



**Wolf Track Software, Ltd.
Implementation Guide**

PO Box 1669
515 Riverland Drive #101
Crested Butte, CO 81224

Toll Free: (800) 908-7654
Phone: (970) 251-5041

Support@wolftrack.com
www.wolftrack.com

Table of Contents

1. Scope and Applicability
 - A. Intent of the PA-DSS
 - B. Scope of this guide
2. Getting Started
 - A. Installing Wolf Track Software
 - B. Upgrading from an Evaluation version of Wolf Track Software
3. Network and Software Components
 - A. A Word about PCI-DSS Scope
 - B. Network Security
 - C. Wireless Networks
 - D. Remote Access
 - E. Non-Console Administrative Access
 - F. Required Protocols, Services, Components and Hardware
4. Previous Software Versions and Historical Data
 - A. Historical Data Removal
 - B. Previous Software Versions
5. Data Protection and Encryption
 - A. Data Retention Settings
 - B. Data Encryption in Storage
 - C. Data Encryption in Transmission
 - D. Data Authentication
 - E. Removal of Old Data
 - F. Operating System Settings
- 6 User Management
 - A. Unique User Accounts
 - B. Setting Up User Accounts
 - C. Strong Passwords
 - D. Cashier Users
 - E. Access Control
 - E. User Accounts for Additional Components
 - F. User Account Security and Lockout
7. Event Logs and Auditing
 - A. Logging Configuration
 - B. Centralized Logging
8. Software Updates
9. Anti-Virus Software
10. Troubleshooting and Service
 - A. Support
 - B. Remote Services
 - C. Best Practices
 - D. Troubleshooting Practices
11. Privacy
 - A. Data Collection
 - B. Cookies
 - C. Information Sharing
 - D. Information Security
 - E. Secure Shopping Guarantee
 - F. Links

1. Scope and Applicability

A. Intent of the PA-DSS

The intent of the PA-DSS is to develop secure payment procedures within Wolf Track Software that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure payment applications support compliance with the PCI-DSS.

B. Scope of this guide

This guide will explain the features included within Wolf Track Software, and the best practices which will help users maintain PCI-DSS Compliance.

2. Getting Started

A. Installing Wolf Track Software

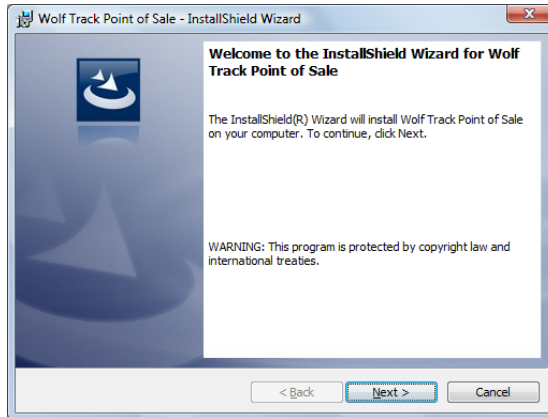


Go to <http://www.wolftrack.com/> select the 15 Day Free Trial option in the upper right hand corner. Fill in the information on the Registration page. After clicking “Sign Up”, you will receive an email with a link to your download. Open that link, and save it on your computer (someplace that you will remember, such as your Desktop)

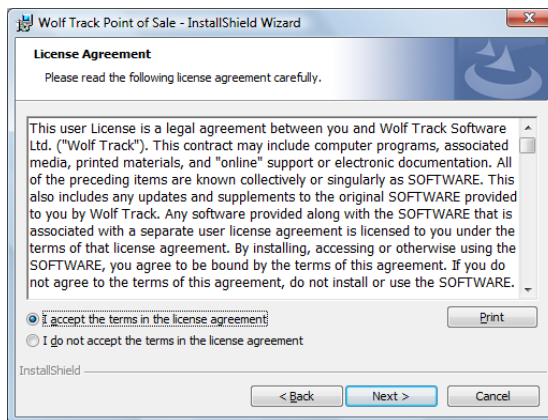
Now that the woltrackdownload.exe has been downloaded, you need to install it. Double click on the woltrackdownload.exe* icon you saved. This will start the InstallShield Wizard for Wolf Track Software.

