StoreNext

WinEPS Release Notes

Version 825.1 SP4

WinEPS Release Notes

Date of Issue	Product Identification Number	Part Number	Brief Description
October 2005	45001/096	89000261	815.3 SP1
April 2006	45001/096	89000303	817 SP2
June 2006	45001/096	89000310	818 SP1
July 2007	45001/096	89000388	821
August 2007	45001/096	89000389	822
August 2007	45001/096	89000390	823
November 2007	45001/096	89000407	823 SP1
January 2008	45001/096	89000414	823 SP2
March 2008	45001/096	89000430	824 SP1
July 2008	45001/096	89000459	825.0 SP2
May 2009	45001/096	89000512	825.1 SP4

Address comments and corrections to:

StoreNext Retail Technologies LLC, Software Program Director
6100 Tennyson Parkway / Suite 130 / Plano, Texas 75024

Table of Contents

Section 1

825.1 SP 4 Information

This section covers changes, bug fixes, and enhancements to the 825.1 SP 4 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 800 x 600 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

Software Requirements for WinEPS

- TCP/IP, FTP and FTPS Protocols
- Any of the following Operating Systems:
  - Microsoft Server 2000/2003 SP 1
  - Microsoft Windows 2000, SP 4
  - Microsoft Windows XP SP2, Professional

WinEPS upgrades require a minimum starting version of 815.3. *If you have a currently installed version of WinEPS older than Version 815.3, it must first be upgraded to 815.3 using previously available upgrade installations. Instead of upgrading a version prior to 815.3, 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, FTP and FTPS Protocols
- Any of the following Operating Systems:
  - Microsoft Server 2000/2003 SP 1
  - Microsoft Windows 2000, SP 4
  - Microsoft Windows XP SP2, Professional
  - Windows XP Embedded
  - WePOS
  - Linux [These versions only]: Red Hat version 2.4.7-10; Fedora version 2.4.20

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 and Windows 95/98.

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)
- 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.

- Windows Vista operating system is not currently supported; this operating system is being researched for future support options.
- 64 bit operating systems and processors are not currently supported; these are being researched for future support options.

Code Versions

WinEPS Versions:

Module	Version
EPSEngineSrv.Exe	825.1.3.740
EPSMenu.Exe	825.1.4.319
Rpt.Exe	825.1.0.275

OpenEPS Versions:

Module	Version	Date
mtx_eps.dll	825.1.0.950	2/18/2009
mtx_pos.dll	825.1.0.99	12/30/2008
libmtx_eps.so	825.1.0.708	3/11/2009
libmtx_pos.so	825.1.0.3	2/24/2009

Terminal Code Versions:

Type	Terminal	Version	Date
SCAT / Script / Terminal Code	C2000	32	1/5/2005
	eN-Crypt 2100	2.40	6/4/2008
	eN-Touch 1000	06.06	1/20/2003
	Everest	49	9/5/2008
	HYP 4100	331	2/13/2009
	HYP 4150	331	2/13/2009
	HYP L4250	331	2/13/2009
	ICE 5500	120	12/10/2007
	ICE 6000	120	12/10/2007
	Mx830/850/870	220N	7/1/2008
	Mx860	220N	7/1/2008
	NCR 5993	13	2/8/2007
	Omni 490	64	12/10/2007
	Omni 7000	54	2/25/2009
	VX670	17	3/12/2008

Stand Beside Code Versions:

Type	Terminal	Version	Date
Stand Beside	Verifone Omni 3750 (No longer PED Compliant)	25	1/31/2008
	VX570 (Replaces the Omni 3750)	25	2/1/2008

Known Issues

Process all offline and TOR transactions prior to upgrade

The upgrade process will update the WinEPS and OpenEPS software to use new encryption keys. Due to this change it is strongly recommended that all offline and TOR transactions be processed prior to upgrade.

Be certain that lanes set to process transactions in Stand in at the POST mode have connectivity to the WinEPS server to ensure that offline transactions that may have been taken at the lanes are forwarded up properly; it may be necessary to sign the POS lane on if it has not been signed on already.

To verify that no offline transactions exist, select the Status button and review the Server Info and Lane Summary tabs. The Pending Transaction Offline Amount should be $0 for the server and the Offline Amount should be $0 for the lanes.

For older WinEPS version that do not have a status screen, go to Inquiry | Reports, and review the Offline Transactions, Forward Pending report.

If offline transactions exist, wait until they forward up to the host before proceeding with the upgrade.

WinEPS and OpenEPS version must match

The WinEPS software suite has been updated to utilize SSL communication. WinEPS and OpenEPS both must be updated to the 825.1 version in order to communicate and process transactions. As part of the upgrade process, a new OpenEPS DLL file will be sent down to the lane automatically to allow for the new communication.

It is important that any location that has disabled downloads of the OpenEPS software either enable the automated download or manually upgrade the POS lanes to the 825.1 OpenEPS version (using the standard OpenEPS installation).

After an upgrade if the POS cannot process transactions, verify that the OpenEPS versions in place on the lane are 825.1. If they are not, upgrade them to 825.1 using the standard OpenEPS installation.

Older, Pre-PKI 4100 terminals must be encrypted prior to upgrade

Older Pre-PKI models of the Hypercom 4100 terminal do not have a security certificate embedded in them. The latest version of the SCAT code, 329, will automatically update the terminal with the proper certificate, but the update process will only work if the terminal is encrypted. Terminals that are not encrypted, and thus not capable of taking PIN-based transactions, will need to be encrypted prior to upgrading.

