



Worldpay Total/ Worldpay Integrated Payment Solution

Integrated Payment Client (IPC-II-Series)

Implementation/Integration Guide For version 2.1.6

Issue 1.21 – March 2017

This document and its content are confidential and proprietary to Worldpay and may not be reproduced, published or resold. The information is provided on an "AS IS" basis for information purposes only and Worldpay makes no warranties of any kind including in relation to the content or sustainability. Terms and Conditions apply to all our services.

Worldpay (UK) Limited (Company No. 07316500 / FCA No. 530923), Worldpay AP Limited (Company No. 05593466 / FCA No. 502597). Registered Office: The Walbrook Building, 25 Walbrook, London EC4N 8AF and authorised by the Financial Conduct Authority under the Payment Service Regulations 2009 for the provision of payment services. Worldpay (UK) Limited is authorised and regulated by the Financial Conduct Authority for consumer credit activities.

Worldpay, the logo and any associated brand names are all trade marks of the Worldpay group of companies.

Change History

Version	Date	Changed By	Changes
0.1	25 November 2014	Vijay Patwa	First Draft
1.0	2 February 2014	Vijay Patwa	Added new Synchronous messages prompt, Refer 10.2.6
1.1	3 June 2015	Baljit Jackson	Added columns for Input/output data type and length, Refer 8.2 Changes done in pre-requisites section for java configuration, Refer 3.1 Changes at various places to provide more clear information.
1.2	23 rd June 2015	Ajay Gupta	Added section 4.3.11 to explain all the possible timeouts that may can be configured used by IPC during transaction.
1.3	14 th July 2015	Ajay Gupta	Added instructions in PA-DSS 2.1 requires section related to Hibernation and Pagination.
1.4	11 th Sep 2015	Ajay Gupta	Changed the Description of attribute 14 regarding to the contactless transaction in section 8.2.2. Removed the request, response attribute and transaction example related to North America and Canada territory. Modified the content of section 2.1 to recommend the encryption of Hard Drive. Modify 2.25, 2.26, 2.27, 2.29, 2.30 sections to remove the SSL as recommended cryptography. Corrected the URL to https://www.yes-pay.net/soap/servlet/rpcrouter
1.5	13 th Sep 2015	Rahul Verma	Modified the description of attribute 8.2.1 regarding special characters in Transaction Reference.
1.6	18 th Sep 2015	Rahul Verma	Modified the description of attribute 8.2.2 regarding in output response field for contactless pos entry mode.
1.7	23 rd Sep 2015	Rahul Verma	Changed the terminology used for “Merchant Subscription Wallet” to “Token”.
1.8	18 th Nov 2015	Rahul Verma	Added the issuer code in 8.2..2.. Added an attribute field 80 in 8.2.2 regarding retrieval reference number.
1.9	15 th Dec 2015	Rahul Verma Aakanksha Nahar	Changes the IPC-2 Version from 1.0.2 to 1.0.3 Added support for DCC and VAT functionality. Added the description for DCC transaction in section 8.4.25. Added the description for DCC Confirmation Request in section 10.3.7 . Modified the description of attribute in section 8.2.2 regarding output response field for contactless pos entry mode for high value contactless. Modified the description of attribute in section 8.2.2 regarding in output response field for dynamic currency conversion.

