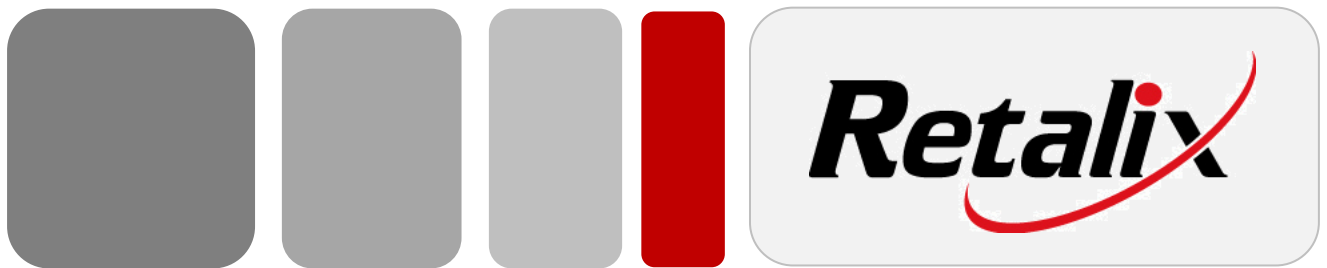


Retalix WinEPS



Release Notes
Version 827.2

Copyright © 2011 Retalix Ltd.

All rights reserved.

Israel

10 Zarhin St.

P.O. Box 2282

Ra'anana 43000, Israel

Tel: +972 9 7766677

Fax: +972 9 7400471

Website: <http://www.etalix.com>

USA

6100 Tennyson Parkway

Suite 150, Plano, TX 75024 USA.

469-241-8400

Website: <http://www.etalix.com>

Retalix technical documentation and the product(s) described herein are protected by one or more U.S. copyrights, patents, foreign patents, or pending applications. No part of this publication may be reproduced or transmitted into any human or computer language in any form or by any means, stored in a retrieval system, transmitted, redistributed, translated or disclosed to third parties, or de-compiled in any way including, but not limited to, photocopy, photograph, electronic, mechanical, magnetic or manual without the expressed written permission of Retalix Ltd., or its licensors, if any. All copies, so authorized, shall contain a full copy of this copyright notice.

Retalix products are licensed products. The product licenses convey the right to use only those specific products, components, modules, features and/or functions specified in the license agreement or contract. This publication may mention or reference products, components, modules, features and/or functions that are not part of a particular license agreement. The customer is not entitled to the receipt of, or use of, any other products, components, modules, features and/or functions that may be referenced in any documentation provided to customer unless additional license fees are paid and an appropriate license agreement is duly executed. Retalix's obligations with respect to its products and services are governed solely by the agreements under which they are provided.

U.S. Government Users Restricted Rights: If the Customer is a United States Government entity, the Retalix products described herein are "commercial computer software" as defined by current Federal Acquisition Regulation ("FAR"), Department of Defense Federal Acquisition Regulation Supplement ("DFAR"), or other applicable Agency regulation provisions. If the Retalix products described herein are other than "commercial computer software," then the United States Government Customer shall receive no greater than Restricted Rights, as defined in the currently applicable version of the FAR, DFAR, or other applicable Agency regulation. In the event that alternative regulatory rights allocation provisions are available to the parties, the provision which provides the Customer with the narrowest rights allocation permitted by law and regulation shall apply. For Civilian Agencies: Restricted Rights. Use, reproduction or disclosure is subject to restrictions set forth in subparagraph (a) through (d) of the Commercial Computer Software Restricted Rights clause at 52.227-19, as applicable, and the limitations set forth in standard Retalix license agreements for software and technical documentation.

This publication is furnished for informational use only and should not be construed as a commitment by Retalix. The information could include technical inaccuracies or typographical errors. Every effort has been made to make this publication as complete and accurate as possible, but it is provided "as is" without warranty of any kind either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. Retalix may make improvements and/or changes in the program(s), product(s), and/or applications described in this publication at any time without notice. Due to continuous development of Retalix Ltd. products, information published in this document may become obsolete.

Third-party products, services, or company names referenced in this document may be trademarked or copyrighted by their respective owners, and are for identification purposes only.

Copyrights, trademarks and license agreements shall be governed and construed in accordance with the laws of the State of Texas and the Federal Arbitration Act, and shall benefit Retalix, its successors, and assigns.

Notice

Retalix reserves the right to make changes to specification at any time and without notice. The information furnished by Retalix in this publication is believed to be accurate and reliable; however, no responsibility is assumed by Retalix and/or its affiliates 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 Retalix and/or its affiliates.

Table Of Contents

TABLE OF CONTENTS..... I

SECTION 1 1

827.2 Information 1

 Minimum System Requirements 1

 Hardware Requirements for WinEPS and OpenEPS 1

 WinEPS and OpenEPS User Account Requirements 2

 Software Requirements for WinEPS 2

 Software Requirements for OpenEPS (Front POS Lanes): 2

 PCI Compliance and Operating Systems..... 3

 Unsupported Systems 3

 Code Versions 4

 WinEPS Versions: 4

 OpenEPS Versions: 4

 OpenIP Versions: 4

 Terminal Code Versions: 5

 Stand Beside Code Versions:..... 5

 Known Issues 6

 Upgrades only supported from WinEPS version 825.0 or higher 6

 WinEPS and POS Lane Windows Accounts Require Registry Access 6

 WinEPS will not run under “Local System Account” 7

 Verifone Vx570 Stand Beside, High Memory Terminal Only 7

 Latest Mercury Host DSI..... 8

 Debit Balances Not Printed on Receipts 8

 Hypercom Terminal Issues 8

 Hypercom 4100 Terminal Code 8

 WinEPS requires Verifone Omni 3750 code version 50 or higher 9

 Linux and SOAP 9

 SOAP Requires Exclusion to DEP 9

 User Account Control (UAC) Must be Disabled..... 12

 Windows 7 Requires Administrative User Account 13

 WinEPS Fixed Issues and Enhancements..... 14

OpenEPS Changes 21

OpenIP Changes 25

Term Handler Changes 25

Host Changes 26

 ACI 26

 Ascendent 26

 Concord: EPC 27

 Concord: H&C Format 27

 Concord: Memphis 28

 Demo 28

 ePicTranz 28

 FLC Check Host 29

 LML 29

 RBS WorldPay / RBS Lynk 29

 LX1 & LX2 (Check) Hosts 30

 Mainsail 30

 Mercury 30

 MPS (Fifth Third) 31

 MTX Receipt Capture Host 31

 Schnucks Check Auth 31

 ServerEPS (Native Format) 32

 SVDot Gift Card Host 32

Terminal Code Changes 33

 Hypercom ICE5500 33

 Hypercom L4100 33

 Hypercom L4150 33

 Hypercom L4150 PCI 2.0 34

 Hypercom L4250 34

 Hypercom L5300 34

 Ingenico eN-Crypt 2100 35

 Ingenico eN-Touch 1000 35

 Ingenico 6550 / 6780 35

 Verifone Everest 36

Verifone MX830/MX850/MX860/MX870/MX880 36

Verifone Mx760/OP 4100 37

Verifone Omni 7000 37

VeriFone Vx670 (Wireless Terminal)..... 37

Stand Beside Code Changes..... 38

 Verifone Vx570..... 38

External Program Changes..... 39

 Engine Monitor and Tray Icon..... 39

 OMNI 7000 Scanmaster Code 39

 Redundancy Service 40

 UpdateXMLFiles.Exe..... 40

 Virtual Terminal 2..... 41

 Voucher Clear Application 41

SECTION 2 42

 New Features 42

 New FLC Check Host 42

 FLC Host Processor Definition Screen 42

 FLC Supported Transaction Types 45

 FLC Additional Information 46

 Voice Authorization Instead of Decline on Offline Purchase 47

 Attempt Voice Auth / Force 47

Section 1

827.2 Information

This section covers changes, bug fixes, and enhancements to the 827.2 release of WinEPS. The items listed below are the changes made only since the previous major release. Previous editions of the WinEPS Release Notes are located on the WinEPS installation CD, in the directory Documents/Old Release Notes, or contact WinEPS support for a copy.

