SecurePOS™
Implementation Guide

Version 1.4 (March 20, 2013)

SecureNet
Payment Systems

STEPS TO ENSURE THAT YOUR POS SYSTEM IS SECURE

About the PCI Security Standards

The Payment Card Industry (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 Data Security Standard (DSS)
- Payment Application Data Security Standard (PA-DSS)
- 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.

This is a set of rules and requirements that when followed will help prevent fraud, hacking, and other threats to private cardholder data. The main objectives of the PCI DSS are as follows:

Build and Maintain a Secure Network

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

Protect Cardholder Data

- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an Information Security Policy

- Maintain a policy that addresses information security

You can find and review the complete specification by visiting the URL below.

https://www.pcisecuritystandards.org/documents/pa-dss_v2.pdf

This guide is intended to help merchants implement the SecureNet's applications in a way that is compliant with version 2.0 of the PCI DSS.

IMPLEMENTATION

Implementing Your Point of Sale - SecurePOS Securely

Of the PA-DSS and PCI DSS criteria that determine the security level and ultimate compliance of your POS system, six areas stand out as requiring particularly close attention:

- Storing card data
- User management
- Logging
- Wireless network considerations
- Remote access
- Encryption over public networks.

Systems Requirements

SecurePOS requires the following:

1. 1GB free space for installation
2. Windows XP/Vista (32 & 64 bit)/Window 7 (32 & 64 bit)
3. .NET Framework 3.5 with Service Pack 1 or newer
4. Devices requiring a driver must be installed with the manufacturer's driver that is compatible with the merchant's operating system/windows based computer configuration.
5. 2GB of memory is required

NOTE: Any previous version of similar software must be uninstalled, your firewall rules may need to be changed, and you will need administrator privileges to download executable files.

Antivirus and Spyware Detection Software

SecureNet considers it mandatory that SecurePOS users have current and up-to-date antivirus and spyware detection software on the workstation.

NOTE: Some of these software packages require SecurePOS to be trusted to allow access to the gateway.

Storing Sensitive Card Data

SecurePOS will never store sensitive card data. There are no debugging or troubleshooting settings that permit sensitive data to be stored. Storing sensitive card data through alternate means should be avoided whenever possible to avoid risk of theft and to minimize PCI compliance requirements. If you must store sensitive card data for a valid business reason, you must ensure you're not storing information deemed prohibited for storage by PCI such as full magnetic stripe, CVV2 or PIN data. If you are storing full account numbers, the card data must be properly encrypted and protected as defined by the PCI Data Security Standard.

Encrypt Sensitive Traffic over Public Networks

SecurePOS uses the SecureNet Gateway to send transactions containing card data over the internet to our servers for payment processing. The transmission is encrypted using SSL, an approved strong encryption protocol.

Attempting to send sensitive card data through alternate means should be avoided whenever possible to avoid risk of theft and to minimize PCI compliance requirements. If you must send sensitive card data for a valid business reason, you must ensure you're sending it encrypted using secure encryption transmission technology (e.g. IPSEC, VPN, and SSL/TLS).

Remote Access

SecurePOS does not require the use of remote access or any other form of remote administration (e.g. Telnet).

If you use an alternate administration interface over the network (e.g. administrative web page, telnet) to access your payment processing environment, the traffic must be encrypted with a secure encryption technology (e.g. SSH, VPN, or SSL/TLS) to maintain PCI DSS compliance.

If you require the use of traditional remote computer or network access, it must meet the following requirements to maintain PCI DSS compliance.

- Do not use remote access solutions requiring "port forwarding" such as VNC and PCAnywhere.
- Incorporate two-factor authentication for remote access. Use technologies such as RADIUS, TACACS with tokens, or VPN with individual certificates assigned to each user.
- Develop usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:

- — Explicit management approval
- — Authentication for use of the technology
- — A list of all such devices and personnel with access
- — Labeling of devices with owner, contact information, and purpose
- — Acceptable uses of the technology
- — Acceptable network locations for the technologies
- — List of company-approved products
- — Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity
- — Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use
- — When accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media

- ■ If vendors, resellers/integrators, or customers can access customers' payment applications remotely, the remote access must be implemented securely

Examples of remote access security features include:

- ■ 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 addresses
- ■ Use strong authentication and complex passwords for logins. Refer to PCI DSS requirements 8.1, 8.3, and 8.5.8–8.5.15
- ■ Enable encrypted data transmission according to PCI DSS requirement 4.1
- ■ Enable account lockout after a certain number of failed login attempts according to PCI DSS requirement 8.5.13
- ■ Configure the system so a remote user must establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed
- ■ Enable logging functions
- ■ 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

Transport Encryption

The PCI DSS requires the use of strong cryptography and encryption techniques with at least a 128 bit encryption strength (either at the transport layer with SSL or IPSEC; or at the data layer with algorithms such as RSA or Triple-DES) to safeguard sensitive cardholder data during transmission over public networks (this includes the Internet and Internet accessible DMZ network segments). Additionally, PCI requires that cardholder information is never sent via email without strong encryption of the data. SecurePOS does not transmit full credit card information via email and when properly installed, SecurePOS uses a minimum of 128 bit encryption with an SSL certificate meeting both of these requirements.

Wireless Networks

SecurePOS does not require the use of a wireless network and SecureNet advises against using one. If you set up or have a preexisting wireless network, take the following precautions to remain PCI compliant.

- If the wireless network is not used by your payment processing systems, make sure that a firewall prevents access to the payment processing systems.
- Wireless networks attached to your payment processing network MUST meet the following PCI DSS requirements:
  - As of April 1, 2009, all newly deployed wireless networks must be using WPA or WPA2 encryption.
  - Existing wireless setups must use WPA or WPA2 encryption when it’s an available option. Some older wireless equipment lack WPA support, but almost all can be updated through firmware and driver updates made available on the manufacturer’s web-site.
  - In the rare case when there are no available updates from the manufacturer that add WPA or WPA2 support, WEP must be used. Those devices must be replaced with newer equipment and the encryption changed from WEP to WPA or WPA2 encryption by July 1, 2010.
  - The default WPA/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.
  - Synchronize the access points’ clocks to be the same as your computers to ensure logged timestamps match.
  - The firmware on wireless devices must be updated and maintained to support strong encryption for authentication and transmission.
  - Encryption keys must be changed anytime anyone with knowledge of the keys leaves the company or changes positions.
- Wireless networks attached to your payment processing network are HIGHLY RECOMMENDED to enable additional security:
  - Do not wait for the July 2010 deadline to update from WEP to WPA. WEP is extremely insecure. Easy to use tools are readily available that only take minutes to discover the WEP key. These tools have been employed for the last several years by criminals to access business networks, leading to several data breaches.
  - 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.
  - Disable SSID Broadcast to make your wireless network less visible to unauthorized users.
  - Use MAC address filtering so that only authorized computers are allowed access to the wireless network.
  - When configuring WPA or 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, and wireless access points, 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 cost up to $70,000, 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 are 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 will almost certainly 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 risk 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 high risk activities such as web browsing and email do not occur inside it. The chance that hackers, malware, or viruses spread to these systems is minimal.

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

1. Protect both business environments from the untrusted environment
2. Protect your card data business environment from the non card business environment

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

User Management

SecurePOS when first installed uses your SecureNet Virtual Terminal login credentials. When a user first logs in she/he is prompted to add the SecureKey which can be found on Virtual Terminal.

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 with anyone else.

It is highly recommended to disable or delete 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.

The following requirements apply to all user accounts and are for PA-DSS compliance and automatically maintained by SecurePOS.

- Passwords are case-sensitive
- Passwords must contain 8 to 12 characters
- Passwords must contain at least:
  - One upper case letter
  - One lower case letter
  - One number
  - One of the following special characters (` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /)
- Passwords may not contain spaces
- Passwords may not contain the user ID
- Users are required to change their password every 90 days*
- Users with administrator access are required to change their password every 45 days
- The last five registered passwords cannot be reused

Additionally, Windows accounts should be configured to meet these secure authentication requirements for PCI DSS compliance.

Audit Settings

For PA-DSS compliance, SecurePOS components must have access controls applied so that only authorized users can modify them. SecureNet recommends enabling audit settings on the installation directory of SecurePOS. See Appendix B.

Logging

Within SecureNet's Environment

SecurePOS transactions are logged on SecureNet's PCI DSS compliant Gateway when transactions enter the system. All logs are stored securely in SecureNet's PCI DSS compliant environment and reviewed for exceptions, unusual activity or for investigation purposes on a daily basis.

Within the Merchant's Environment

For compliance with PCI PA-DSS, SecurePOS creates logs containing system and application level events for review and use. When configuring SecurePOS, these logs must be enabled at all times and incorporated into a centralized logging server. Disabling the logs will result in non-compliance with PCI PA DSS.

SecurePOS logs are written to UDP port 514 (a native SysLog) port and using a software solution, can be incorporated into a centralized logging server. Refer to Appendix C for SecureNet's instructions to meet this requirement.