Triple DES Encryption Support for the Everest+ Terminal

Triple DES (3DES) encryption is supported for the Everest+ terminal, but only for newer models. Specifically modes whose number ends in -1X (where X is the final model number such as -10, -11, -12, etc) do support 3DES encryption where modes ending in -0X (such as -01, -02, -03, etc) are NOT capable of supporting 3DES encryption.

The basic Everest version (non-Everest+) does not support 3DES.

Models that do not support 3DES encryption have been discontinued by Verifone.

Partial Approvals not allowed for transactions with Cash Back

Because of recent issues with partial payments that include cash back a change was made to the OpenEPS dll. On any transaction that includes cash back the Amount Change Allowed field will be set to False, even if the POS sets True.

This change will cause WinEPS to not send the partial approval flag to the host, and thus not allow a partial approval for any transaction that includes cash back.

If no cash back is in the order the partial approval flag set by the POS will be honored as normal.

WinEPS Fixed Issues and Enhancements

Enhancement	Description
1. Buttons misnamed on Lane Definition cancel warning	• Fixed • The information message for canceling a lane change states “Click Exit to continue, click Save and Exit to save changes" but the buttons provided did not match. • The buttons have been updated to correctly reflect the text and desired functionality.
2. Updated Encryption Keys	• Update • The internal encryption keys used by the WinEPS software suite have been changed. • New encryption keys are implemented at least yearly as required by PCI regulations. • No user action is required because of this update.
3. WinEPS/OpenEPS SSL Communication	• Enhancement • Communication between WinEPS and OpenEPS has been enhanced to utilize SSL to encrypt network traffic. • This new encryption is in addition to the previous encryption of sensitive card data fields and serves as an extra layer of defense. • SSL Encryption has also been implemented in communicating with the PIN Pad terminal. Not all terminals currently support SSL. • SSL works with redundancy, such that if the primary server fails, OpenEPS will connect up to the backup server using SSL communication. An additional Setup.Txt port entry has been added to facilitate the change over.
4. IBM to WinEPS Interface	• Enhancement • A new interface to the IBM SA has been added to WinEPS. This interface allows updated IBM code to connect directly to the WinEPS software. • The IBM interface supports the following transaction types: Credit – Purchase, Void, Return Debit – Purchase, Void EBT Food – Purchase, Void, Return, Balance Inquiry EBT Cash – Purchase, Void, Return, Balance Inquiry Private Credit (PAC Card) – Purchase, Void, Return Gift Cards – Purchase, Void, Return, Balance Inquiry, Activation, Recharge ConnectPay (ACH) – Purchase, Void Check – Purchase, Void • The IBM interface also supports FSA amounts, and Offline processing at WinEPS and at the POS back office. • The IBM lanes use a new IBM SA Terminal type in lane definition • WinEPS will not decline voids in the IBM environment, but instead will place them into the offline queue and always forward them to the host.

Enhancement	Description
5. Storeconfigurations.xml marked as critical file	• Fixed • WinEPS has been updated to include the storeconfigurations.xml as a 'critical' file in the FVersion.Txt file. • Previously, if the [Custom] tag was utilized with the FVersion.Txt and the storeconfigurations.xml was removed from the file list, it would not be sent to the OpenEPS lane. As the storeconfigurations.xml file is required for proper operation, this file is now included automatically.
6. SSL available for Fuel Lanes	• Enhancement • As part of the general SSL enhancement to the WinEPS product, Fuel Lanes may now connect up to WinEPS utilizing SSL. • The available SSL port number defaults to 6202 and may be changed in WinEPS under the Site Information | Processing Options | Payment Terminals Settings Tab. • WinEPS continues to support non-SSL fuel lanes. • Full details on this feature are included in Section 2.
7. WinEPS Web Service lane removed	• Enhancement • Web Service lane type is no longer available.
8. SSL BIOMTX socket	• Enhancement • The Biometrics socket has bee updated to support SSL. • The following versions are supported: SSL3, TLS1 and TLS1.1.
9. Exception in trouble messages	• Fixed • Corrected an issue that was causing an exception error to appear in the trouble messages section of the main WinEPS viewer screen.
10. Archive Encryption Key update	• Enhancement • As part of implementing new encryption keys, if a location performs an upgrade to the current version, all of the archive files will be updated to the latest encryption keys and methods.
11. Updated ECC Text	• Enhancement • The Electronic Check Conversion text that is supplied to the POS for printing on the receipt has been updated to comply with the most recent NACHA requirements.