Minimum System Requirements

- If the minimum requirements for the operating system you are using are higher than what is listed below, use those requirements instead.

Hardware Requirements for WinEPS and OpenEPS

- Pentium III (Intel or compatible) 500 MHz processor (1 GHz or faster recommended)
- 256 MB of RAM (512 MB or more recommended)
- VGA, or higher, resolution monitor set at 1024x768 or better
- CD-ROM drive for software installation
- Ethernet Card
- Drive Space Requirement for WinEPS server:
 - 600 MB of available hard disk space on the WinEPS server (1.5 Gb of drive space is recommended).
 - WinEPS requires approximately 300 Mb of space to install to; in addition a busy store can generate up to 10 Mb of log files per day. The default of 30 days storage can use up to 300 Mb of extra space resulting in the minimum requirement of 600 Mb of drive space.
 - 30 Days of log retention requires a total of 600 Mb free Hard Drive space.
 - 60 Days of log retention requires a total of 900 Mb free Hard Drive space.
 - 90 Days of log retention requires a total of 1.2 Gb free Hard Drive space.
- Drive Space Requirement for OpenEPS on each POS lane:
 - 100 Mb free drive space for configuration files and logs

WinEPS and OpenEPS User Account Requirements

The User-Updatable Encryption Keys utilize the Windows registry to store a key-part of the encryption key in use. This means that the user account under which WinEPS runs as well as the user account under which the POS system runs must have both read and write access to the registry.

If the user account does not have the appropriate rights, WinEPS will not be able to process transactions, and OpenEPS will provide an error to the POS and will likewise be unable to process transactions.

Software Requirements for WinEPS

- TCP/IP Protocol
- Any of the following Operating Systems:
 - Windows 7, 32 or 64 bit
 - Microsoft Vista SP1
 - Windows Server 2008, 32 or 64 bit
 - Microsoft Windows XP SP2, Professional
 - Microsoft Server 2003 SP 1

Caution:

WinEPS upgrades require a minimum starting version of 825.0. If you have a currently installed version of WinEPS older than Version 825.0, it must first be upgraded to 825.0 using previously available upgrade installations. Instead of upgrading a version prior to 825.0, it is highly recommended to make a backup of your WinEPS, perform a new installation, and configure your new version from scratch

Software Requirements for OpenEPS (Front POS Lanes):

- TCP/IP Protocol
- Any of the above Operating Systems, plus:
 - Windows XP Embedded
 - WePOS
 - Linux [These versions only]: Red Hat version 2.4.7-10; Fedora version 2.4.20

Under Windows Vista and above, non-administrative users may not stop or start services; the Stop and Start buttons in WinEPS will be grayed out if you are logged in to Windows on as a non-administrative Windows user.

PCI Compliance and Operating Systems

PCI requires that the security patches for software in the payments environment be tested and installed in a timely fashion. Several Microsoft operating systems have past their supported security update lifespan, and no additional security patches will be released. These operating systems include Windows NT 4.0, Windows 95/98, and 2000.

Due to the vulnerability that a lack of security patches represents, these operating systems are no longer supported for use with the WinEPS/OpenEPS product suite. Only the operating systems listed under the [Software Requirements](#) section above are supported.

Refer to information at <http://support.microsoft.com/> for the most up to date security related articles and end of support dates for all Microsoft operating systems.

Unsupported Systems

The following operating systems and hardware are not supported:

- Windows NT 4.0 is no longer supported (See PCI compliance section above)
- Windows Win95/Win98 is no longer supported (See PCI compliance section above)
- Microsoft Server 2000 is no longer supported (See PCI compliance section above)
- Microsoft Windows 2000 is no longer supported (See PCI compliance section above)
- WinEPS will not function on non NT-based Windows versions, such as Windows ME.
- XP Home version is **not** supported due to its limited scope.

Code Versions

WinEPS Versions:

Module	Version
EPSEngineSrv.Exe	827.2.0.391
EPSMenu.Exe	827.2.0.358
Rpt.Exe	827.2.0.284

OpenEPS Versions:

Module	Version	Date
mtx_eps.dll	827.2.0.390	12/3/2011
mtx_pos.dll	827.2.0.85	12/3/2011
libmtx_eps.so	827.2.0.115	12/3/2011
libmtx_pos.so	827.2.0.85	12/3/2011

OpenIP Versions:

Module	Version
OpenIPSRV.exe	826.1.0.1
TermHandlerSTSSrv.exe	825.2.0.49

Terminal Code Versions:

Terminal	Version	Additional Version Info	Date
eN-Crypt 2100	2.40		6/4/2008
eN-Touch 1000	06.06		1/20/2003
Everest	51		8/27/2010
HYP 4100	232		1/25/2007
HYP 4150	425	FPE 5.P.115	8/19/2010
HYP L4250	425	FPE 5.P.115	8/19/2010
HYP L5300	Not Yet Available		
Mx830/850/870/880	221E	RFS 18	2/17/2011
Mx860	221E	RFS 18	2/17/2011
Mx760/OP 4100	221E		2/17/2011
Omni 7000	57		1/27/2011
VX670	20		2/28/2008

Stand Beside Code Versions:

Terminal	Version	Date
Verifone Omni 3750 (No longer PED Compliant)	51	7/5/2011
VX570 (Replaces the Omni 3750)	52	9/7/2011

Known Issues

Upgrades only supported from WinEPS version 825.0 or higher

The current WinEPS install package only supports upgrades from previous versions of WinEPS 825.0 or higher. If you have a currently installed version of WinEPS older than version 825.0, it must first be upgraded to 825.0 using previously available upgrade installations. For this purpose, it is recommended to use the 826.0 installation package; the 826.0 install package supports upgrades from as old a version number as 815.3. Once an older system has been brought up to at least 825.0, the current installation package may be used to complete the upgrade to the latest version.

The 826.0 installation package can be found on the WinEPS installation CD.

If your WinEPS version is older than 815.3 it is highly recommended to make a backup of your WinEPS, perform a new installation, and configure your new version from scratch. If you do need to upgrade from a version prior to 815.3, contact MTX Support for assistance.

When performing an upgrade from the 825.0 version (only), TOR transactions will not be converted; it is therefore recommended that any location on the 825.0 version that is upgraded should begin the upgrade process only after a successful End of Day has processed to ensure there are no outstanding TOR reversals pending.

WinEPS and POS Lane Windows Accounts Require Registry Access

The new User-Updatable Encryption Keys utilize the Windows registry to store a key-part of the encryption key in use. This means that the user account under which WinEPS runs as well as the user account under which the POS system runs must have both read and write access to the registry.

If the user account does not have the appropriate rights, WinEPS will not be able to process transactions, and OpenEPS will provide an error to the POS and will likewise be unable to process transactions.

