WinEPS User's PCI Recommendations Guide

Version 821.0
March 2007

This document is compliant with PCI Version 1.1
For details on the latest PCI Standards visit www.pcisecuritystandards.org

Notice

MTXEPS, Inc. reserves the right to make changes to specification at any time and without notice. The information furnished by MTXEPS, Inc. in this publication is believed to be accurate and reliable; however, no responsibility is assumed by MTXEPS, Inc. for its use, nor for infringements of patents or other rights of third parties resulting from its use. No license is granted under any patents or patent rights owned by MTXEPS, Inc.

MTXEPS, Inc.
Telephone: (949) 614-1600
Fax: (949) 614-1650
Help Desk (949) 614-1616

85 Argonaut, Suite 150
Aliso Viejo, CA 92656 USA

Table of Contents

PCI Standards

PCI Introduction

What is PCI?

The Cardholder Information Security Program (CISP) was initiated by the Visa card company to create a set of standards for securing cardholder information. These CISP requirements have formed the basis for the latest set of standards: Payment Card Industry (PCI) Data Security Standard. These PCI standards are now administrated by an independent PCI Security Standards Council, and embraced by credit issuers such as American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International.

The latest information on PCI standards can be found on the PCI Security Council website: www.pcisecuritystandards.org.

What does PCI mean to me?

The information contained in this document defines the responsibilities of the user to create and maintain a PCI compliant environment for the WinEPS software.

Failure to maintain a PCI compliant environment may result in fines, penalties, restrictions, and financial responsibility for misused cardholder information.

To meet PCI requirements, the environment in which WinEPS is deployed must be properly configured. WinEPS and its supporting applications have been made compliant with PCI standards, but for the entire system to properly maintain the required security for cardholder information, specific further setup is required.

This document is designed to define the methods of deployment for the WinEPS product and its supporting applications that uphold PCI requirements and best practices. This document outlines requirements for creating a PCI compliant environment for the WinEPS software only; the user is responsible for knowing an adhering to all additional, current PCI requirements beyond those addressed within this document.

WinEPS PCI Environment

WinEPS Installation Environment

The WinEPS software suite has been updated to be PCI compliant, but the environment into which it is installed has an impact on the safety and security of cardholder information that WinEPS utilizes to process transactions.

Network and physical security are the responsibility of the end user; for the production environment to be fully PCI compliant the below recommendations have been made. Again, it is advised to review the PCI requirement document that can be acquired by contacting the PCI Security Council, or visiting their web site (www.pcisecuritystandards.org).

Network Requirements

PCI requires that the production environment be engineered to protect cardholder information. It is the user's responsibility to provide a secure networking environment, including providing security for any needed web based access and properly managing any external network connections such as VPNs and remote software access.

WinEPS should not be installed on servers that provide a different network function than payment processing; this means that WinEPS can be installed on the same system that runs the POS back office, or other payment applications, but should never be installed on systems that perform network functions such as DHCP, DNS, routing, web services etc (PCI section 2.2.1).

Make sure that virus scanning software is present within the payments environment. PCI requirements state that virus scanners be up to date, active, and be capable of writing log files.

PCI requirements state that all software in the payments environment must have the latest security updates and that all security related updates be installed within a month of their release.

The PCI standard requires that access to all systems in the payment processing environment be protected through use of unique user accounts and complex passwords. Unique user accounts indicate that every account used is associated with an individual user and/or process with no use of group accounts (accounts which are used by more than one user or process). This ensures that actions taken can be logged and traced back to individual, authorized users.

Additionally any default accounts provided with operating systems and/or devices should be removed/disabled/renamed (PCI section 2.0) before implementation in the payments environment.

The PCI standard requires the following password complexity for compliance:

- Passwords must be at least 7 characters
- Passwords must be include both numeric and alphabetic characters
- Passwords must be changed at least every 90 days
- New passwords can not be the same as the last 4 passwords

Below are the other PCI account requirements beyond uniqueness and password complexity:

- If an incorrect password is provided 6 times the account should be locked out.
- Account lock out duration should be at least 30 minutes (or until an administrator resets it).
- Sessions idle for more than 15 minutes should require re-entry of username and password to re-activate the session.

Networks should be tested for vulnerability on a regular basis. Many systems are required to be tested at least quarterly (Se PCI sections11.2 - 11.3)

LAN Setup

The Local Area Network requires both physical and electronic security. It is the responsibility of the Merchant to provide appropriate physical and electronic security to protect customer card information. This section covers some specific suggestions for LAN network security relating to WinEPS.

Merchants should prevent unauthorized access to the OpenEPS directory on the POS lane, and to the EPS directory on the WinEPS server. Only the WinEPS Windows User Account (see next section) and valid administrators require access to the EPS directory. Allowing unauthorized access could endanger card information; the merchant is responsible for locking down access to the EPS directory and OpenEPS directory to prevent unauthorized or malicious changes to the program or direct manipulation of configuration files.

Similarly, the OpenEPS directory on the POS lane should only be accessible by valid administrators, the OpenEPS and POS software.

Merchants should install and maintain firewalls according to PCI Requirements section 1 to prevent unauthorized access to the payments network.

Servers and systems containing customer card information must also be protected physically. The computer that WinEPS resides on should be placed in a secure server room to prevent unauthorized access to the physical hardware which could compromise security.

POS systems at the lane should be made as difficult to gain unauthorized physical access to as feasible.

Wireless Networking

When installing WinEPS into an environment that includes wireless networking, additional requirements must be met. PCI requirements include specific instructions on the use of wireless networking within the production environment. PCI requirements section 1, 2 and 4 (specifically 1.3, 2.1.1, & 4.1.1) should be reviewed for complete information on wireless setup. The following information is provided to assist in wireless setup:

- Vendor supplied defaults (administrator username/password, SSID, and SNMP community values) should be changed
- For wireless networks that transmit cardholder data, encryption must be in use, such as: WPA or WPA2, IPSEC VPN, SSL/TLS at 128 bit. If WEP (Wired Equivalency Protocol) is used, it must have at least a 104-bit encryption key and 24 bit-initialization value and must be used with WPA or WPA2, IPSEC VPN, SSL/TLS.
- Messages between WinEPS (on the server) and OpenEPS (at each POS lane) are encrypted; this encryption satisfies PCI requirements on card holder data transmission across wired LAN networks, but additional encryption and security is necessary for wireless networks, as noted above.
- If WEP keys are changed manually, they must be rotated at lease quarterly and whenever key personnel leave. Keys may be rotated automatically if the hardware supports this.
- Wireless connection points should be secured with the appropriate use of firewalls.
- Firewall/port filtering services should be placed between wireless access points and the payment processing environment with rules restricting access.
- Access points should restrict access to known authorized devices (using MAC address filtering).

WinEPS Windows User Account

When installing WinEPS, the user should log on as a Windows administrator. This allows the install process to perform actions like writing to the registry, and granting the ‘log on as service’ right. The account that the service runs under (its WinEPS Windows User Account) is not required to be an administrator; it is recommended that the service under which the WinEPS service runs be defined as a member of the Window’s Power Users group.

Other than administrative Windows accounts, no other account should be given access to the EPS directory on the server, or the OpenEPS directory on the POS lanes. Restricting access to these directories will assist in preventing unauthorized access, and potential manipulation of the program or configuration files contained therein.

Note: Manually stopping and starting the WinEPS service requires administrative rights; therefore, any user who wishes to stop or start the WinEPS service must be logged on to Windows under a Windows administrator account. It is not necessary to log in as an administrator to perform configuration changes or other standard uses of WinEPS.

Any Windows user that must have the ability to access WinEPS for configuration purposes should have the following:

- The Windows user requires the rights to read and write to the EPS directory and all sub directories. Additionally, the account must be given the right to write to any path which the user specifies that WinEPS is to write to. Examples of additional locations include the path to the MTXAUTH.DAT file in a Scanmaster environment, the path for the CSV Export, and the path of the backup of the WinEPS configurations, if specified.

- Unless the account is an administrative account, the Windows user account used to log in to perform configuration changes should not have access to any other directory that those required.

