PA-DSS Implementation Guide For OneTouch® Suite

Version 5.33X0.XXXX

July 2020

Table of Contents

Introduction

Product Overview

Triple E Technologies' OneTouch® Suite Version 5.33X0.XXXX is a Point of Sale (POS) application, developed and tested for implementation on PC platforms running Microsoft Windows 10 Professional Edition. OneTouch® Suite uses Microsoft SQL Server 2016 for its database structure.

In keeping with industry payment application best practices and for purpose of compliance with the Payment Card Industry (PCI) Payment Application Data Security Standard (PA-DSS), OneTouch® Suite includes the following security features:

- Use of Microsoft Windows' built-in, host-based firewall to protect cardholder data; firewall drops all incoming traffic not corresponding to traffic sent in response to a host request.
- Disabled or removed vendor-supplied defaults for passwords and other security parameters prior to system use.
- Non-retention of payment card authentication data; full magnetic stripe, PIN and card validation code data are not stored. Except when an employee has physical possession of a customer payment card, the full account number is never revealed.
- Supported use and updating of anti-virus software, with specific configuration settings for OneTouch® Suite servers.
- Assignment of specific User access rights and permissions based on predefined group accounts and merchant-determined privileges.
- Windows authentication of user login credentials; presentation and authorization of a unique ID and password required for each user requesting access to OneTouch® Suite.
- Event logging of user activities such as logins, logoffs, security rights changes and accesses to database objects.

In keeping with PCI requirements, the following Windows services, protocols, components and dependent software are required for OneTouch® Suite application functionality:

Software Dependencies

MS Windows 10 Professional - O/S
MS SQL Server 2016

Hardware Dependencies

Ingenico ISC250, UIA VERSION = 18.0.2 (Vanguard only)
Ingenico iUR250 MSR, UIA VERSION 18.0.2 (Sentinel only)
Ingenico iUP250 PinPad, UIA VERSION 18.0.2 (Sentinel only)

Protocols and Ports

Internal (LAN) Communication

The applications and services in OneTouch Suite communicate amongst each other over IP on the LAN using TCP and UDP protocols. These LAN port values are configurable.

The applications also communicate over the LAN with the SQL Server instance running on the local Navigator over port 1433 and with ccEngine over port 1443, both protected by SSL/TLS.

External (WAN) Communication
The ccEngine card processing service utilizes port 443 outbound over TCP/IP protected by TLS 1.2 to communicate with the credit card processing host.

The AutoUpdaterClient service utilizes port 2113 outbound over TCP/IP protected by TLS 1.2 to communicate with the AutoUpdate Server. It uses port 2114 for downloading the upgrade packages.

The optional OneTouchSync service responsible for syncing private charge account data utilizes a default port value of 443 outbound over TCP/IP protected by SSL. This port value can be configured.

Product Versioning

Triple E Technologies' OneTouch® Suite products employ the following schema to assign unique names to all new software releases and updates:

Major Change	Minor Change	Impact	Maintenance	Placeholder	Build
1-9.	1-9	0-3	1-9	0	.1001-9999

- **Major Change**: Sequence number indicating a major change that contains substantial changes (e.g., interface overhaul, change in compatibility, EMV, etc.); increases for each subsequent Major Change release.
- **Minor Change**: Sequence number indicating a minor change (e.g., improvement of existing interfaces, new feature or functionality, etc.); increases for each subsequent Minor Change release; resets to '1' after each new Major Change release.
- **Impact**: Change impact on previous software release. Linked to the Major.Minor release tuple; does not change with each maintenance or build increment. Either:

  0 = No Impact
  1 = PCI Impact
  2 = Security Impact
  3 = PCI and Security Impact

- **Maintenance**: Sequential number indicating a maintenance change, which is representative of a planned maintenance patch to existing features and functionality; increases for each subsequent Maintenance release; resets to '1' after each Major or Minor version value change. This is a Wildcard incremented for changes that do not require PA-DSS validation
- **Placeholder**: Not used; defaults to '0'. Does not display by default; included as part of the Maintenance/Build wildcard string.
- **Build**: Sequential number identifying improvements or bug fixes to current major, minor, maintenance build tuple; resets to .1001 after each Major, Minor or Maintenance update. This is a Wildcard incremented for changes that do not require PA-DSS validation. To see application full version number, including the placeholder and build value:
  - Click the Triple E control panel, then click **Open Dashboard**.

EXAMPLE:
5.3310.1020 = Fifth Major release, third Minor change in fifth Major release, with security and PCI impact, first Maintenance release in the Major/Minor tuple, with a build value of 1020.

Document Purpose and Use

This guide provides general and detailed instructions for implementing OneTouch® Suite 5.33X0.XXXX into your business environment in a manner compliant with the Payment Card Industry (PCI) Data Security Standard (PCI-DSS). The PCI-DSS is a set of security standards created by the PCI Security Standards Council to guide development, implementation and use of payment card applications.

Please note that this document is not intended as a complete implementation guide for OneTouch® Suite; rather, it provides guidelines and instructions only for implementing OneTouch® Suite in a manner that facilitates and supports compliance with established PCI standards.

This guide applies only to OneTouch® Suite 5.33X0.XXXX, and only as formally released by Red River Software/Triple E Technologies. Any subsequent modification of the application and/or the PCI-DSS must be reviewed and evaluated to determine continued PCI compliance.

This guide is available to OneTouch® Suite owners and their designees. We will publish and distribute updates annually, or sooner if otherwise demanded by either product or PCI-DSS requirements. Updates can also be obtained by going our website at http://www.e3tek.com.

For purpose of this guide, the following versions of PCI requirements and standards apply:

PCI-DSS Version 3.2

PA-DSS Version 3.2

Building and Maintaining a Secure Network

Using a VPN Router

For the purpose of secure OneTouch® Suite implementation and subsequent operation, PCI-DSS recommends that merchants use a VPN router for establishing remote connections into the Site Controller environment. VPN router configuration should follow these standards:

- Restrict inbound Internet traffic only to protocols necessary for the cardholder data environment; specifically deny all other inbound traffic.
- Always use two-factor authentication for remote access into the environment
- Limit external outgoing internet traffic to only those sites required by the OneTouch® Suite application, or as specified to meet business needs
- Do not use default passwords
- Require use of personal firewall product for connecting laptop or personal computer

Installing Firewall and Router Configurations

PCI-DSS 1.1-1.5 require OneTouch® Suite system owners to install network firewall and router configurations to protect cardholder data from unauthorized public access (Internet, other networks and hosts). In keeping with this requirement, adhere to the following standards and procedures before and after implementing OneTouch® Suite into your network environment.