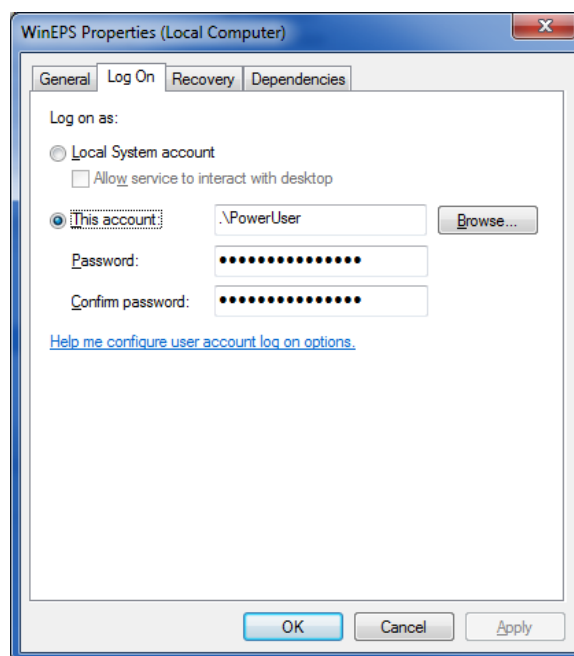
WinEPS installations using the Redundancy Service should note that the Redundancy Service also requires registry access on both the Primary and Backup WinEPS server in order to successfully transfer the key data during a synch. The user account that RS runs under should also have access to the Windows Registry.

WinEPS will not run under “Local System Account”

Due to the necessity of consistent read and write access to the Windows Registry, as well as limiting account scope to satisfy PCI requirements, WinEPS will not run if the WinEPS service is configured to use a Local System Account.

If the WinEPS Service is configured to use Local System Account, the WinEPS service will abort start up, and will shut down processing.

The account provided to run the Service should be specific pre-defined account used only to run the WinEPS and RS services.



In order to prevent accidental selection of the Local System Account option, the WinEPS Service Installation process will ONLY provide the option to enter specific account information. If you are upgrading from a previous version and have a Local System Account defined, then as part of the upgrade, the installation will prompt for the entry of new account information.

Verifone Vx570 Stand Beside, High Memory Terminal Only

Due to enhancements to the Vx570 code version 50, WinEPS now supports only the high memory version of the Vx570 terminal.

High memory terminals contain at least 12 MB of memory.

Latest Mercury Host DSI

The latest Mercury Host DSI version 2.50.3851 is required for processing with 826.1 SP1 or later. If you do not have the latest DSI, it can be found on the WinEPS release CD, in the /Tools/ Mercury Host DSI Installer/ directory.

Debit Balances Not Printed on Receipts

Some hosts incorrectly return a balance file for debit transactions linked to customer accounts. For all debit transactions, balances will not be printed on the receipt.

Hypercom Terminal Issues

The previous USB driver was reported to have issues in the field; however, when using the latest version of the USB driver provided by Hypercom, Hypercom terminals using the non-powered version of the USB cable lose connection at points during the transaction processing. As such MTXEPS is not releasing the latest driver USB driver with the 826.1 WinEPS release.

No updated USB driver is available from Hypercom that corrects both of the above issues as yet. For locations experiencing issues with their current USB driver, you may wish to contact Hypercom to receive their latest version, providing the terminal is not using the non-powered USB. Locations using non-powered USB are recommended to continue using the older driver.

Hypercom 4100 Terminal Code

The Hypercom 4100 terminal continues to be released with the most recent version of code that functions for all versions of the 4100, which is version 232. The most recent version of the Hypercom code is version 425; however, due to differences in the Hypercom 4100 units themselves, this code version will not load on all models.

For the 425 code version to load successfully, the Hypercom 4100 unit must be the high-memory version. This code will not function on the low memory version, and attempting to load it on the low memory version could damage the terminal. To determine if you have the high or low memory version of the 4100, contact your terminal vendor.

The 4100 terminal will not be able to take advantage of the new features for entry of PAN or CCV2 at the terminal without the latest 425 code version.

If you determine that your 4100 is the high memory version and would like to acquire the latest terminal code for it, contact MTXEPS Support.

WinEPS requires Verifone Omni 3750 code version 50 or higher

Locations using the older Omni 3750 terminal (not the VX570) must upgrade their 3750 terminals to code version 50 or later prior to upgrading to WinEPS version 827.0.

To upgrade the terminal code, take the latest code from the 827.0 install CD ([CD Drive]:\OpenEPS\SCAT Code\Vx570 & Onmi 3750 Verifone IP Stand Beside\OMNI 3750 Stand Beside), OMNI 3750 Term Code.zip and place it into the C:\Program Files\MicroTrax\EPS\config\terminalcode folder. Verify that your lane configuration for the 3750 has that file selected for its terminal code [OpenEPS Lanes button | select terminal config | Pin Pad Configuration tab, Terminal code File selection box]. Once the terminal code has been configured, stop and restart WinEPS, then sign on with the terminal to allow automatic upgrade.

After upgrade of the 3750 completes, you may proceed with upgrading WinEPS to 827.

Linux and SOAP

OpenEPS now uses SOAP instead of FTP to transfer files; in full installations of Linux, the proper libraries are already present to support SOAP functionality; however, some POS systems use reduced capacity Linux loads that may not have all the required library files.

In order to install the potentially missing libraries, go to the \OpenEPS\Linux OpenEPS\ directory on the WinEPS installation CD. Extract the extra.soap.so.tgz file to the /usr/lib/ directory. Use the change mode command (chmod 777) to set the attributes.

You must also update the locale (/etc/sysconfig/i18n) with the following information:

- LANG="en-US.utf8"
- SUPPORTED="en_US.utf8:en_US:en"
- SYSFONT="lat0-sun16"
- SYSFONTACM="iso01"

SOAP Requires Exclusion to DEP

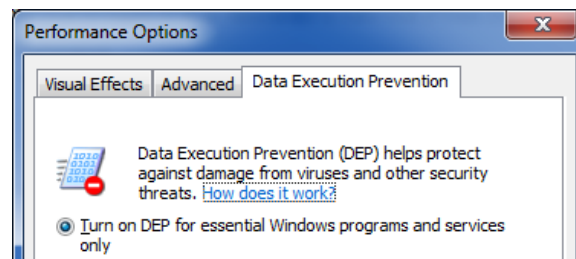
Windows Server 2008, Windows 7 and Windows XP all contain a security feature called Data Execution Prevention. In Windows Server 2008 and Windows 7, the Windows Data Execution Prevention is defaulted to on for all programs; in Windows XP it can be manually configured.

The update to the use of SOAP for file transfer requires that computer systems running any component that requires the use of SOAP have that component excluded from DEP, if DEP is running.

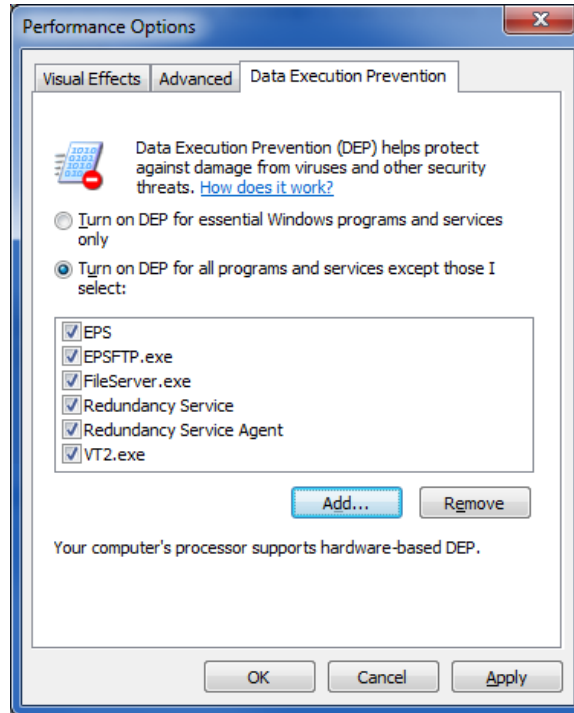
For WinEPS servers, this means excluding the WinEPS engine executable from DEP; for OpenEPS POS lanes, the POS executable that loads OpenEPS must be excluded and if running Virtual Terminal, the Virtual Terminal executable must be excluded. Finally, if using Redundancy, the redundancy executables must be excluded.