*When installing in Windows Vista or Windows 7:

1. Disconnect or disable any external hard drives you may have connected to the PC. If you have already started installing Wolf Track, then you may need to restart the installation.
2. Rather than double clicking the icon, please right-click the woltrackdownload.exe icon, and select “Run as Administrator.” Not selecting the Run as Administrator option will cause the software to not update correctly.



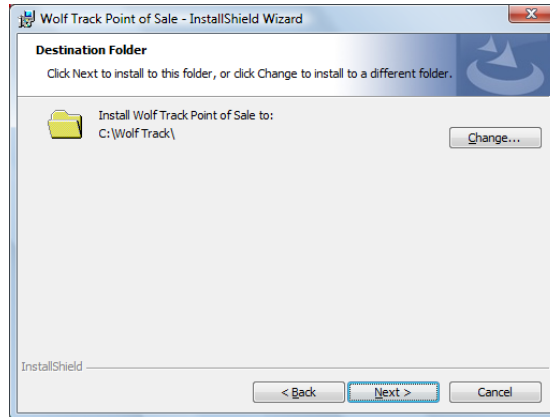
Please read the EULA and accept it if you agree with the terms.



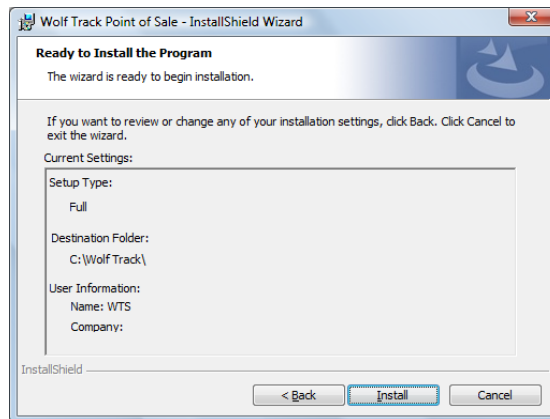
You will then be given the default username and password. Take note of this, as this is the information you will need to begin using Wolf Track Software.



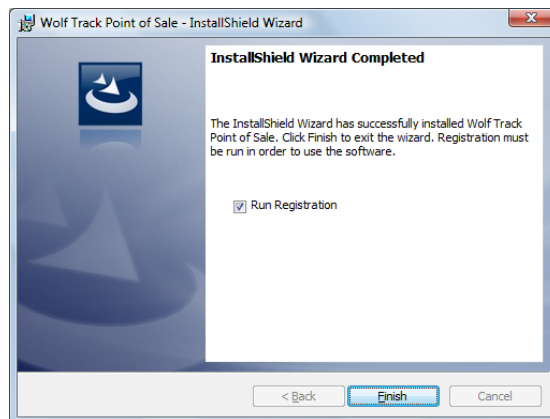
The next screen will ask what directory you would like to use. Please use the default directory (C:\Wolf Track\).



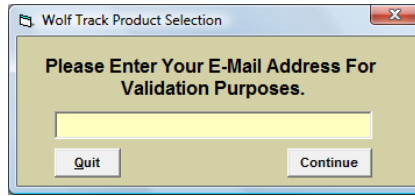
The following page is a summary. It will list out the options you have selected. If you agree that everything is correct, press the install button at the bottom of the screen.



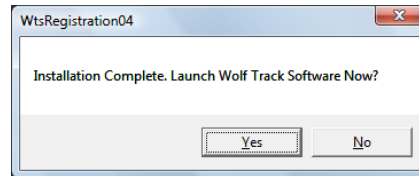
After you select “Install,” installation will begin. When installation has completed, please make sure the “Run Registration” box is selected, and press finish.



You will be prompted to enter your email address. You must enter the same email address you used to download your evaluation of Wolf Track Software.



Once you have validated your installation, you will be prompted to run Wolf Track Software



Congratulations, you have installed Wolf Track Point of Sale Software. Once you launch Wolf Track Software, you will be brought to the opening splash screen. You can now click anywhere and start using the software.



Now that the software is installed you will launch Wolf Track Software from the icon* that the installation has placed on your desktop, or from the listing in the Windows Start Menu under Wolf Track Software menu.