NOTE: For general firewall or router installation instructions, refer to documentation provided with product.

1. Credit Card data (and therefore OneTouch® Suite) must not reside on systems that are not protected by a software or hardware firewall. If needed, a network DMZ (Demilitarized Zone) should be set up to segment the network such that machines in the DMZ are separated from the machines on the network responsible for processing credit cards.
2. Use the DMZ to filter and screen all traffic, and to prohibit direct routes for inbound and outbound Internet traffic. Ensure firewalls installed at each Internet connection and between Demilitarized Zone (DMZ) and internal network zone.
3. Identify firewall interfaces allowing traffic into OneTouch® Suite's network and DMZ networks. Determine services destined for cardholder environment; ensure services are necessary and originate in an interface connected to an interface within the DMZ. Devise and install DMZ to limit inbound and outbound traffic only to protocols necessary for OneTouch® Suite cardholder data environment.
4. Ensure firewall limits inbound internet traffic data connections only to IP addresses within the DMZ. Create policy stating all traffic between inbound requested connections between the internet and Internal networks is are denied.
5. Ensure firewall performs Stateful Packet Inspection (SPI) to keep track of each network connection (e.g., TCP stream, UDP communication, etc.) traveling across it. Confirm firewall can distinguish legitimate packets for different types of connections, and that only packets matching known ("remembered") connection states can pass through.
6. Ensure firewall configuration has anti-spoofing rule to prevent internal addresses from passing from Internet into DMZ.

7. Identify internal network segments accessible from outside and DMZ, including routable addresses. Examine rule trails individually for natting. Ensure firewall hides all internal network IP addresses.
8. Verify that all mobile and/or employee-owned computers having both network access and direct Internet connectivity have personal firewall software installed and active. Ensure personal firewall software configured by Administrator in keeping with standards contained herein and are not alterable by mobile computer users.
9. Except for one emergency account, do not configure local user accounts on router. Router must require user authentication, and only Administrators should have access. Ensure 'enable password' on router kept in secure, encrypted form and set to current production password.
10. Ensure router denies all inbound and outbound traffic not specifically allowed. Add router access rules as business needs arise.
11. Document all router configuration files. Secure router configurations through use of access and physical controls, and ensure configuration files are synchronized.
12. Ensure each router has following statement in clear view:

> You have accessed a [company name] restricted device. The actual or attempted unauthorized access, use or modification of this system is strictly prohibited. Unauthorized users are subject to disciplinary proceedings and/or criminal and civil penalties under state, federal or other applicable domestic and foreign laws. The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity we may provide the evidence of such activity to law enforcement.

The following ports and protocols are used by the Triple E Suite to facilitate communication between the POS systems and the Navigator Site Controller. The purpose of this information is to serve as a guide when setting up firewall software on the POS systems and Navigator or when putting a firewall between machines on the local network.

Navigator Site Controller

Outbound Connections (LAN)

TCP 6627: tPortController → NeXGen
TCP 9999: PedestalViewer → Pedestal (Sentinel POS)
TCP 443: ccEngine → Payment Processor
TCP 1433: POS → SQL Server (port for SQL connections accessing DB on Navigator)

Outbound Connections (WAN)

TCP 433: ccEngine → Payment Processor

Sentinel POS (Pedestal service)

Outbound Connections (LAN)

TCP 1433: POS → SQL Server (port for SQL connections accessing DB on Navigator)
TCP 1443: POS → ccEngine (secured with TLS 1.2. Used to securely transmit SAD)
TCP 5556: POS → tPortController (POS sends fuel dispenser commands to tPortController and receives status updates)
TCP 9999 PedestalViewer → Pedestal Service

Vanguard POS

Outbound Connections (LAN)

TCP 1433: Register→ SQL Server (running on Navigator)
TCP 1443: Register→ ccEngine (secured with TLS 1.2. Used to securely transmit SAD)
TCP 5556: Register→ tPortController (POS sends dispenser commands to tPortController and receives status updates)

Additional Protocols & Ports for Optional Components (LAN)

ICMP: Enabled (for pings)
UDP 138: MS File and Printer Sharing (NB-Datagram-In)
UDP 137: MS File and Printer Sharing (NB-Name-In)
TCP 139: MS File and Printer Sharing (NB-Session-In)
TCP 445: MS File and Printer Sharing (SMB-In)
TCP 5900: UltraVNC viewer for viewing networked machines on the LAN

Additional Protocols & Ports for Optional Components (WAN)

TCP 2113 [Outbound]: AutoUpdaterClient Service → AutoUpdate Server (communication channel)

TCP 2114 [Outbound]: AutoUpdaterClient Service → AutoUpdate Server (file download channel)

TCP 13450 [Outbound]: nxlog (PaperTrail Windows Event Log Aggregator)

Disabling Vendor-Supplied Default Accounts

PCI-DSS 2.1 requires OneTouch® Suite system owners to change or disable any administrative default account as provided by vendors to install operating systems, servers, databases and applications. In keeping with this strategy, Triple E Technologies disables the Microsoft SQL Server “sa” admin account. However, there are three other default Windows accounts associated with OneTouch® Suite that are not PCI compliant if used as-is. Therefore, to maintain system integrity and ensure continued PCI compliance, perform the following procedures both as part of OneTouch® Suite implementation and every ninety days thereafter. Secure authentication should be used for these accounts even if they are to be disabled or not used. These accounts need to be managed as regular Windows accounts.

Procedures

Change passwords for any disabled and/or not-in-use accounts, and for the following OneTouch® Suite default accounts:

- Administrator
- Manager
- POS

For each such account, devise (strong) replacement password using the following complexity standard:

- At least seven characters.
- No user name, real name or company name.

- No complete dictionary word.
- Characters from each of the following four groups:

Group	Examples
Uppercase letters	A, B, C …
Lowercase letters	a, b, c …
Numerals	0, 1,2, 3, 4, 5, 6, 7, 8, 9
Symbols	` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /

EXAMPLE: 4&q6md13?J

Next, replace default passwords with new passwords using Windows Local Users and Groups. You must be logged-on as Administrator to perform functions associated with changing default account passwords.

