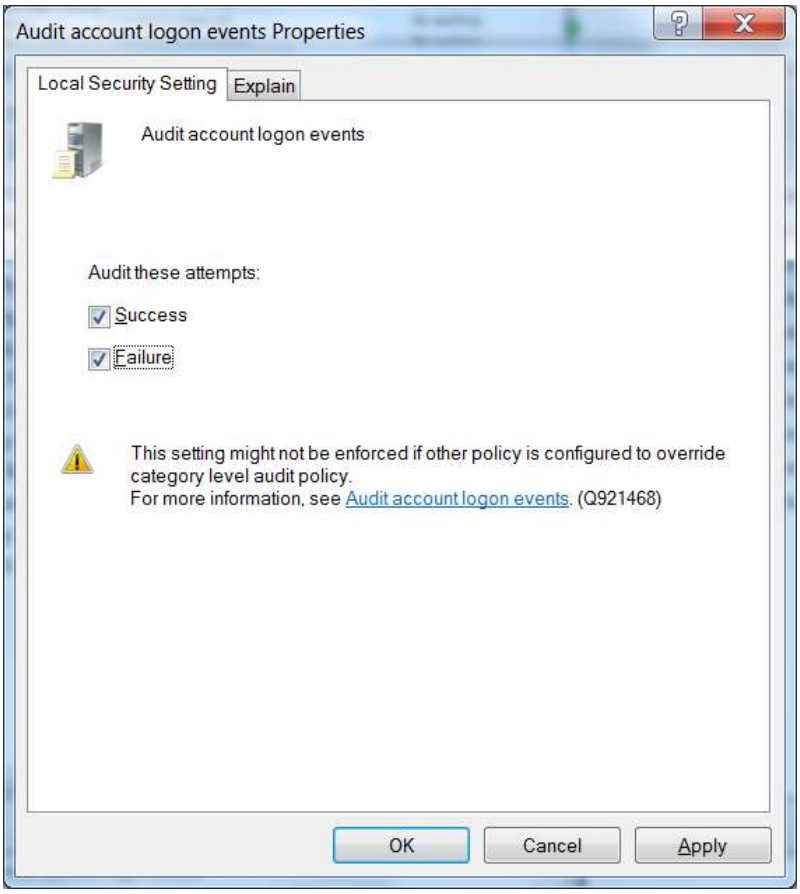
- Log in to Windows as the Administrative User
- Click the *Search* button
- In the search bar, type "secpol.msc /s" and press <ENTER>

- Go to Local Policies - > Audit Policy, and double click on "Audit Account Logon Events".



Logging Windows Events (Continued)

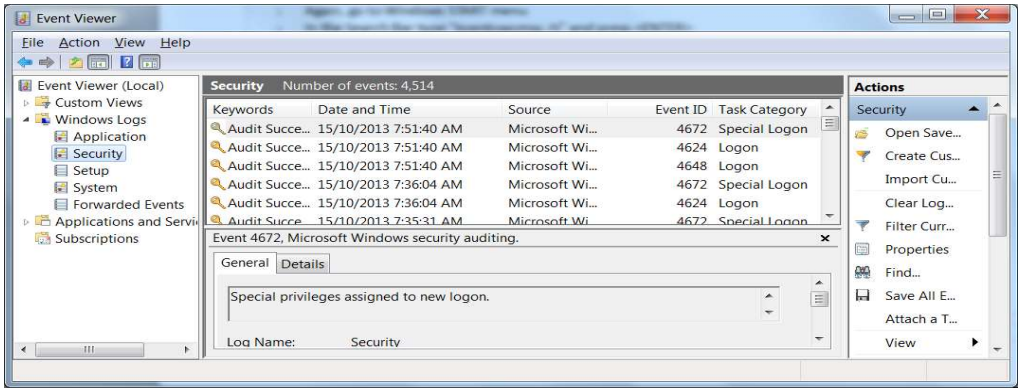
- Make sure “Success and Failure” are both checked. Click “OK” when done.