To log into Wolf Track Software, Click anywhere on the Splash Screen. A window will open asking you for your log in credentials. Enter your user name in the text entry box saying “Enter User Name Here” and enter your Password in the text entry box saying “Enter Password Here”.

* When Running on Windows Vista or Windows 7:

1. Right click the icon and select Properties
2. Select the Compatibility tab
3. Check the always “Run as Administrator” option.
 - a. If this option is not available then you will need to right click the link and select the “Run as Administrator” option manually each time you load the software
 - b. Adjusting your User Account Controls should make the “Run as Administrator” option become available.

B. Upgrading from an Evaluation version of Wolf Track Software

The upgrade from the evaluation version of Wolf Track Software comes with a complementary walk-through and setup. This session gives the user an opportunity to have any questions answered and ensures that the hardware and printers are configured properly. In order to

upgrade to the full version, please call Wolf Track Software at (800) 908-7654 to schedule an upgrade. You can also start off the process by going to <http://www.wolftrack.com> and clicking the “Buy Now” link. This will walk you through the secure online purchase and you will receive an email with your account information.

3. Network and Software Components

A. A Word about PCI-DSS Scope

The PCI-DSS is a set of comprehensive requirements for enhancing payment account data security. It was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. to help facilitate the broad adoption of consistent data security measures on a global basis.

The purpose of the PCI-DSS is to:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test Networks
- Maintain an information security policy

This implementation guide is designed to help maintain PCI-DSS compliance while using Wolf Track Software.

B. Network Security

Securing a network is very important when using Wolf Track Software as you may be transferring customers’ personal financial data over that network. When using a standard wired network, it is imperative that no unauthorized user has access to the network in which credit card data be transferred. We advise that any routers and switches be placed in a location that is secure, and each computer has strong login passwords. For more information on strong user passwords, please see section 6.C Strong User Passwords. If for any reason card holder data is stored on a server in your network that server cannot be an Internet-accessible system. In example a web server and a database server cannot be located on the same machine that is storing card holder data. Failure to do this will cause you to be out of PCI-DSS compliance.

C. Wireless Networks

Securing a wireless network is of the utmost importance when working with Wolf Track Software. Since Wolf Track Software handles credit card payments, and will potentially transfer encrypted personal data, then it is advised that you do not have Wolf Track Software on a network with any other Non-Wolf Track system that may be connected to the Internet. This will reduce the risk of theft and will help maintain PCI-DSS Compliance.

If you choose to use a wireless network rather than the traditional “wired” network, then please consider the following for wireless network use, failure to follow these guidelines will result in PCI-DSS Non-Compliance:

- When setting up your wireless network, change all passwords to any access points from the default.
- Change the default encryption keys, and use at least WPA2 encryption on any wireless network in which payment information is transferred.
- Install perimeter firewalls which must deny or control all traffic from the wireless environment into the cardholder data environment.
- Change the default Simple Network Management Protocol (SNMP) community strings.

Change any other default values as applicable.
Hide the Service Set Identifier (SSID) so that it is not easily accessible or found.
Only allow trusted MAC addresses access to the network.
Stay up to date with hardware firmware to support strong encryption and transmission
Change encryption keys (before installation and whenever anyone with knowledge of the keys leaves the company or changes positions)

For more information regarding PCI-DSS compliancy with a wireless network, see https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf.

D. Remote Access

Remote access can only be initiated by the end user, and will only be requested by a Wolf Track support person for the purpose of initial installation of Wolf Track Software, and for support calls if all other support procedures are unsuccessful. In order to remain PCI-DSS compliant, do not allow anyone other than Wolf Track authorized support to remotely access any system running Wolf Track Software.

A built in system for accessing Wolf Track software is not currently available. It is advised that third party applications are not used to access the Wolf Track system. Wolf Track Software, Ltd. will not be responsible for any information lost or stolen due to the use of any applications that allow remote access to your desktop, including, but not limited to Windows Remote Desktop.

Remote access can only be granted by the current user of the workstation. Wolf Track support uses a non-reusable blind key for any remote access, and is unable to run administrative tasks without the permission of the terminal user.