Transmitting Encrypted Data

PCI-DSS Requirement 4.1 mandates use of strong cryptography and at least 128-bit encryption techniques (either at the transport layer with TLS or IPSEC or data layer with encryption algorithms such as RSA or AES) to safeguard cardholder data during transmission over public networks, including the Internet and Internet-accessible DMZ network segments. In this regard, OneTouch® Suite transfers all data to the card processor via TLS 1.2 secure protocol over TCP/IP. If applicable, any connections coming into the system from the Internet should also be established with TLS 1.2. Owners are advised that changing encryption settings below 128-bit encryption will result in PCI non- compliance.

Encrypting All Non-Console Administrative Access

Non-console administrative access to the cardholder data environment (application and servers) requires two-factor authentication and either SSH, VPN or TLS for encryption. It is your responsibility to implement two-factor authentication in order to comply with PCI-DSS requirements. You must provide demonstrable means for:

1. Identifying all services to the firewall and their attendant rules and policies and noting management services with administrative access.
2. Encrypting all communication between administrative console and firewall.
3. Ensuring interface access to all management services uses strong encryption technologies such as SSH, VPN and TLS-encrypted HTTPS protocol.
4. Implementing and managing multi-factor authentication access control mechanisms for all remote access to systems involved with handling of any PAN or SAD.
5. Reviewing system service and parameter files to ensure Telnet FTP, 'r*' protocols and other insecure remote login commands are disabled.

Protecting Cardholder Data

Preventing Storage of Full Magnetic Stripe, Validation Code or Value (CAV2, CID, CVC2, CVV2) or PIN Block Data

Current and previous OneTouch Suite® versions do not store magnetic stripe, card validation code or PINs/PIN block data. OneTouch Suite® software uses strong encryption algorithms (AES and RSA-2048) to encrypt this data while present in volatile memory. The software takes advantage of Microsoft's SQL Server Data Encryption Hierarchy to protect all encryption keys utilized to encrypt the volatile memory cardholder data. Preventing storage of such confidential card payment data is required for PCI compliance.

It is the merchant's responsibility to ensure that the card payment transactions they process do not store magnetic stripe data, card validation codes, PINS or PIN block data, or cryptographic key material, even when such data is encrypted; it is OneTouch® Suite's responsibility to provide the means.

When a card needs to be authorized at a POS terminal, the sensitive authentication data (SAD) is immediately encrypted using 256-bit AES. The application establishes a secure TLS 1.2 connection over TCP to the ccEngine service (the only application in OneTouch Suite® that authorizes credit cards) running on the Navigator Site Controller. This secure stream contains the encrypted track data and other transaction details, allowing ccEngine to authorize the transaction. During this process, the SAD resides encrypted within volatile memory only and is never stored on disk or within the database.

Important: In the case of power failure or system/application shutdown, the encrypted SAD, including PAN, will be permanently irretrievable. **It is strongly recommended that you equip your system with a UPS in order to prevent loss of transaction data prior to post-authorization for environments with fuel dispensers, particularly if Sentinels are installed.**

Inadvertent Capture or Retention of Cardholder Data

PA-DSS 2.1 requires that you configure your underlying software or systems (e.g., OS, databases, etc.) in such manner as to prevent inadvertent capture or retention of cardholder data.

Encrypting the Page File

New systems shipped from Triple E have the Windows Paging File already encrypted and are set to clear pagefile.sys upon shutdown. However, to encrypt the Page File for an upgraded system, you must first ensure your computer hard disk is formatted using NTFS, and then perform the following steps:

1. On Windows task bar, click the Windows **Start** menu icon and type **cmd**.
2. On menu that displays, right-click **cmd.exe**, and then click **Run as Administrator** on next menu.
3. At prompt, type **fsutil behavior set EncryptPagingFile 1** to encrypt page file.
4. To verify configuration, type **fsutil behavior query EncryptPagingFile**; **EncryptPagingFile=1** message displays.

In the event you need to disable Paging File encryption, complete the steps above and set the value to 0 rather than 1.

Clearing the Page File

New systems shipped from Triple E are preset to clear pagefile.sys upon shutdown, thereby purging all encrypted temporary data such as application passwords and cardholder PANs. However, to clear the

Page File for an upgraded system, you must first perform the steps outlined below. Note that the result of such performance may increase your Windows shutdown time.

1. On Windows task bar, click the Windows **Start** menu icon and type **regedit**.
2. On menu that displays, right-click **regedit.exe**, and then click **Run as Administrator** on next menu.
3. On Registry Editor, click **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ Session Manager\Memory Management**.
4. If the **ClearPageFileAtShutdown** entry is present, continue to **Step 5**. Otherwise:
   - Right-click in right pane
   - Click **New**, then click **DWORD (32 bit) value**
   - Type **ClearPageFileAtShutdown**
5. Double-click on the **ClearPageFileAtShutdown** entry and change value from **0** to **1**.
6. Click **OK**; close **regedit**.

Disabling Windows Error Reporting

The Windows error reporting feature has the potential to capture and retain cardholder data. Perform the following steps to disable Windows error reporting:

1. On Windows task bar, click the Windows start menu icon and type **regedit**.
2. On menu that displays, right-click **regedit.exe**, and then click **Run as Administrator** on next menu.
3. On Registry Editor, click **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting**.
4. If the **Disabled** entry is present, continue to **Step 5**. Otherwise:
   - Right-click in right pane;
   - Click **New**, and then click **DWORD (32 bit) Value**
   - Type **Disabled**
5. Double click on the **Disabled** entry and change value from **0** to **1**.
6. Click **OK**; close **regedit**.

Storing Cardholder Data

Sensitive cardholder data must always be encrypted when being stored. OneTouch Suite 5.33X0.XXXX never displays full cardholder PAN data, meaning PAN data is always masked by default on all displays. The application cannot be configured to allow viewing of full PAN data.

Per PCI-DSS Requirements 1.3 and 1.3.4, never store cardholder data on Internet-accessible systems that are listening for inbound connections (e.g., a web server and the database server must not be on the same machine) or on machines that are in the network's DMZ. Although OneTouch® Suite does use Microsoft SQL Server to distribute the application internally to your network, this server should NOT be used for any external web applications. It is recommended that access to this server from the Internet be severely restricted through use of a VPN firewall. Please see the section on remote access for clarification on how to use VPN access to view OneTouch® Suite data remotely.