Recommended Setup of the Windows User Account:

- Before installing WinEPS, define a separate Windows user account. This account should be a Power User, not an administrator. Do not use already existing accounts, or accounts that are installed in the operating system by default, like the Administrator account.

- WinEPS Windows User Account should have a unique and recognizable name, as well as a unique and complex password.

WinEPS Directories and Access

It is recommended that only administrative personnel be allowed to directly modify WinEPS program files; users other than administrators should be prevented from making changes directly to the WinEPS software or to its configuration files. To prevent this, the use of Access Control Lists is suggested.

WinEPS is installed to the C:\Program Files\MicroTrax\EPS\ directory by default. As stated above, only administrators should be given direct access to any file or folder from the \MicroTrax\ and below; administrators will require access to these folders to in order to install patches and performs upgrades. It is therefore recommended to restrict access to the \MicroTrax\ folder and below, including the EPS directory, and potentially the RS directory (if Redundancy Service is also installed).

In addition it is highly recommended that the EPS and OpenEPS directories be protected through the use of a File Integrity Monitoring System. The EPS and OpenEPS directories contain configuration information that could potentially be altered with malicious intent. Specific vulnerable files are the host files and the Setup.Txt, as these contain the IP addresses in use and could be manipulated potentially redirect payment processing traffic.

Recommended File Integrity Monitoring Systems include the Tripwire Security Suite, and GFI; has a free file integrity monitoring tool. File Integrity Monitoring Systems keep track of changes to files or applications and can alert technical staff when changes are made; undesirable changes can be easily tracked and removed.

When using a File Integrity Monitoring System, be aware that certain files (typically log or database files: *.tor, Spool*, actlog*, jrnl*, Offlines) are constantly changing. It is often useful to either exclude these files from alerts completely, or configure the alerting software to allow the

WinEPS software to freely manipulate files within its directory structure, and to configure alerts for when files are directly manipulated by users or when manipulated by other software.

The WinEPS directory structure contains the following folders:

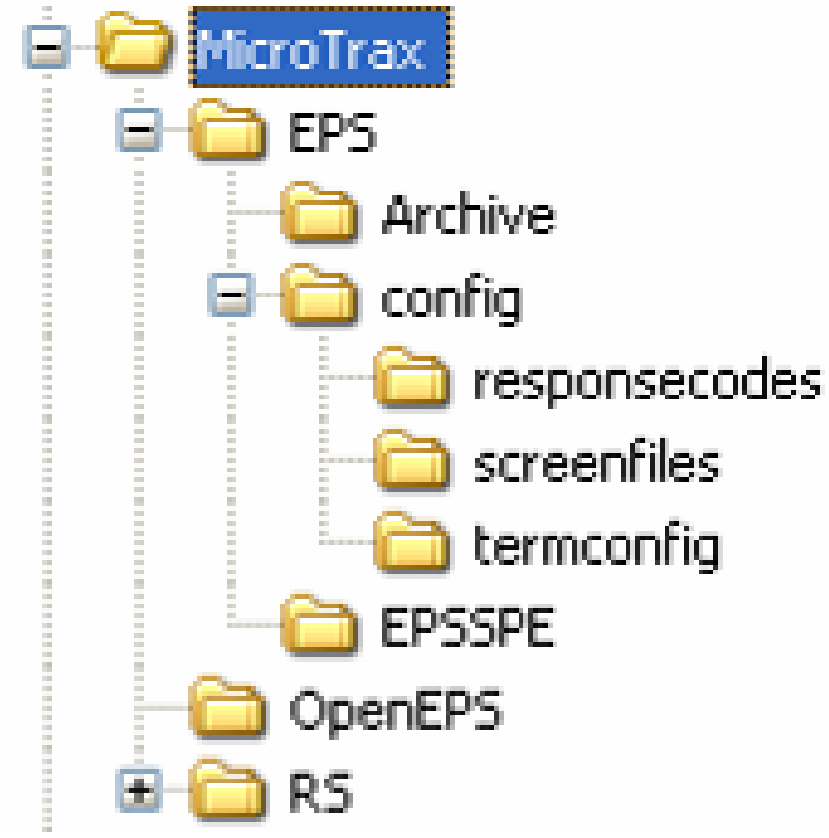
- EPS
- EPS\Archive
- EPS\Config
  - EPS\Config\responcecodes
  - EPS\Config\screenfiles
  - EPS\Config\termconfig
- EPS\EPSSPE

If RS is installed:

- RS\

If Virtual terminal is installed (or other OpenEPS integration):

- OpenEPS\



All directories listed should deny access to non-administrative users and be monitored by a File Integrity Monitoring System.

OpenEPS environments, such as the POS lanes, have a directory structure of C:\Program Files\MicroTrax\OpenEPS\. This directory is populated from the WinEPS server, and access should be restricted to administrators only.

WinEPS Protocols and Ports and Components

WinEPS uses a variety of ports to communicate with its various components, including, but not limited to OpenEPS on the POS lane and the payments hosts. The list of components, services and ports that WinEPS requires be allowed to be opened or unrestricted is listed in the WinEPS User's Guide in the WinEPS System Requirements section of Chapter 1.

Secure File Transfer Protocol (FTPS) is used to transfer files between WinEPS and the POS lanes. This protocol is necessary for WinEPS/OpenEPS payments to function properly.

WAN Setup / External Connections

This section covers requirements for WAN setup and external connections, such as VPNs into the LAN, and connections from WinEPS to the payments processor.

WinEPS and its components should never be deployed onto systems with direct internet access. WinEPS software should be deployed on servers that reside behind firewalls, with communication to the financial processor secured and allowed through the firewall. The firewalls must be configured to protect cardholder information contained within WinEPS by limiting the incoming and outgoing connections to only those which are required. PCI Section 1 covers firewall requirements.

To successfully process payments, WinEPS will require a network route to the payments processor. While WinEPS contains encryption technology to prevent the interception of card holder information in transit within the LAN, it is the responsibility of the user to ensure that the connection to the financial processor is properly encrypted and/or secured according to PCI requirements.

PCI Requirements state that it is necessary to use strong encryption technology such as Secure Sockets Layer (SSL), Point-to-Point Tunneling Protocol (PPTP), or Internet Protocol Security (IPSEC) to secure communications over any public network, such as the internet.

Remote Network Connections

It is recommended to establish secure methods of determining the identities of users who will be granted access to the local network. Use an access request form that is filled out when any outside party, including MTXEPS personnel, need to remotely connect to a production environment system. This form should contain, at minimum, information on who is accessing the network, their contact information and the contact information of their immediate superior, the purpose of the access, and the expected duration of the access. Vendor access accounts must also be disabled while not in use.

For remote access requests, the identity of the requesting individual should be firmly established. Establish contact with known personnel, such as the account manager or their designate that is assigned to your company. This may also entail contacting the requesting individual or company at a known telephone number or e-mail address.

Remote access accounts must be granted only to individuals; a single access account must not be given to a group of individuals for common use. Remote access should be logged in an auditable format.

When giving access to any computer in the payments environment, it is recommended to use two-factor authorization for remote access (username/ password and an additional authentication item such as a token or certificate). A user account should automatically lock out access after a maximum of 6 failed login attempts, for a minimum time period of 30 minutes before a new login attempt is allowed.

After 15 minutes of inactivity, a remote access session should terminate connection and force the user to log back on.

All passwords for remote access should be unique, complex, and allow change by the authorized party. Complex passwords must be at least 7 characters long, contain at least one capital letter and one number, and may not be the same as the last four passwords used, if applicable. Additionally, if the access is for a long duration, the password must be changed every 90 days.

Remote access accounts should be enabled only for the duration of the approved access. After the duration of the remote access, user accounts should be disabled and removed. Any account that is unused for 90 days must be removed.

All remote access accounts should use the highest encryption method possible. This includes RDP (Remote Desktop Protocol) sessions conducted with high encryption setting, utilizing Secure Shell (SSH), and software such as pcAnywhere utilizing 128 bit or higher encryption.