E. Non-Console Administrative Access

Wolf Track Software does not include any features which allow non-console administrative access. If you choose to allow Non-Console Administrative Access to your system through you must use a strong cryptography such as SSH, VPN or SSL/TLS.

F. Required Protocols, Services, Components and Hardware

Wolf Track Software does require a few protocols, services, components and/or hardware in order to for the software to integrate with our payment processors.

Required Protocols:

SSL-128 Bit for data transmission

Required Services:

Internet Connection

Required Components:

DSIClientX.ocx - Integration for Mercury Payment Processing through Datacap Systems Inc.

Required Hardware:

Windows Compatible USB 3 Track Card Swipe

4. Previous Software Versions and Historical Data

A. Historical Data Removal

Wolf Track Software does not store or retain any personal payment information such as Credit Card Numbers, CVV2, CVC2, CID or CAV2. Because no credit card information is stored within

Wolf Track Software, and all updates are made automatically, there is little need purge historical data.

B. Previous Software Versions

Wolf Track Software has never and does not ever plan to save any card holder data. In the event that any card holder data is stored in unexpected fields or note sections of the software we will remove it during the update process.

5. Data Protection and Encryption

A. Data Retention Settings

Wolf Track Software does not store any card holder data. Since there is no storage of card holder data there is no need to remove data from Wolf Track Software. In the case that you ever store card holder data anywhere on the computer system you must purge this information from the computer in order to remain PCI-DSS compliant.

B. Data Encryption in Storage

Wolf Track Software does not store credit card information, all records are stored within an unencrypted password protected database. If card holder data is ever stored it must be encrypted and rendered irretrievable in order to remain PCI-DSS compliant.

C. Data Encryption in Transmission

Wolf Track Software offers built in support for Mercury Payment Systems (MPS). Information transferred to processor servers is encrypted and secured based on the processor's APIs. MPS uses Datacap Systems, Inc. in order to process transactions. Datacap uses a Windows ActiveX control called DSIClientX. The DSIClientX Software is designed to communicate exclusively with Datacap's ePay server products using Internet Protocol (IP). Messages exchanged between the DSIClientX and the server are encrypted for secure transmission of open networks (such as Internet).

D. Data Authentication

At no point during authentication or pre-authentication will Wolf Track Software save or store any sensitive authentication data.

E. Removal of Old Data

Wolf Track Software does not store any Card Holder Data. There is no need to purge card holder data after any customer defined retention period. Any customer information can be removed at any time by opening the Customer in Store Settings and removing any of the information requested.

F. Operating System Settings

Setup your operating system for restore points or backups as you normally would. Since Wolf Track Software does not store any card holder data there is no need to adjust your backup procedures or restore points.

6 User Management

A. Unique User Accounts

Assigning each user a unique user account will help track all activities within the system and is required to be PCI-DSS compliant. Also note that using group, generic, or shared accounts and passwords is prohibited to remain PCI-DSS compliant. You cannot create multiple accounts with

the same User ID. Wolf Track Software enforces Unique User Accounts and Strong Passwords (See 6.C) by requiring the user to create new User Accounts by the completion of the applications installation. These Unique User Accounts and passwords cannot be redistributed and must be remembered in order to run the software after the installation.

It is necessary to create new unique user accounts not only in Wolf Track Software, but also within the Windows Operating System, as well as strong unique user passwords (See 6.C). You also need to disable or delete any accounts that are not in use. Failure to do so will result in non-compliance to PCI-DSS guidelines.

Wolf Track Software stores the employee information in an a password protected database in the Wolf Track folder. The passwords are stored using a SHA512 Hash, which makes use of a unique salt per password. This makes sure that the passwords are never visible in clear text whether in the software or in the database. This also means that end users must remember their user name and password because it cannot be retrieved for any reason.