Enhancement	Description
12. Response code changes require engine stop and restart	• Enhancement • The response codes data is now loaded when the WinEPS engine starts; changes to the response code table are implemented only after a stop and start or end of day. • A new notice message has been added that will inform the user that an engine stop and start is needed when changes are made to the response codes.
13. Added Fields to CSV Export	• Enhancement • The following new fields have been added to the CSV export; ZipCode (Field 86) ZipCodeEntry (Field 87) FSACard (Field 88) FSAAmount (Field 89) RXAmount (Field 90) DentalAmount (Field 91) MedicalAmount (Field 92) VisionAmount (Field 93) ProgramID (Field 94) PinPadSerial# (Field 95)
14. Local MTX Decline missing descriptive text	• Fixed • On the WinEPS main display screen, when a transaction was given a local decline, the transaction data was written to the screen without the typical descriptive text. This has been corrected so that the descriptive text is included with the decline code.
15. Sort PIN Pad dropdown list	• Enhancement • The list of available pin pad types displayed in the drop down of the Pin Pad Tab of Terminal Configuration has been sorted to improve ease of use.
16. PanHash - change existing hash process	• Enhancement • The PanHash function call has been internally improved for increased security. • The updated hash value uses the customer last name as part of the hash instead of a fixed hash value. The sequence of data has been adjusted and uses a SHA-1 hash algorithm
17. Trouble Messages log not created with EOD	• Fixed • Due to revisions in the End of Day procedure, the Trouble Message log was not being created until WinEPS needed to write a new message to it. This has been corrected so that the log is created immediately after the End of Day completes.
18. Exception in GUI after launch when bad printer is defined	• Fixed • An exception occurred in the WinEPS viewer if it was launched when a bad printer was defined that would prevent the status of the Engine and Lanes from being displayed properly. • This issue has been corrected so that if an invalid printer is defined, the WinEPS viewer is not negatively impacted.

Enhancement	Description
19. Prompting for Key after upgrade	• Fixed • Customers upgrading from prior versions of WinEPS were being prompted for a new activation key. The menu has been updated to validate the activation key properly and not prompt previously-activated systems for a new key.
20. Corrected allowable card prefix page error	• Fixed • Corrected an issue in the allowable card prefix menu where when using the arrow keys to select a tender type it would not sync properly.
21. WinEPS Update Enhancement	• Enhancement • The update program for Service Pack 3 will update the global parameters version for every XML file in the configuration folder. This will cause new parameters to load upon the first sign on after upgrade. • This parameter load is required to support the upgrades to the new Hypercom encryption logic.
22. Corrected issue with activation key re-prompting	• Fixed • The WinEPS Menu was updated to prevent customers who are upgrading from prior versions of WinEPS from being prompted for a new activation key.
23. WinEPS ERC Host GUI issues	• Fixed • The ERC host would generate an error on some systems where if the merchant ID was of a certain length, an error would be shown that said "Merchant ID length must be greater than zero". This would happen even if the value of the merchant ID was actually larger than zero.
24. Improved Engine stability during EOD	• Fixed • Addressed engine stability issues where engine failed after an end of day process. Included more efficient routines for IP connections released during day close process and addressed access violations that caused the engine instability.
25. EpsEngineSRV.exe	• Fixed • Corrects an issue with spacing on certain checks that would cause Telecheck to interpret the account as new. The engine has been updated to keep whatever spacing that is passed to it from the MICR reader and send it unedited to the host for processing.
26. Restart service on internal shutdown	• Enhancement • In the event of an internal error that closes TCP/IP connectivity, the engine will be automatically stopped and restarted to restore the connectivity. Previously the engine would simply stop.

OpenEPS Changes

Enhancement	Description
1. Manual Debit timing allows transaction selection	• Fixed • Manual debit is not allowed; however, under specific timing conditions a manual debit transaction could get as far as tender selection prior to being marked as invalid. This has been revised so that the transaction is marked as invalid as early as possible, just after the tender type selection.
2. 825.1 Offline Debit Void Sequence has data from intermediate Credit transaction	• Fixed • When processing an offline debit void to the ServerEPS host, the void improperly contained information from transactions other than the void and was declined by ServerEPS. • This has been corrected so that the void contains only the correct information
3. Remove Receipt Capture if already doing Signature Capture	• Enhancement • If the O – Signature Capture TAC is present in the transaction sequence along with the C – Receipt Capture TAC, the Receipt Capture TAC will be removed. • Signature Capture already includes a copy of the receipt text, so it is not necessary to have both TACs present in the sequence.
4. Update OpenEPS Direct resubmit codes	• Enhancement • The following ServerEPS Response codes will no longer generate a resubmission for an offline transaction by OpenEPS: 55 – Invalid PIN 56 – Exceed max retry 96 – System Error
5. Interval message not turning off	• Fixed • When the interval message option was used and then subsequently the option was turned off on the terminal configuration screen, OpenEPS continued to store the old setting in memory and continued to display the interval message. • This has been corrected so that OpenEPS reads the new configuration setting whenever parameters are downloaded.
6. Remove Purchase Amount on Balance Inquiry transactions	• Enhancement • Balance Inquiry transactions have no purchase amount associated with them. If a purchase amount is set by the POS for any balance inquiry transaction, the amount will be removed (set to zero). • This change will eliminate potential confusion if a purchase amount is printed as part of the receipt or picked up by the POS as part of processing.
7. Log Terminal OS Version	• Enhancement • Terminal Operating System version data is captured and sent up to WinEPS for all terminals that supply this data. • The Operating System information is stored in the LaneStatus.Xml file.