Logs must be reviewed at least daily and follow-up required on any exceptions identified. Also, the logs need to be retained for a least one year, with a minimum of three months immediately available for analysis.

Recommendations

This document contains only recommendations. Merchants are responsible for implementing their own PA PCI DSS compliant environment. The purpose of this document is to assist you in your implementation by providing sufficient information regarding the installation, configuration, and operation of SecurePOS to help in your PCI compliance efforts.

Scope and Target Audience

This guide covers SecurePOS and is intended for merchant's who wish to implement SecurePOS in accordance with guidelines set forth by the PCI.

Version Management

SecurePOS Version Management

SecurePOS version can be identified from the **"About SecurePOS"** under help menu.

It comprises of 4 digits A.B.C.D:

- A—Refers to a major version
- B—Refers to a minor version
- C—Refers to bug fixes and minor changes
- D—Minor changes to non-transactional functions

Major Version (A): This number will be incremented if the application has a major change in functionality and process flows and new addition of major features.

Minor Version (B): This number will be incremented if the application has a minor change in functionality and additional of minor features which does not impact the day to day use.

Bug Fixes (C): This number will be incremented if the any bugs or know issues are fixed within the scope of A and B.

Non-transactional functions (D) This number will be incremented if minor changes are made to non-transactional functions.

Whenever there is a change in the version number, SecurePOS will prompt for application update.

INSTALLATION

- Go to http://spos.securenet.com
- Locate the SecurePOS application on the screen
- Click on Download Executable for the current version of SecurePOS

NOTE: You may Run or Save the application. Depending on which version of Windows you are using and your PC environment the procedures to install SecurePOS may vary. Carefully read all prompts thoroughly during the downloading process. Continue through the installation until the SecurePOS Setup Wizard has been completed by clicking Finish.

CARD READER

- Plug in your USB card reader device into a USB port.
- Log into SecurePOS with your username and password.
- Click Settings.
- Click Input Device Settings.
- Select your card reader from the drop down menu.
- Click Save.
- Click Ok.
- SecurePOS will need to restart to enable these changes.
- Click Ok.
- Log back into SecurePOS with your username and password.

RECEIPT PRINTER

Because the version of Windows and your PC environment may vary, it is recommended to follow the installation instructions that were provided with your printer. Additional instructions can be located within the SecurePOS User Guide at http://spos.securenet.com/WebHelp/SPOS_Help.htm

- Log into SecurePOS with your username and password.
- Click the Settings tab.
- Click Application Settings.
- Under the Choose Default Receipt Printer drop down, select your printer.

- Click Save.
- Click Ok.

ADDITIONAL INFORMATION

To view all compatible devices or installation information, please visit http://spos.securenet.com or access the SecurePOS Online User Guide.

SETUP

The following steps should be taken before the merchant begins processing transactions:

CREATE USER ACCOUNT(S)

The username and temporary password are sent to the merchant upon account set up. Because of PCI Compliance the username and password are sent in separate emails. It is strongly recommended that each user have a unique user account.

- Log into the Virtual Terminal with your username and password.
- Click the Settings tab.
- Click Manage Admin and User Access.
- Click Add New User.
- Type in the required fields (First Name, Last Name, Username, and Email Address).
- If you would like this User to have Admin Rights, select the Access Type from the dropdown.
- Check off any emails the user will receive.
- Click Submit.

SETUP SECUREKEY TO AUTOMATICALLY UPDATE

- Log into the Virtual Terminal with your username and password.
- Click the Settings tab.
- Click Manage Admin and User Access.
- Select a user and click the flag icon.
- Click the check box to Allow for SecureKey to be automatically downloaded to SecurePOS application.
- Click Submit.

SETUP SETTLEMENT TIME

The terminal is automatically defaulted to batch out at 10:00PM (EST). Change if necessary.

- Log into the Virtual Terminal with your username and password.
- Click the Settings tab.
- Click Transaction Cut-Off Time.
- Select Manual or Auto Settle option.
- If you select Auto Settle, you will also need to select the Batch Cut-Off Time.
- Click Ok.

SETUP TIME - OUTSETTING

- Log into SecurePOS with your username and password.
- Click the Settings tab.
- Click Applications Settings.
- Click the Additional Settings tab within the Application Settings box.
- Under the Idle Time Out Settings, change the number of minutes to meet your business requirements. If the idle time out settings are increased over 15 minutes, the SecurePOS application will no longer be PCI-DSS compliant.
- Click Save.
- Click Ok.

ADDITIONAL APPLICATION SETTINGS

Merchants who process transactions using SecurePOS can access a range of settings that are beneficial to their business needs. We offer merchants the capability to customize receipts, include comment lines, create a customized prompt, and add a logo to their receipt. For more details, please refer to the SecurePOS Online User Guide at http://spos.securenet.com.

BASIC TRANSACTIONS

SALE TRANSACTION

- When logged into SecurePOS, click on the Sale tab.
- Swipe the credit card or manually enter the full credit card number and expiration date.
- Type in the Amount.
- Click Process.

NOTE: A message will be displayed in the Transaction Result box.

Restaurant merchants can click Print Receipt to provide the receipt to the customer to enter in the tip amount and total. Once the receipt is retrieved, the transaction must be captured to include the tip amount. Please go to the section labeled Capture of the user guide.

REFUND TRANSACTION

- When logged into SecurePOS, click on the Refund tab.
- Swipe the credit card or manually enter the full credit card number and expiration date.
- Type in the Amount.
- Type in the Transaction ID
- Click Process.

NOTE: A message will be displayed in the Transaction Result box.

VOID

- When logged in, click the Void tab.
- Type in the Transaction ID
- Click Look up.
- The last four digits of the credit card number, expiration date, and amount of the original transaction will appear.
- Click Process.

NOTE: A message will be displayed in the Transaction Result box.

CAPTURE

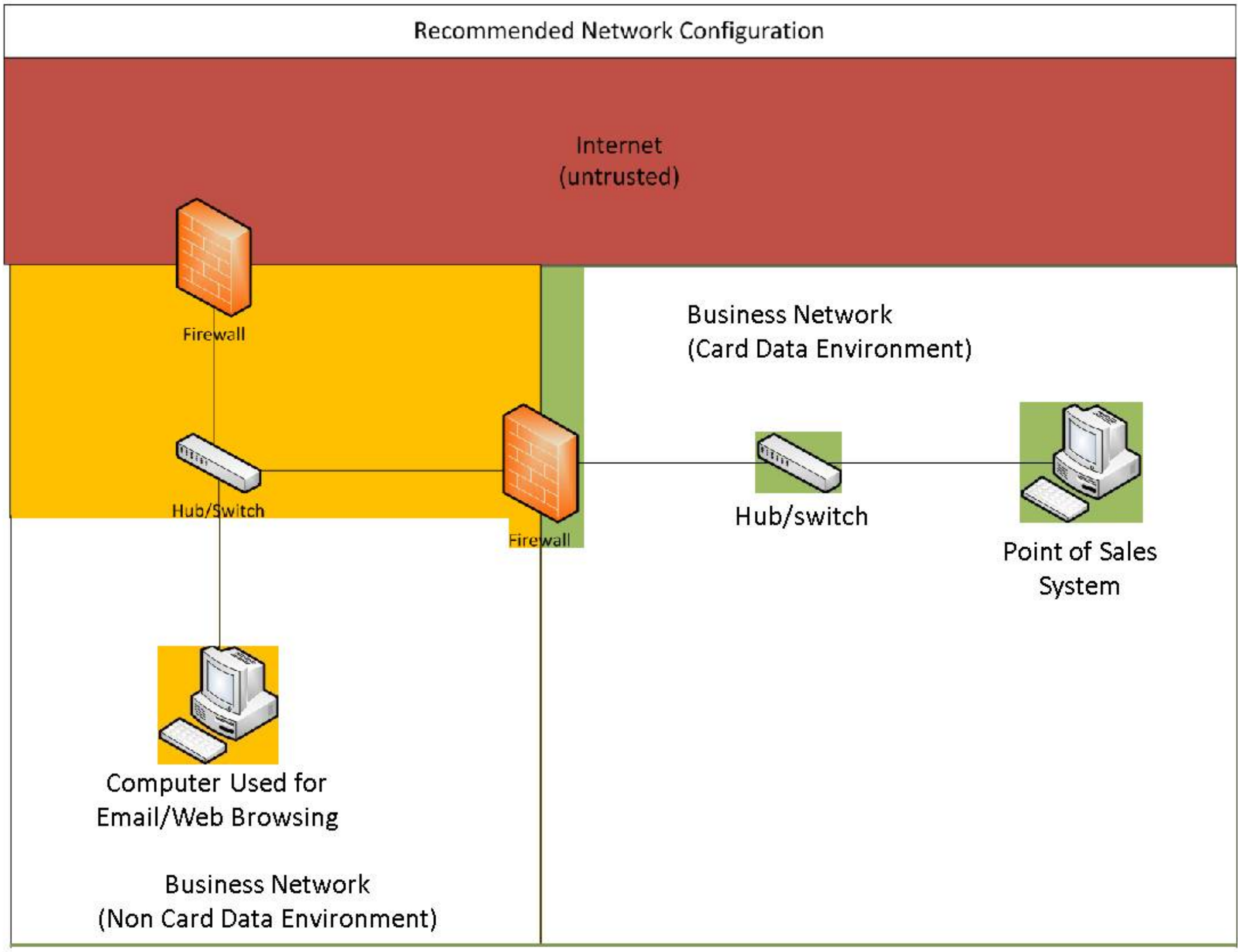
- When logged into SecurePOS, click on the Capture tab.
- Type in the Transaction ID
- Click Look up.
- The last four digits of the credit card number, expiration date, and amount of the original transaction will appear.
    - Restaurant merchants may need to key in the tip amount written on the signed receipt and SecurePOS will recalculate the total.
- Click Process.