The WinEPS software can only be accessed by users directly at the WinEPS server console. If the users wish to access the WinEPS server remotely, they must utilize secure technologies such as SSH, VPN, or SSL/TLS (transport layer security) for this purpose.

Insecure protocols such as Telnet and rlogin must never be used, and must not be enabled on the WinEPS server. It bears noting again that remote access should never be a permanent feature of the WinEPS server, and should only be enabled for the duration such access is required.

Transmission of Cardholder Data over Public Networks

The PCI standard requires the use of strong cryptography and encryption techniques (at least 128 bit) such as Secure Sockets Layer (SSL), Point-to-Point Tunneling Protocol (PPTP), and Internet Protocol Security (IPSEC) to safeguard sensitive cardholder data during transmission over public networks (like the Internet).

Additionally PCI requires that cardholder information never be sent via e-mail without strong encryption of the data.

Security Policy

It is mandatory for PCI compliance that a comprehensive security policy be in place in a production environment. Review section 12 of the PCI document for complete information on the current requirements.

Reporting Security Breaches

The WinEPS product utilizes a variety of encryption keys to keep cardholder information safe. If it is known or suspected that any encryption method utilized by WinEPS or its components is breached, contact MTXEPS, Inc. immediately.

Notification of New Patches

MTXEPS, Inc delivers security/encryption related patches within 7 business days after notification of the security breach. The patch will be made available to all WinEPS users; MTXEPS, Inc will post a notice on its public web site (www.mtxeps.com) about such a patch, but cannot individually contact all software users. It is therefore recommended that all users of the WinEPS software periodically check the web site to determine if any new security related patches are available. MTXEPS Support can also be contacted directly to request current patch information.

When a security related patch is received, PCI recommends that it be tested before deployment.

WinEPS PCI Settings

Settings Required by PCI

The following section details setting and configuration recommendations for the WinEPS software.

Upgrade From Previous WinEPS Version

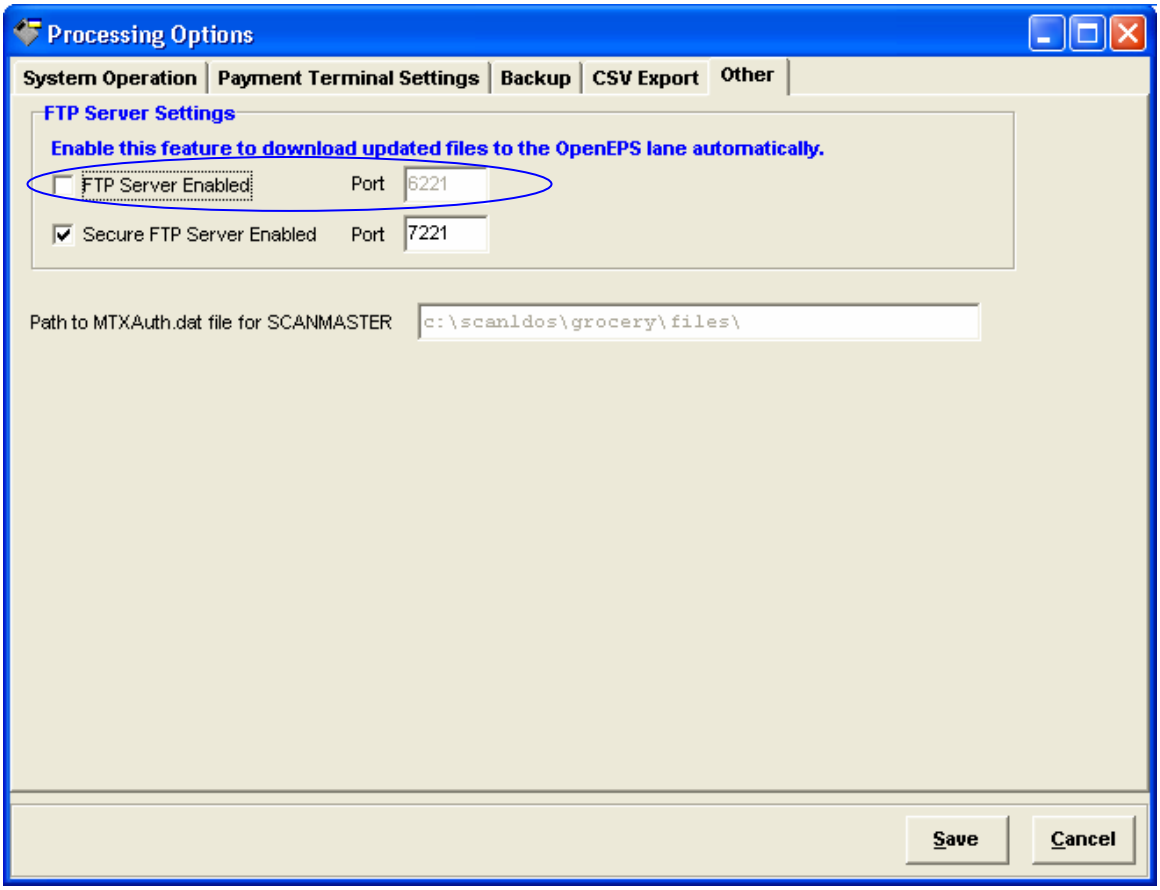
Disabling FTP

WinEPS versions previous to 816.1 utilized FTP to transfer configuration files to the OpenEPS POS lanes. This protocol has been replaced by FTPS (Secure FTP). To allow the upgrading of POS lanes that previously utilized FTP, the FTP service has remained operational. **To become PCI compliant, it is necessary to disable the Non-Secure FTP or turn on the Secure FTP service (see steps below).**

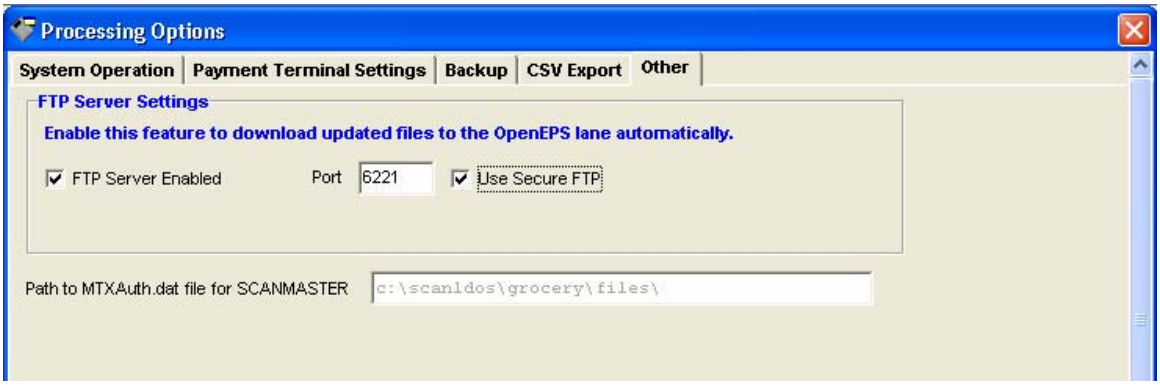
For upgrades from WinEPS versions prior to 816.1, it is recommended that the upgrade be performed first, allowing the lanes to update to the most recent version that supports Secure FTP, before shutting off the Non-Secure FTP.

Follow the steps below after upgrading to update POS lanes and turn off the FTP service.

1. After WinEPS is upgraded, verify that WinEPS is started.
2. Sign on to each POS lane to update the OpenEPS software on each lane. If the lane does not utilize OpenEPS, instead move on to the next step.
3. In WinEPS, go to Site Information | Processing Options.
4. Select the Other Tab.
5. You will see one of the two screens below.