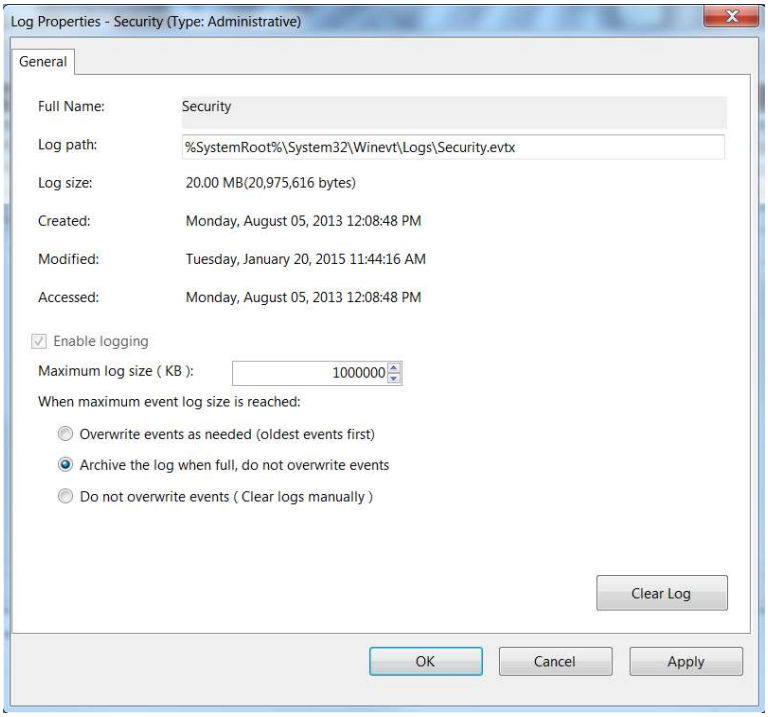
- Make sure that the Security Settings are set to Success /Failure for the following Policies: Audit Account Logon Events, Audit Account Management, Audit Logon Events, Audit Object Access, Audit Policy Change, and Audit System Events.
- Close the Local Security Policy window
- Click the *Search* button
- In the Search Bar, type “Event Viewer” and press <ENTER>

Logging Windows Events (Continued)

- Double-click Windows Logs



- Right click on “Security” and left click on “Properties”.
- Change the maximum log size to 1000000. Then select “Archive the log when full, do not overwrite events”
- Click OK when done.

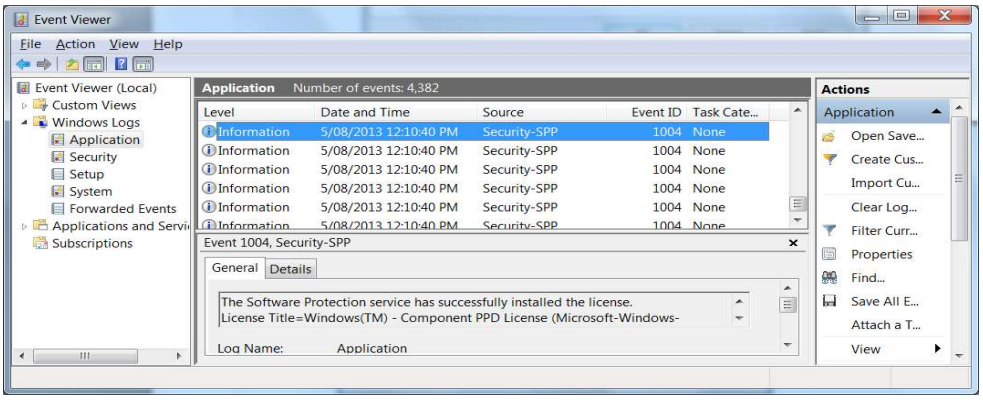


- Close the Event Viewer window.