To modify the DEP settings use the following instructions:

1. On Windows 7/Server 2008, Go to start/windows logo, right click Computer and select Properties.
On Windows XP, Right click My Computer, choose Properties.
2. On Windows 7/Server 2008, Click on Advanced system setting on the left side of the screen under Control Panel Home.
3. Go to the Advanced tab and click the Settings button under Performance, then select the Data Execution Prevention tab.
4. If the DEP is set to the first radio button, where it is turned on only for Windows programs and services, you do not need to make any changes.



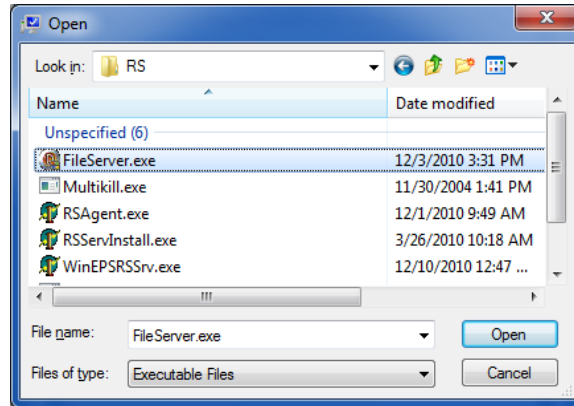
5. If it turned on for all programs and servers as shown below, click the Add button.



6. Use the opened selection box to select the executables that require exclusion from DEP. The following list details all MTXEPS files that require exclusion:
 - WinEPS
 - EpsEngineSrv.exe
 - OpenEPS
 - VT2.exe
 - POS Executable [The executable that loads the OpenEPS mtx_pos.dll file]
 - Redundancy Service:
 - WinEPSRSSrv.exe
 - FileServer.exe
 - RSAgent.exe

All of the above file use SOAP to communicate and to download files.

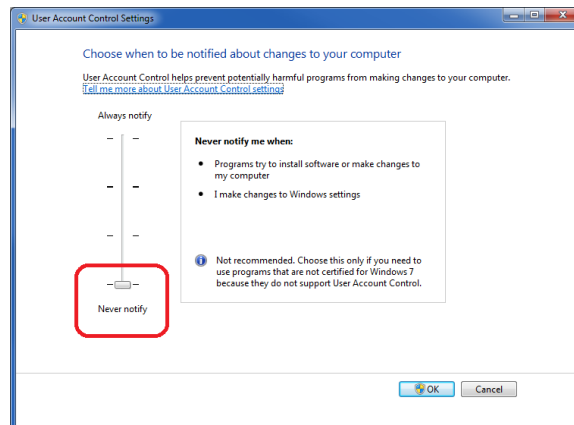
7. Add all the relevant executables to the exclusion list.
 - The WinEPS executables are located by default in the C:\Program Files\MicroTrax\EPS folder.
 - The OpenEPS executables are located by default in the C:\Program Files\MicroTrax\OpenEPS folder.
 - RS executables are located by default in the C:\Program Files\MicroTrax\RS folder.



8. Browse to the appropriate directory and select the executable, then click Open and the executable will appear in the DEP exception list. Do the same for all the executables to be added on the current PC. The PC may not have all three applications loaded (WinEPS, OpenEPS and RS), so add the executable from the applications that are loaded.
9. Restart the PC for the changes to take effect.

User Account Control (UAC) Must be Disabled

When using WinEPS or OpenEPS on any of the Microsoft Operating Systems that utilize User Account Control (Windows Vista, Windows Server 2008, Windows 7) the system must be set to the “Never Notify” level.



Failure to set the User Account Control properly can result in a failure to process transactions, as the UAC can prevent WinEPS from properly accessing the Windows Registry.

Windows 7 Requires Administrative User Account

The user account that WinEPS & Redundancy Service runs under is typically recommended to be a Power User account, however in Windows 7, the Power User group and account type have been deprecated and no longer have the elevated access required to run the WinEPS software suite. As such, when installing WinEPS or RS on a Windows 7 OS, the account used must be a Windows administrator account.

WinEPS Fixed Issues and Enhancements

Enhancement	Description
<p>1. TOR sent to host incorrectly updates pending offline</p>	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected an issue with offline pending transaction when it's corresponding TOR was processed to the host.
<p>2. Improve handling of potential bad KEK3 in registry (827.2)</p>	<ul style="list-style-type: none"> ▪ Enhancement ▪ During the End of Day process, WinEPS will verify the current encryption against the stored value; if different WinEPS will automatically generate a new key and re-encrypt all encrypted transaction files with the new key.
<p>3. Local System Account not supported</p>	<ul style="list-style-type: none"> ▪ Update ▪ Due to the necessity of consistent read and write access to the Windows Registry, as well as limiting account scope to satisfy PCI requirements, WinEPS will not run if the WinEPS service is configured to use a Local System Account. ▪ If the WinEPS Service is configured to use Local System Account, the WinEPS service will abort start up, and will shut down processing. ▪ Upgrade and installation packages have been updated to prompt the user for new account information in the event that the service was previously installed, and found to be using a "Local System Account". ▪ See the Known Issues section for additional information.
<p>4. Retry critical file access</p>	<ul style="list-style-type: none"> ▪ Enhancement ▪ When accessing critical files, if the file is unavailable, WinEPS will try multiple times to access the file instead of failing immediately. This will assist in overcoming issues that might arise due to short term file locks, such as during a virus scan or system operation.

WinEPS Fixed Issues and Enhancements

Enhancement	Description
5. Shut down on critical registry access error	<ul style="list-style-type: none"> ▪ Enhancement ▪ To prevent the possibility of incorrect file handling due to missing registry security information, in the event that WinEPS is unable to read/write to the Windows registry, the WinEPS service will shut down with a warning message listed on the WinEPS menu.
6. WinEPS SOAP download fail after EOD	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected an issue where file download would fail after WinEPS performed an End of Day.
7. Medigate/OTC Gift Card Support	<ul style="list-style-type: none"> ▪ Enhancement ▪ Add support for Over The Counter gift cards. ▪ When a gift card range is defined with an OTC ProgramID in the Gift Card Card Prefix Table, the gift card will be identified with the ISOTC flag when it is used at OpenEPS. The POS can pick up this flag and perform specific functionality related to this card type. ▪ OTC cards support only purchase, return and balance inquiry transactions.
8. 10054 Error	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrects an issue where a TCP/IP error 10054 was not being correctly handled which could cause the engine to become unresponsive.
9. Update WinEPS encryption modules	<ul style="list-style-type: none"> ▪ Enhancement ▪ WinEPS has been updated with the latest version of encryption modules.
10. Updated WIC Packages	<ul style="list-style-type: none"> ▪ Enhancement ▪ The latest WIC packages have been included in the installation and upgrade packages for WinEPS.