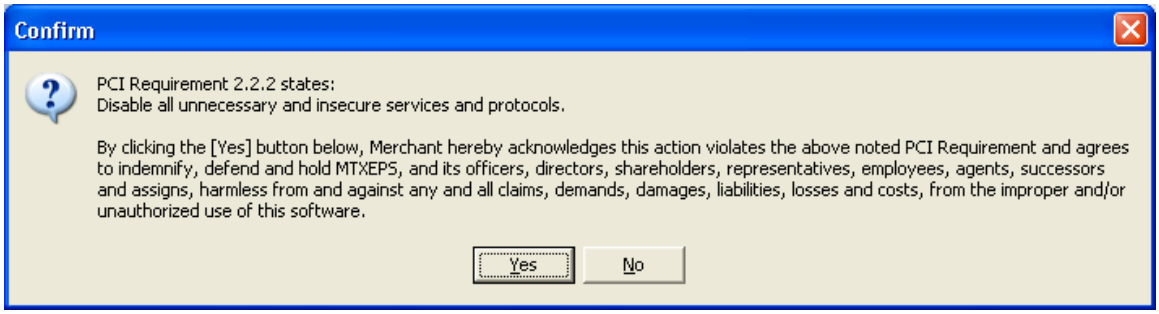


1. For the screen above, Uncheck the box next to FTP Server Enabled, leaving the Check mark next to the Secure FTP Server Enabled option.



2. For the screen above, Verify that the Use Secure FTP box is checked.

Since the use of FTP is not within PCI requirements, turning the FTP Server back on is not recommended. Reactivating the feature will prevent WinEPS from operating in a PCI compliant manner; WinEPS will prompt the user as shown below.



WinEPS users must agree to indemnify MTXEPS when reactivating this feature, as MTXEPS cannot be held responsible for any consequences resulting from becoming non-PCI compliant through the use of this feature.

WinEPS Patches

Currently no universal method exists for MTXEPS, Inc to contact all of its customers. If a security related patch is released, MTXEPS will utilize current contact information to contact known customers, but cannot guarantee successful contact.

It is highly recommended that all users keep their WinEPS system up to date by acquiring the latest WinEPS patches. All WinEPS users can contact WinEPS support for a list of available patches; additionally the MTXEPS web site (WWW.MTXEPS.COM) Support page will contain lists of patches for all supported WinEPS versions; current WinEPS users should contact the MTXEPS sales staff to acquire a username and password for the support section of the web site.

It is recommended that WinEPS Users receive patches either directly from MTXEPS support staff or the MTXEPS web site, or though a known and trusted chain of personnel. This will ensure authenticity and that the received patch is the most recent.

WinEPS Operators: Roles and Rights

Operators are user accounts for the WinEPS software. These accounts allow the configuration of WinEPS settings, and may give access to card holder information. The examples in the Sample Recommended WinEPS Operator Configurations section below indicate typical user configurations of rights. These examples limit the available rights of each user account to only those rights required to fulfill their function. Only the Administrative user illustrated below is expected to need to configure WinEPS settings.

There must be no ‘universal’ accounts. This means that no individual account name and password combination should be defined on multiple WinEPS systems with then intension that the account information be available to more than one person. Do not create an account at multiple locations with the intension to make it a ‘default’ account that all administrators can log onto, for example.

It is permissible to create the same account on multiple systems, so long as that account’s information (username and password) is maintained by a single individual and is not available to anyone else.

The option in WinEPS to create Windows Group Operator accounts can relieve administration difficulty in maintaining individual WinEPS operator accounts by allowing WinEPS access to be regulated by use of Windows security groups. See below for additional information, and see the WinEPS User’s Guide for information on setting up Operator accounts as Windows Groups.

When an administrative Operator creates an individual account, it is highly recommended that they utilize a unique password for that account. The first logon to any individual account prompts for a change of password.

Limit WinEPS operators to only those personnel necessary. The fewer personnel with access, the more secure the system can be. If a user must be given access, grant only those operator rights necessary to fulfill their assigned role. Specifically, the right to view credit card numbers should be closely monitored, and granted only to those personnel to whom viewing full card information is essential to their business roll. This is true for individual user operator accounts as well as Windows Group accounts; do not allow wide access to WinEPS by defining a group that has many members who do not need assess to WinEPS.

If a user that is assigned an Operator account is terminated, immediately remove the assigned Operator account. If the user has accounts on multiple WinEPS installations, their Operator account information must be removed at each location.

Individual Operators Vs Windows Group Operators

WinEPS offers two methods of providing Operator accounts: Individual Operators and operator accounts based on Windows Groups.

Individual accounts work by requiring a username and password be entered in WinEPS (separate from the Windows user account) whereupon WinEPS grants the user the rights associated with that individual account. According to PCI requirements, multiple users may not use the same account, so when using individual Operators, a separate account must be configured for each person who will access WinEPS, and the passwords for those accounts must be changed ever 90 days or less.

Windows Group Accounts work by creating an account in WinEPS that is named the same as a Windows group, and specifically marking that account as a 'group' in WinEPS. The group is then assigned rights dependant on the type of user who would be a member of that group. For example, the Administrators group typically has wide ranging permissions, and it might be appropriate to grant all WinEPS permissions to that group, whereas Power Users may be given more limited options. WinEPS does not track passwords for group accounts because access is based on a user's Windows account and group membership. This method is also PCI compliant so long as the Windows environment is set up properly; WinEPS retains its ability to log actions by individual user accounts, and with the use of Windows Groups, can track the specific Windows account that the user logs in under as well as which groups that user is a member of.

As with standard Windows group membership, if a user is a member of multiple groups, their rights will be a combination of the rights off all groups they are members of.

Windows default groups and WinEPS

Windows has several default groups already built in. Here is an example list:

Name	Description
Administrators	Administrators have complete and unrestricted access to the computer/domain
Backup Operators	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files
Guests	Guests have the same access as members of the Users group by default, except for the Guest account w
Network Configuration ...	Members in this group can have some administrative privileges to manage configuration of networking fea
Power Users	Power Users possess most administrative powers with some restrictions. Thus, Power Users can run lega
Remote Desktop Users	Members in this group are granted the right to logon remotely
Replicator	Supports file replication in a domain
Users	Users are prevented from making accidental or intentional system-wide changes. Thus, Users can run cer
HelpServicesGroup	Group for the Help and Support Center

When setting WinEPS up to use Windows Groups to regulate access, it is important to note that not all default groups should be given access to WinEPS. Never define groups such as Everyone or Guests.

Not all levels of WinEPS access are represented in the default groups. It may be necessary to create new security groups and assign Windows user memberships to these new groups based on their required access in WinEPS.

For example, you may create a WinEPS Reporting group that allows users to view WinEPS reports:

WinEPS Reporting	Group for users who have access to WinEPS and the right to view reports

The next section shows several recommended Operator configurations for different security levels. Examples of appropriate Windows Groups for those operators are also given.

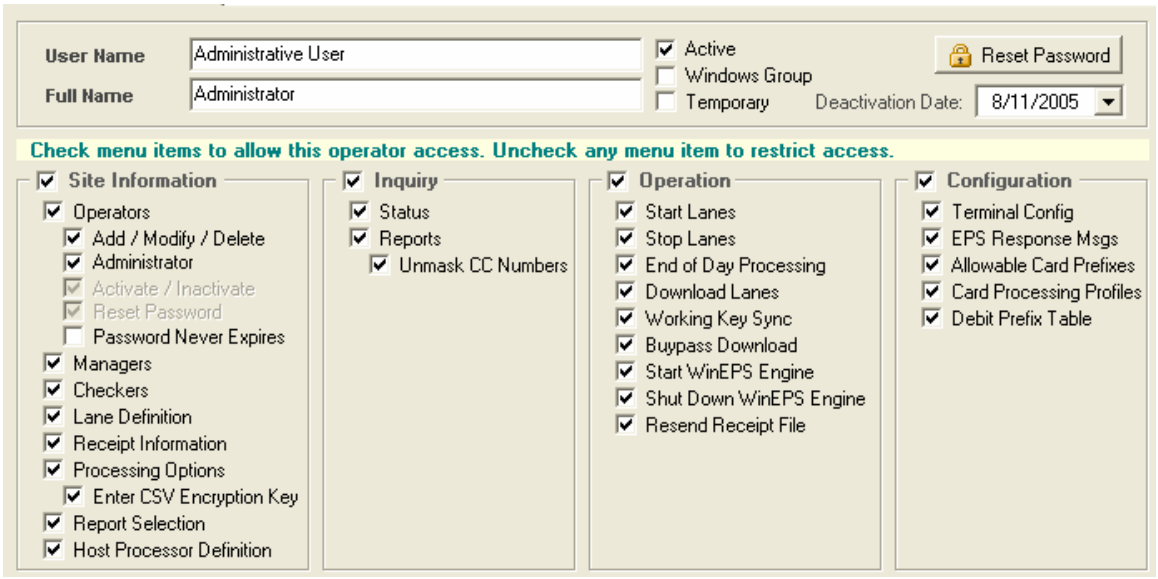
Sample Recommended WinEPS Operator Configurations

Below is a list of several example accounts and security levels that can be configured in WinEPS. Actual security and accessibility should be adjusted according to need. The basic philosophy is that a user should not be granted more rights than necessary to perform their job.