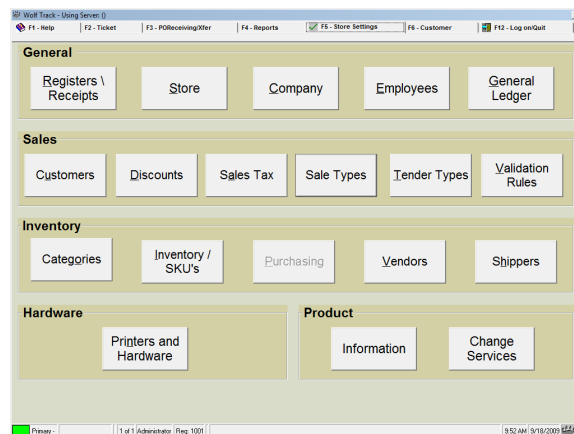
B. Setting Up User Accounts

During Software Installation:

Wolf Track Software will require the end-user to create 3 default user accounts during the installation process. You will be walked through the process at the time of registration. The first account created will be an Administrator User and will have full rights to the software. The next account created is a Manager Account and has limited rights. The third account created is a Clerk account and has very limited rights to the software. Please refer to Unique User Accounts (6.A) and Strong Passwords (6.C) for information on the mandatory settings for the Usernames and Passwords in the system.

After Software Installation:

To set up a user account, first make sure you are logged in as a user that has rights to add users. Press F5 or go to the Store Settings tab.



Select "Employees"

Store Settings >> Employee << F12 to Return			
Code	000	Status	A
Title		Permission Code	Administrator
First Name	Highest Level	Hire Date	
Initial		Termination Date	
Last Name	Employee	Last Ticket	
Address Line 1		Gender	
Address Line 2		DL SS	000-00-0000
City		DOB	
State		Pay Rate	
Zip		Pay Frequency	
Home Phone		User Name	admin
Business Phone		Password	admin
FAX Number		Username/Password change	Yes
Emergency Contact 1		Clocked in ?	No
Emergency Phone 1		Insurance ?	No
Emergency Contact 2		Misc 1	
Emergency Phone 2		Misc 2	
E-Mail Address		Misc 3	
Store	1	Notes	
Department			
Supervisor			

<<First <Prev Next> Last>> Add Employee Delete Cancel Save Exit

At the bottom of the screen, select “Add Employee”

Store Settings >> Employee << F12 to Return			
Code	000	Status	A
Title		Permission Code	
First Name		Hire Date	
Initial		Termination Date	
Last Name		Last Ticket	
Address Line 1		Gender	
Address Line 2		DL SS	
City		DOB	
State		Pay Rate	0.00
Zip		Pay Frequency	
Home Phone		User Name	
Business Phone		Password	
FAX Number		Username/Password change	Yes
Emergency Contact 1		Clocked in ?	No
Emergency Phone 1		Insurance ?	No
Emergency Contact 2		Misc 1	
Emergency Phone 2		Misc 2	
E-Mail Address		Misc 3	
Store	1	Notes	
Department			
Supervisor			

<<First <Prev Next> Last>> Add Employee Delete Cancel Save Exit

Red text signifies that a field is a required field. Any field that is either blue and underlined or red and underlined has a drop down menu available for selection. To get to the drop down menu, you can click on the text, or from the text box, press your home key.

It is very important to select the proper permission code for the employee you are entering. This will determine what access they have in Wolf Track (Read section 6.4 for more information about Access Control). Once you have entered all required information and any additional information as you see fit, select “Save” in the lower right hand corner.

Employees will log in with the User Name and Password that you set up when creating the new employee.

C. Strong Passwords

Since users are authenticated by their Unique User Account and Strong Password, using strong log in passwords greatly reduces the risk of a security breach. By using strong passwords you make it much more difficult for a potential attacker to enter your system/network. Wolf Track Software enforces the use of strong passwords during the account creation process and while updating passwords in the system.

A strong user password contains at least seven (7) characters. Passwords must contain both numeric and alphabetic characters. It should also be a password that is easy for the user to remember but not one that someone else can easily guess.

Passwords should be changed at least every 90 days, and when changing a password, none of the

four last used passwords should be re-used. When a Password is over 90 days old, after logging in the user will be prompted to update their password.

If a user fails to log in after six (6) attempts the the account will be locked out until an administrator resets the account or for 30 minutes (See 6.F).