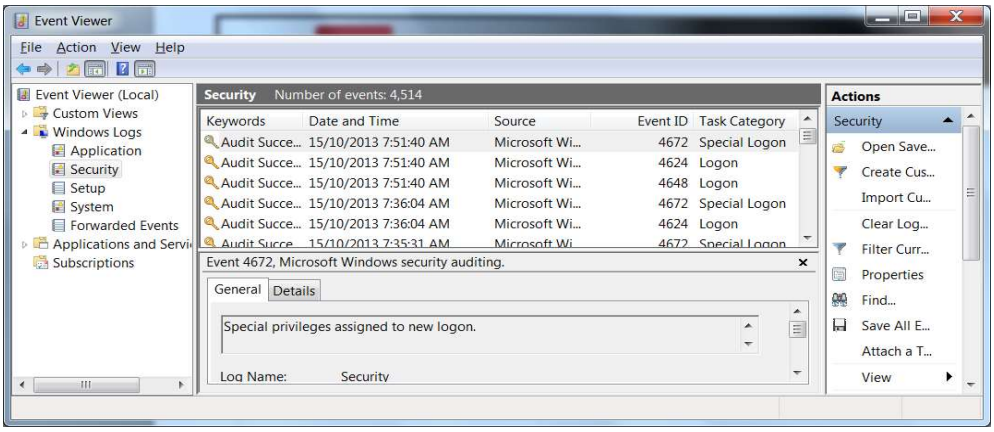
Logging Windows Events (Continued)

Events and audits for System, Applications, and Security are logged and can be viewed using the Event Viewer located under Control Panel - > System and Security - > Administrative Tools - > Event Viewer.

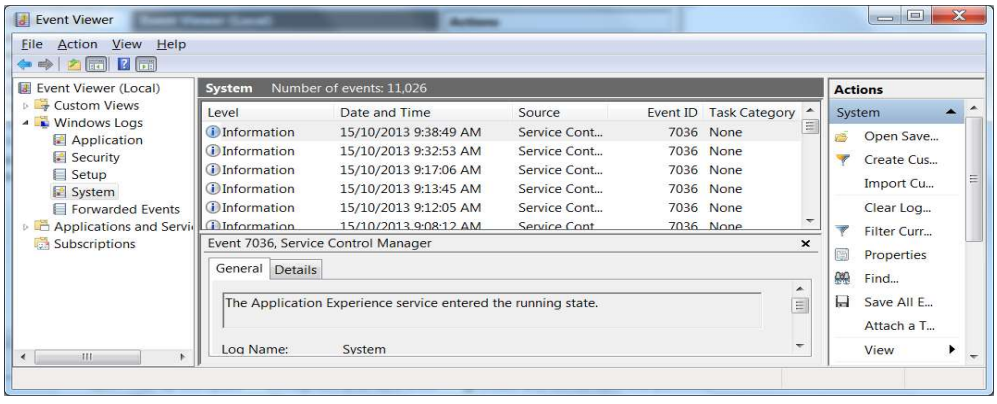
Application log file example:



Security log file example:



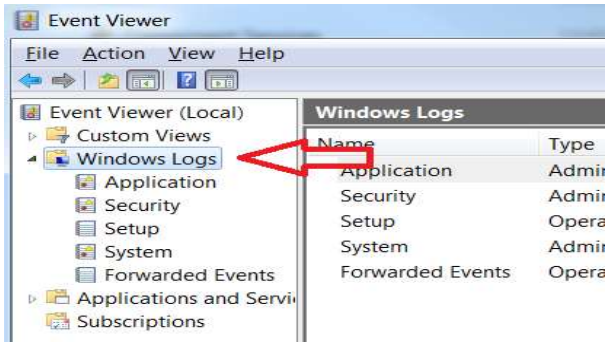
System log file example:



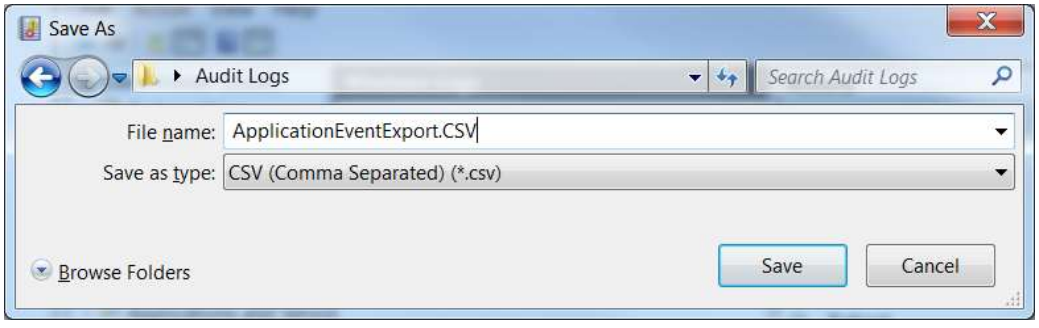
Exporting Windows Audit Logs

The audit trail configured in the previous section can be exported to a Comma Separated Variable (CSV) format for import into a centralized log environment if required. The following steps detail the export of log data consolidated in the Windows Event Viewer. Contact the WashCard Systems technical support department if there are any questions regarding this process.

- Log into Windows as the Administrative User
- Click the Windows *Search* button
- In the search bar, type "Event Viewer" and press <Enter>
- Expand Windows Logs on the left hand side of the Event Viewer program window



- Right-click on the log type required for the export (Application, Security, System, etc)
- Select the "*Save All Events As...*" option from the resulting pop up menu
- Select CSV (Comma Separated) as the Save as type:
- Browse to the desired path (in this example, a folder named Audit Logs)
- Name the export file as required by the central logging interface, and click SAVE



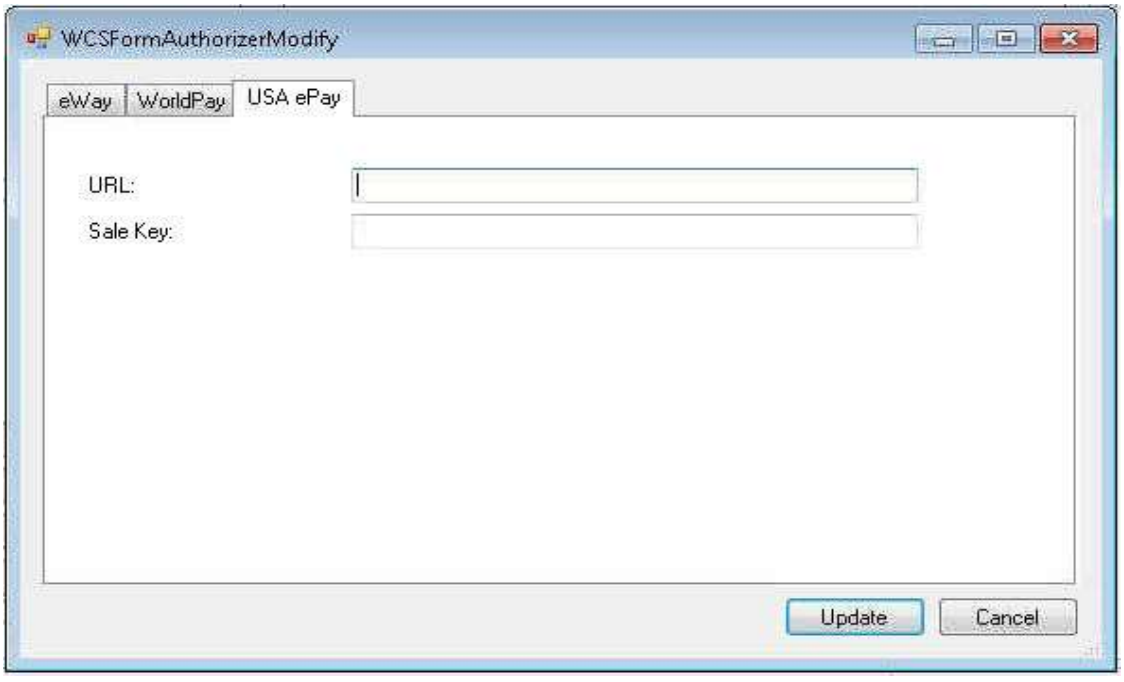
Credit Card Processor Configuration and Management

On initial installation of your Site Management Controller (and each time you change your credit card processor), your credit card processor configuration will need to be updated in the Satellite Server program. When a credit card is swiped at one of the devices on location, the Satellite Server program uses this credit card processor information to contact your gateway and authorize the credit card for the amount of preauthorization or sale. WashCard Systems and Satellite Server supports two processing gateways in the Unites States and Canada: Vantiv (WorldPay) and USA ePay. WashCard Systems and Satellite Server supports one processing gateway in Australia: eWay.