Managing stored cardholder data

OneTouch® Suite Version 5.33X0.XXXX does not store any sensitive cardholder data on disk or in the database, encrypted or otherwise.

The non-sensitive data that is stored in the database for reporting purposes only includes Masked PAN and Expiration Date.

Masked PAN may be output in the following DataManager reports:

- Credit Card Reconciliation Report
- Daily Card Sales Report
- eee2016.rpt- Last 4 only
- eee2017.rpt- Last 4 only
- eee2037.rpt- Last 4 only
- eee2080.rpt- Last 4 only
- eee2028.rpt- Last 4 only
- EMVChipTransactions.rpt- 1st 6 and Last 4

Masked PAN may also appear in the following applications/systems:

Register
Final screen - 1st 6 digits (ISO) + Last 4 digits, on all swipes/inserts of card data
Receipt - Original and reprint - Last 4 digits only

Dispensers
Receipt - Original - Last 4 digits only

Sentinel
Receipt - Original - Last 4 digits only

Purging cardholder data

OneTouch® Suite Version 5.33X0.XXXX does not store any sensitive cardholder data on disk or in the database, encrypted or otherwise. Thus, a purging routine is not necessary.

Managing cryptographic material

In keeping with PCI-DSS Requirement 3.6, all cryptographic material (encryption keys and encrypted cardholder data) must be securely removed. In this regard, the process of implementing OneTouch® Suite Version 5.33X0.XXXX will automatically purge encrypted data from previous transactions, if any exists. Removal of this cryptographic material is absolutely necessary for PCI compliance.

Following implementation, system encryption keys must be changed at least annually and whenever deemed necessary or prudent because of actual or suspected security compromise. Keys must also be changed whenever anyone with knowledge of them changes positions or leaves the company. OneTouch® Suite provides system functionality to securely change encryption keys currently used to protect cardholder data, and will automatically change encryption keys annually if not otherwise performed more frequently.

Encryption Key Storage

PA-DSS 2.4. requires that access to keys must be restricted and must be stored securely in the fewest possible locations and forms.

Data encryption keys are protected by Microsoft SQL Server key encryption and protection mechanisms.

All utilized keys are stored and protected in separate levels of hierarchy. The Master Data Encryption Key (DEK) is stored doubly-encrypted in the Master Database. The DEK is encrypted by the RSA2048 Key-Encrypting-Key 'eeeCCKey' and stored in an encrypted SQL object in the Master DB. The RSA2048 KEK resides in the ccEngine database to physically separate the KEK storage from the DEK storage.

The process of generating new encryption keys is contained within an encrypted stored procedure. The keys are generated partly by way of the built-in SQL server symmetric master key generation and asymmetric key generation. Regenerating encryption keys causes SQL server to regenerate its Database Master Key (DMK) and the asymmetric RSA2048 key 'eeeCCKey' that functions as the KEK. Additionally, several bytes of random entropy are added to the Master DEK when it is regenerated.

Moreover, restricted access to the site controller machine via Windows Accounts is the true layer of security guarding against unauthorized key modification. The administrator account that installed the SQL Server instance as well as members of the PCIGroup can manipulate the DEK.

The Symmetric Master Key (SMK) is protected by the Windows Data Protection API (DPAPI) and tied to the physical machine key and service account credentials. The Database Master Key (DMK) in each DB is protected by the SMK which is created at SQL Server setup and tied to that unique instance of SQL server. The asymmetric key 'eeeCCKey' is protected by the DMK and thus the data residing in the underlying databases can only be decrypted on the physical SQL Server instance where installation was performed.

Key Locations

The DEK is stored encrypted by the KEK on disk in the 'Master' database within an encrypted SQL object. The asymmetric key 'eeeCCKey' which serves as the DEK-Encrypting-Key is stored in the ccEngine database on disk. Encryption storage key locations are not configurable and thus cannot be changed.

Viewing Audit Logs on a Centralized Log Server

Trace files automatically generated by the SQL Server for events related to accessing the DEK, encryption key maintenance and other significant events are logged to the C:\EEETechnologies\EEETrace folder and its sub-folders on the Navigator SiteController machine. The files in this folder must be viewed with SQL Server Profiler or other SQL Trace File Viewer application of your choosing. These files must be transferred to a centralized logging server on a regular interval to avoid system shutdown due to the primary disk storage being exhausted.

If the system detects that the hard disk C:\ is nearing capacity, it will alert the user via a popup and will begin compressing entries arriving into C:\EEETechnologies\SavedLogs to save significant space. To ensure proper function of the software, the POS will shut down any time the available disk space falls below 2GB:

If your system is running low on storage, it is recommended that you transfer archived log files to clear up disk space. You can move the trace log folder's contents from the Navigator to your logging server using your preferred file transfer method. Some valid options include FTPS to a secured FTP server, file transfer via UNC on Windows to a mapped drive, a secure file transfer service such as Google Drive, or a physical medium, among others. All .trc files except the active file locked by SQL Server can be moved.

Trace audit logs will never contain any SAD. All of the .trc audit logs can be reviewed with an SQL viewer application. A customer can utilize the .trc audit logs that have been transferred to a log server inside SQL Server Profiler or equivalent viewer. It is through utilization of the profiler or a viewer application that customers gain the ability to view audit logs on a centralized log server.
Additionally, application event logs are also written to the following locations:

- C:\EEETechnologies\OnetouchLogs
- C:\EEETechnologies\SavedLogs
- C:\Windows\System32\winevt\Logs

The files found in **OneTouchLogs** and **SavedLogs** can be viewed with any text editor. These logs show transaction messages and cashier interactions, as well as any errors that were encountered during operation in proprietary formats specific to the OneTouch Suite.

Windows event logs must be viewed with Windows Event Viewer – knowledge of Windows events is necessary to understand the entries written. Explanation and interpretation of the Windows events are outside the scope of this document – refer to Windows auditing resources for further details.