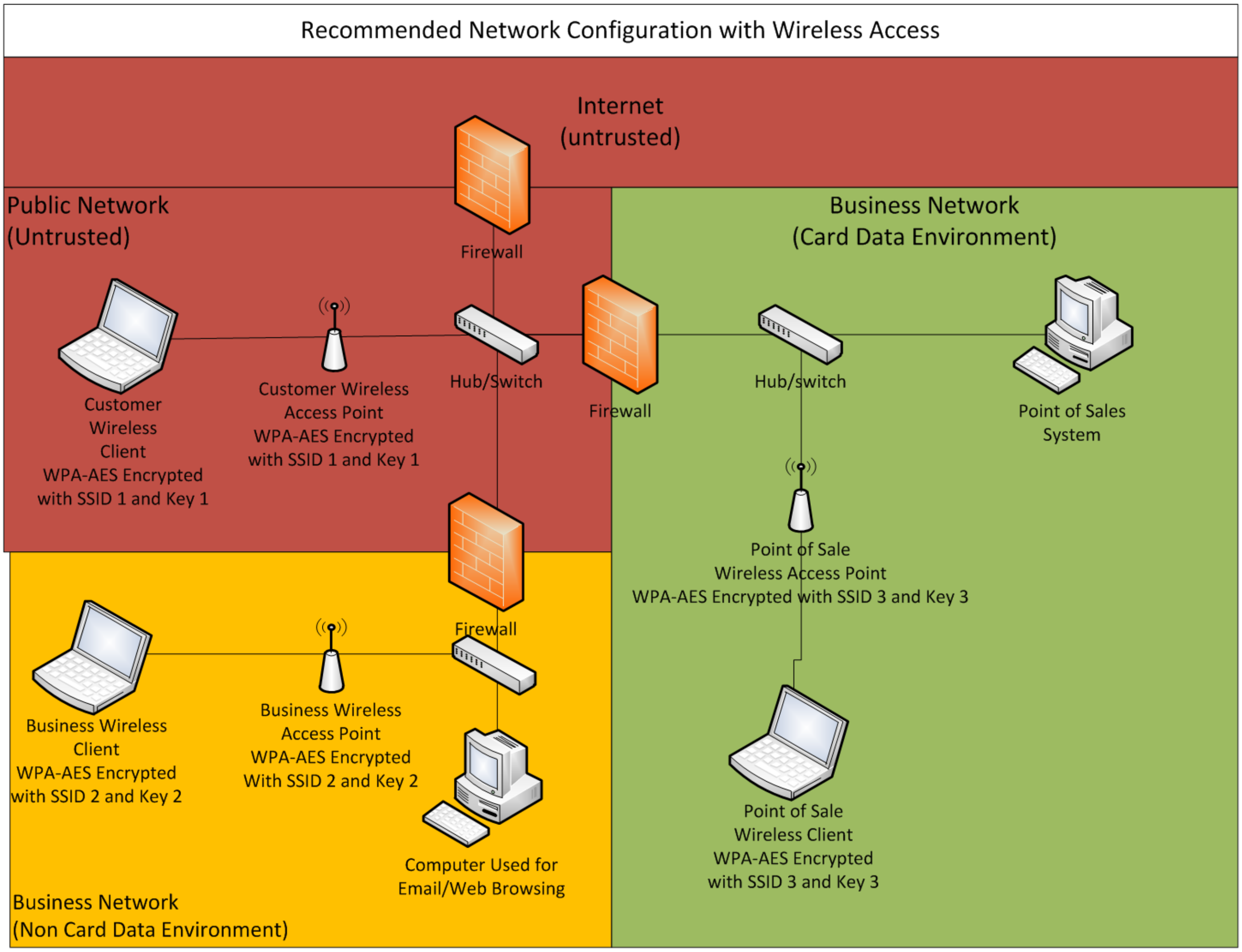
NOTE: A message will be displayed in the Transaction Result box.

ADDITIONAL INFORMATION

The SecurePOS Quick Reference Guide is the simplest way to learn how to process transactions in a retail and restaurant environment. Depending on the device(s) connected to the software application, how a merchant processes a transaction may differ slightly. For exact details on how to run a transaction while using a particular device, please visit http://spos.securenet.com or refer to the SecurePOS User Guide online.

Appendix A: Recommended Network Configurations



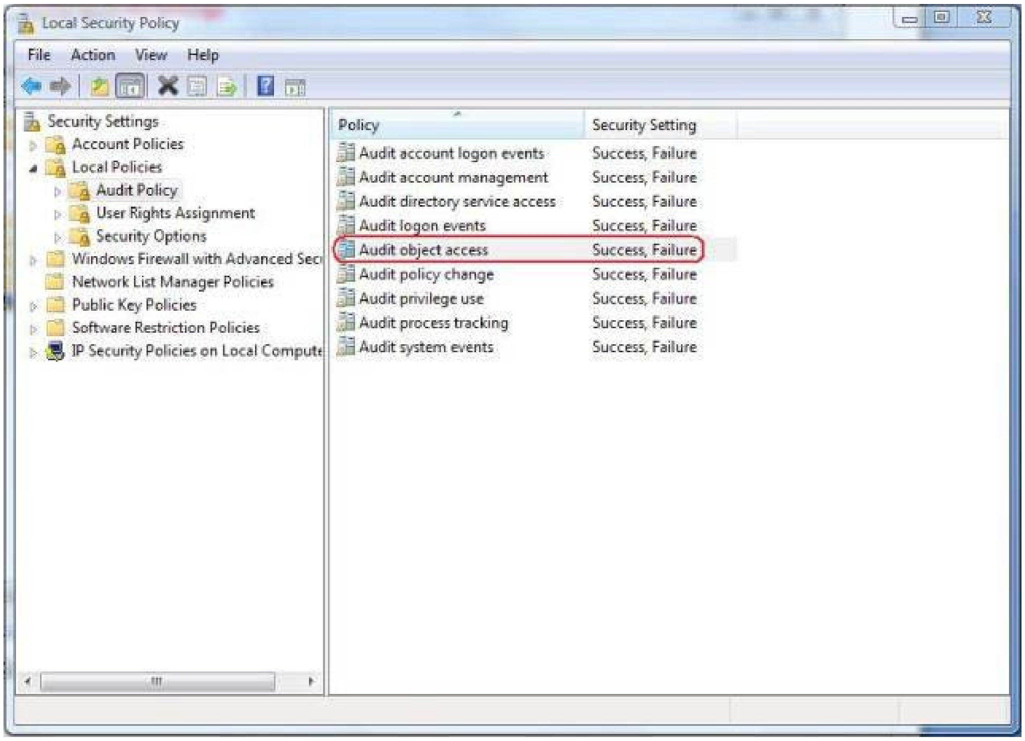

Recommended Network Configuration with Wireless Access
Internet
(untrusted)
Public Network
(Untrusted)
Firewall
Business Network
(Card Data Environment)
Customer
Wireless
Client
WPA-AES Encrypted
with SSID 1 and Key 1
Customer Wireless
Access Point
WPA-AES Encrypted
with SSID 1 and Key 1
Hub/Switch
Firewall
Hub/switch
Point of Sales
System
Point of Sale
Wireless Access Point
WPA-AES Encrypted with SSID 3 and Key 3
Firewall
Business Wireless
Client
WPA-AES Encrypted
with SSID 2 and Key 2
Business Wireless
Access Point
WPA-AES Encrypted
With SSID 2 and Key 2
Computer Used for
Email/Web Browsing
Point of Sale
Wireless Client
WPA-AES Encrypted
with SSID 3 and Key 3
Business Network
(Non Card Data Environment)

Appendix B: Enabling Audit Settings

This demo was installed in the Windows Vista operating system environment. The actual screen images seen during installation may be different from the screen shots shown.