When configuration changes or new accounts are made at any of the above referenced processing gateways, setup sheets will be provided to the business owner. Each processing gateway requires different information for successful transaction processing. However, these setup sheets will contain all required information to configure Satellite Server to communicate and authorize credit cards with the processing gateway in question. Whenever your credit card processor changes, utilize the following steps to reconfigure Satellite Server with the updated information provided in these setup sheets:

- From Satellite Server menu bar, click *View*
- Click *Config and Login* in the resulting drop down list
- Enter your user credentials (as configured in above section *Satellite Server User Management*)
- Click <OK>
- The following form will appear:

NOTE: The pictured screen shots here show a sample, non-functional USA ePay configuration. If you have any questions or concerns regarding the configuration process for this or any of the processing gateways, please contact WashCard Systems Technical Support for assistance:
888-439-5740 x: 200
support@washcard.com

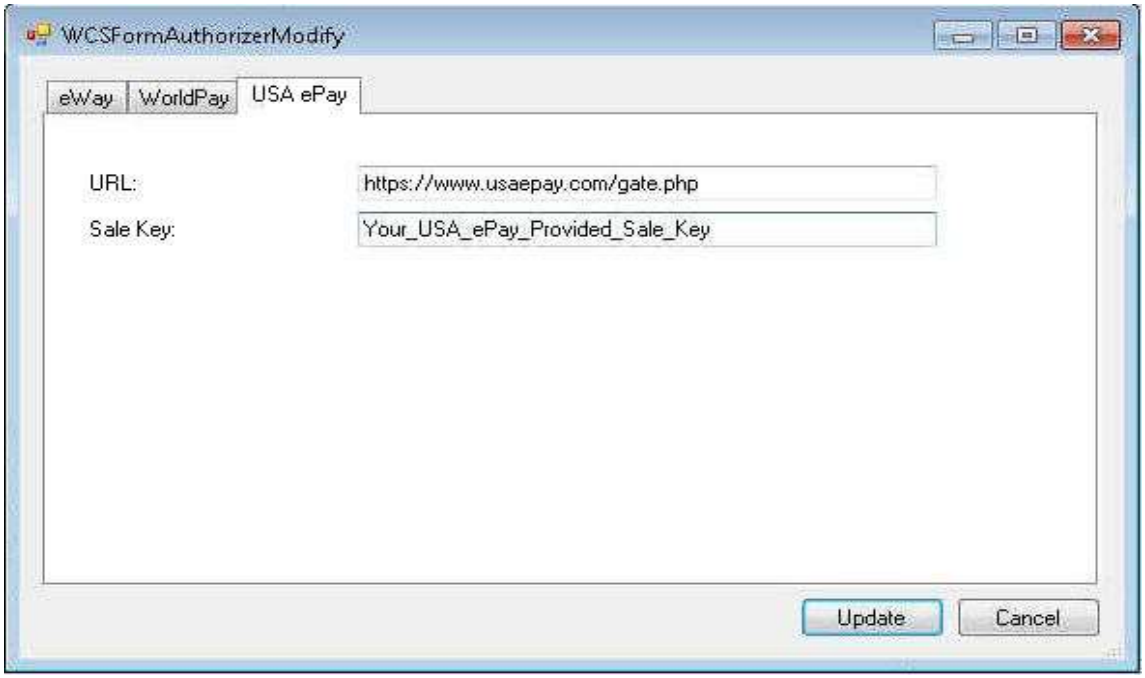


Credit Card Processor Configuration and Management (Continued)

NOTE: Of key importance is the fact that the processing gateway you are configuring as *ACTIVE* is the gateway tab which is *ACTIVELY SELECTED*. In other words, the processing gateway tab selected is the processing gateway you are activating within Satellite Server through this configuration interface. In the following steps and images, USA ePay is shown as the active tab. Therefore, when the update button is clicked, USA ePay will be the processor utilized by Satellite Server.