Encryption Key Custodian

Key encryption management is largely handled by the OneTouch Suite application. However, limited personnel should be designated key custodian roles to manage certain additional functions. The following is a list of key custodian responsibilities:

- Ensure timely generation of new keys as defined in company information security policy and periodically change keys accordingly
- Ensure only authorized users have access to systems with OneTouch Suite software, specifically Datamanager, that have ability to regenerate keys
- Fully document key management processes

PA-DSS 2.6 requires each Administrator or other person assigned encryption key custodianship responsibilities to formally sign a document indicating they understand and acknowledge their assigned responsibilities. A sample form is provided below:

<Company Name>

Encryption Key Custodianship

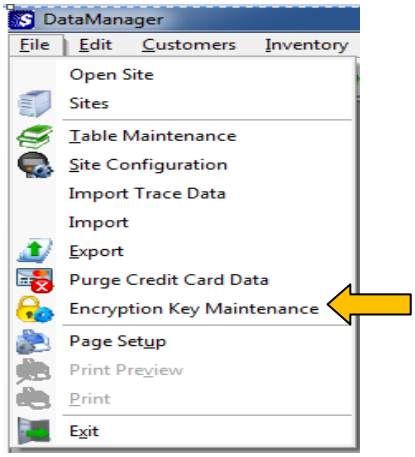
The undersigned herewith acknowledges understanding and acceptance of all responsibilities assigned as <*Company Name*> Encryption Key Custodian.

Custodian Name:_____ Approved By:_____
Custodian Signature:_____ Approver Signature:_____
DATE: __/____/_____ DATE: ___/____/_____

Changing encryption keys

You must be logged-on as an Administrator or a member of the PCIGroup to perform the encryption key maintenance function. To change the encryption key following OneTouch® Suite implementation, follow the procedure below:

1. From OneTouch DataManager **Connect** menu, click **File**, and then click **Encryption Key Maintenance** in drop-down menu.



Change Encryption Key dialog displays:

2. Click Create.

NOTE: OneTouch® Suite generates an Encryption Key Change record in the audit log each time encryption key maintenance is performed. All data encrypted with old keys currently in volatile memory will no longer be decryptable as the keys are forcibly removed.

Implementing Strong Access Control Methods

Restricting Cardholder Data Access by Business Need-To-Know

NOTE: OneTouch® Suite Version 5.33X0.XXXX does not store any sensitive cardholder data on disk or in the database, encrypted or otherwise.

OneTouch® Suite strongly advises limiting access to any PC and servers that interact with cardholder data by requiring unique User IDs and passwords for purpose of secure authentication. OneTouch® Suite does not have provision for setting up user accounts and relies on Microsoft Windows functionality to setup user accounts and assign users to user groups. A Windows user account defines the actions a user can perform by establishing the privileges (rights and permissions) for that user. Each OneTouch® user must be a member of at least one user group. The rights and permissions assigned to a user group are the same for all members of that group.

OneTouch® is pre-configured with four distinct user groups with the appropriate privileges already assigned. The privileges associated with each user group are described below. As good practice, you should assign users to the group or groups having the least privileges allowing satisfactory performance of assigned duties. For reason of system integrity and PCI compliance, never modify the privileges assigned to OneTouch® user groups.

The groups listed below are in order of least restrictive to most restrictive. Further, each group inherits features/functions of the group below, i.e. they are additive.

Administrator Group

An Administrator Group account can make system-wide Windows and server changes, such as install programs and access all files on the computer. Only an Administrator has complete access to other user accounts. Administrator group members are used to perform system updates, modify database objects, make Windows configuration changes, and install new software. Do not run your day to day while logged in as a member of the Administrator group. An Administrator Group member can:

- Create, change and delete user accounts.
- Assign users to groups, i.e. Administrator, PCIGroup, Managers, Users
- Create, reset and delete user account passwords.

Administrator Group members cannot change their own account type to another account type unless there is at least one other user with an Administrator account type. This is to ensure that there is always at least one Administrator in the system.

Administrators have no restrictions regarding features/functionality and inherit all features/functions of the other defined groups. As previously stated, this group is utilized specifically when system changes/updates occur and not for the day to day activities.

PCI Group

PCI Group accounts allow equivalent DataManager functionality to that of the Administrator group. However, PCI Group accounts are still just as restricted as a Manager/User when it comes to Windows permissions. Being a member of this group specifically grants the user access to PCI related features listed below. PCI Group members cannot make system-wide changes, install programs, create or access other user accounts or modify SQL objects.

- Encryption Key Maintenance

Manager Group

A Manager Group account provides access to all DataManager functionality equivalent to that of the PCI group, with exception of PCI-specific functions such as encryption key maintenance. Managers cannot make system-wide changes, install programs, create or access other user accounts, or modify SQL objects. A Manager Group member shares User Group level features and has the same Windows based user limitations. Some key features include:

- Customer and PrivateCard management capabilities.
- A/R related capabilities
- Import/Export capabilities

User Group

User Group members have limited access to system menu and reporting functions inside Datamanager. Users are also restricted to having limited windows permissions and only have permissions on OneTouch related folders/registry keys. User Group members cannot make system-wide changes, install programs, create or access other user accounts or modify SQL objects. Users are primarily involved with viewing reports and performing inventory activities. User Group members are restricted to the following Datamanager functions/features:

- Access all sales and inventory related reports
- Ability to configure Vanguard Quick Menus
- Inventory Management functions such as adding items, changing prices, inventory receiving/adjustments

Screensaver Display Setting

To minimize observance of cardholder data displayed on temporarily vacated workstations, specify Windows screen saver default setting of 15 minutes or less with automatic lock when screensaver activates.

User Account Password and Lockout Policies

OneTouch® Suite uses pre-configured Windows settings for the following account password and system lockout settings:

- Minimum Password Age = 0
- Maximum Password Age = 90
- Minimum Password Length = 7
- Password Complexity = 1
- Lockout Bad Count = 3
- Reset Lockout Count = 30
- Lockout Duration = 30

For purpose of system integrity and PCI compliance, do not change these default settings to less than values specified. NOTE: Windows operating system keeps password history and requires new passwords be assigned at least every ninety (90) days and differ from previous four.

Assigning Unique ID and Password to Each Application User

Each OneTouch® Suite Version 5.33X0.XXXX user must have a unique User ID and password. You must be logged-on as Administrator to perform functions associated with setting up the required user accounts. To create a user account, follow instructions provided with your operating system software.

Accessing Cardholder Data Remotely

NOTE: OneTouch® Suite Version 5.33X0.XXXX does not store any sensitive cardholder data on disk or in the database, encrypted or otherwise.

PCI-DSS requires that if employees or vendors are to be granted remote access to cardholder data, such access must employ two-factor authentication (username/password and an additional authentication method such as a token or certificate). This includes remote administrative access. Acceptable two-factor authentication requires a method from two out of the following three categories:

- Something you know (e.g., personal identification number (PIN) or password)
- Something you have (e.g., phone number, email account)
- Something you are (e.g., fingerprint, voice scan)

Additionally, vendor access should be limited only to time necessary to provide required service, with access rights limited only to minimum required to provide that service. In all cases, remote access activity should be robustly audited daily by merchant or Administrator account personnel.