Enhancement	Description
8. Receipt text update	• Enhancement • To make the receipt text more applicable to both the WinEPS and ServerEPS products, the text "WinEPS Sequence #" has been updated to "EPS Sequence #".
9. OpenEPS Direct for Linux	• Enhancement • The OpenEPS Direct solution supported for Linux.
10. Improve Receipt for Private Debit with Signature	• Enhancement • The receipt for Private Debit with Signature now includes additional spaces to give room for the customer to sign.
11. Specify DUKPT Slot number	• Enhancement • OpenEPS has been updated to instruct the terminal to use a specific DUKPT key slot number to encrypt the PIN data for specific transactions. • This allows more configuration variety by allowing each PIN based tender type to potentially be sent to a separate host. • New Setup.Txt keywords have been implemented to allow this configuration: DEBITKEYSLOT=x EBTFSKEYSLOT=x PRIVATEDEBITKEYSLOT=x • If one or more of the above keywords exist, OpenEPS will request the specified slot be used by the PIN pad during the PIN entry request. • Only for use with the OpenEPS Direct solution. • OpenEPS will only send the slot request for terminals that support this functionality. This currently only for use with the Mx800 series terminals.
12. Mismatched cash back not giving error	• Fixed • Fixed an issue where if both the H – Cashback - Cashier and J – Cashback - Customer TACs were in the sequence and both were set, OpenEPS would instead take the POS amount and not supply the cash back mismatch error. • This has been fixed so that if a cash back mismatch occurs between the amount entered by the customer and the amount entered by the cashier, an error is set.
13. Support 5 digit Julian dates for WIC	• Enhancement • 5 digit Julian dates are now supported for WIC. The OpenEPS Date Length in the Start_WIC_Session function call has been expanded to 5 digits. • If 4 digits are received, the 4 digit date will be padded with an extra zero.

Enhancement	Description
14. Field passing issues	• Fixed • The HostReferenceNumber was not being passed to the POS from OpenEPS and this caused the date to not be printed on the receipt in the Storeline environment. The latest OpenEPS version will pass all of the necessary fields. • Also fixed an issue with the velocity information not being passed correctly from the ACI host.
15. Updated ReloadPreviousTransaction call	• Fixed • When the POS used the ReloadPreviousTransaction call, the MTX sequence number was not being incremented. This caused force transactions at the lane to fail. • OpenEPS now increments the sequence number and notes this in the journal.
16. SCATStatus 4 when not connected	• Fixed • OpenEPS has been corrected to provide a SCATStatus to 4 <Error> when OpenEPS is not connected to WinEPS and Stand in at the POST is turned off. This change will allow POS systems to recognize much faster when initiating a transaction that transaction processing is down.
17. Corrected Allowable Card Prefix GUI Bug	• Fixed • Corrected an issue in the allowable card prefix menu where using the arrow keys to select a tender type would not sync properly.
18. OpenEPS sets ReadyStatus_NonF = 1 after each reset	• Enhancement • To correct an issue with out-of-order signatures that was caused by a POS system calling Transaction Complete outside an order, OpenEPS was hardened and now sets ReadyStatus_NonF = 1 after every reset called by the POS. • Previously ReadyStatus_NonF = 1 was only set the first time, as OpenEPS was still in the same state.
19. Ensure lane journal logging	• Fixed • There was an issue in the ACS/IR and ACS environments where under certain conditions, where OpenEPS stopped writing to the lane journal. The latest changes will allow OpenEPS to continue to write to the lane journal file.
20. Partial approvals not allowed for transactions with cash back	• Enhancement • Because of recent issues with partial payments that include cash back a change was made to the OpenEPS dll. On any transaction that includes cash back the Amount Change Allowed field will be set to False, even if the POS sets True. • This change will cause WinEPS to not send the partial approval flag to the host, and thus not allow a partial approval for any transaction that includes cash back. • If no cash back is in the order the partial approval flag set by the POS will be honored as normal.

Enhancement	Description
21. Corrected two issues	• Fixed • Compensated for an issue with manually entered checks when using the JDA POS. Because the JDA POS s off spec and does not use the MICR TAC sequences when a check was manually entered only the check # was being sent to the host for authorization, which caused the transactions to go local. Manually entered checks should now process as before. • Fixes an issue with out of order signature capture for Open Accounts.
22. Fixed issue with WIC lockup	• Fixed • OpenEPS had an issue where if "Select Payment Type" was the first terminal action and a WIC session was started and cancelled, OpenEPS would not send the first terminal action to the PIN pad resulting in a PIN pad lockup.
23. Shutdown offline thread when not in use	• Enhancement • Adjusted OpenEPS processing so that the offline thread will shut down when no offline files are present to process.

OpenIP Changes

Enhancement	Description
1. Balance formatting and Zip Code forwarding	• Fixed • When returning balances to the POS, OpenIP was not correctly formatting the balance information. The formatting has been corrected so that it matches the OpenIP specification. • When OpenIP retained the customer for zip code during a split tender, it was not being forward properly to WinEPS. This has been corrected so that the zip code is forward to WinEPS for every transaction.

Host Changes

ACI

Enhancement	Description
1. FSA BIN Download	• Enhancement • Automated FSA BIN download is supported for the ACI Host.
2. Move Post Transaction # into bit 3-15 token 26	• Enhancement • The POST Transaction number will now be sent up to the ACI host in bit 3-15 token 26.
3. Support Additional Check Types to ACI	Enhancement Additional check types are now supported for the ACI host interface. The following checks types are supported: 01 Check Type 00 Personal Check 01 Payroll Check 02 Government Check 03 Business Check 05 WIC Check • Check type is sent in Bit Map 1 - Field 31.
4. Frequent Shopper Checks	• Fixed • Corrected an issue with checks being run using only the Frequent Shopper # TAC.
5. OpenEPS not passing HostReferenceNumber	• Fixed • The HostReferenceNumber was not being passed to the POS by OpenEPS and this caused the date to not be printed on the receipt in the Storeline environment. The latest module will pass the necessary fields. • Also provided a fix for the velocity information not being passed correctly from the ACI host.
6. Correct FTP path for receipt upload	• Fixed • Corrected an issue where the FTP path chosen for the upload of receipts was not being read correctly.