Example Recommended User Types:

- Administrative User
- Transaction Research
- General User
- Reporting

Administrative User – User with full access to all WinEPS features and functions. At least one administrative account must exist in each WinEPS installation. Administrative Operators must possess all rights to be able to create other accounts with those rights, as well as perform WinEPS configuration setup. Since an Administrative Operator possesses all rights, access to an administrative operator should be restricted to only those personnel who require the ability set up WinEPS and to make configuration changes.

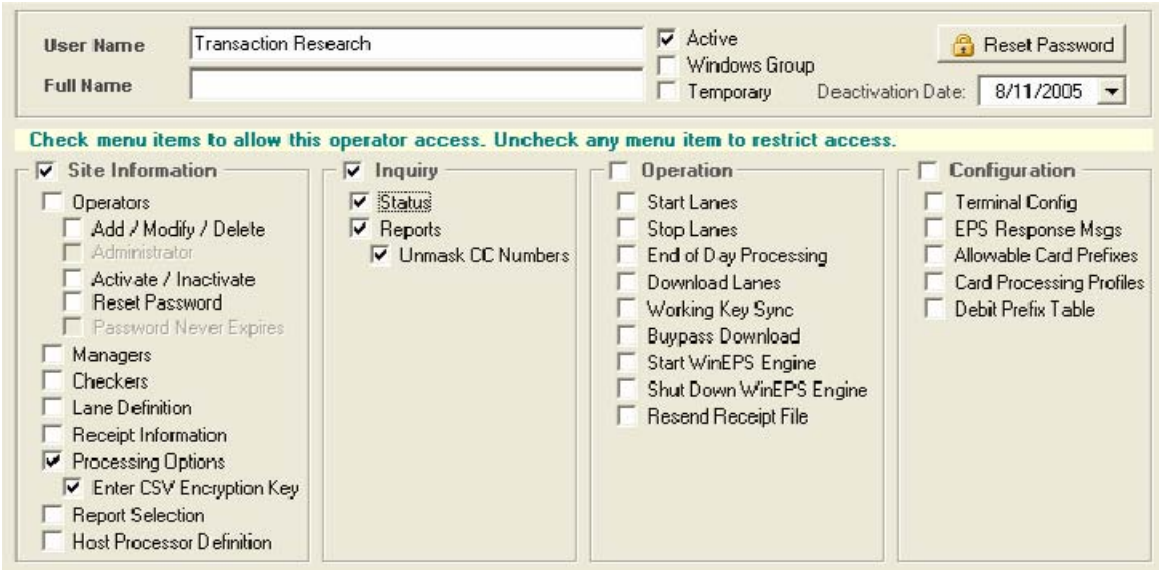


Typical Administrative User Rights

For setup as a WinEPS Windows Group Operator, the *Administrative User* is approximately equivalent to the Administrators group.

Transaction Research – User with access to only report information, but who sees the full account numbers to allow research to be performed on specific transactions. Access to non-report functions is restricted, as this user has no need to make changes to the WinEPS configurations or service. Access to Credit Card numbers should be limited to those people with a "business need to know" according to PCI requirements. The rights granted to this user are shown below: Inquiry Menu, Status, Reports, Unmask CC Numbers.

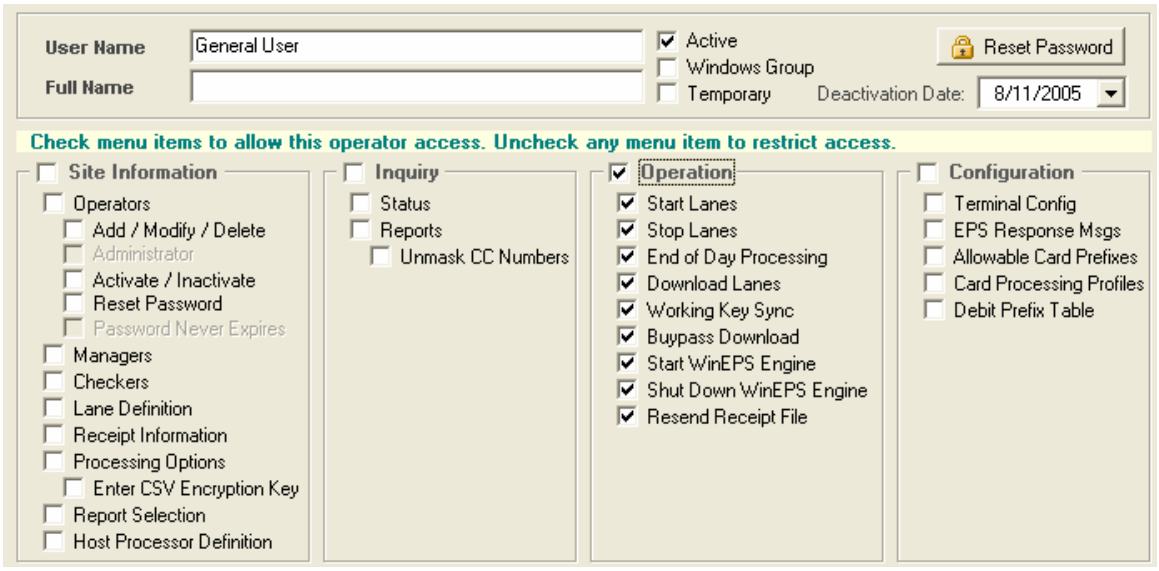
They may optionally possess the right to change the CSV encryption key (Processing Options | Enter CSV Encryption), if this user is responsible for the periodic changing of the encryption keys. If this user is not responsible for changing keys, this right should not be given.



Typical Transaction Research User Rights

There is no direct correlation between the *Transaction Research* WinEPS account and any default Windows Group; it is therefore recommended to create a new Windows group of 'WinEPS Transaction Researchers' and assign membership in this group by Windows users based on their security requirements in WinEPS.