Use technologies such as remote authentication and dial-in service (RADIUS), terminal access controller access control system (TACACS) with tokens or VPN (based on IPSEC or TLS) with individual certificates. Triple E Technologies again recommends using a secure, encrypted VPN for remote access; authentication may be accomplished by specifying a unique VPN user name and complex password, as well as token or certificate.

Regardless of remote access software used, implement the following security features:

- Do not use group (shared) or generic account name and passwords
- Change default password settings in remote access software; assign unique ID and password to each remote user
- Never allow remote access connections directly from the internet; only allow connections from specific (known) IP/MAC addresses
- Use strong authentication and complex passwords for remote logins, per PCI-DSS requirements 8.1, 8.3 and 8.5.8 – 8.5.15
- Enable encrypted data transmission, per PCI-DSS Requirement 4.1
- Enable account lockout after a certain number of failed login attempts, per PCI-DSS Requirements 8.5.13
- Configure system so remote user must establish connection using VPN router and firewall before access is allowed
- Enable the logging function for auditing purposes
- Establish customer passwords per PCI-DSS Requirements 8.1, 8.2, 8.4 and 8.5
- Restrict access to customer passwords to authorized vendor personnel
- Restrict access to customer environment to authorized vendor personnel

- Restrict access to remote control software to administrative personnel only
- In cases of Red River Software / Triple E Technologies technical support requests:
    - Contact Red River Software / Triple E Technologies to request support.
    - Enable remote control software only for duration of required support.
    - Confirm site-unique information provided by support representative to ensure you have reached Red River Software / Triple E Technologies.
    - Disable remote control software immediately after use

Monitoring and Testing Network

Tracking Network Resources and Cardholder Data Access

NOTE: OneTouch® Suite Version 5.33X0.XXXX does not store any sensitive cardholder data on disk or in the database, encrypted or otherwise.

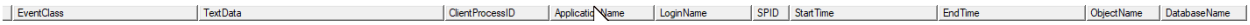
PCI DSS Requirement 10 specifies OneTouch® Suite system owners must track and monitor individual accesses to network resources and cardholder data. Owners must provide a central log server and establish policies and procedures for server setup, log migration and log modification prevention.

Logging is enabled by default when the system is shipped. The default log settings within the application are non-configurable. The trace files generated by the SQL Server are automatically written to C:\EEETechnologies\EEETrace and can be viewed with a SQL Server Profiler or other trace file viewer software.

OneTouch Suite does not store or allow access to cardholder data from the application. The trace files that are logged only include pertinent events related to encryption and keys.

The trace files will typically only contain 'Encrypted Text' events which are expected and indicate normal, secure access of encryption keys in the database by the POS applications and ccEngine.

Below is an example of a trace log file opened within SQL Server Profiler showing normal, encrypted activity. When reviewing logs for unexpected activity, this normal behavior should be filtered out using your log file viewer tool.



Note that the TextData is simply '- - Encrypted Text'

Any activity that is unexpected will not appear as 'Encrypted Text' but will rather be plaintext SQL in the log. Plaintext events in the log that could be of concern will pertain to the following keywords:

- eeeChangeEncryptionKey
- DEK

If any of these keywords appear in the trace files and do not consist solely of 'Encrypted Text', this is an indication that there was an attempt to modify a SQL object that interacts with encryption keys by a potentially unauthorized source. This would be cause for additional review to determine the source of the unexpected activity.

Note: During an administrative software update, SQL objects that are changed/updated as part of the update package will appear in the trace files in plaintext. If the update was performed at a scheduled date and time, seeing this activity during the process is not of any concern.

Below is an example that could potentially be unauthorized database activity, or it may simply be a scheduled software update:

EventClass	TextData	ClientProcessID	ApplicationName	LoginName	SPID	StartTime	EndTime	ObjectName	DatabaseName
Trace Start						2019-03-20 14:01:31...			
Audit Schema Object Manag...	DROP PROCEDURE Decrypt		SQLCMD	ETEK_ID\ru...	51	2019-03-20 14:01:32...		Decrypt	ccEngine
Audit Object Derived Perm...	DROP PROCEDURE Decrypt	5792	SQLCMD	ETEK_ID\ru...	51	2019-03-20 14:01:32...		Decrypt	ccEngine
Object:Deleted		5792	SQLCMD	ETEK_ID\ru...	51	2019-03-20 14:01:32...		Decrypt	ccEngine
Audit Schema Object Manag...	CREATE Procedure [dbo].[Decrypt] @B...	5792	SQLCMD	ETEK_ID\ru...	51	2019-03-20 14:01:32...		Decrypt	ccEngine
Object:Created		5792	SQLCMD	ETEK_ID\ru...	51	2019-03-20 14:01:32...		Decrypt	ccEngine
Audit Schema Object Manag...	DROP PROCEDURE eeeChangeEncryptionKey	5792	SQLCMD	ETEK_ID\ru...	51	2019-03-20 14:01:32...		eeeChan...	ccEngine
Audit Object Derived Perm...	DROP PROCEDURE eeeChangeEncryptionKey	5792	SQLCMD	ETEK_ID\ru...	51	2019-03-20 14:01:32...		eeeChan...	ccEngine
Object:Deleted		5792	SQLCMD	ETEK_ID\ru...	51	2019-03-20 14:01:32...		eeeChan...	ccEngine
SP:StmtStarting	CREATE PROCEDURE [dbo].[eeeChangeEn...	5792	SQLCMD	ETEK_ID\ru...	51	2019-03-20 14:01:32...		eeeChan...	ccEngine
Audit Schema Object Manag...	CREATE PROCEDURE [dbo].[eeeChangeEn...	5792	SQLCMD	ETEK_ID\ru...	51	2019-03-20 14:01:32...		eeeChan...	ccEngine
Object:Created		5792	SQLCMD	ETEK_ID\ru...	51	2019-03-20 14:01:32...		eeeChan...	ccEngine
SP:StmtCompleted	CREATE PROCEDURE [dbo].[eeeChangeEn...	5792	SQLCMD	ETEK_ID\ru...	51	2019-03-20 14:01:32...	2019-03-20 14:01:32...	eeeChan...	ccEngine
Object:Created		5792	SQLCMD	ETEK_ID\ru...	51	2019-03-20 14:01:32...		eeeChan...	ccEngine
Object:Deleted		5792	SQLCMD	ETEK_ID\ru...	51	2019-03-20 14:01:32...		eeeChan...	ccEngine
Object:Created		5792	SQLCMD	ETEK_ID\ru...	51	2019-03-20 14:01:32...		Decrypt	ccEngine
Object:Deleted		5792	SQLCMD	ETEK_ID\ru...	51	2019-03-20 14:01:32...		Decrypt	ccEngine
SP:StmtStarting	ALTER PROCEDURE [dbo].[eeeChangeEnc...	9624	SQLCMD	ETEK_ID\ru...	51	2019-03-20 14:01:36...		eeeChan...	rlCustome...