Albertsons

Enhancement	Description
1. -No Change to Host -	•

Ascendent

Enhancement	Description
1. Support approval for lesser amount	• Enhancement • The Ascendent host now sends the approval from a lesser amount in response bit 4. If bit 4 is blank it will be assumed that full amount was approved, for backwards compatibility.
2. Send Tax Amount	• Enhancement • The WinEPS has been updated to send the purchase tax amount to the Ascendent host. • The tax amount is submitted to Ascendent as “Tax Amount 1” in bit 93, tableID 39.
3. Corrected OpenEPS issues related to Asecendent host	• Fixed • Addressed an issue where voids by post transaction number were not processing correctly and were being switched to a void last transaction. This would keep the POS from processing voids from prior transactions. • Addressed an additional issue where MICR data was not being accepted and approved correctly. • This issue only affected systems using the Asecendent host for processing.
4. Resend unsuccessful settlement	• Fixed • An issue was found where if the host settlement message was not successful WinEPS was not sending another request after the EOD. This would cause all transactions to go local. WinEPS will now re-send the settlement message until a response is received, however until that time transactions will still be taken locally as per host logic rules.

BioPay

Enhancement	Description
1. -No Change to Host -	•

Chase

Enhancement	Description
1. -No Change to Host -	•

Concord: EPC

Enhancement	Description
1. -No Change to Host -	•

Concord: H&C Format

Enhancement	Description
1. Certegy Check Interface	• Enhancement • WinEPS now supports a new check interface to the Certegy host. • For this check host only, if a second ID needed decline is received, the POS may send up an override for the decline instead of supplying the ID information.
2. Support AVS declines	• Enhancement • Address Verification is now supported for the Concord H&C host for use with Zip Code validation. • To Enable AVS, a new check box has been added to the host screen. • When AVS is turned on, if a zip code is entered for the transaction and the AVS field is returned from Concord with an value that indicates the zip code entered was not correct, WinEPS will automatically reverse the transaction and pass a decline back to the POS lane.

Enhancement	Description
3. 2nd ID override for Certegy Checks	• Enhancement • A new TAC has been added that allow the override of the requirement to get secondary ID for Certegy checks. • TAC a – Mgr#/Override Seq (Bit 107) • For NF, 'Require ID" declines, if the 'a' TAC is in the first action in the override sequence, the POS may skip the ID entry by providing a manager ID. • This functionality is only for use with the Concord H&C host, Certegy check processing.
4. Add Cashier number to message Certegy	• Enhancement • The Cashier number field has been added for check transaction messages to the Concord H&C host when using the Certegy check format.
5. TORs and Offlines updated from pre-823 releases are misformatted	• Fixed • TOR and Offline files upgraded from pre-823 WinEPS versions were not being properly updated. This has been corrected so that any system with TORs or Offlines that are a version prior to 823 are formatted correctly when an upgrades occurs.
6. Correct fid N value	• Fixed • Corrected an issue with checks where First Data had an issue with the lane # fid N if send with the "Buycheck" indicator.

Concord: Memphis

Enhancement	Description
1. Short cashier numbers not being sent to host	• Fixed • The cashier number set during the processing of personal checks was expected to be 6 digits in length, however only three digits were sent by the POS; the host module has been updated to correctly format and pass along the three digit cashier numbers provided.
2. Corrected cashier number length	• Fixed • Resolves an issue with personal checks sent to Concord: Memphis where the cashier number supplied was the wrong length.
3. Fixes issue with dropped characters	• Fixed • The host module has been updated to address issues with dropped characters at the end of the host message.

Demo

Enhancement	Description
1. -No Change to Host -	•

Elavon (was NOVA)

Enhancement	Description
1. -No Change to Host -	•

ePicTranz

Enhancement	Description
1. Updated ECC Text	• Enhancement • The Electronic Check Conversion text that is supplied to the POS for printing on the receipt has been updated to comply with the most recent NACHA requirements.
2. Host connection closing issue	• Fixed • Addressed issues in the way that the host module blocks out or closes connection to host. Improper closing affected certain systems, causing the engine to become unstable or drop when the host connection was lost.
3. Corrected issue with closing connections	• Fixed • Addressed issues in the way that the host module blocks out or closes connection to host. This could affect systems and cause the engine to become unstable and drop when the host connection is lost.

LML

Enhancement	Description
1. -No Change to Host -	•

Lynk

Enhancement	Description
1. Support SSL to RBS Lynk	• Enhancement • The Lynk host now supports SSL connection. • To enable SSL, a new checkbox has been placed onto the Lynk host configuration screen.
2. Increase Message Format Version field	• Enhancement • The Message Format Version has been increased in length from 15 to 16 characters.
3. Updated Resubmit logic	• Enhancement • The resubmit logic for certain declines from Lynk for gift card activation has been updated.
4. Update 015 decline handling	• Fixed • Added new logic for in-store gift cards: If an 015 decline is received WinEPS retries the transaction immediately and then once every 4 hours. • Also includes fixes for stack overflow issues that were noted in the host interface.
5. Corrected Stack Overflow Issue	• Fixed • Addressed stack overflow errors that can cause the engine to shut down. • If attempts to connect to the Lynk SSL host connection were unsuccessful, the SSL component continued to cycle the attempt and caused a "stack overflow" error. In a multiple host environment, this was caused by successive connection attempts from those hosts and generated the error.
6. Added missing 019 response code	• Fixed • The Lynk Host response codes did not include a mapped response for the 019 code. This code is now included as an approval for gift cards to allow partially approved gift cards to function.