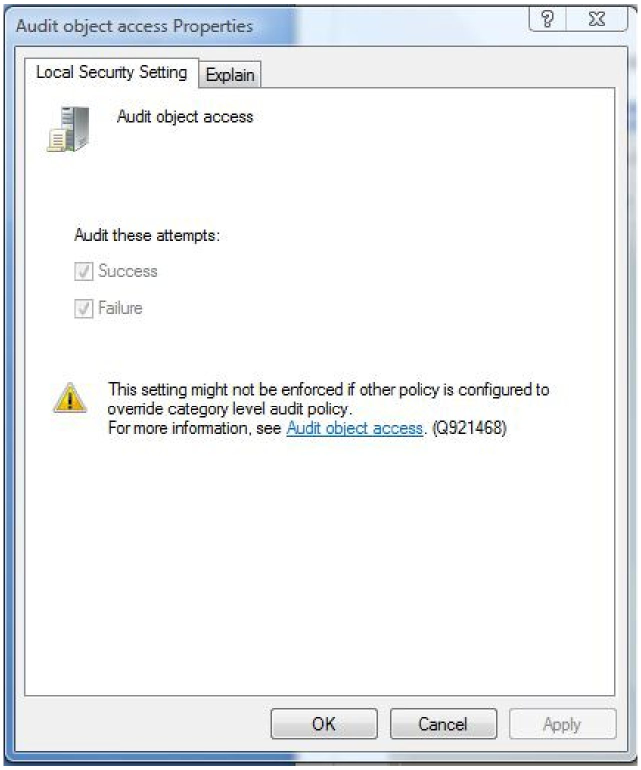
Step 1: From the desktop, click the Start Menu, type "secpol.msc" in the Start Search data field and click the "Local Security Policy" under Programs.

Step 2: Double-click "Local Policies", double-click "Audit Policy", and double-click "Audit object access" in the right side of the window



Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Success, Failure
Audit system events	Success, Failure

Step 3: Verify success and failure are selected and click "OK".



Audit object access

Audit these attempts:

☑ Success

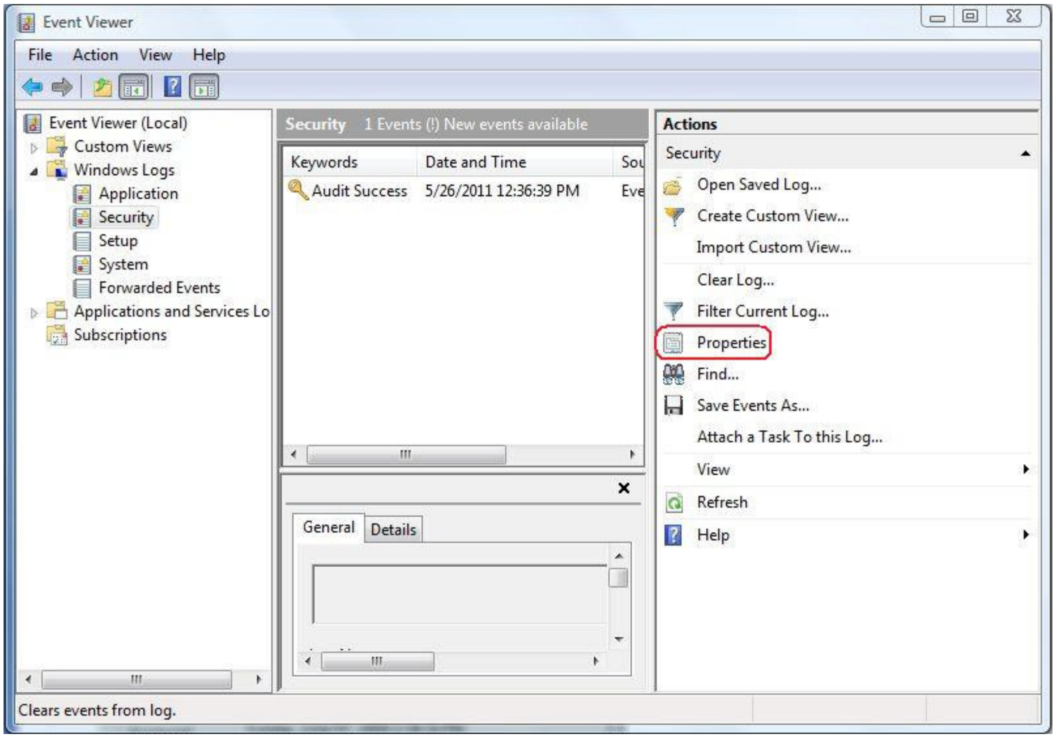
☑ Failure

This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit object access. (Q921468)

Step 4: Close the Local Security Policy window.

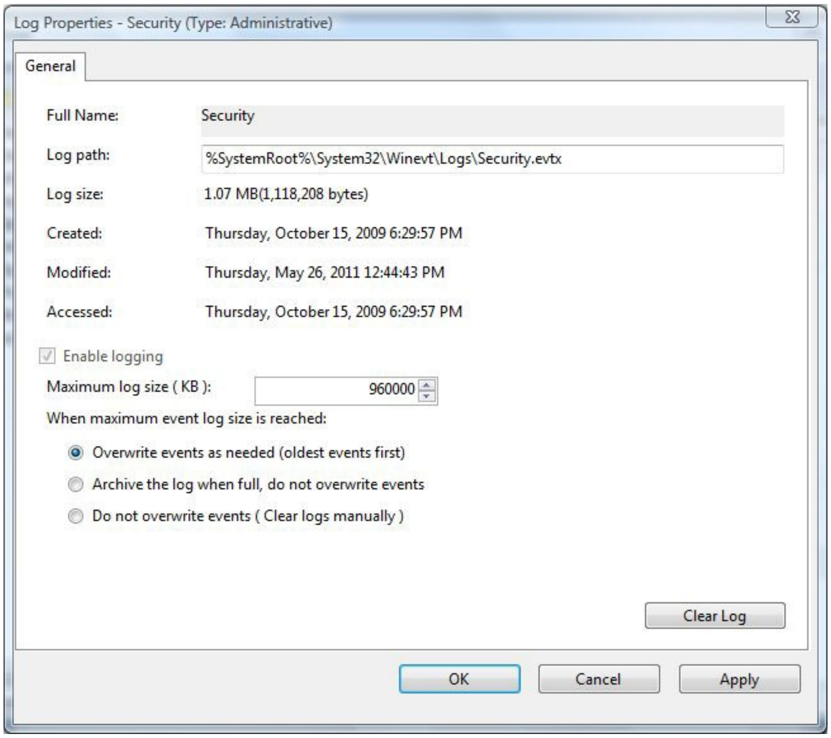
Step 5: From the desktop, click the “Start Menu”, type “eventvwr.msc” in the Start Search data field.

Step 7: In the Actions column, double-click on properties.



Step 8: Change the maximum log size to 960,000 KB, select "Overwrite events as needed (oldest events first)" and click "OK".

Step 9: Close the Event Viewer window.



Log Properties - Security (Type: Administrative)

General

Full Name: Security

Log path: %SystemRoot%\System32\Winevt\Logs\Security.evtx

Log size: 1.07 MB(1,118,208 bytes)

Created: Thursday, October 15, 2009 6:29:57 PM

Modified: Thursday, May 26, 2011 12:44:43 PM

Accessed: Thursday, October 15, 2009 6:29:57 PM

☑ Enable logging

Maximum log size (KB): 960000

When maximum event log size is reached:

- ● Overwrite events as needed (oldest events first)
- ○ Archive the log when full, do not overwrite events
- ○ Do not overwrite events (Clear logs manually)

Appendix C: Creating a Centralized Logging Environment

There are various tools available in the marketplace to facilitate creation of a centralized logging environment to comply with the PCI PA DSS requirement. SecureNet has tested Splunk's Splunk software to facilitate centralized logging in SecurePos.

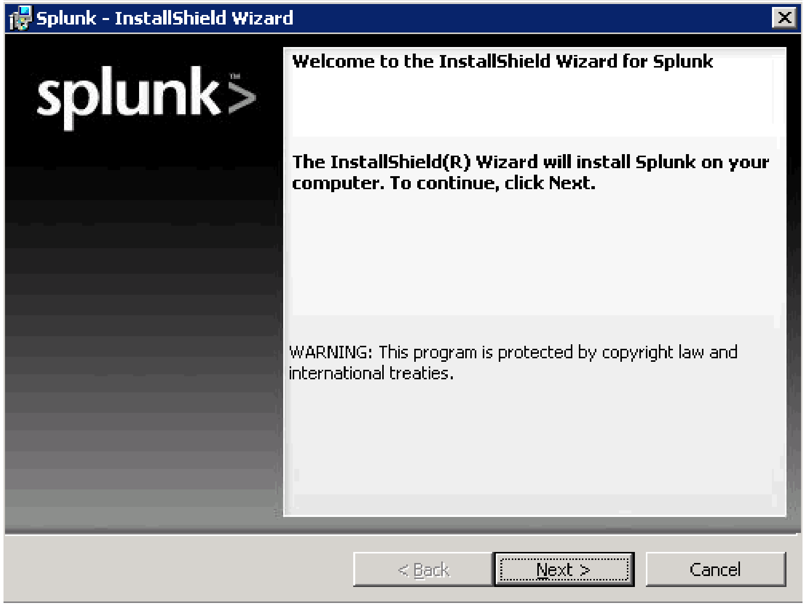
Splunk provides a freeware version of its software which comply with PCI requirements relating to log retention, review, change monitoring and reporting.   The software meets requirememts to collect, retain, search, alert and report and is operates in the environments upon which SecurePOS generates its logs (i.e., Windows XP, Vista (32 and 64 bit) and Windows 7. For training and other assistance, visit:

http://www.splunk.com/services

Instructions for using Splunk to incorporate SecurePOS application logs are included on pages 19 through 26.   Also, refer to Appendix B for the instructions to Enable Audit Settings to create the events stored in the audit logs.