WinEPS Fixed Issues and Enhancements

Enhancement	Description
11. Remove unused term code box	<ul style="list-style-type: none"> ▪ Fixed ▪ Removed Terminal Code File box and selection button from WinEPS GUI for VX670, VX570, and Omni 3750 stand beside terminals, as that option was not used for these 3 terminal types. ▪ Removed Terminal Code File box and selection button from WinEPS GUI for the Everest and Omni 7000 terminal as the terminal code files in use by these terminals are not dynamic.
12. Old process.xml setting interfering with CPP xlm 'Skip sig' setting	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected an upgrade issue where the previous global setting for skipping the signature under a given \$ amount was not correctly added to the new card process profile setting and deleted from the old configuration file location. ▪ OpenEPS has also been updated to ignore the old setting, so as to prevent interference with the current configuration in any store location that has already performed an upgrade.
13. Remove Mainsail Host	<ul style="list-style-type: none"> ▪ Removed Host ▪ Mainsail host has been removed from WinEPS. Once upgraded to the 827.2 version, this host will no longer be available for processing.
14. b - Verify Card option to Verify Last 4 Card Digits	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected menu issue with selecting and configuring the b – Verify Card TAC.
15. Invalid socket handle	<ul style="list-style-type: none"> ▪ Fixed ▪ Resolved an issue where the server was receiving repeated Windows errors related to socket disconnects, which affected transaction processing.

WinEPS Fixed Issues and Enhancements

Enhancement	Description
16. SOAP File uploads stream in 1MB packets	<ul style="list-style-type: none"> ▪ Enhancement ▪ File transfer using SOAP now streams files in 1 MB packets. Previously the whole file was loaded into memory and transferred as one packet, which caused larger amounts of memory to be required to transfer successfully.
17. Credit/Fleet Prefix logic change	<ul style="list-style-type: none"> ▪ Enhancement ▪ Updated the WinEPS Fuel interface so that if a transaction is received from fuel lane with a tender type of credit and the card number used is located successfully in both the Credit and Fleet prefix tables, the transaction will be handed as a Fleet transaction, and the request for additional Fleet data will be returned to the fuel lane pump.
18. BDE installation removed	<ul style="list-style-type: none"> ▪ Enhancement ▪ The Borland Database Engine installation has been removed from WinEPS and will no longer install with WinEPS. WinEPS no longer requires the use of BDE. ▪ The Configuration Terminal Configuration > Other Lanes settings have been removed. BDE was previously used for these lanes.
19. EBT voucher with void not set to host	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected an issue where the Void of an Offline EBT Food voucher transaction is set up to the host, but the original purchase was not. This has been revised so that both the initial purchase and the void are correctly processed to the host.
20. Remove signature lines on Credit Voids	<ul style="list-style-type: none"> ▪ Enhancement ▪ Removed Signature line from Credit Void receipts. Signatures are not required for voids.
21. OpenEPS receipt message format	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected an issue with unformatting card numbers sent to WinEPS as part of the signature capture receipt transactions.

WinEPS Fixed Issues and Enhancements

Enhancement	Description
<p>22. Update Engine to match current Backup.bat file</p>	<ul style="list-style-type: none"> ▪ Fixed ▪ Resolved an issue where not all files were zipped up into the Backup.Zip file during the end of day process.
<p>23. Added Discover Korean BC Credit Prefix Ranges</p>	<ul style="list-style-type: none"> ▪ Enhancement ▪ New Discover Card ranges have been added to WinEPS for the Korean BC card. These new prefixes are linked to the standard DS Discover card code.
<p>24. Status info listed in the log</p>	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected the formatting of the status message in the WinEPS Log file, and limited the size of the string printed.
<p>25. CC #'s masking asterisks issue</p>	<ul style="list-style-type: none"> ▪ Fixed ▪ Resolved an issue where after an upgrade, reporting would not correctly display the first 6 and last 4 of the card data.
<p>26. Increase default for archives stored</p>	<ul style="list-style-type: none"> ▪ Enhancement ▪ In the event that the configuration file is missing or corrupted, the default time for storing archives is set to 90 days to allow for troubleshooting and avoid any potential loss of info.
<p>27. SOAP File Download changes</p>	<ul style="list-style-type: none"> ▪ Enhancement ▪ To improve the speed of lanes becoming active, some changes have been made to the SOAP file download feature. Instead of having a 3 minute time out for all files, if the file to be transferred is under 2MB, timer is set to 30 seconds instead; files over 2MB will retain the full 3 minute time out. ▪ File transfers that fail will be retried multiple times, in order to attempt to transfer the time to the lane. ▪ Additional logging has been put in place in the engine to identify the IP address lane that is making the file download request.

WinEPS Fixed Issues and Enhancements

Enhancement	Description
<p>28. Increased memory use getting MAC address</p>	<ul style="list-style-type: none"> ▪ Fixed ▪ Fixed an issue where increased handles and memory use happens when WinEPS Engine perform MAC address checks on the NIC card.
<p>29. Add module date stamp to logging</p>	<ul style="list-style-type: none"> ▪ Enhancement ▪ To improve the ability to identify the files in use, in addition to the standard logging of the module version numbers, the change data will also be reported in the logs.
<p>30. Transaction uses wrong buffer</p>	<ul style="list-style-type: none"> ▪ Fixed ▪ Resolved an issue with the ScanMaster Version 1 interface where transactions coming in from other lanes in the middle of an ongoing transaction were using wrong buffer.
<p>31. MS Discontinued Support for Windows 2000</p>	<ul style="list-style-type: none"> ▪ Deprecate Windows 2000 ▪ According to the Microsoft site, Microsoft has discontinued support for the Windows 2000 operating system. As such, this OS is no longer a supported operating system for the WinEPS/OpenEPS software.
<p>32. Uptime logging error</p>	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrects an issue that would cause “catastrophic error” to be incorrectly and unnecessarily logged in the spool.
<p>33. Lane start up logging</p>	<ul style="list-style-type: none"> ▪ Fixed ▪ Update logs so that lane type logged is consistent with what is listed in WinEPS menu.
<p>34. Add Digital ID config to B TAC</p>	<ul style="list-style-type: none"> ▪ Enhancement ▪ Added Digital ID setting to the B – Slide Card TAC.

WinEPS Fixed Issues and Enhancements

Enhancement	Description
<p>35. Correct ZIP file process failure</p>	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected an issue where a large number of lane journal files uploaded to WinEPS at the same time would cause zip archiving failures. Archiving is now handed in series by creating a queue of log file to zip.
<p>36. Import of DebitBIN.eps</p>	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected an issue with the import of the DebitBIN.EPS file provided by the ServerEPS Bin File Service. This file will now import correctly and update the BIN file listing in WinEPS.

OpenEPS Changes

Enhancement	Description
<p>1. POSVerifyCardLast4 incorrectly defined</p>	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected the POSVerifyCardLast4 function call so that it is properly defined as per the specification.
<p>2. Tender Type Status set to Loop for Gift and EBT</p>	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected an issue where the tender type status was not being set to OK if the POS set EBT Food or Gift as the tender, with the \$ - Purch/Bal Inq TAC in the transaction sequence.
<p>3. OpenEPS Not Downloading Files from Backup Server</p>	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected an issue where OpenEPS would not switch over to the backup WinEPS server to download files when the primary server was no longer available.
<p>4. Revise credit cash back</p>	<ul style="list-style-type: none"> ▪ Fixed ▪ To prevent unnecessary prompting, the Cashier Ok Cashback TAC will not be processed for credit when the cashback amount is \$0.
<p>5. Travelers Checks declined for cash back only</p>	<ul style="list-style-type: none"> ▪ Fixed ▪ Fixed an issue with Travelers checks being incorrectly declined at the POS if only cash back was entered.