Enhancement	Description
7. Addressed SSL issues	• Fixed • Addressed issues that could cause the EPSEngine to crash when there are connection issues over SSL to the Lynk host.

LX1 & LX2 (Check) Hosts

Enhancement	Description
1. Support Negative Gift Card Balances	• Enhancement • WinEPS now supports negative Gift Card balances when they are returned from the LX host. • Negative balances received from the host will be passed to OpenEPS for display and printing to the receipt.
2. Support SSL to LX Host	• Enhancement • The LX host now supports SSL connection. • To enable SSL, a new checkbox has been placed onto the LX host configuration screen.
3. Batch Activation Issue	• Fixed • Corrected a timing issue with batch Blackhawk gift card activation. The issue appeared to log an error to the journal, but the actual transaction was later successfully forwarded.
4. Send original Balance from Redemption or Void	• Fixed • On a void the original balance information is now sent up to the host.
5. Corrected SSL error handling	• Fixed • Corrected error handling with the SSL socket component to prevent communication errors from locking up the WinEPS services. • The included LX host modules have the debugging messages removed.

Mainsail

Enhancement	Description
1. -No Change to Host -	•

Mercury

Enhancement	Description
1. -No Change to Host -	•

MPS (Fifth Third)

Enhancement	Description
1. Fixed incorrect KSN padding	• Fixed • Corrected an issue where when the KSN received from the lane was already 20 digits long and WinEPS would attempt to pad it anyway. This caused the KSN to be blanked out to a value of all 0's.

MTX Receipt Capture Host

Enhancement	Description
1. XML Loading	• Fixed • The ERC host module would attempt to load XML configuration files too early in the startup process which would cause access violations to be logged. This has been corrected so that the XML files are loaded properly.
2. Incorrect merchant ID length check	• Fixed • On the ERC host screen, on some systems Merchant IDs of specific lengths would generate an incorrect error indicating that the "Merchant ID length must be greater than zero" even if the value was a non-zero amount. This has been corrected to actually check the Merchant ID length.

Enhancement	Description
3. MTX Receipt Capture Host file loading	• Fixed • The ERC host module would attempt to load XML configuration files too early in the startup process and this would cause access violations to be logged in the spool file.
4. Receipt host module stop sending receipts during settlement	• Fixed • This change to the Receipt host module is to address a random engine failure. This latest Receipt Host module will now stop sending the receipts when settlement is started and will restart sending after the host dll is reloaded after the End of Day has completed.
5. Corrected errors	• Fixed • Addressed errors that occur in a limited number of installations.

Paypoint

Enhancement	Description
1. -No Change to Host -	•

Pay by Touch

Enhancement	Description
1. -No Change to Host -	•

ServerEPS (Native Format)

Enhancement	Description
1. ServerEPS host module in WinEPS	• Enhancement • The WinEPS engine has been updated with a new ServerEPS host communication format. This host sends transactions to the ServerEPS payments host in its native format. • Currently this host is for use for fuel lane support only.
2. Internally Certify Fuel to ServerEPS through WinEPS Host Module	• Certification • Fuel lane communication through the new ServerEPS native host has been internally certified.

Shared (BigY)

Enhancement	Description
1. Host connection closing issue	• Fixed • Addressed issues in the way that the host module blocks out or closes connection to host. Improper closing affected certain systems, causing the engine to become unstable or drop when the host connection was lost.
2. Corrected issue with closing connections	• Fixed • Addressed issues in the way that the host module blocks out or closes connection to host. This could affect systems and cause the engine to become unstable and drop when the host connection is lost.

Terminal Code Changes

Hypercom ICE5500

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

Hypercom ICE6000

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

Hypercom L4100

Enhancement	Description
1. Internal certification of new Hypercom USB to Rs232 Driver	• Certification • An internal certification has been performed with the latest Hypercom USB to Rs232 Driver version.
2. Encrypting Track II with Hypercom Pin Pads	• Enhancement • The Hypercom pin pads have been updated to support encryption of the track 2 data. • Terminal Model: 4100 The latest screen files will update the encryption certificate and should not require shipping back to Hypercom.
3. Hypercom SCAT Version 329	• Enhancement • The latest SCAT Code version supports the Hypercom terminal encryption enhancement. • Older, Pre-PKI models of the Hypercom 4100 terminal do not have a security certificate embedded in them. The latest version of the SCAT code, 329, will automatically update the terminal with the proper certificate, but the update process will only work if the terminal is encrypted. Terminals that are not encrypted, and thus not capable of taking PIN-based transactions, will need to be encrypted prior to upgrading.

Enhancement	Description
4. Numeric entry of host port number, only	• Fixed • The WinEPS Menu has been updated to prohibit the entry of alpha characters into the Port field of the Host Processor Definition. The Port field allows only numeric entry.
5. Corrected issues with new encryption logic	• Fixed • Corrected 2 issues with the Hypercom terminals as it relates to the new encryption logic. • 1. Support split messaging if the terminal does not do a parm load after upgrading or loading screen files. • 2. An issue was corrected that could cause a 2 minute delay in downloading new parameters following a screen file load, on certain POS systems this could cause a longer sign on period before the POS is able to process.