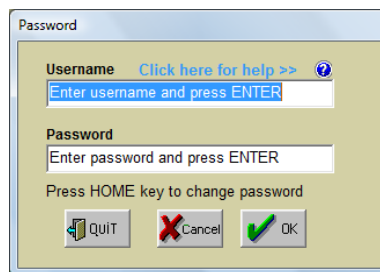
D. Cashier Users

Cashier Users have direct access to the all types of tender, including credit cards. While Wolf Track Software does not store credit card information, you still want to know who is handling the cash your customers hand to the cashier. That is why it is very important to make sure that each cashier, as well as every other user, logs in to the register when the register is in use, and then logs out when it is no longer in use.

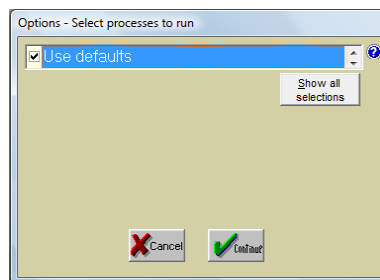
E. Access Control

As an administrator, you have all the tools available to you to manage who has access to which features Wolf Track Software offers. You can restrict cashier accounts to placing orders, and require a supervisor account to accept returns.

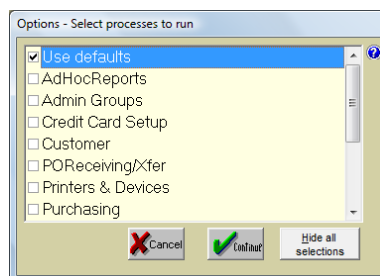
In order to setup access control, start a new session by pressing F12 if you are already in the system. If you are not currently logged in, then simply log in.



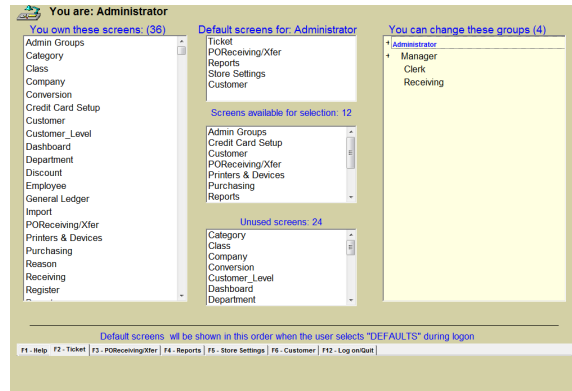
Once you have entered your user-name and password you will see this screen:



Select the "Show all selections" button



Select "Admin Groups" and click on Continue



This screen will allow you to change permissions for your user groups. In order to assign access privileges to users, a group must be assigned in the user setup.

E. User Accounts for Additional Components

Please use caution when setting up user accounts on any components that are either directly connected or will have access to a system running Wolf Track Software. This includes using strong passwords and unique user names for any routers, servers, or any other system that is running Wolf Track Software.

F. User Account Security and Lockout

The system has various settings options available to help maintain PCI-DSS compliance and help keep your system more secure. Many of these features can be accessed through the Store Settings menu.

Activating the splash screen timer and instance password will force the splash screen to appear after the set amount of time (no more than 15 minutes to remain PCI-DSS compliant), and then force you to enter your password. This will ensure that no unauthorized personnel will have access to the system.

Account Lockout occurs when a user enters an incorrect password six times. This forces that user out of Wolf Track for thirty minutes. Once a user has been locked out, there is no way to clear the user account except to wait for the thirty minute lockout period.

The login screen will time-out after twenty-five seconds of no activity. If you have entered data into the login screen before a time-out, that information will need to be re-entered.

7. Event Logs and Auditing

A. Logging Configuration

Wolf Track Software includes a logging system, which logs changes within the following:

- System Errors

- Transactions

- Employee running transaction

- Ticket Amount

- Credit Card Processing Approval Code

- Tenders

- Changes to Credit Card Processing

- Any use of payment application's identification and authentications mechanisms

- Updates to payment application's settings

- Changes to Employee Settings

- All Actions Taken by Administrative Accounts including audit logs

- Invalid and Valid Log in Attempts.

Logged information includes what action was taken, the logged in user, which resource was affected, and the time of the action. Wolf Track Software also logs the success or failure of the action. Creation and deletion of any system-level objects are also recorded. Wolf Track Software also logs anytime the access logs are accessed.