Step 1: Download Splunk software from: http://www.splunk.com

Step 2: Install the Splunk software on your equipment. Click Next to continue to the next screen.



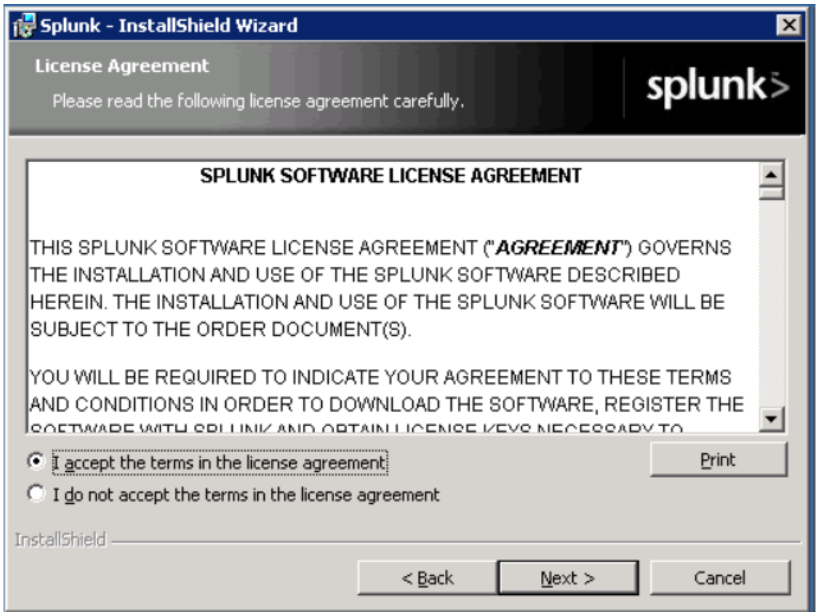
Welcome to the InstallShield Wizard for Splunk

The InstallShield(R) Wizard will install Splunk on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Step 3: Read and Click "I accept the terms in the license Agreement"

Step 4: Select Next to Continue


Splunk - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
splunk>
Print
InstallShield
< Back
Next >
Cancel

SPLUNK SOFTWARE LICENSE AGREEMENT

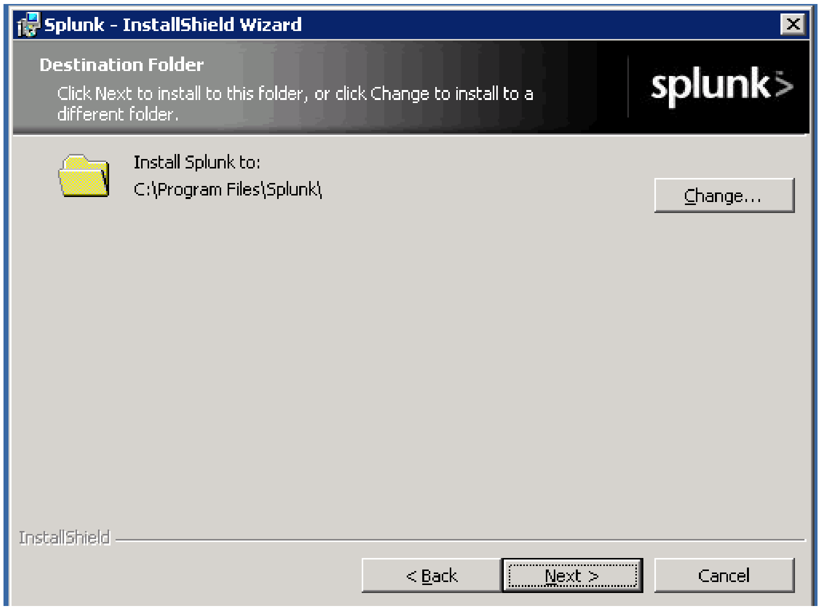
THIS SPLUNK SOFTWARE LICENSE AGREEMENT ("*AGREEMENT*") GOVERNS THE INSTALLATION AND USE OF THE SPLUNK SOFTWARE DESCRIBED HEREIN. THE INSTALLATION AND USE OF THE SPLUNK SOFTWARE WILL BE SUBJECT TO THE ORDER DOCUMENT(S).

YOU WILL BE REQUIRED TO INDICATE YOUR AGREEMENT TO THESE TERMS AND CONDITIONS IN ORDER TO DOWNLOAD THE SOFTWARE, REGISTER THE SOFTWARE WITH SPLUNK AND OBTAIN LICENSE KEYS NECESSARY TO

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Step 5: Click Next to install the Splunk software in the C:\Program Files\Splunk folder



Splunk - InstallShield Wizard

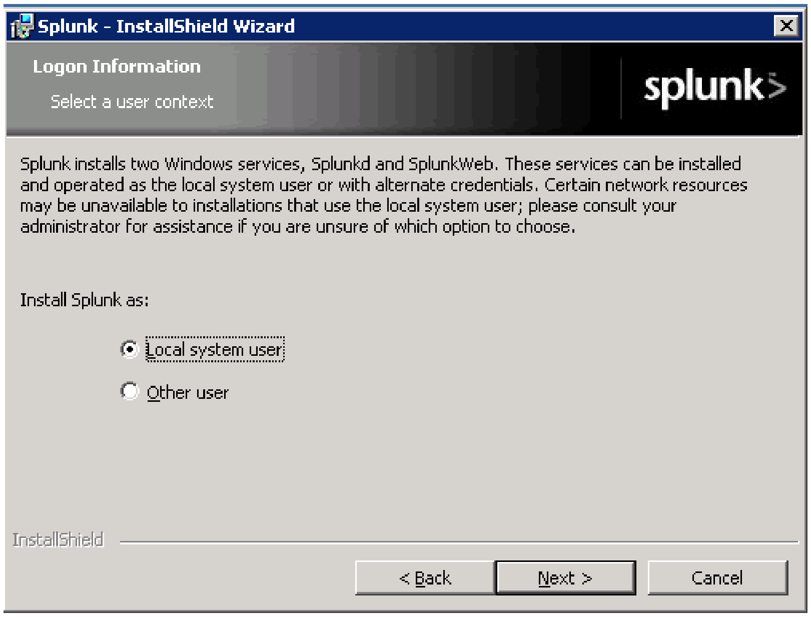
Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install Splunk to:
C:\Program Files\Splunk\

Step 6: Click "Local system user"

Step 7: Select Next to continue



Splunk - InstallShield Wizard

Logon Information

Select a user context

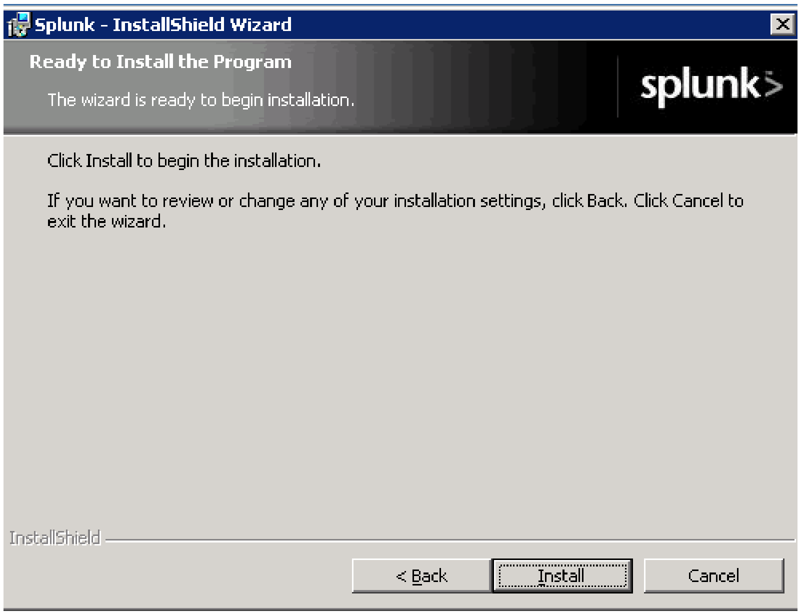
Splunk installs two Windows services, Splunkd and SplunkWeb. These services can be installed and operated as the local system user or with alternate credentials. Certain network resources may be unavailable to installations that use the local system user; please consult your administrator for assistance if you are unsure of which option to choose.