Hypercom L4150

Enhancement	Description
1. Encrypting Track II with Hypercom Pin Pads	• Enhancement • The Hypercom pin pads have been updated to support encryption of the track 2 data. • Terminal Model: 4150 4150 model terminals should already have the encryption certificate and should not require shipping back to Hypercom.
2. Hypercom SCAT Version 329	• Enhancement • The latest SCAT Code version supports the Hypercom terminal encryption enhancement.
3. Corrected daily terminal reboot	• Fixed • The latest terminal code for the 4100, 4250 and 4150 corrects an issue where the pin pads were rebooting once every 24 hours.
4. Corrected issues with new encryption logic	• Fixed • Corrected 2 issues with the Hypercom terminals as it relates to the new encryption logic. • 1. Support split messaging if the terminal does not do a parm load after upgrading or loading screen files. • 2. An issue was corrected that could cause a 2 minute delay in downloading new parameters following a screen file load, on certain POS systems this could cause a longer sign on period before the POS is able to process.

Hypercom L4250

Enhancement	Description
1. Encrypting Track II with Hypercom Pin Pads	• Enhancement • The Hypercom pin pads have been updated to support encryption of the track 2 data. • Terminal Model: 4250 The customer will have to check with Hypercom to see if the terminal needs to be shipped back to implement the encryption certificate.
2. Hypercom SCAT Version 329	• Enhancement • The latest SCAT Code version supports the Hypercom terminal encryption enhancement.
3. Corrected daily terminal reboot	• Fixed • The latest terminal code for the 4100, 4250 and 4150 corrects an issue where the pin pads were rebooting once every 24 hours.
4. Corrected issues with new encryption logic	• Fixed • Corrected 2 issues with the Hypercom terminals as it relates to the new encryption logic. • 1. Support split messaging if the terminal does not do a parm load after upgrading or loading screen files. • 2. An issue was corrected that could cause a 2 minute delay in downloading new parameters following a screen file load, on certain POS systems this could cause a longer sign on period before the POS is able to process.

Ingenico eN-Crypt 2100

Enhancement	Description
1. Ingenigo signature enhancement	• Enhancement • Enhanced the signature capture for the Ingenico OPOS terminals. • The signature data from the terminals is now converted to the Hypercom signature format using a dynamic routine that retains the maximum resolution possible while capturing the entire signature. The previous routine had a fixed resolution which resulted in truncation of portions of longer signatures. • This was a change in OpenEPS only, not in the terminal code.

Ingenico eN-Touch 1000

Enhancement	Description
1. Ingenigo signature enhancement	• Enhancement • Enhanced the signature capture for the Ingenico OPOS terminals. • The signature data from the terminals is now converted to the Hypercom signature format using a dynamic routine that retains the maximum resolution possible while capturing the entire signature. The previous routine had a fixed resolution which resulted in truncation of portions of longer signatures. • This was a change in OpenEPS only, not in the terminal code.

Ingenico 6550

Enhancement	Description
1. Ingenigo signature enhancement	• Enhancement • Enhanced the signature capture for the Ingenico OPOS terminals. • The signature data from the terminals is now converted to the Hypercom signature format using a dynamic routine that retains the maximum resolution possible while capturing the entire signature. The previous routine had a fixed resolution which resulted in truncation of portions of longer signatures. • This was a change in OpenEPS only, not in the terminal code.

IVI C2000 Protégé

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

NCR 5993

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

Verifone Everest

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

Verifone MX830/MX850/MX860/MX870

Enhancement	Description
1. Enhance Mx800 Terminals	• Enhancement • The MX800 terminal code has been enhanced with the following: OpenEPS will now set the Pin Pad Serial Number for all Mx800 terminals The default fmagent.sys for Mx800 terminals have been updated to support the KP200 overlay by default. This will change the look of the Pin Entry screen OpenEPS has been enhanced to load the parameters in the fmagent.sys into the Mx800 pin pads whenever screen files are loaded. Previously parameters were loaded only upon load of the forma agent.
2. Pin Pad Encryption	• Enhancement • In cooperation with Verifone, a dynamic encryption key has been implemented to encrypt traffic between the Mx800 series terminals and OpenEPS.
3. Certify Pin Pad 1000 with Mx800 pin pads	• Certification • The Pin Pad 1000 has been certified to work properly with the Mx800 series terminals.
4. MX800 Button lock up	• Fixed • If a card slide was performed and then a tender key was quickly pressed twice, the top terminal button would no longer function until a transaction reset occurred. This has been corrected so that quick buttons presses will no longer cause an issue.
5. New MX800 series Screen Files	• Enhancement The signature display on the screen has been updated fro improved clarity; signatures will use thicker lines when displayed.

Enhancement	Description
6. MX800 version search	• Enhancement • OpenEPS will no longer search for the MX800 series screen files version number in the MTXBK.frm. It was found that if the MTXBK.frm was searched for the version number, this would cause the screen files to re-download.
7. Invalid card slide not recognized correctly	• Fixed • Corrected an issue with invalid card data on the MX terminals only that would not properly treat the slide as invalid. During an invalid slide the PIN Pad would appear to lock up, but a reset on the PSO or cancel on the PIN pad would clear the issue. • OpenEPS will now treat such slides as invalid data and ask for another card slide until manual mode is reached.

Verifone Omni 490

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

Verifone Omni 7000

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

VeriFone Vx670

Enhancement	Description
1. 3DES support	• Enhancement • The Vx670 terminal code has been updated to support the use of 3DES encryption.