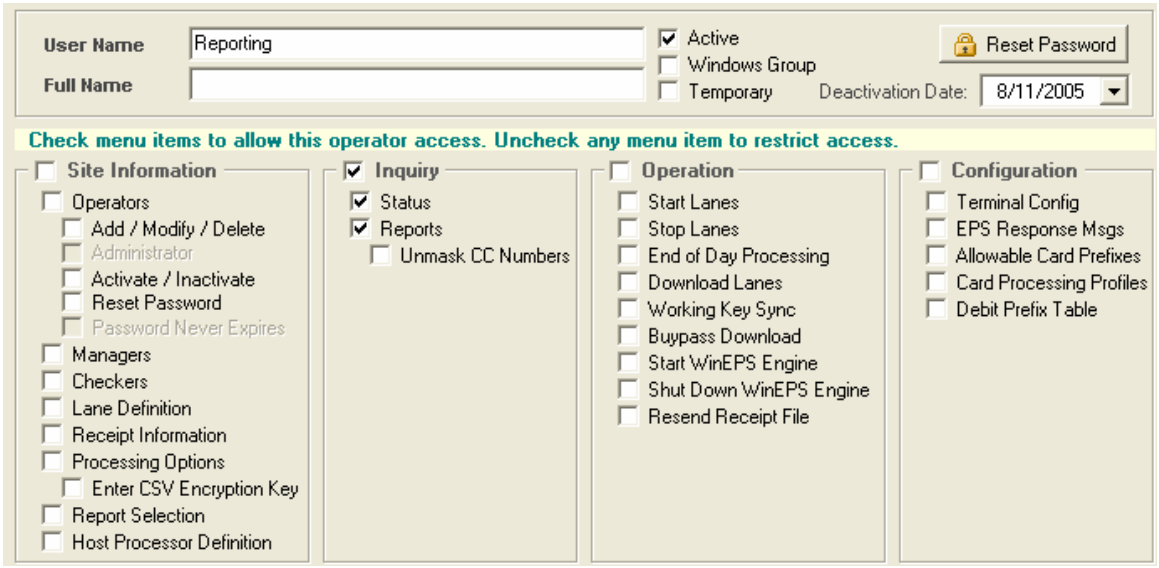
General User – User such as a store manager who has no need to configure the WinEPS system, but may be used to view store reports for totals and start or stop the WinEPS service. This user should not be given the ability to view credit card numbers as they are not needed to generate daily store-business oriented reports. The rights granted to this user are shown below: Inquiry Menu, Status, Reports; All Operation menu items.



Typical General User Rights

For setup as a WinEPS Windows Group Operator, the *General User* is approximately equivalent to the Power Users group, though it may be necessary to create a new Windows group instead, such as 'Managers' if store managers are not granted membership to the Power Users group.

Reporting – User that only needs access to view reports on store financial information; sees only masked account information. The rights granted to this user are shown below: Inquiry Menu, Status, Reports.

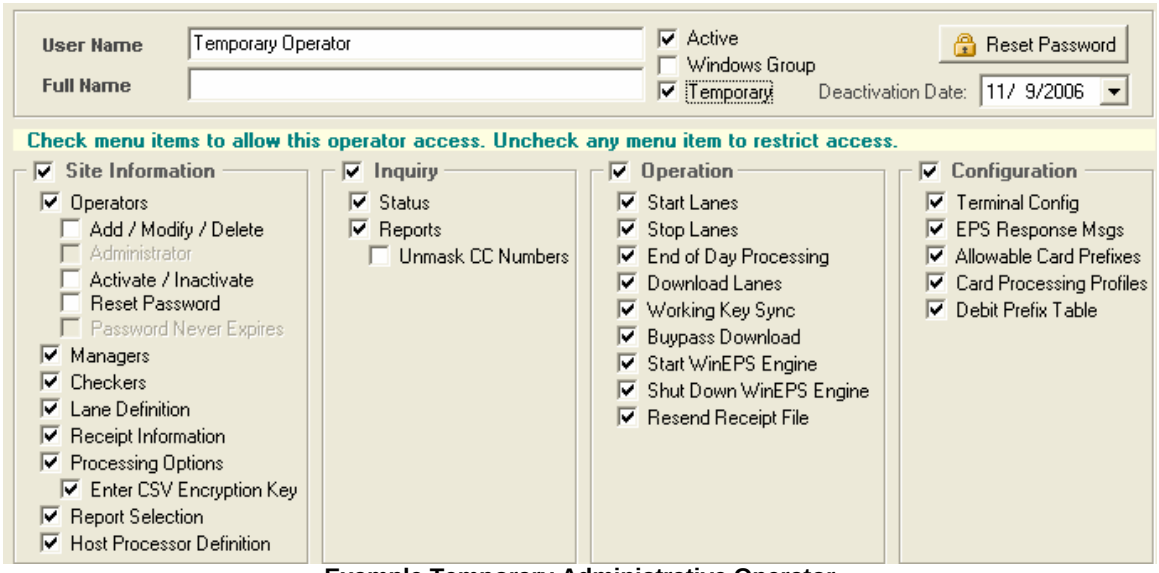


Typical Reporting User Rights

Similar to the *Transaction Research* Operator, there is no direct correlation between the *Reporting* WinEPS account and any default Windows Group. In this case it is recommended to create a new Windows group of 'WinEPS Reporting' and assign membership in this group by Windows users based on their security requirements in WinEPS.

Using Temporary Operator Accounts

When it is necessary to grant temporary access to the WinEPS software, a new operator account should be created with the temporary flag enabled. When creating a temporary Operator, they should not be granted the right to change other operators, and should not be given the right to view full credit card numbers unless there is express business need to do so.



Example Temporary Administrative Operator

It is recommended to utilize temporary accounts when offsite support must network into a site to perform any function; this can include MTXEPS staff who are evaluating a reported bug or assisting in WinEPS configuration.

Set the duration for the temporary account for only the expected length of time which the user will have and require access to the system. Even though the account access will lapse automatically at the expiration date, it is highly recommended that the account be disabled by an administrative Operator once the need for the temporary account is over. Only enable remote access and Operator accounts when they are needed; disable remote access and associated operator accounts when not in use.

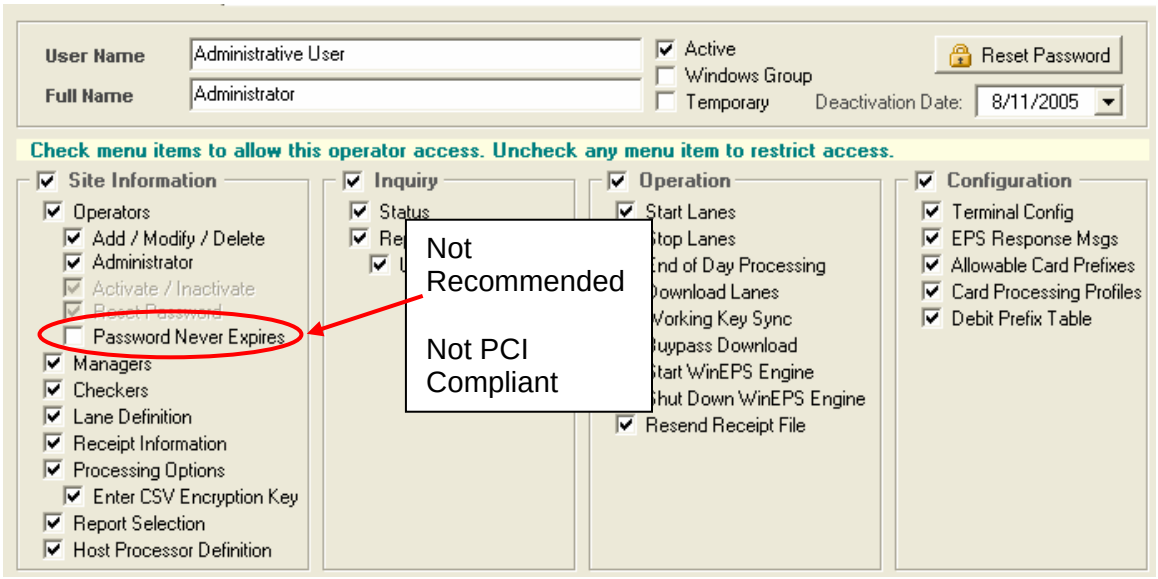
Operator Passwords

The WinEPS application enforces PCI required operator password requirements (8 character password minimum, 1 capital letter, 1 number). Additionally, the maximum number of days that the password may remain unchanged is 90 days; any login after the set duration will prompt for new password.

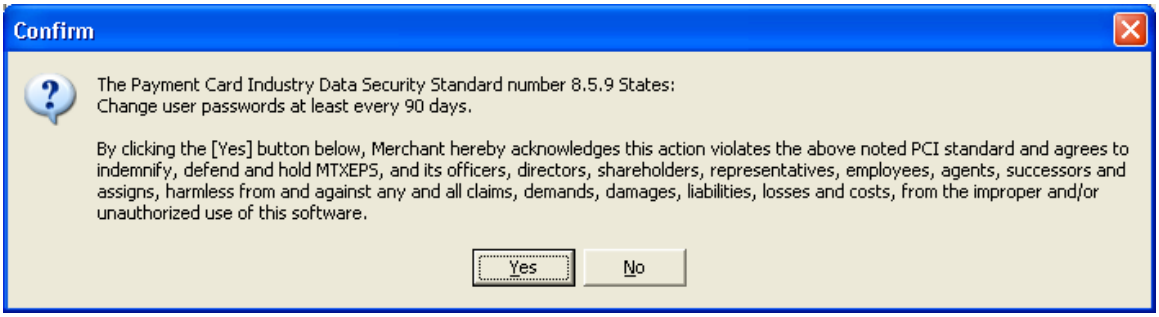
A password may not be the same as any of the previous four passwords used for that Operator.