Version	Date	Changed By	Changes
1.10	22 nd Jan 2015	Aakanksha Nahar Mamta Jain Dharmendra Patidar	Changes the IPC -2 Version from 1.0.3 to 1.1.0 . Added the description for IPC-Updates in Section 8.5 Added the description for Software Upgrade in Section 8.5.1 Added the description for Firmware Upgrade in Section 8.5.2 Added the description for Proxy Setting in IPC in Section 8.6 4.3.6 Look n Feel changed the Image and added the description of new labels 4.3.8 Software Upgrade changed the Image and description 10.3.7 remove section DCC Confirmation request 10.3.7 Added new transaction type Cancel
1.11	17 March 2016	Mamta Jain	8.5.1 Added the description and Images for 3 retries handling when firmware files downloads into PED.
1.12	30 th March 2016	Ajay Gupta	8.5 Added instructions to configure local machine to resolve domain name to IP address if DNS is not available.
1.13	1 st April	Faisal Ahmad	10.3 Changed Format type of Post Code from Numeric to Alpha Numeric
1.14	27 th May	Kavita Patidar Rahul Verma	8.4.27 Added TaxFree Voucher (VAT Refund Voucher) for Cash Transaction for Fintrax. 11 Added APPENDIX (H) for Print Command details required for processing VATRefundVoucher.txt file 8.5.3 Added the description of Firmware Upgrade for Vx820-7816 PED. 7.6 Appended Semi-attended mode in appendix E. 8.2.2 Updated CVM field in Output Response Attributes for a new value of unknown CVM. 8.2.2 Added a new field "Available Offline Spending Amount" in Output Response Attributes.
1.15	5 th July	Rahul Verma	Changes the IPC -2 Version from 2.1.0 to 2.1.1. It has some changes/Bug fixes which are mentioned in "ReleaseNotes_IPC-2-211.docx".
1.16	24 th August 2016	Kavita Patidar	8.2.2 Added Note 2/table for PEM value in case of contactless refund transaction. 8.4.2 Updated refund response.
1.16	24 th August 2016	Kavita Patidar	Changed the IPC -2 Version from 2.1.1 to 2.1.2.
1.16	5 th September 2016	Mamta Mehta	Changes done for P2PE in section 4.2.1 General Configuration Changes done for P2PE in section 4.3.8 Software Upgrades

Version	Date	Changed By	Changes
1.16	5th September	Rahul Verma	Added Miura Pinpad Supported Transactions type list in section 12.
1.16	5th September	Rahul Verma	Added support of VATRefundVoucher with socket mode. Added 3.2.1 IPC Windows startup section. Changed done on section 8.4.1 for the output response of checkStatus transaction type.
1.17	28 October	Rahul Verma	Changed the IPC-2 Version from 2.1.2 to 2.1.3.
1.18	12 December	Sabine Lainer Mamta Mehta	Changes in section 3.1 related to Integrity check Changes in section 2.7 and added 2.7.1 and 2.7.2 Added section 2.22, 2.33, 2.34 and 2.35
1.19	10 January 2017	Rahul Verma	Changed the IPC-2 Version from 2.1.3 to 2.1.4. Added support of HVC cards with IWL-250 PEDs on RAM 1606. Barclay acquirer is supported with IPP350 PEDs on RAM 1606.
1.20	02 February 2017	Rahul Verma	Changed the IPC-2 Version from 2.1.4 to 2.1.5. Added support of Miura PEDs for contact and contactless cards. Removed section 3.2.1 - IPC Windows startup configuration changes as it is not required in IPC-2-214 onwards.
1.20	20 February 2017	Rahul Verma	Updated the configuration utility section
1.21	22 March 2017	Rahul Verma	Updated the section 3.1 – Pre-requisites , 4.2.1 – General Configuration , 4.3.10 - Hosted IPC.

Related Documents

Reference	Name	Ver.	Date	Description
1.	Payment Card Industry (PCI) Payment Application Data Security Standard	3.2	Oct 2014	

Circulation List

EPOS Software Vendor Partners, Resellers, Merchants

Document Sign-off

Integrated Payment Client-II-Series

Implementation/Integration Guide issue 1.21 For version 2.1.6

Version	Status	Date	Approved by	Job Designation
1.18	approved	13 Dec.2016	Billy Lewis	Head of Integrated Payments

Table of Contents

1	Introduction	11
1.1	IPC-II-Series and History	11
1.2	Glossary	11
1.3	PCI Data Security Standard.....	12
1.4	Difference between PCI DSS Compliance and PA-DSS Validation.....	13
1.5	References.....	13
1.6	About this Guide.....	13
2	PA-DSS requirements implementation in IPC.....	14
2.1	PA-DSS 1.1.4 requires	14
2.2	PA-DSS 1.1.5 requires	15
2.3	PA-DSS 2.1 requires	16
2.4	PA-DSS 2.2 requires	17
2.5	PA-DSS 2.3 requires	18
2.6	PA-DSS 2.4 requires	19
2.7	PA-DSS 2.5 requires	19
2.7.1	Key Retirement and Replacement	19
2.7.2	Key Change in Emergency / Compromised Situation	20
2.8	PA-DSS 2.6 requires	20
2.9	PA-DSS 3.1 requires	21
2.10	PA-DSS 3.2 requires.....	22
2.11	PA-DSS 4.1	22
2.12	PA-DSS 4.2.1 requires.....	24
2.13	PA-DSS 4.2.2 requires.....	24
2.14	PA-DSS 4.2.3 requires.....	24
2.15	PA-DSS 4.2.4/5 requires	24
2.16	PA-DSS 4.2.6 requires.....	24
2.17	PA-DSS 4.2.7 requires.....	25
2.18	PA-DSS 4.3 requires.....	25
2.19	PA-DSS 4.4 requires.....	25
2.20	PA-DSS 5.5.4 requires.....	26