Now that the main processing gateway configuration form is open, the steps required to configure Satellite Server credit card processing functionality are as follows:

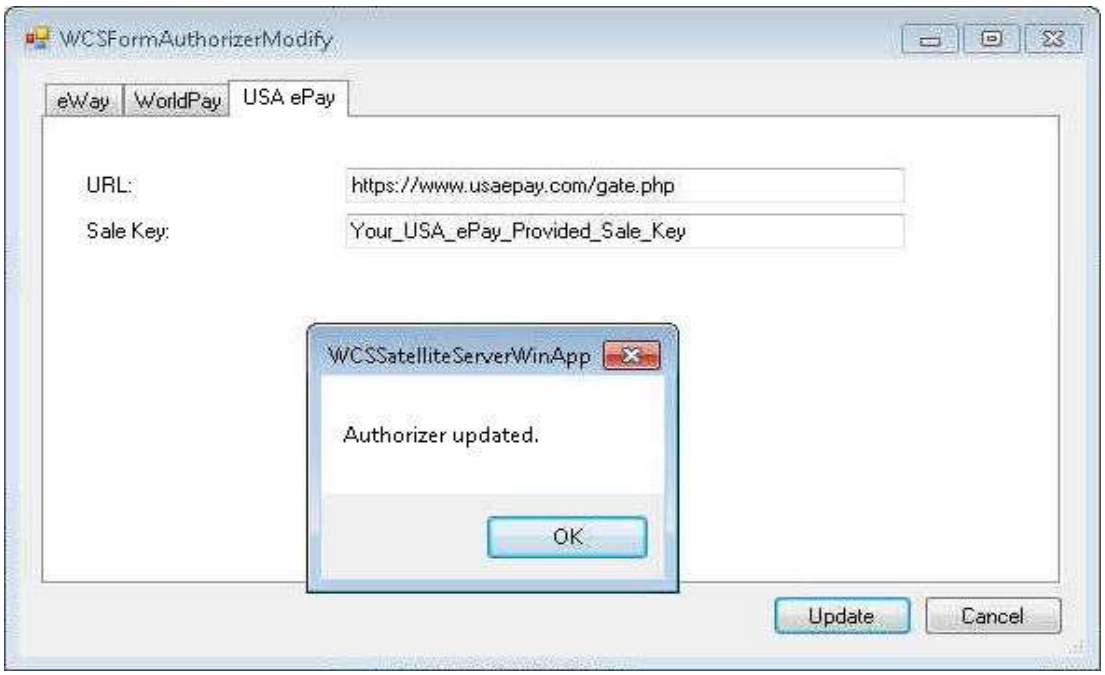
- Select the tab for the credit card processing gateway you will be utilizing
- In this example, USA ePay is selected
- Enter the information from the setup sheets (provided by the processing gateway) into the required fields presented on the selected tab



- Click <Update>

Credit Card Processor Configuration and Management (Continued)

- The following confirmation dialog box will appear



- Click <OK> to close the confirmation dialog
- Close the main processing gateway configuration form by clicking <Cancel> or <X>
- Test swipe an active credit card on site to test sale functionality
- After the device activates, contact your credit card processor to confirm the test transaction appears in the records for your processing account as a completed sale
- If the test swipe fails, repeat above steps 1 – 8 and confirm the configuration against the setup sheets provided by your credit card processor.