Install Splunk as:

● Local system user

○ Other user

Step 8: Click_Install to begin installation



Splunk - InstallShield Wizard

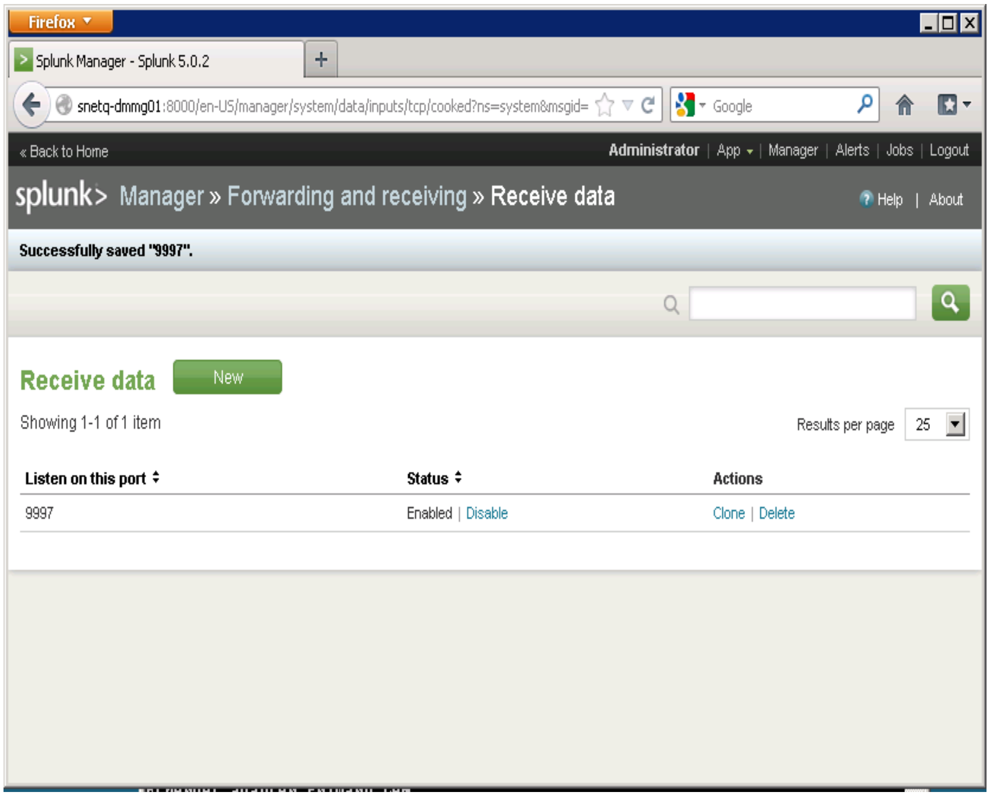
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Step 9: In Splunk Manager, Enable the Index listener at Manager / Forwarding and Receiving / Receive Data 9997



Firefox
Splunk Manager - Splunk 5.0.2
snetq-dmmg01:8000/en-US/manager/system/data/inputs/tcp/cooked?ns=system&msgid=
Google
« Back to Home
Administrator | App | Manager | Alerts | Jobs | Logout
splunk> Manager » Forwarding and receiving » Receive data
Help | About
New

Successfully saved "9997".

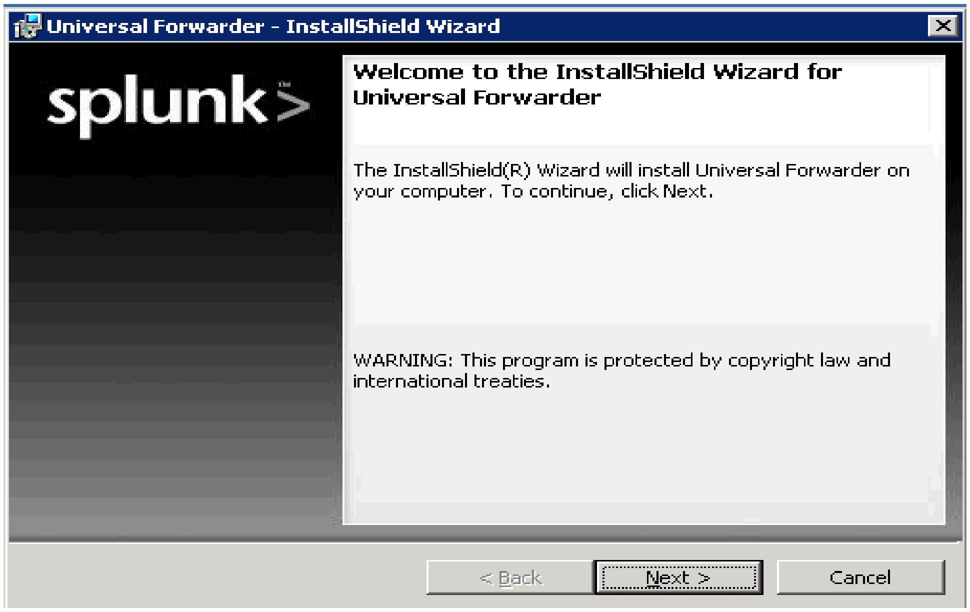
Receive data

Showing 1-1 of 1 item

Results per page 25

Listen on this port	Status	Actions
9997	Enabled | Disable	Clone | Delete

Step 10: Click Next to continue. In the Splunk Universal Forwarder Setup, this software is installed on your SecurePOS web server.



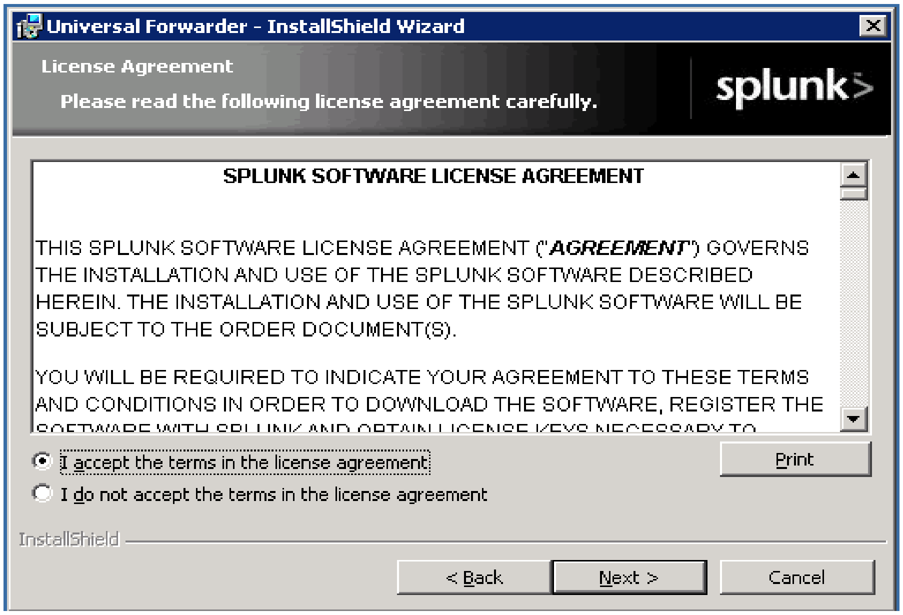
Welcome to the InstallShield Wizard for Universal Forwarder

The InstallShield(R) Wizard will install Universal Forwarder on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Step 11: Click “I accept the terms in the license agreement”

Step 12: Click Next to continue



License Agreement

Please read the following license agreement carefully.

SPLUNK SOFTWARE LICENSE AGREEMENT

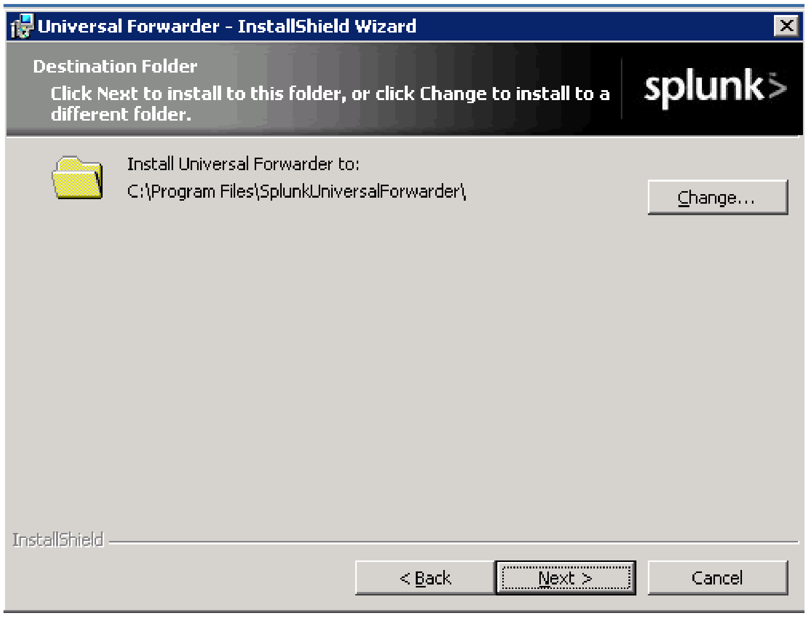
THIS SPLUNK SOFTWARE LICENSE AGREEMENT ("*AGREEMENT*") GOVERNS THE INSTALLATION AND USE OF THE SPLUNK SOFTWARE DESCRIBED HEREIN. THE INSTALLATION AND USE OF THE SPLUNK SOFTWARE WILL BE SUBJECT TO THE ORDER DOCUMENT(S).