2.21	PA-DSS 6.1,6.2 and 6.3 requires.....	28
2.22	PA-DSS 7.2.3 requires.....	28
2.23	PA-DSS 8.2 requires.....	29
2.24	PA-DSS 9.1 requires.....	29
2.25	PA-DSS 10.1 requires.....	30
2.26	PA-DSS 10.2.1 requires.....	31
2.27	PA-DSS 10.2.3 requires.....	31
2.28	PA-DSS 11.1 requires.....	32
2.29	PA-DSS 11.2 requires.....	32
2.30	PA-DSS 12.1 requires.....	33
2.31	PA-DSS 12.2 requires.....	33
2.32	IPC Monitoring/change detection Instruction	33
2.33	Changes to PA DSS requirements and changes to IPC.....	34
2.34	Changes to operating systems and Java	34
2.35	Notifications	34
2.35.1	Critical patches	34
2.35.2	IPC upgrades and bug fixes.....	35
2.36	Dissemination of the integration guide and installers.....	35
3	Appendix A – IPC Installation Instructions.....	36
3.1	Pre-requisites	36
3.1.1	For Windows.....	37
3.1.2	For Linux.....	38
3.2	IPC Terminal.....	38
3.2.1	Installation steps.....	38
4	Appendix B – IPC Configuration guide	46
4.1	YESEFT folder contents.....	46
4.2	Minimum Configuration Required	48
4.2.1	General Configuration	48
4.2.2	Communication Interface	50
4.3	Detailed Terminal Configuration	51
4.3.1	Common	51
4.3.2	Instance.....	52
4.3.3	Instance Properties.....	53

4.3.4	Interfacing	54
4.3.5	Receipt	55
4.3.6	Look n Feel	57
4.3.7	AVS Rules	58
4.3.8	Software Upgrade	60
4.3.9	Canadian	63
4.3.10	Hosted IPC	64
4.3.11	Time Outs	65
5	Appendix C – Secure delete Instructions	67
5.1	For Windows	67
5.2	For Linux (Ubuntu, CentOS, Suse)	67
6	Appendix D – Activity Logging	69
6.1	Auditing user activity on the system	69
6.2	Auditing user access to YESEFT/conf and YESEFT/properties folder	70
6.2.1	Object Access Policy on Windows	71
6.2.2	Enabling Audit Trail	72
6.3	Centralized logging mechanism	74
6.3.1	For Windows	74
6.3.2	For Linux	76
7	Appendix E – IPC Integration Guide	85
7.1	IPC Integration Mode	85
7.2	IPC Environments	85
7.3	IPC for Retail	85
7.4	IPC for Lodging	86
7.5	IPC for Kiosks	86
7.6	IPC for Semi-Attended	86
8	IPC INTERFACE	87
8.1	General	87
8.2	IPC Integration Attributes	87
8.2.1	Input Request Attributes	87
8.2.2	Output Response Attributes	92
8.3	IPC Socket Interface	100
8.4	Typical Transaction Requests and Responses	100