Note that the TextData is in plaintext, not encrypted. It can be seen that objects are being dropped and created.

To satisfy the PCI logging requirement, you must be able to verify logging of the following seven events:

1. All individual access to cardholder data or related SQL objects through the payment application.
2. Actions taken by any individual with administrative privileges to the payment application.
3. Access to audit trails managed by or within the payment application.
4. Invalid logical access attempts.
5. Use of payment application's identification and authentication mechanisms.
6. Initialization of application audit logs.
7. Creation and deletion of system-level objects within or by the application.

Note: Of the seven items listed above, only item 1 is tracked in SQL trace files found in C:\EEETechnologies\EEETrace. **Tracking of items 2 – 7 is your responsibility and must be performed by your own means**. **See the *Event logging guidance* section below for additional information on tracking these items.**

At minimum, OneTouch® Suite identifies the following for each of the above:

- Individual causing event
- Event type
- Event date and time
- Event success or failure
- Component on which event occurred
- Components or data affected by event

Because OneTouch® Suite Version 5.33X0.XXXX has predefined database auditing capabilities, you will have no level of customization over the audit output files.

Please note, however, that disabling or subverting the logging function of OneTouch® Suite in any way will result in non-compliance with PCI-DSS. Additionally, OneTouch® Suite owners are advised to have work policies and procedures in place calling for the following prior to system installation:

- Minimum daily review of log files for activity auditing purposes
- Limitation of log file review authority to Administrator account level only
- Timely backup and secure storage of log files

- Timely backup of audit files to a centralized server or media difficult to alter
- Retention of log files for at least one year

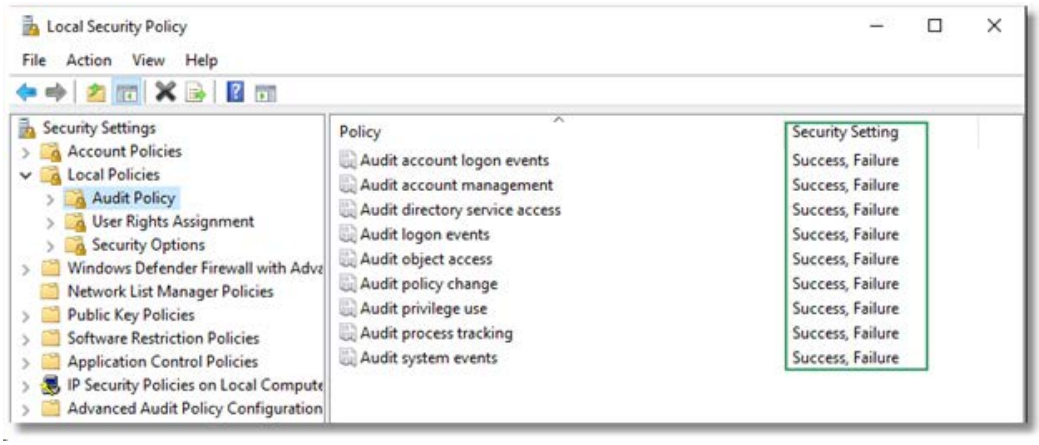
Event logging guidance

Tracking of the following items is your responsibility and must be performed by your own means to satisfy PCI requirements. This section provides guidance on suggested tracking methods.

2. Actions taken by any individual with administrative privileges to the payment application.

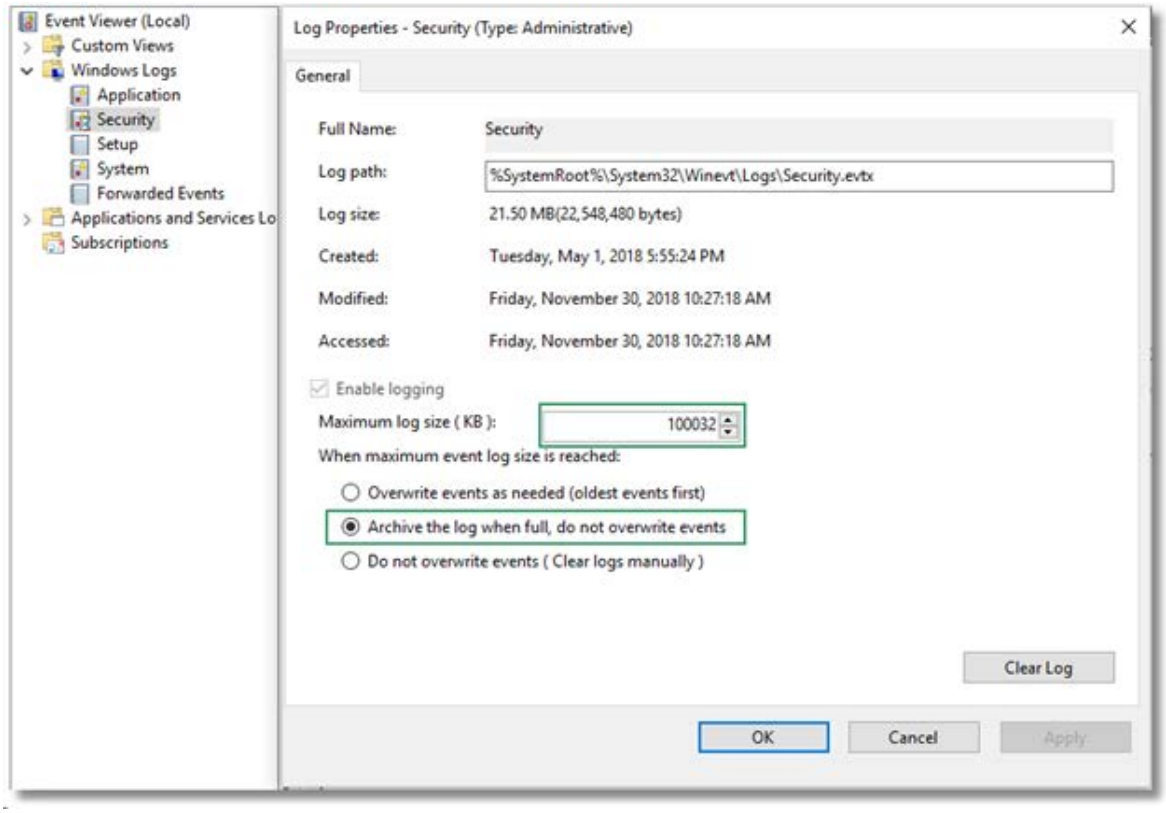
To audit all administrative actions, it is recommended that you use Windows auditing policies:

- On the **Start** menu, type **secpol.msc**, then press **Enter**.
- Navigate to **Local Policies** > **Audit Policy**.
- Enable auditing for all available policies where both **Successes** and **Failures** are tracked.



In addition to enabling the policies, you will need to ensure that the security log file size is large enough and that automatic archival without overwrite is enabled.

- In the **Event Viewer**, enter a **Maximum log size** (e.g., less than 100mb per file).
- Select the **Archive the log when full, do not overwrite events** radio button.
- Click **OK** to save changes.



Note: Enabling administrative auditing can generate a substantial amount of files, so it is recommended that you create a plan for moving files to your centralized log server to avoid disk space issues.

3. Access to all audit trails

Logs are not accessed through the OneTouch Suite application. You will need to monitor file and folder access to audit trails via third-party tools not supplied by OneTouch Suite.

Important logs and their locations are listed below:

- **Trace logs**: C:\EEETechnologies\EEETrace
- **Windows security event logs, others**: C:\Windows\System32\winevt\Logs
- **Application logs**: C:\EEETechnologies\OneTouchLogs and C:\EEETechnologies\SavedLogs

4. Invalid logical access attempts:

The available OneTouch Suite menu options vary by user group – for example, only PCI Group and Administrator Group users will be able to access the change encryption key function; this option is not visible or accessible for the Manager/User groups. Any other access failures or errors will be raised as program exceptions and will be written to an error log.

Additionally, the OneTouch Suite application uses the Windows operating system for login authentication, so there are not records of invalid access attempts within the application itself. You will need to access the Windows Event Viewer to find logs for these kinds of failures.

5. Use of payment application's identification and authentication mechanisms

The OneTouch Suite application is not responsible for user management and authentication. You will need to use the Windows user account management and auditing features.

It is recommended that you use Windows resources regarding account management and configuring security audit policy settings.

6. Initialization, stopping, or pausing of the audit logs

Trace logging is automatically enabled when the SQL Server starts, and application error logging is automatic and can't be started/stopped. An entry is automatically recorded to C:\EEETechnologies\EEETrace with an event class of 'Trace Start' when tracing starts.

Logs cannot be initialized, stopped, or paused outside of this process.

7. Creation and deletion of system-level objects within or by the application

The OneTouch Suite application does not create or delete system level objects. It is your responsibility to implement logging for these objects – this is usually done through file integrity monitoring packaging.

Securely Implementing Wireless Technology

Testing wireless security systems and processes

Red River Software / Triple E Technologies supports the use of OneTouch® Suite over a wireless network on the Vanguard Mobile POS. OneTouch® Suite uses the secure encryption methods specified in the Protecting Cardholder Data section of this document to transmit cardholder data over a wireless network.

Wireless access on the Vanguard Mobile POS is managed via the built-in Windows 10 Wi-Fi. The Vanguard Mobile POS must always have a wireless connection in order to function in both docked and undocked modes. It is recommended that users set up a strong router near the tablet docking station for the best connection.

System owners using the wireless functionality of OneTouch® Suite are required to provide security assessments for data loss or intrusion due to wireless technology implementation (PCI-DSS Requirements 1.2.3, 2.1.1 and 4.1.1). In this regard:

1. Install and configure perimeter firewalls between wireless networks and systems that store credit card data per PCI Requirement 1.2.3. Configure such firewalls to block all traffic except that required for business operation and authorized traffic between the wireless environment and the cardholder data environment.
2. Do not implement Wired Equivalent Privacy (WEP) key-exchange.
3. Per PCI Requirement 2.1.1, change all security-related wireless vendor defaults and settings as follows:

    - Change Default Service Set Identifier (SSID)
    - Disable SSID broadcasts
    - Change default passwords
    - Change default encryption keys
    - Change SNMP community strings
    - Change other security-related wireless defaults
    - Enable WIFI protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable

4. Encrypt wireless transmissions of cardholder data using industry best practices for authentication and transmission. Never rely on Wired Equivalent Privacy (WEP) to protect confidentiality and access to a wireless LAN. Change encryption keys at least annually and whenever deemed necessary or prudent because of actual or suspected security compromise. Change encryption keys whenever anyone with knowledge of them changes positions or leaves the company.
5. Ensure firmware for any wireless device communicating with OneTouch® Suite is updated to use strong encryption algorithms for authentication and transmission.

Delivering PCI Compliant Software Updates

As a software development company, Triple E Technologies must keep current with security concerns and vulnerabilities affecting our area of responsibility and expertise. We do this by subscribing to relevant data feeds and news services that inform us of potential security issues.

We recommend that your Windows server be maintained automatically by using Microsoft's automatic update service to download security patches as they become available. If we identify a relevant vulnerability not covered by these automatic updates, we work to develop and test a patch to protect OneTouch® Suite and using merchants against the new vulnerability and strive to publish a patch within thirty days of vulnerability identification. We then contact merchants to notify them of the availability of the patch via our secure AutoUpdater service. Typically, merchants are expected to respond quickly and install the patch within thirty days of receipt. In all cases, merchants should contact Red River Software / Triple E Technologies for assistance when applying updates and patches and to validate the authenticity of a software patch.

For receiving updates via remote access, use a personal firewall product to secure these "always-on" connections, per PCI Data Security Standard 1.3.10. Please see **Building And Maintaining A Secure Network** section (above) for description of how we recommend your high-speed connection be secured using two-factor authentication.

Release notes for software updates are available on our website.