Enhancement	Description
<p>6. Freq Shopper / Digital ID Enhancement</p>	<ul style="list-style-type: none"> ▪ Enhancement ▪ Added a new feature to the B - Slide Card TAC to display a Digital ID button. ▪ When configured and using the screen files that support this new button, the Digital ID button will appear on the screen for customer selection. The customer can then either slide their payment card or select the Digital ID button. When selected the customer is prompted for their Frequent Shopper number, which is then stored in the FrequentShopperData function for the POS to pick up. ▪ New screen files for Digital ID support are available for the MX terminals only. ▪ When a customer uses the new Freq Shopper / Digital ID and enters a number on the PIN Pad, the value entered will be set to the new FrequentShopperData function. ▪ To supplement the acquisition of the Digital ID, the new FrequentShopperData function has been added. See next enhancement.
<p>7. New FrequentShopperData function & Data Entry Mode 13</p>	<ul style="list-style-type: none"> ▪ Enhancement ▪ A new FrequentShopperData function call has been added to allow POS to pick up data after customer selects Freq Shopper/Digital ID button. ▪ A new EntryMode of 13 (Numeric entry OR Payment Card Slide) is now available for the Data Entry function call. This Entry Mode is used in DigitalID prompting, and activates both the keyboard and the MSR, with any keyboard entry placed in DataEntryValue, and the Card swipe treated as a payment card. ▪ When using the DataEntry call new EntryMode Value of 13, if OpenEPS gets a numeric entry by the customer, the value will be set in both the standard DataEntryValue function, and OpenEPS will also populate the FrequentShopperData function with that same entered value.

Enhancement	Description
<p>8. DataEntry Continue</p>	<ul style="list-style-type: none"> ▪ Enhancement ▪ Added new call DataEntryContinue to OpenEPS that the POS can call in order to instruct OpenEPS to move on to the next action sequence.
<p>9. Revise OpenEPS startup</p>	<ul style="list-style-type: none"> ▪ Enhancement ▪ Improved OpenEPS startup routine in order to avoid potential issues that could cause hanging.
<p>10. New function to provide original card type to POS</p>	<ul style="list-style-type: none"> ▪ Enhancement ▪ The new WinEPSCardTypeOriginal function has been added to OpenEPS that provides the Card Type data prior to any conversion of the card type to FSA. This function is useful in determining the original card type used by the customer in an FSA transaction.
<p>11. Driver's License invalid card</p>	<ul style="list-style-type: none"> ▪ Fixed ▪ Resolved an issue where sliding a driver's license in place of a check read would always cause an "Invalid Card Decline."
<p>12. Customer display not correct on manual entry</p>	<ul style="list-style-type: none"> ▪ Fixed ▪ Fixed issue when manual entry is selected during the transaction, and get PAN from PIN pad is not set, the appropriate prompt was not displayed.
<p>13. File Downloading impacts payment connection</p>	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected an issue were file downloads that took a long period of time, or that failed were causing the payments connection from the lane to WinEPS to disconnect. The issue has been corrected by limiting the re-tries of failed files, and ensuring that the payments connection does not disconnect regardless of the success or failure of the file downloading.
<p>14. Unsupported card error when Raw MICR set as Primary ID</p>	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected an issue with PrimaryID getting invalid MICR when Raw MIRC was set in the field.

Enhancement	Description
<p>15. Void Last transactions getting MTX-131 declines</p>	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected an issue where Void Last transactions were receiving a decline incorrectly.
<p>16. Check with Secondary ID and cashback issue</p>	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected an issue where a check that uses the Secondary ID Prompt for Check Type with the customer cash back TAC would cause the POS to loop indefinitely on waiting for the SCAT Status.

OpenIP Changes

Enhancement	Description
1. - No Change to OpenIP -	---

Term Handler Changes

Enhancement	Description
1. - No Change to Term Handler -	---

Host Changes

ACI

Enhancement	Description
1. ACI host use timer delay on offlines	<ul style="list-style-type: none"> ▪ Enhancement ▪ Updated ACI host to use the 'secs to wait to cycle offline queue' setting when determining the time for sending out an offline generated by a Try for Local response from the host.
2. Debit BIN import incorrect	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected an issue where the debitbin.txt file was not correctly imported into WinEPS at the end of day, resulting in incorrect card ranges.
3. Corrected PrePaidBin.txt import at EOD	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected an issue where the PrePaidBin.txt was not properly importing. This has been corrected so that the import works properly when the ACI host is defined.

Ascendent

Enhancement	Description
1. - No Change to Host -	---

Concord: EPC

Enhancement	Description
1. - No Change to Host -	---

Concord: H&C Format

Enhancement	Description
1. Correct manual checks to 1st Data	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected manual checks so that that WinEPS sends Transit and account info, as well as sending the Check number in Fid h, while keeping the MICR type as 18.
2. Valulink TOR sending Pan and Exp Date instead of Track2	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected an issue where WinEPS was not sending the discretionary data on ValuLink Gift Card TORs.
3. SVS Offline Gift Card Redemption Authorization	<ul style="list-style-type: none"> ▪ Enhancement ▪ A new feature has been added to convert Gift Card Redeem transactions that are attempted offline into Voice Authorizations. ▪ To assist in supporting this feature, the M - Auth Number TAC has a new "Request SVS Auth Number" setting; when this option is selected the SVS Auth number will be requested instead of the standard authorization number. ▪ Full details on this are included in Section 2.

Concord: Memphis

Enhancement	Description
1. Declines for \$0 Amount	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrects an issue with the Concord: Memphis host that was incorrectly declining an approved \$0 completion.

Demo

Enhancement	Description
1. - No Change to Host -	---

ePicTranz

Enhancement	Description
1. - No Change to Host -	---

FLC Check Host

Enhancement	Description
2. New FLC Host	<ul style="list-style-type: none"> ▪ Enhancement ▪ The New FLC Check Host has been added to WinEPS for the PULSE Project. ▪ This check host includes new functionality handling a new Soft Approval and 2 new Soft Decline types. ▪ Full details on this are included in Section 2.

LML

Enhancement	Description
1. - No Change to Host -	---

RBS WorldPay / RBS Lynk

Enhancement	Description
1. Blackhawk requires LA#	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected an issue with Lynk host Blackhawk Gift Cards where the WinEPS local authorization number was not properly passed to the host in the Auth Code field on activations.

LX1 & LX2 (Check) Hosts

Enhancement	Description
<ol style="list-style-type: none"> Slot released too early on invalid partial approval 	<ul style="list-style-type: none"> Fixed Corrected an issue where a partial approval returned for a lane that does not support partial approvals would result in WinEPS releasing the slot prior to the reversal being sent up. The slot is now held until the reversal is sent.

Mainsail

Enhancement	Description
<ol style="list-style-type: none"> - No Change to Host - 	---

Mercury

Enhancement	Description
<ol style="list-style-type: none"> - No Change to Host - 	---

MPS (Fifth Third)

Enhancement	Description
1. - No Change to Host -	---

MTX Receipt Capture Host

Enhancement	Description
1. - No Change to Host -	---

Schnucks Check Auth

Enhancement	Description
1. - No Change to Host -	---

ServerEPS (Native Format)

Enhancement	Description
1. - No Change to Host -	---

SVDot Gift Card Host

Enhancement	Description
1. Declines for \$0 Amount	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrects an issue with SVDot host that was incorrectly declining an approved \$0 completion.

Terminal Code Changes

Hypercom ICE5500

Enhancement	Description
1. Remove support for Ice 5500	<ul style="list-style-type: none"> ▪ Terminal removed ▪ Removed support for the Hypercom Ice 5500 terminals from WinEPS.

Hypercom L4100

Enhancement	Description
1. WIC Enhancement: Remove Card	<ul style="list-style-type: none"> ▪ Enhancement ▪ Improved the handling of the "Remove_WIC_ICC" POS call to enable the Hypercom PIN pads to display an appropriate message.

Hypercom L4150

Enhancement	Description
1. WIC Enhancement: Remove Card	<ul style="list-style-type: none"> ▪ Enhancement ▪ Improved the handling of the "Remove_WIC_ICC" POS call to enable the Hypercom PIN pads to display an appropriate message.