8.4.1	Transaction Type Sale	100
8.4.2	Transaction Type Refund	101
8.4.3	Transaction Type Sale CNP	102
8.4.4	Transaction Type Refund CNP	103
8.4.5	Transaction Type Pre-Authorisation	104
8.4.6	Transaction Type Pre Sales Completion	105
8.4.7	Transaction Type Cancel	105
8.4.8	Transaction Type Keyed.....	106
8.4.9	Transaction Type Forced Keyed Referral.....	107
8.4.10	Transaction Type CheckCard	109
8.4.11	Transaction Type CheckStatus.....	110
8.4.12	Transaction Type Check Pinpad Connection	111
8.4.13	Transaction Type Print Duplicate Merchant Receipt	111
8.4.14	Transaction Type Print Duplicate Customer Receipt.....	112
8.4.15	Transaction Type Get Number of Offline Stored Transactions	112
8.4.16	Transaction Type Get Pinpad Serial Number	112
8.4.17	Transaction Type Get Territory	113
8.4.18	Transaction Type Cash transaction	113
8.4.19	Transaction Type Close IPC.....	114
8.4.20	X Report.....	114
8.4.21	Z Report	115
8.4.22	Tokenization Of Card Numbers	116
8.4.23	Sample Request for Charging a Token	116
8.4.24	Sample Request to Refund a Token	117
8.4.25	Sale with Dynamic Currency Conversion (DCC).....	118
8.4.26	Transaction Type Last Transaction Result	119
8.4.27	Transaction Type TaxFree Voucher for Cash Transaction	121
8.5	IPC Updates	122
8.5.1	Connections to enable Upgrade	122
8.5.2	Software Upgrade.....	122
8.5.3	Firmware Upgrade	124
	Firmware Upgrade process for Vx820-7816.....	128
8.6	Proxy Settings for IPC	136

8.7	Customer Image/Logo Display.....	137
8.7.1	Customer Image display on IPP350 PED	137
8.7.2	Customer logo display on Vx820-7816 PED.....	138
9	Appendix F - IPC Receipt Generation	139
10	Appendix G - IPC console Message to socket interface	143
10.1	Asynchronous Mode	143
10.2	Asynchronous mode messages	146
10.2.1	Sale	146
10.2.2	Refund	146
10.2.3	Sale CNP.....	147
10.2.4	Refund CNP.....	148
10.2.5	Cancel	148
10.2.6	Check Card.....	149
10.2.7	Last Transaction Status.....	149
10.2.8	X – Report / Batch Totals.....	149
10.3	Synchronous Mode	149
10.3.1	Accept/reject Signature.....	154
10.3.2	Referral Request.....	155
10.3.3	FallBack Confirmation Request	155
10.3.4	CNP Confirmation Request.....	156
10.3.5	CashBack Confirmation Request	156
10.3.6	Address and Postcode (Zip Code) Enter Request	156
10.3.7	Cancel Transaction Request	158
11	Appendix H - Print Command details for Tax Free Voucher	159
12	Miura Pinpad Configuration and Supported Transactions	163

1 Introduction

The purpose of this document is to provide guidance to partners, resellers and merchants on how to implement and integrate the Integrated Payment Client-2 (IPC-2) application into their environment in a PCI DSS compliant manner. The software, if installed according to the guidelines provided in the document, should facilitate and support a merchant's PCI DSS compliance.

For more detailed information concerning PCI compliance, please refer to the PCI Security Standards Council website, <https://www.pcisecuritystandards.org/>.

1.1 IPC-II-Series and History

The EasyVTerminal application is a thick client that manages EFT transaction processing. The application is owned by Worldpay UK as a result of the acquisition of YESpay International in March 2013. During the course of 2014 the application underwent PA-DSS certification. In order to meet the PA-DSS certification requirements, some necessary changes have been made within the application.

Following certification the EasyVTerminal application has been re-launched with a different name and versioning methodology. EasyVTerminal is now renamed as **IPC-2 (Integrated Payment Client-2)**. A new versioning system starting from 1.0.0 has been adopted and will be used and will be used for all future releases. All previous EasyVTerminal installations will be upgraded to the new IPC-2 releases. **IPC-2 is referred as IPC in this document. All versions of EasyVTerminal prior to IPC are referred to as EVT in this manual.**

The IPC software manages the processing of the EFT transaction. The IPC components are the IPC Console, which manages the Interaction with the EPOS application; and the YESEFT kernel module, which manages the interaction with the PINPAD and the Worldpay Payments Hub. Please refer to [Appendix E](#) for detailed information.