If you have continuing questions or concerns regarding the above configuration steps, please contact WashCard Systems Technical Support for assistance:

888-439-5740 x: 200
support@washcard.com

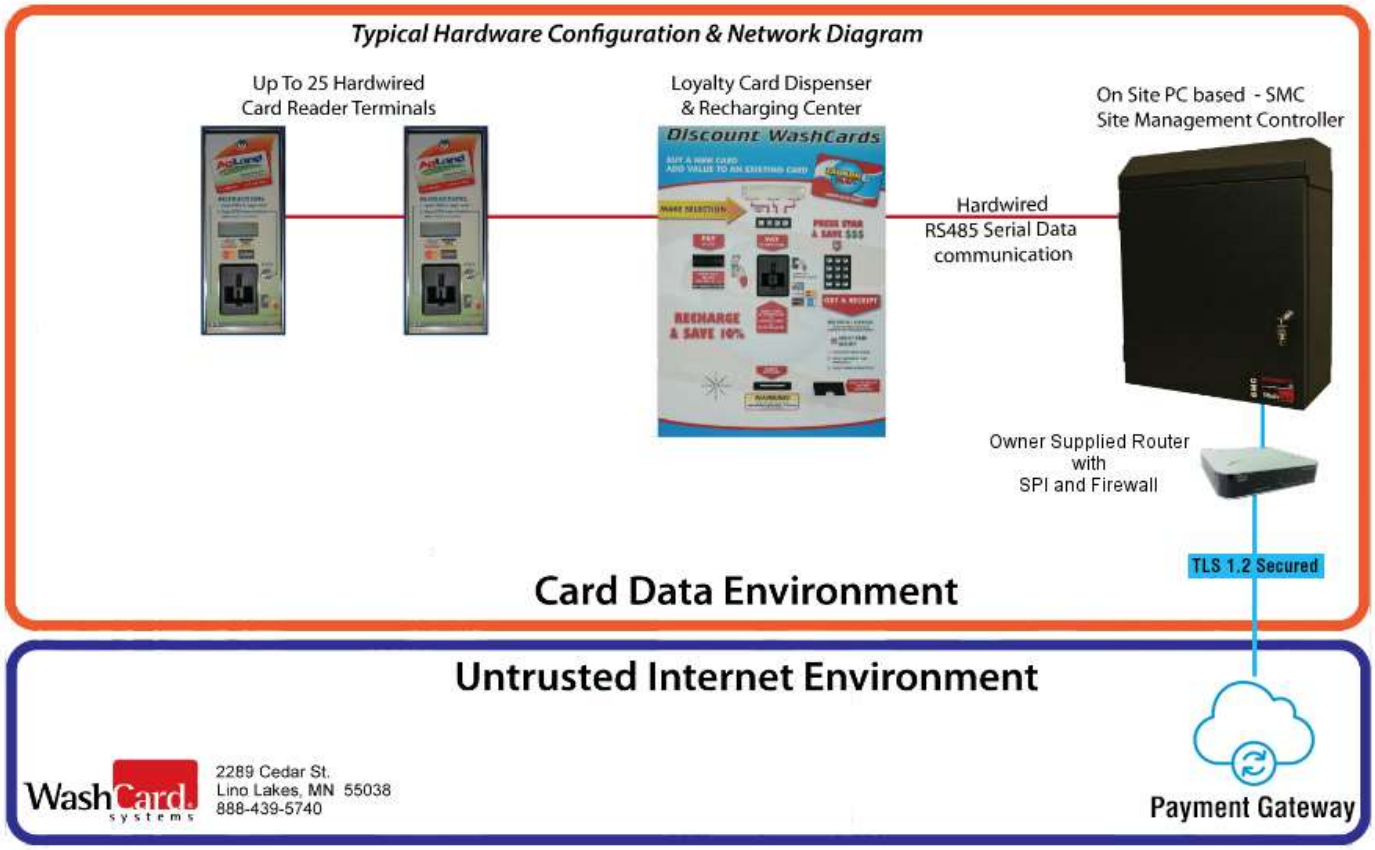
Satellite Server Update Process

The Satellite Server application update process is completely automated and requires no user interaction at the Site Management Controller (SMC). When an update becomes available from WashCard Systems, the application will detect its availability when it next synchronizes with the centralized server. At that time, the application downloads the required, Authenticode verified, updated configuration files and sets the update as pending. This download is performed over a TLS 1.2 secured HTTPS connection to the WashCard Systems production web server at the following address:
https://secure3.washcard.com/WCSSatelliteServerWinApp451/

In the early AM hours, after checking for currently active users and confirming no ongoing activity, the application will initiate the update process, restart itself, and re-synchronize with the centralized server marking the update as complete. Should there be activity, the application will continue to attempt the update each successive morning until the update, restart, and re-synchronization is completed.