Passwords Never Expire

Users of previous versions of WinEPS are familiar with the option to prevent WinEPS Operator account passwords from expiring. PCI requirements state that passwords must be changed at least every 90 days.



Activating the feature will prevent WinEPS from operating in a PCI compliant manner; WinEPS will prompt the user as shown below.



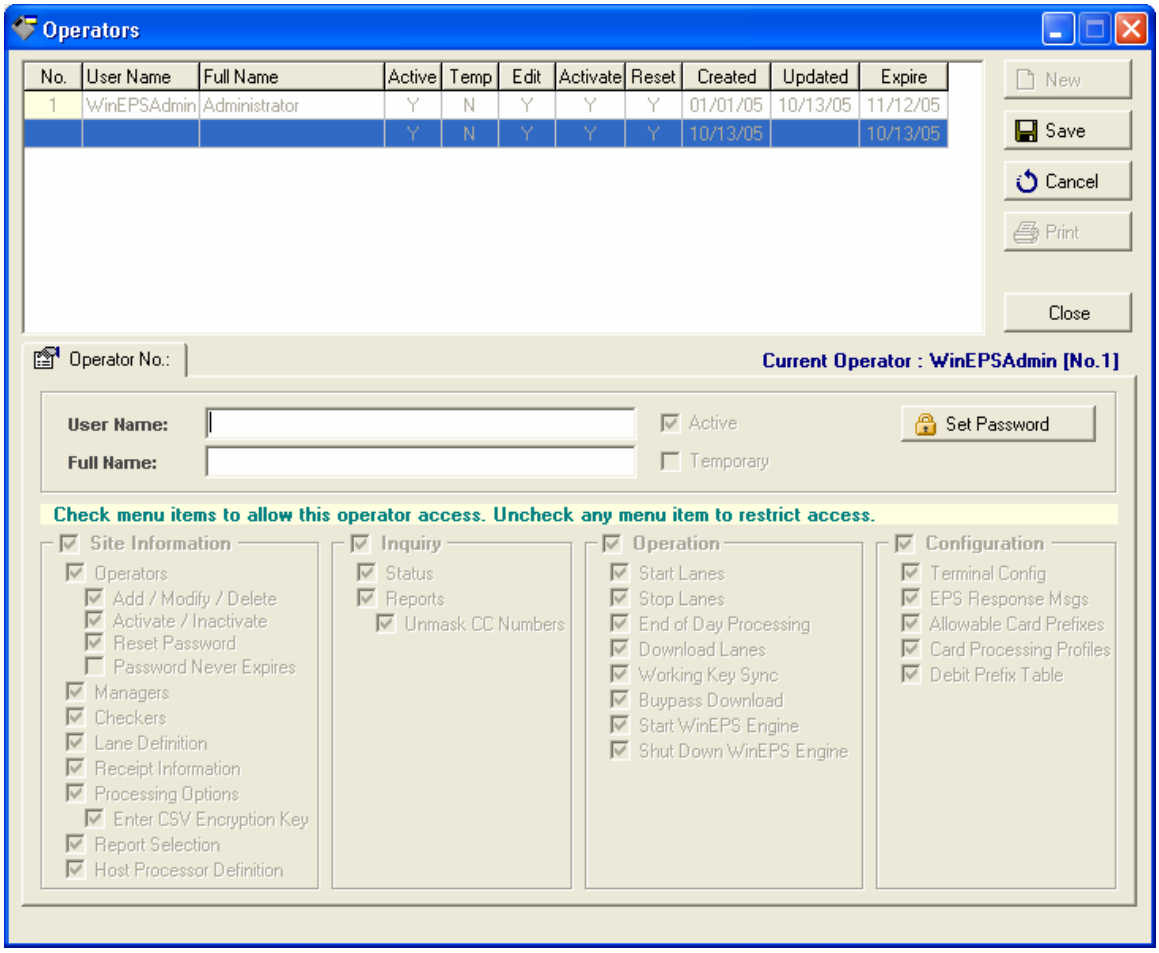
WinEPS users must agree to indemnify MTXEPS when activating this feature, as MTXEPS cannot be held responsible for any consequences resulting from becoming non-PCI compliant through the use of this feature.

The Default Operator

On a fresh installation of WinEPS, the default operator's login name is WinEPSAdmin, with an original password of Password1. While during the first login the password must be changed from the default, it is also recommended that the login name be changed to something other than WinEPSAdmin.

Follow the steps below to change the default Operator's Name.

1. After logging in to WinEPS, go to Site Information | Operators.

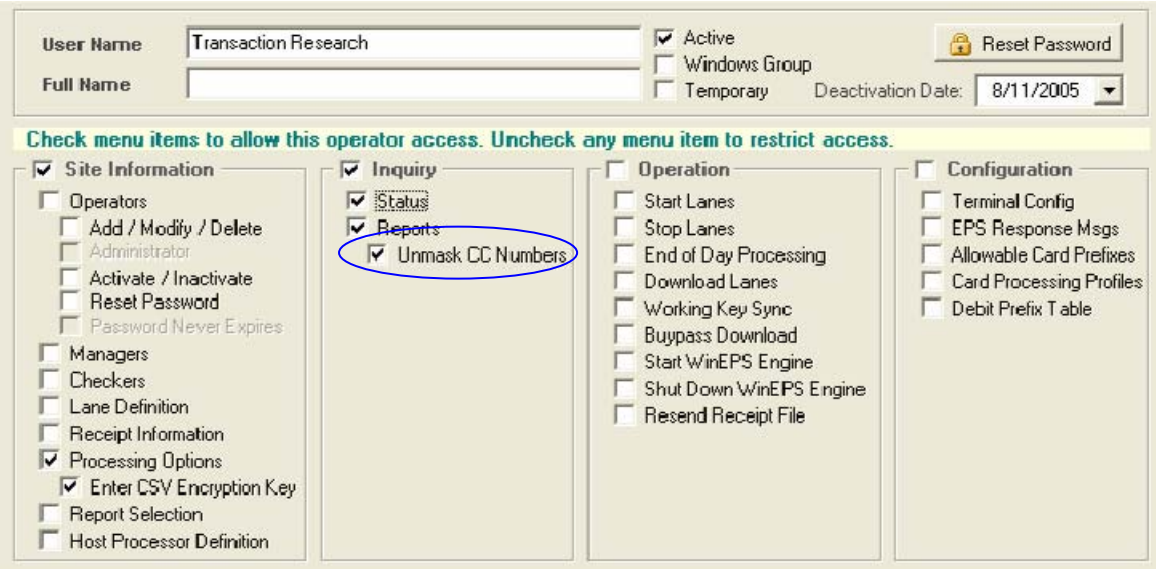


2. It is necessary to create a new Operator with the permission to alter other operator accounts. Click New.
3. Enter a User Name, and Full Name.
4. Select the Add / Modify / Delete right.
5. Click Save and enter a password.
6. Log Off WinEPS.
7. Log back onto WinEPS using the new account information
8. Go to Site Information | Operators.
9. Select the WinEPSAdmin account; change the User Name, and Full Name and save the changes.
10. Log off of the new user account, log back on as the renamed admin account, and delete the other operator.

View Full Account Number Right

As noted above, WinEPS Operators may be given the right to view full account numbers. This right must be carefully controlled and granted only to those users who must have this right in order to fulfill their job requirements.

The example from above notes that the Transaction Research user type might be required to view the full account number to properly execute of their duties.