No credit cardholder data is stored anywhere in Wolf Track Software. The system logs any changes made to any of these modules by any users that are able to access these modules. Access to these modules can only be granted by an administrator.

System logging is enabled by default, and there is no apparatus to disable logging changes, as disabling logging would result in non-compliance with the PCI-DSS.

B. Centralized Logging

Wolf Track Software allows for exporting the log in a comma delimited file that can then be imported into a centralized logging system. To export these logs login to the software. Select the show all selections option. Check the Tools option and Click Continue. Click the Show Log File button. In the bottom right corner of the log window click the export as CSV button.

8. Software Updates

Once the software has been upgraded to the full version of Wolf Track Software, the system will check for updates every time it is shut down. Normal updates are added approximately once a month. Currently, there is no set schedule for upgrades. Wolf Track Software will not check for updates unless it is shut down. It is very important to shutdown the system at least once a week in order to check for software updates.

9. Anti-Virus Software

In order to remain PCI-DSS compliant, it is a requirement to run software to protect any computer that may be processing credit card data. Wolf Track Software has been tested with most industry standard anti-virus software applications. Many of the anti-virus providers now offer a built-in software firewall or a utility to restrict non trusted applications. If you choose to use one of these programs, then you may need to make Wolf Track Software a trusted application with access to connect to the Internet, as it must connect to update the software, and also for any online back-ups. Failure to “trust” Wolf Track Software could result in errors when running in a multiple register environment or when attempting to update or backup.

10. Troubleshooting and Service

A. Support

Wolf Track Software phone technical support is paid for through monthly licensing fees as part of our per register system, and is available to any current Wolf Track customer. Phone support is available between the hours of 9:00 am and 5:00 pm CST Monday through Friday at toll-free (800) 908-7654. Our e-mail support is 24/7 by either going to the Contact Us page on our website or by e-mailing support@wolftrack.com.

B. Remote Services

For remote service, Wolf Track Software uses GoToAssist Corporate. This is a third party customer initiated remote support service. When we need to perform remote service for our customers we ask them to go to our Web site (www.wolftrack.com). They will then click on the

Help & Support link. They will then enter their name and a 9 digit code created by GoToAssist Corporate. GoToAssist Corporate is managed entirely independent of the Wolf Track Software.

In order to remain PCI-DSS compliant, any remote services, access initiated from a location external to the network, must have a two-factor authentication. During any remote services, the user still has full access to the system, and can discontinue the remote service at any time. Wolf Track support does not have access to any stored Windows or Wolf Track Software passwords. If a password is requested to perform a task, Wolf Track support will request the user to enter the password.

While Wolf Track software does not have a built in utility for remote access, we do understand that there are third party applications which do allow remote access to a remote desktop. We recommend that these programs are not used on any computer running Wolf Track Software, but if the user chooses to use one of these programs to remotely access their system, you must use the following as best practices:

- Require unique usernames for all remote users
- Require passwords for authentication
- Prohibit the use of share, generic, or group user accounts or passwords
- Require password changes at least every 90 days
- Require strong alphanumeric passwords consisting of at least 8 characters
- Do not reuse any of the last four used passwords
- Select an application which will lock a user out after 6 invalid login attempts for at least 30 minutes
- Select an application that will time out users after at least 15 minutes of idle time
- Select an application that has logging enabled and review those logs regularly
- Do not share any passwords with anyone except authorized personnel
- Change default settings in the remote access software (for example, change the default passwords and use unique passwords for each customer)
- Allow connections only from specific (known) IP/MAC addresses
- Enable encrypted data transmission
- Enable account lockout after a certain number of failed log in attempts.
- Configure the system so a remote user must establish a Virtual Private Network (“VPN”) connection via a firewall before access is allowed
- Restrict access to customer passwords to authorized reseller/integrator personnel.
- Establish Strong Customer Passwords (See 6.C)

C. Best Practices

Wolf Track Software has been designed with security in mind, but unfortunately even the most secure platform cannot protect a computer if the user is engaging in risky behavior. Wolf Track advises that all users only accept downloads from trusted sources. We also advise that if a problem does occur, the user only use Wolf Track authorized support to troubleshoot any problems concerning Wolf Track Software.