For additional information on Microsoft's Authenticode technology see the following URL:
https://docs.microsoft.com/en-us/windows-hardware/drivers/install/authenticode

Appendix A:
Recommended Network Configurations



Appendix B:
Satellite Server Version Numbering

WashCard Systems Satellite Server utilizes a 3 position Semantic Versioning (SemVer) format of Xx.Yy.Zzz

- Xx – MAJOR version update which is not backwards compatible with existing dependencies
  - Only released as a new benchmark (for example, 5.0.0)
  - Base value for the Xx element is 0
- Yy – MINOR version update with backwards compatible program changes related to security or PA-DSS requirements
  - Only released as a new benchmark (for example, 4.2.0 and not 4.2.1)
  - Base value for the Yy element is 0
- Zzz – MINOR version update with backwards compatible program changes not related to security or PA-DSS requirements
  - This is a WILDCARD element in the Satellite Server application versioning format
  - Base value for the Zzz element is 0
- Each version number is numeric only and can range between 0 and 9

Major updates - Changes requiring an update to the Xx version segment are rare. Examples of a change at this level would be a complete redesign of the underlying database used by the application, or a change to the programming language in which Satellite Server is written. Changes of this level require not just an update to the existing platform, but a complete re-installation of the Satellite Server application at the new functionality level.

Minor Updates (Security/PA-DSS Related Changes) – The Yy version segment is updated any time functional changes are implemented in the application which impact PA-DSS compliance. Such changes would include management of PAN data in memory, how PAN data is masked, the way application users and passwords are encrypted and stored, the method in which credit card authorizations are processed, etc. When a security related minor update occurs, the PCI SSC website listed version of the application must also be updated to reflect the change.

Minor Updates (Wildcard: No Security/PA-DSS Related Changes) – The Zzz version segment is updated any time functional changes are implemented in the application which are not related to PAN data, data security, or PA-DSS requirements. *If any such security changes are being implemented, the Yy version segment must instead be updated.* Changes which would fall into the non security minor update category include: A new wash device type being implemented (utilizing the same already existing authorization processes), an update to the application user interface to expand loyalty card based functionality, or small scale changes to the underlying application database.

This version maintenance will be performed on each minor (non security), minor (security), and major application update.

Appendix C:
Implementation Guide Version History

Date	Details	PA-DSS Version
January, 2016	Initial document creation for v3.1 PA-DSS compliance with guidance from Sikich (PA-QSA)	v3.1
January, 2017	Reviewed. No changes required.	v3.1
January, 2018	Reviewed. No changes required.	v3.1
January, 2019	Reviewed. No changes required.	v3.1
May, 2019	This guide has been updated to document PCI-DSS compliant configuration for Windows 10 64-bit professional.	v3.1
June, 2019	Updated application version number to 4.5.x throughout the document. Updated section *Encrypt Traffic Over Public Networks* to note that TLS 1.2+ is required, and trusted keys and certificates must be used at all times. Updated section *About This Document* with information about how this document is delivered and how to acquire a replacement copy. Updated section *Wireless Networks* to better instruct users on securely configuring wireless networks per PA-DSS requirement 6.3. Updated section *Satellite Server Update Process* to specifically identify the verification done on update files as Authenticode Verification. Added section *Non-Console Administrative Access.* Added page numbers.	v3.2

	Added .NET Framework 4.6.1 to *Required Components and Protocols.* Corrected *Satellite Server User Management* to state that Satellite Server uses SHA256 encryption in the password encryption process. Updated *Appendix A: Recommended Network Configurations* with a new graphic.	