Stand Beside Code Changes

Verifone Vx570

Enhancement	Description
1. -No Change to Verifone Vx570 code -	• ---

485 LAN Stand Beside

485 LAN Stand Beside support has been discontinued.

Enhancement	Description
1. Discontinue Support for Stand Beside	• **Discontinued Support** • 485 LAN Stand Beside systems are no longer supported. • This change affects the following 485 LAN integrations: IVI C2000 Protégé Verifone Everest Verifone Omni 490 • The above terminals remain supported as part of the OpenEPS integration (only).

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 Scanmaster Code -	• ---

Redundancy Service

Enhancement	Description
1. Update for Redundancy Service	• Enhancement • The Redundancy Service has been updated for use with 825.1. • To improve functionality, the way the WinEPS service all has been changed; previous versions of the Redundancy service are incompatible with the service changes. • Only the most recent version of redundancy service, version 825.1, will work properly with the 825.1. If a location is running Redundancy service and upgrade to WinEPS 825.1, the Redundancy service should likewise be updated.
2. RS SSL Encryption	• Enhancement • The Redundancy service has been upgraded to utilize the same SSL Encryption features throughout the WinEPS software suite.
3. Add Secure FTP to Redundancy Service	• Enhancement • The Redundancy Service has been enhanced to use Secure FTP to transfer files.

Enhancement	Description
4. RS SSL Optimization	• Fixed • Optimized the SSL component for the RS Service, also corrected a small handle leak that occurred during EOD Synchs.
5. Redundancy Service Fix	• Fixed • Corrected an issue where a transaction in flight when the backup server had a network issue would cause the EPS Engine to crash or lock up the CPU cycles.
6. Corrected issue with server socket	• Fixed • Corrected an issue when attempting to destroy the server socket that would cause the RS Service to hang until another stop was called. The error did not affect the reconnection of the Server socket nor general day to day functionality.
7. RS Issue causing WinEPS service crash	• Fixed • An issue was found and corrected where a Redundancy Service message would cause the WinEPS service to either quit, use up all the PC's CPU cycles, or the Primary Redundancy Service itself would fail to reconnect to the backup service.

UpdateXMLFiles.Exe

Enhancement	Description
1. Unprintable characters in XML preventing reading	• Fixed • If unprintable characters were encountered in an XML file, the UpdateXMLFiles program was unable to open and edit that XML. The latest new version of the UpdateXMLFiles corrects this issue and will be able to open and edit XML files with unprintable characters. • Updates using the action files will also work correctly.

Virtual Terminal 2

Enhancement	Description
1. Multi-Store Virtual Terminal	• Enhancement • Virtual Terminal has been enhanced with a new parameter, Multi-Store Functionality, which is for use only with the OpenEPS Direct solution. • For additional information on Multi-Store Functionality, refer to the Virtual Terminal User's Guide.

Section 2

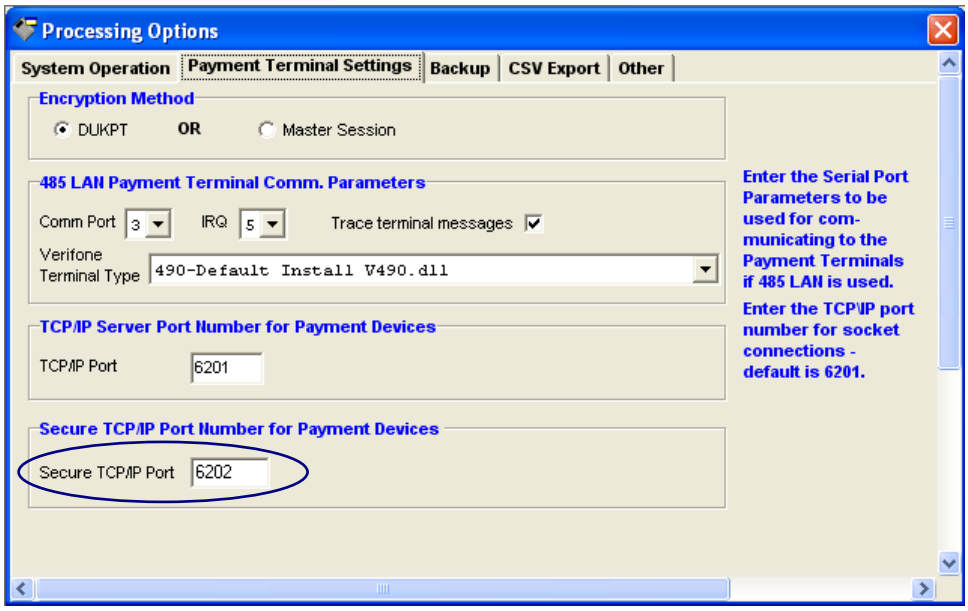
New Features

WinEPS Fixed Issues and Enhancement - #7:

SSL for Fuel Lanes

Secure Socket Layer connectivity is available for fuel lanes. The default port is 6202 for SSL; this port may be changed in WinEPS. Fuel lanes are not required to support SSL and may to connect to WinEPS using the standard TCP/IP communication.

To change the SSL port, go to Site Information | Processing Options | Payments Terminal Settings Tab.



The Secure TCP/IP setting may be updated by entering a new port number and saving. Be sure that if a new port is chosen it does not conflict with already existing port numbers.

StoreNext Retail Technologies LLC
6100 Tennyson Parkway, Suite 130
Plano, Texas 75024

P/N 89000512
PIN 45001/096