Hypercom L4150 PCI 2.0

Enhancement	Description
1. WIC Enhancement: Remove Card	<ul style="list-style-type: none"> ▪ Enhancement ▪ Improved the handling of the “Remove_WIC_ICC” POS call to enable the Hypercom PIN pads to display an appropriate message.

Hypercom L4250

Enhancement	Description
1. WIC Enhancement: Remove Card	<ul style="list-style-type: none"> ▪ Enhancement ▪ Improved the handling of the “Remove_WIC_ICC” POS call to enable the Hypercom PIN pads to display an appropriate message.

Hypercom L5300

Enhancement	Description
1. Add HYP5300 to WinEPS	<ul style="list-style-type: none"> ▪ Enhancement ▪ Added support for the Hypercom 5300 terminal. ▪ Terminal code for this terminal is not yet available.

Ingenico eN-Crypt 2100

Enhancement	Description
1. - No Change to Terminal Code -	---

Ingenico eN-Touch 1000

Enhancement	Description
1. - No Change to Terminal Code -	---

Ingenico 6550 / 6780

Enhancement	Description
1. - No Change to Terminal Code -	---

Verifone Everest

Enhancement	Description
1. - No Change to Terminal Code -	---

Verifone MX830/MX850/MX860/MX870/MX880

Enhancement	Description
1. Allow Cent Entry for Customer Cash Back on MX terminals	<p>Enhancement</p> <ul style="list-style-type: none"> ▪ A new option has been added to the Terminal Configuration, PIN Pad Configuration Tab that will allow customer entered cashback amounts to be in cents instead of whole dollars for the MX 800 series terminals. ▪ This change only affects the “Other” cashback button where customers can determine and enter their own cashback amount. Other default amounts will remain in whole dollars.
2. MX terminal code to 221e	<ul style="list-style-type: none"> ▪ Certification ▪ The latest MX code version 221e has been included in the WinEPS installation.
3. Send Packages Info in Status Message	<ul style="list-style-type: none"> ▪ Enhancement ▪ Expand the status MX status message field to add an <AdditionalInfo> tag where the package info can be sent to WinEPS for monitoring and reporting purposes.
4. Add Tender buttons 5 and 6 to MX880 terminal	<ul style="list-style-type: none"> ▪ Enhancement ▪ The MX880 terminal interface has been improved by adding in support for buttons 5 and 6.

Verifone Mx760/OP 4100

Enhancement	Description
1. - No Change to Terminal Code -	---

Verifone Omni 7000

Enhancement	Description
1. Omni 7000 terminal code not downloading	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected an issue where the terminal code for the Omni 7000 was not properly included in the installation for download to the lanes.
2. Omni 7000 code version 57	<ul style="list-style-type: none"> ▪ Certification ▪ Version 57 of the Omni 7000 terminal code has been certified and is now included in the WinEPS installation.

VeriFone Vx670 (Wireless Terminal)

Enhancement	Description
1. - No Change to Terminal Code -	---

Stand Beside Code Changes

Verifone Vx570

Enhancement	Description
1. Correct gzip bug	<ul style="list-style-type: none">FixedRemoved change to the GZIP routine that prevented code update to the v51 code.
2. VX-570 code updated to handle unused items	<ul style="list-style-type: none">FixedUpdated terminal code to ignore unused bits in incoming messages, and to handle unused tags in downloaded XML configuration files.
3. Version 52 terminal code for the VX-570 terminal	<ul style="list-style-type: none">CertificationVersion 52 (9/7/2011) of the Vx570 terminal code has been certified.

External Program Changes

Engine Monitor and Tray Icon

Enhancement	Description
1. - No Change to Engine Monitor and Tray Icon -	---

OMNI 7000 Scanmaster Code

Terminal code for the Scanmaster system is written and maintained by Concord. It is distributed on the WinEPS installation CD for convenience only.

Enhancement	Description
1. - No Change to OMNI 7000 Scanmaster Code-	---

Redundancy Service

Enhancement	Description
1. RS will remove expired archives from Backup	<ul style="list-style-type: none"> ▪ Enhancement ▪ The redundancy service has been enhanced to remove expired archive files from the Backup server. RS uses the WinEPS archive settings to determine when archive files expire, so no additional configuration is required for this enhancement. ▪ Archive files are deleted securely, to comply with PCI requirements.
2. RS Archive viewing error	<ul style="list-style-type: none"> ▪ Fixed ▪ Corrected an issue where viewing the Archived RS reports would incorrectly overwrite and delete the current actlog.
3. RS Logging and Messaging Improvements	<ul style="list-style-type: none"> ▪ Enhancement ▪ Redundancy Service logging has been improved for clarity. All WinEPS communication lines will be logged with "WINEPS MESSAGE", failed synchs will be displayed on the RS GUI; File transfer will be logged as OK, Failed or Hashes Match, No Transfer.
4. Build the transaction list after critical file synch	<ul style="list-style-type: none"> ▪ Enhancement ▪ To improve performance, RS will now build the actlog transaction list just after the critical file transfer.

UpdateXMLFiles.Exe

Enhancement	Description
1. - No Change to UpdateXMLFiles.Exe-	---

Virtual Terminal 2

Enhancement	Description
1. - Virtual Terminal 2-	---

Voucher Clear Application

Enhancement	Description
1. Allow 'Never Expires' option for Voucher Operators	<ul style="list-style-type: none"> ▪ Enhancement ▪ To allow Voucher Clear user accounts to persist, the Operator account screen has been updated to allow the selection of the “Never Expires” option if the Operator account created has the Voucher Clear application access right. ▪ Operator accounts designed to access the voucher clear application are recommended to only have access to that application, and not to WinEPS functionality.

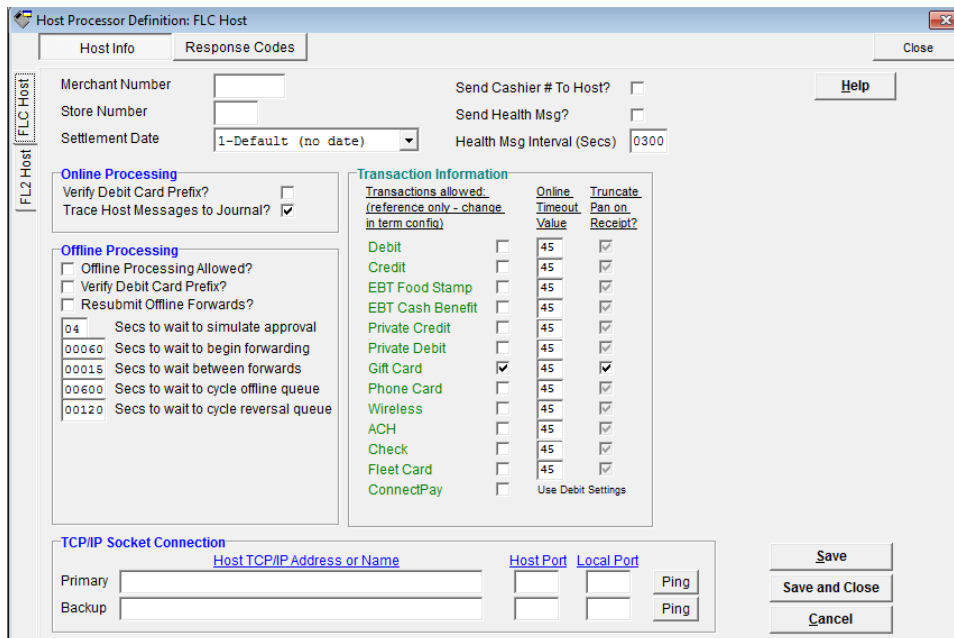
Section 2

New Features

New FLC Check Host

FLC Host Processor Definition Screen

This screen contains all the configuration options pertaining to the selected host.