YOU WILL BE REQUIRED TO INDICATE YOUR AGREEMENT TO THESE TERMS AND CONDITIONS IN ORDER TO DOWNLOAD THE SOFTWARE, REGISTER THE SOFTWARE WITH SPLUNK AND OBTAIN LICENSE KEYS NECESSARY TO

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Step 13: Click Next to install the software in the C:\Program Files\SpunkUniversalForwarder folder



Universal Forwarder - InstallShield Wizard

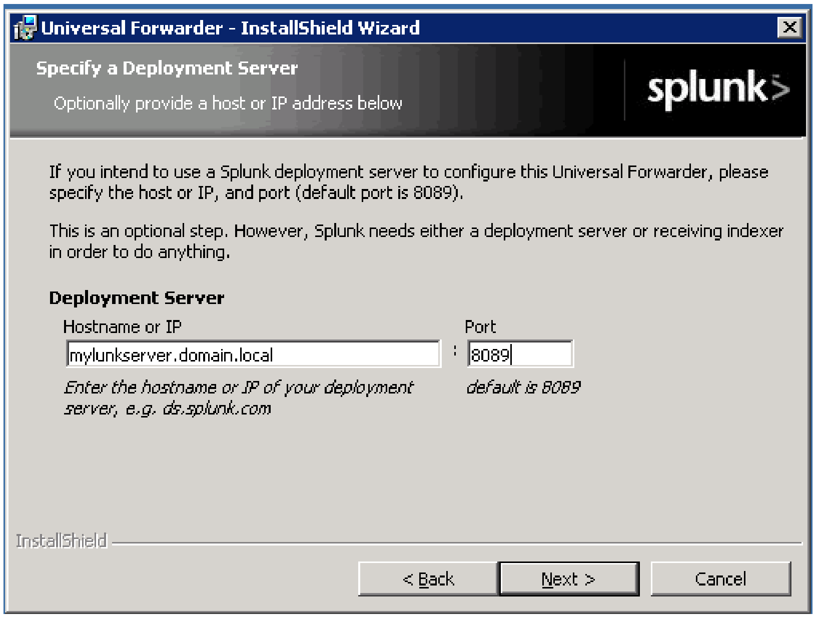
Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install Universal Forwarder to:
C:\Program Files\SplunkUniversalForwarder\

Step 14: Enter the hostname or IP address (of the equipment where SecurePOS is installed) and port 8089

Note: The hostname is included for illustration purposes only



Universal Forwarder - InstallShield Wizard

Specify a Deployment Server

Optionally provide a host or IP address below

If you intend to use a Splunk deployment server to configure this Universal Forwarder, please specify the host or IP, and port (default port is 8089).

This is an optional step. However, Splunk needs either a deployment server or receiving indexer in order to do anything.

Deployment Server

Hostname or IP: mylunkserver.domain.local

Port: 8089

Enter the hostname or IP of your deployment server, e.g. ds.splunk.com

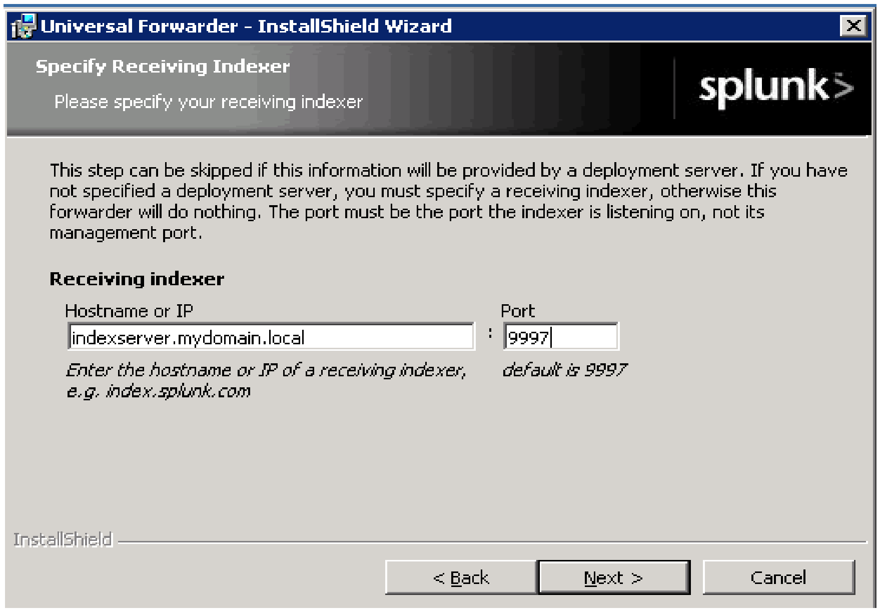
default is 8089

Step 15: Enter the hostname or IP address (of the equipment where SecurePOS is installed) and port 9997.

If the hostname is the same as step 14, do not enter the hostname.

Note: The hostname is included for illustration purposes only

Step 16: Click Next to continue



Universal Forwarder - InstallShield Wizard

Specify Receiving Indexer

Please specify your receiving indexer

This step can be skipped if this information will be provided by a deployment server. If you have not specified a deployment server, you must specify a receiving indexer, otherwise this forwarder will do nothing. The port must be the port the indexer is listening on, not its management port.

Receiving indexer

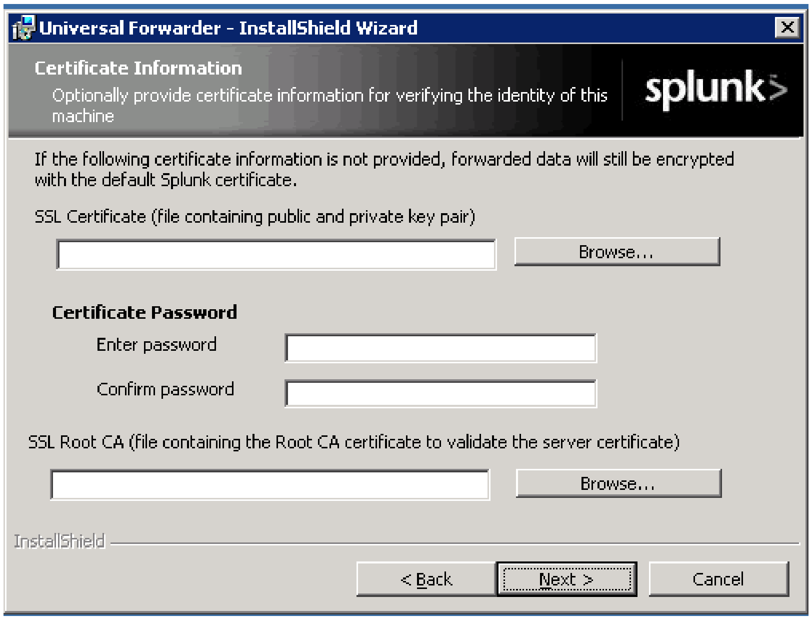
Hostname or IP: indexserver.mydomain.local

Port: 9997

Enter the hostname or IP of a receiving indexer, e.g. index.splunk.com

default is 9997

Step 17: Click Next to continue



Universal Forwarder - InstallShield Wizard

Certificate Information

Optionally provide certificate information for verifying the identity of this machine

If the following certificate information is not provided, forwarded data will still be encrypted with the default Splunk certificate.