WinEPS must provide access to view the full account number in order for merchants to correct billing mistakes. This includes a failure to charge a customer for goods or services rendered for which the customer agreed to pay, or to grant a refund to a customer for a charge that they should not have incurred.

Therefore, the only users that should have access to view full card numbers are those users authorized to make charges or refunds on a customer's account outside of a transaction; typically this includes only store managers or other high-level personnel. If there is any question about whether viewing full account numbers is necessary, disable the feature for that user, and re-enable it only in the event that a legitimate and necessary use is determined.

CSV Encryption Key

WinEPS transaction information can be exported to CSV file; this file can contain sensitive cardholder information for the purpose of tracing specific transactions. Production of a CSV file that contains full card numbers requires the use of a user-generated CSV encryption key.

First it should be determined if it is a business need to view transaction information that contains full card information. If no business need exists, it is recommended that no CSV encryption key be entered and the default PCI compliant masked CSV version be utilized.

Assuming that a business need exists to export and view full card information, a CSV encryption key is necessary; this entails key management on the part of the WinEPS user.

Refer to the WinEPS Users Guide for instructions on entering the CSV encryption key, and setting the path for the CSV export. The information below pertains to initiating security measures pertaining to the CSV export itself and handling the CSV export key.

Key Generation

CSV Encryption/Decryption keys are composed of two 16-character keys; allowed characters are the numbers 0 to 9 as well as the letters A through F.

In WinEPS, the CSV encryption key can be entered as two separate halves, 16 characters each, of the complete 32 character key. Key entry was broken into two parts to facilitate a dual control environment, with split key knowledge.

Keys should be generated randomly, with knowledge of a key half only available to the person who will generate and enter it. No one user should have knowledge of the entire key; two users should each enter their portion of the key to generate the complete encryption key.

Entering the key must be done in both WinEPS and in the Decryption Software. Doing so creates an .ini file for each application (one for WinEPS and a separate one for the Decryption Software) that contains an encrypted version of the entered key. These files should be kept safe and distributed as detailed in the Key Distribution section.

Key Storage

Keys should be stored in a dual control environment and secured against theft or acquiring through the use of physical security (kept in a safe, for example). Similarly access must be restricted to the *wineps-decrypt-key.ini* file, as this and the decryption software can be used to read encrypted CSV files that contain customer card information.

Detailed information should be maintained about what personnel have access to keys and key files. This information will be needed if any personnel leave company employment to determine when keys need to be changed.

Key Distribution

Instead of distributing key information directly, the .ini files can be distributed to provide encryption or decryption without direct knowledge of utilized keys. The *wineps-key.ini* file

contains the CSV encryption key. This file can be placed into the EPS directory and will be used by WinEPS to encrypt exported CSV files. This file can be packaged with other configuration files as part of a pre-configured roll-out package.

The Decryption Software generates a file called *wineps-decrypt-key.ini.* This file can be distributed along with the Decryption Software to specific personnel who have the business need to view full credit card information. Access to the Decryption Software and the *wineps-decrypt-key.ini* file should be tightly controlled, and the *wineps-decrypt-key.ini* file should never be transmitted over e-mail or any other potentially unsecured medium.

A generated key file (*wineps-key.ini*) is only good for the version that it is generated on. If a CSV encryption key is still in use when a WinEPS upgrade occurs, it will be necessary to re-enter the encryption key in the new WinEPS version, and re-distribute the newly generated *wineps-key.ini* to all WinEPS locations.

If the Decryption Software version changes, it will be necessary to reenter and redistribute the *wineps-decrypt-key.ini* to all Decryption software users.

Key Changes

Keys must be changed periodically. The recommended length of time is one year. Older keys may be kept to decrypt items from previous years.

In the event that an employee with knowledge of encryption keys is terminated, or otherwise leaves the company, all keys which that employee had decryption information on shall be changed immediately and implemented in the production environment as soon as feasible.

CSV Decryption

Generally, it should not be necessary to perform decryption at the WinEPS location. The decryption software and associated ini file should never reside on the same computer that is running WinEPS.

As stated above, access to decryption software and the *wineps-decrypt-key.ini* should be limited to personnel with a business need to view unencrypted card information.

Key Security

Limit knowledge of encryption/decryption keys to the fewest number of people possible. Store keys only in a limited number of secure locations. Do not store any of the keys, decryption software or encrypted card data in the same location.

Report breaches in security, and report known or suspected loss of key security immediately to those personnel tasked with key security responsibilities.

If a compromise in the WinEPS software is detected which may reveal cardholder information report the potential security breach immediately to MTXEPS.

Unencrypted CSV Storage

Once unencrypted, the CSV file must be stored in a secure location where only authorized personnel have access to it. The unencrypted file should only be stored for as long as it is actively being reviewed; storing an unencrypted CSV file containing full card information beyond the active review period is not in compliance with the PCI Data Security Standard.

It is not recommended to store the CSV in unencrypted format unless necessary.

Never store the decryption software with the ini decryption key file on the same computer that encrypted files are stored on, as this presents a security risk should an unauthorized user gain access to the system, they will have access to both the encrypted files with card information and the method to decrypt them.

It is prohibited to transmit unencrypted CSV files containing sensitive information over e-mail or any other potentially unsecured medium. Only the masked or encrypted CSV files should be sent via e-mail.

Clearing Out After Testing

Typically test systems are kept separate from production environment units. Occasionally a test unit will be moved to a production environment, or a production environment unit will be tested briefly after installation. In either case it is important that all test data be cleared out of the system.

WinEPS cuts over and archives all log files during an End of Day. Therefore the simplest method for clearing out extra information is to perform an End of Day. Follow the steps below to clear out information by running an End of Day.

1. Verify that the information on the WinEPS system is test information and not production information.
2. Unplug the network cable to prevent communication with the network and host.
3. Log on to WinEPS with an Operator that has the right to perform End of Day.
4. Go to Operation | End of Day Processing.
5. After the End of Day is finished, reconnect network cable.

Log Review

PCI recommends that a review of log files occur daily. It is therefore recommended that the WinEPS spool file be reviewed for unauthorized user activity. This review can be accomplished by searching for specific text relating to unauthorized activity.

Example Log line:

09/29/05 11:00:17 EPSMENU - UAL: User 1 successfully signed on.

The spool file can be searched for all User Access Logging by performing a text search on 'UAL:' and then each access can be individually evaluated. These log entries comply with PCI sections 10.2 and 10.3.

A complete list of logged activities can be found in the WinEPS Users Guide, Chapter 10, under the heading: User Activity Logging. Below is a list of access items that should be closely evaluated to determine whether the operation was performed legitimately. This list represents actions that could indicate access to customer card information:

User XXX Exported Transaction Data
User XXX Turned CSV Export OFF|ON
User XXX Entered New CSV Export Key
User XXX Modified CSV Export Path
User XXX Launched Report Module (for users that possess the ability to view credit card numbers)

Spool File Vulnerability

WinEPS logs user activity to a single file, the spool file. This file is vulnerable to direct manipulation by Windows users that have the permission to enter the EPS directory and make changes. This could allow the deletion of the logs that detail unauthorized access to card information, for example.

Due to the vulnerability of the Spool file, it is highly recommended that access to the EPS directory be severely limited to only those users that have a business need to directly access WinEPS configuration, log, and program files. Additionally, it is recommended that file integrity monitoring software such as TripWire or GFI be run that will log access to specific files.

Log Retention

WinEPS records are removed automatically after the duration set in the WinEPS Processing Options, ranging from 7 to 90 days. To retain log files beyond this time it is necessary to move the archived zip files from the /EPS/Archive/ directory to a different location.

The location these files are moved to should be secure, as these logs contain encrypted customer card information. PCI recommends that log files be retained online for three months and that offline storage (such as tape backups) be maintained for one year.

When logs are no longer required, PCI requires that cardholder data be destroyed; this can include backups or offsite copies. Since comprehensive destruction is required, it is important to have a tracking policy to ensure that all copies of the data can be cleansed when appropriate.