FLC Host Info Screen

Enhancement	Description
Merchant Number	Supplied by host
Store Number	Supplied by host
Settlement Date	Default (No Date) Current date Current data minus 1
Online Processing	Verify Debit Card Prefix? <ul style="list-style-type: none"> ▪ Check this box to force verification of Debit prefixes against the WinEPS debit bin file Trace Host Messages <ul style="list-style-type: none"> ▪ Should always be checked; this provides additional information for troubleshooting.
Offline Processing	Offline Processing allowed? <ul style="list-style-type: none"> ▪ Indicates whether offline processing for this host is allowed. Verify Debit Card Prefix? <ul style="list-style-type: none"> ▪ Check this box to force verification of Debit prefixes against the WinEPS debit bin file Resubmit Offline Forwards? <ul style="list-style-type: none"> ▪ Check to save and resubmit offline forwards that were declined due to insufficient funds; attempts over the next several days to complete the offline transaction.
Send Health Msg?	If checked, a health message is sent to the host.

Enhancement	Description
Health Msg Interval (Secs)	If the Send Health Msg? option is checked, this option determines how often the health message is sent up, in seconds.
Primary Addr or Name	Supplied by host
Backup Addr or Name	Supplied by host

Buttons	Description
Help	Brings up this Help screen
Save	Saves configuration changes without closing screen.
Save and Close	Saves configuration changes and closes the screen.
Cancel	Closes screen without saving changes.

FLC Supported Transaction Types

	Purchase / GC Redeem	Purch w/ CB	Cash Back Only	Return	Force [Voice/Voucher]	Return Voucher	Balance Inquiry	Activation	Deactivation	Recharge	PreAuth / Completion
ACH	X	X	X	X	X	NA	NA	NA	NA	NA	X
Check (Electronic Check Conversion)	O (VO)	O (VO)	O (VO)	NA	X	NA	NA	NA	NA	NA	NA
Check (Standard)	O (VO)	O (VO)	O (VO)	NA	X	NA	NA	NA	NA	NA	NA
Connect Pay	X	NA	NA	X	NA	NA	NA	NA	NA	NA	NA
Credit Card	X	X	X	X	X	NA	NA	NA	NA	NA	X
Debit	X	X	X	X	NA	NA	NA	NA	NA	NA	X
EBT – Cash	X	X	X	X	X	NA	X	NA	NA	NA	X
EBT – Food Stamp	X	NA	NA	X	X	NA	X	NA	NA	NA	NA
Fleet	X	NA	NA	X	X	NA	NA	NA	NA	NA	X
Gift Card	B	NA	NA	X	X	NA	X	X	X	X	X
Phone Card	NA	NA	NA	NA	NA	NA	NA	X	X	X	NA
Private Credit	X	X	X	X	NA	NA	NA	NA	NA	NA	X
Private Debit	X	X	X	X	NA	NA	NA	NA	NA	NA	X
Wireless	NA	NA	NA	NA	NA	NA	NA	X	X	X	NA

Legend:
O – Online only
B – Both On & Offline
B/Disc – As **B**, with Discover Card only
(V) – Transaction Can be Voided
(VO) – Can be Voided Online Only
X – Not Supported
NA – Not Applicable to Transaction Type

FLC Additional Information

ECC Conversion can only occur for online transactions

Offline check approvals are governed by the standard Offline amounts, as defined in the Card Processing Profile. If the transaction is under the approval amount, the check will be approved as a paper auth and the cashier will need to keep the check.

Offline Paper check auths are not stored and forwarded to the host

Offline Void of Online ECC is stored and sent up to the host later, when the host connection is reestablished.

Voids of Paper Auth checks are supported, but are not required to be performed, as paper auths are not considered financial transactions.

The FLC host supports using the following new response codes:

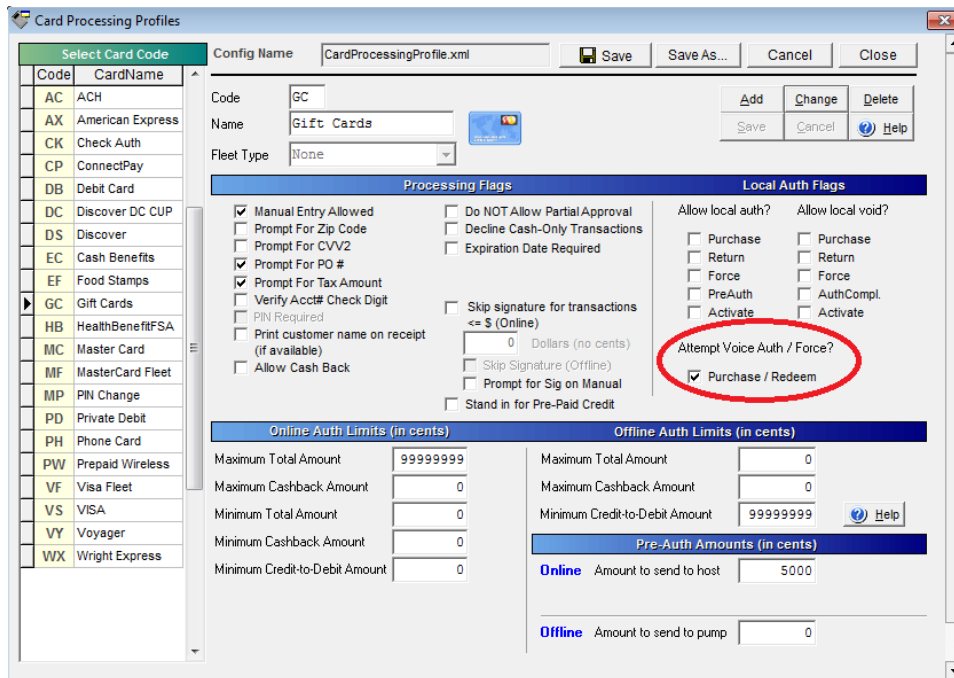
- AS – Soft Approval; Indicates that Telecheck has approved the transaction for ECC and requires signature confirmation before proceeding.
- NE – Soft Decline, request for additional information
- NG – Soft Decline, request for additional information

When the FLC host is defined, the FL2 host will automatically be defined as well. The FL2 host is not in use at this time, however. The FL2 host should have its primary IP address defined as 127.0.0.1, with a port defined as an open port on the local machine, such as 5110.

Voice Authorization Instead of Decline on Offline Purchase

Attempt Voice Auth / Force

A new option for Purchase / Redeem transactions has been added to the Card Process Profiles screen that will attempt perform a Voice Authorization for offline transactions, instead of declining. To use this option, the POS must support the NV Soft Decline response code.



When the Attempt Voice Auth / Force option is selected for Purchase / Redeem, whenever a Purchase / Redeem transaction is attempted offline, instead of receiving a hard decline, WinEPS will provide an NV soft decline to the POS, which will prompt the cashier to attempt to perform a Voice Authorization. If a voice auth is performed, and an approval number is entered, the transaction is then stored for processing to the host at a later time as a pre-approved Force transaction.

Attempt Voice Auth / Force is available only for Purchase / Redeem transactions.

The Attempt Voice Auth / Force takes the place of standard offline processing where a dollar amount is specified for approval; if Attempt Voice Auth / Force is configured for Purchase / Redeem, the standard offline process will be disabled for Purchase / Redeem, and any amounts listed for Offline will be ignored for Purchase / Redeem transactions.