SSL Certificate (file containing public and private key pair)

Certificate Password

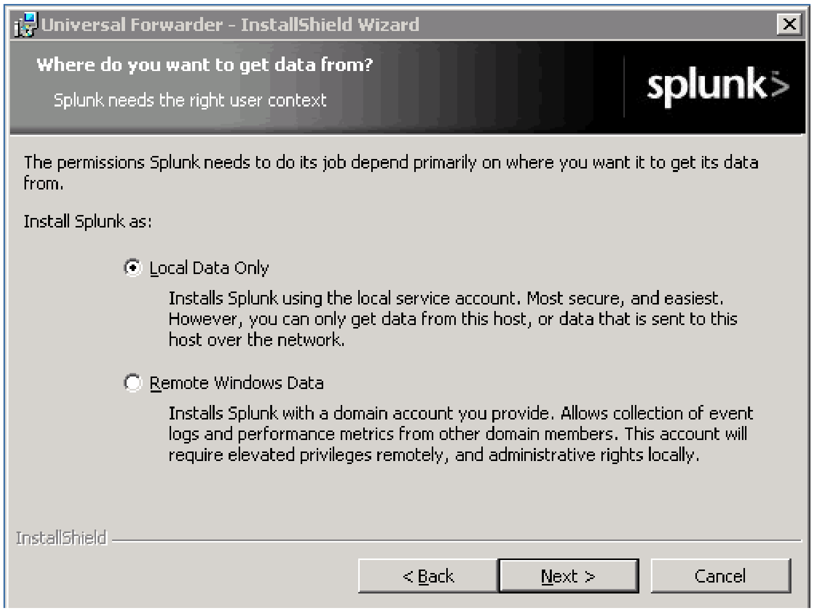
Enter password

Confirm password

SSL Root CA (file containing the Root CA certificate to validate the server certificate)

Step 18: Click “Local Data Only”

Step 19: Click Next to Continue



Universal Forwarder - InstallShield Wizard

Where do you want to get data from?

Splunk needs the right user context

The permissions Splunk needs to do its job depend primarily on where you want it to get its data from.

Install Splunk as:

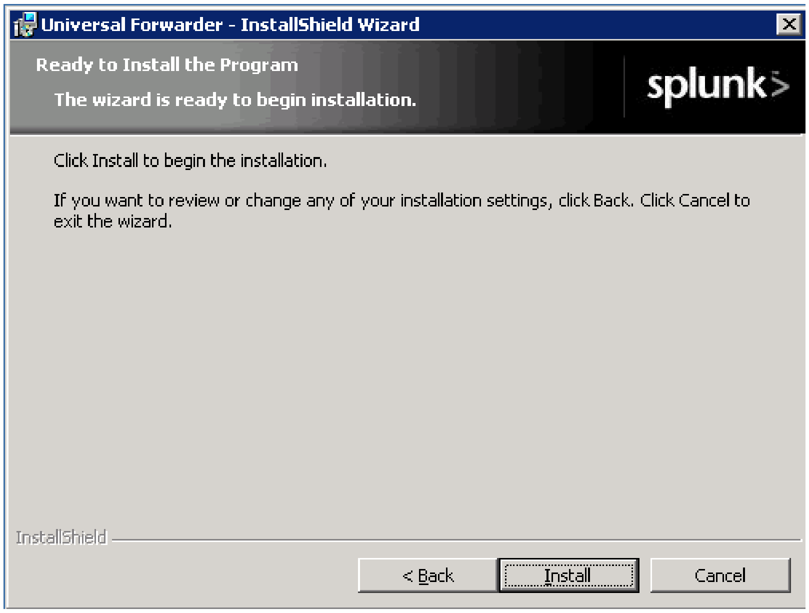
● Local Data Only

Installs Splunk using the local service account. Most secure, and easiest. However, you can only get data from this host, or data that is sent to this host over the network.

○ Remote Windows Data

Installs Splunk with a domain account you provide. Allows collection of event logs and performance metrics from other domain members. This account will require elevated privileges remotely, and administrative rights locally.

Step 20: Click Install to begin the installation



Universal Forwarder - InstallShield Wizard

Ready to Install the Program

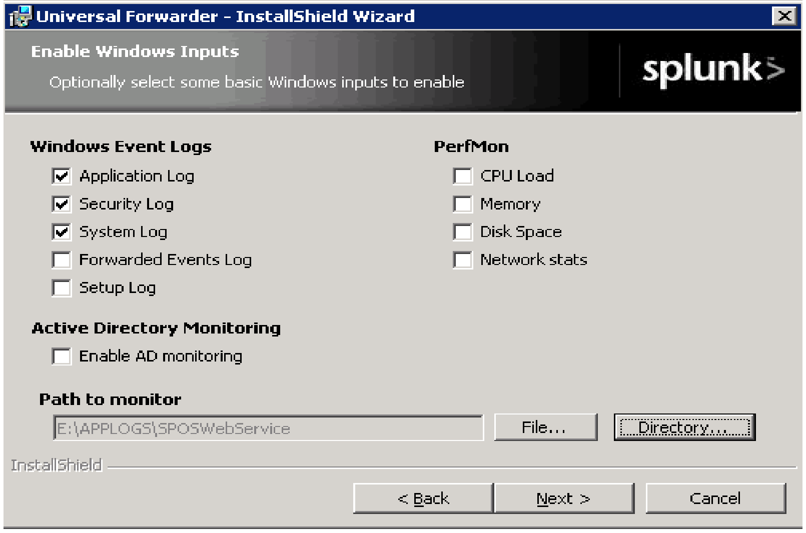
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Step 21: Click Application Log, Security Log and System Log

Step 22: Click Next to Continue



Enable Windows Inputs

Optionally select some basic Windows inputs to enable

Windows Event Logs

- ☑ Application Log
- ☑ Security Log
- ☑ System Log
- ☐ Forwarded Events Log
- ☐ Setup Log

PerfMon

- ☐ CPU Load
- ☐ Memory
- ☐ Disk Space
- ☐ Network stats

Active Directory Monitoring

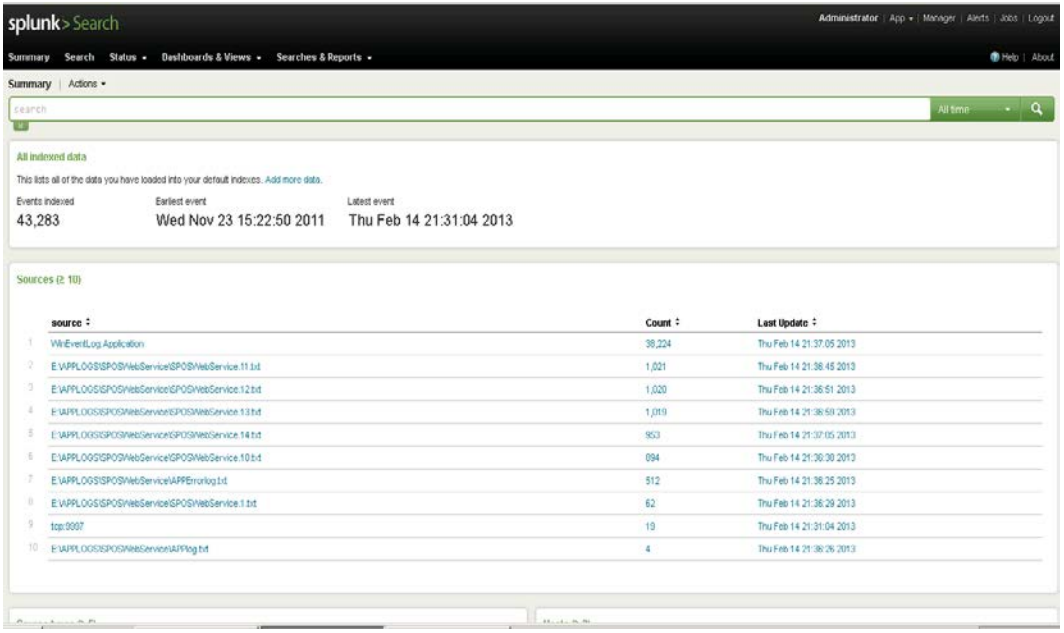
- ☐ Enable AD monitoring

Path to monitor

E:\APPLOGS\SPOSWebService

Step 23: This screen displays the Windows and Applications logs to do various events and incident driven responses.

Step 24: Click on the logs to review the data



All indexed data

This lists all of the data you have loaded into your default indexes. Add more data.

Events indexed	Earliest event	Latest event
43,283	Wed Nov 23 15:22:50 2011	Thu Feb 14 21:31:04 2013

Sources (≥ 10)

	source	Count	Last Update
1	WinEventLog:Application	38,224	Thu Feb 14 21:37:05 2013
2	E:\APPLOGS\SPOSWebService\SPOSWebService.11.txt	1,021	Thu Feb 14 21:38:45 2013
3	E:\APPLOGS\SPOSWebService\SPOSWebService.12.txt	1,020	Thu Feb 14 21:36:51 2013
4	E:\APPLOGS\SPOSWebService\SPOSWebService.13.txt	1,019	Thu Feb 14 21:36:59 2013
5	E:\APPLOGS\SPOSWebService\SPOSWebService.14.txt	953	Thu Feb 14 21:37:05 2013
6	E:\APPLOGS\SPOSWebService\SPOSWebService.10.txt	094	Thu Feb 14 21:36:30 2013
7	E:\APPLOGS\SPOSWebService\APPErrorlog.txt	512	Thu Feb 14 21:38:25 2013
8	E:\APPLOGS\SPOSWebService\SPOSWebService.1.txt	62	Thu Feb 14 21:36:29 2013
9	tcp:9997	19	Thu Feb 14 21:31:04 2013
10	E:\APPLOGS\SPOSWebService\APPlog.txt	4	Thu Feb 14 21:36:26 2013