D. Troubleshooting Practices

When troubleshooting issues, Wolf Track Software will not collect any magnetic stripe data, card validation codes, PINs or PIN blocks. Wolf Track Users should not collect or distribute any magnetic stripe data, card validation codes, PINs or PIN blocks during troubleshooting any issues they might encounter. Since we will never save any card holder data on the computer or in the software, there is no file to securely delete or to encrypt.

If you must collect cardholder data for any reason during troubleshooting, make sure to:

- Collect data only when needed to solve a specific problem
- Store data only in specific, known locations with limited access

Collect as little of data as necessary to solve the specific problem
Encrypt data when stored
Securely delete data immediately after use

11. Privacy

The following principles apply to the personally identifying information we ask for and that you provide. "Personally identifying information" is information that individually identifies you, such as your name, physical address or email address.

A. Data Collection

Wolf Track Software collects limited non-personally identifying information your browser makes available whenever you visit our website. This log information includes your Internet Protocol address, browser type, browser language, the date and time of your download and in some cases, one or more cookies that may uniquely identify your browser. We use this information to operate, develop and improve our services.

Some of our services require you to register. Wolf Track Software asks you for some personal information in order to create an account (typically your name, email address, physical address, and phone number) and we will use that information to provide the service. For certain services, such as Buy Now, we may request credit card or other payment information which we do not keep or store on our servers.

When we require personally identifying information, we will inform you about the types of information we collect and how we use it. We hope this will help you make an informed decision about sharing your personal information with us.

B. Cookies

To enhance your experience with our site, some of our web pages use "cookies." Cookies are small text files we place in your computer's browser to store your preferences. Cookies, by themselves, do not tell us your e-mail address or other personally identifiable information unless you choose to provide this information to us by, for example, by registering at our site. However, once you choose to furnish the site with personally identifiable information, this information may be linked to the data stored in the cookie.

We use cookies to understand site usage and to improve the content and offerings on our site. For example, we may use cookies to personalize your experience at our web pages (e.g. to recognize you by name when you return to our site). We also may use cookies to offer you products, programs, or services.

C. Information Sharing

We do not rent or sell your personally identifying information to other companies or individuals, unless we have your consent. We may share such information in any of the following limited circumstances:

We have your consent.

We provide such information to trusted businesses or persons for the sole purpose of processing personally identifying information on our behalf. When this is done, it is subject to agreements that oblige those parties to process such information only on our instructions and in compliance with this Privacy Policy and appropriate confidentiality and security measures.

We conclude that we are required by law or have a good faith belief that access, preservation or disclosure of such information is reasonably necessary to protect the

rights, property or safety of Sunbelt Software, its users or the public. In the event of a transfer of ownership of Wolf Track Software (including any publications), such as acquisition by or merger with another company, we will provide notice before any personally identifying information is transferred and becomes subject to a different privacy policy.

We may share aggregated information with others. Examples of this include the number of users who downloaded a specific product or how many users clicked on a particular advertisement.

D. Information Security

We take appropriate security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of data.

We restrict access to your personally identifying information to employees who need to know that information in order to operate, develop or improve our services.

We provide mechanisms for updating and correcting your personally identifying information for many of our services.

You may send an e-mail or letter to the following e-mail or street address requesting access to or correction of your personally identifiable information:

Wolf Track Software
PO Box 1669
515 Riverland Drive #101
Crested Butte, CO 81224
email: support@wolftrack.com

E. Secure Shopping Guarantee

The purchase areas of our site are secure. This means that any information you send us is protected by encryption to prevent unauthorized access to your information. The secure site is indicated in the URL with the use of "https://" (SSL), and often reflected at the bottom of your browser with a lock or key graphic.

F. Links

This website and any newsletter issued by any site affiliated with this site may contain links to other websites with whom we have a business relationship. Wolf Track Software does not review or screen these sites, and we are not responsible or liable for their privacy or data security practices, or the content of these sites.

Additionally, if you register with any of these sites, any information that you provide in the process of registration, such as your email address, credit card number or other personally identifiable information, will be transferred to these sites. For these reasons, you should be careful to review any privacy and data security policies posted on any of these sites before providing information to them.