1.2 Glossary

ATR	Answer to reset
CNP	Card not Present
CP	Card present i.e. the card is processed via the pinpad
WPH	Worldpay's Payment Hub
EMV	Europay, Mastercard and Visa
EPOS	Electronic Point of Sale
EVT	EasyVTerminal – The name of the YESpay/Worldpay EFT application before it was relaunched as IPC

EPOS or POS	Point of Sale
IPC	Integrated Payment Client – Worldpay’s EFT application.
FEK	File Encryption Key
EKEK	Encrypted Key Encryption key
EFEK	Encrypted File Encryption key
iKEK	Initial Key Encryption Key
KEK	Key Encryption Key
MSR	Magnetic Stripe Reader
OS	Operating System
PA-DSS	Payment Application Data Security Standard
PAN	Primary Account Number
PCI DSS	Payment card Industry Data Security Standard
PIN	Personal Identification Number
sFTP	Secure File Transfer Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
YESEFT	Worldpay’s EFT Kernel

1.3 PCI Data Security Standard

The PCI DSS requirements apply to all system components within a payment application environment: defined as any network device, host or application included in, or connected to, a network segment where cardholder data is stored, processed or transmitted.

The PCI Data Security Standard, listed below, consists of twelve basic requirements supported by more detailed sub-requirements:

Build and Maintain a Secure Network

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

Protect Cardholder Data

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

Maintain a Vulnerability Management Program

- Protect all systems against malware and regularly update anti-virus software or programs.

Integrated Payment Client-II-Series

Implementation/Integration Guide issue 1.21 For version 2.1.6

- Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

- Restrict access to cardholder data by business need to know.
- Identify and authenticate access to system components.
- Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

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

Maintain an Information Security Policy

- Maintain a policy that addresses information security for all personnel.

1.4 Difference between PCI DSS Compliance and PA-DSS Validation

PA-DSS is the standard against which payment applications have to be tested, assessed, and validated.

The PA-DSS validation is intended to ensure that the payment application will help you achieve and maintain PCI DSS compliance with respect to how the payment application handles encryption, and other security requirements.

The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the PCI Data Security Standard (DSS). The security requirements defined in the PCI DSS apply to all members, merchants, and service providers that store, process or transmit cardholder data.

1.5 References

This PA-DSS implementation guide references PA-DSS requirements. The following versions are referenced in this guide:

PA-DSS version 3.2

1.6 About this Guide

This guide will be distributed to all Worldpay integrators, merchants and resellers. It covers all applicable PA-DSS requirements and explains any that are not applicable to Worldpay IPC software. It also includes installation instructions for IPC and guidelines to integrate IPC with an EPOS application. This document is reviewed and updated as needed for all major/minor/wild card changes to the payment application or changes in PA-DSS requirements.

2 PA-DSS requirements implementation in IPC

2.1 PA-DSS 1.1.4 requires

Securely delete any track data, card verification values, PINs or PIN blocks, stored by previous versions of the payment application, in accordance with Industry accepted standards for secure deletion.

Implementation in IPC

The removal of historical data is necessary in order to meet PCI DSS compliance. Older versions of EasyVTerminal (the predecessor to IPC) may have temporarily stored the full track 2 data, prior to automatically removing it after online authorisation was completed.

Where EVT is being un-installed or being re-installed from the system then the following files need to be deleted securely using the **SDelete tool or Shred tool**. (Please refer to [Appendix C](#) for further information on how to use these tools.)

- YESEFT/properties/jce.BKSkeystore
- YESEFT/properties/truststore
- YESEFT/conf: all filenames beginning "YESEFTTransactionLog".

If multiple instances have been created to run multiple pinpads with a single EVT installation then the following files also need to be deleted

- YESEFT/INSTANCE_XX/properties/jce.BKSkeystore
- YESEFT/INSTANCE_XX /properties/truststore
- YESEFT/INSTANCE_XX /conf: all filenames beginning "YESEFTTransactionLog".

XX is the number of the instance e.g. 01, 02...10, 11....99. Please refer to [Appendix B](#) regarding multiple instances.

To uninstall EVT please follow the steps below:

Prior to version 3.4.1.4

1. Windows 7/8

- Go to control panel
- Click **Programs and Features**: you can search the EVT application on right side top corner: type "Easy" to find the EVT application.
- Select EasyV Terminal and press Uninstall button
- A popup box will appear for confirmation.
- Click Yes button to uninstall.

Or

- Go to YESEFT/Uninstall folder.
- Double click on UnInstallEasyV.exe.
- A screen will appear which displays the version of EasyV Terminal selected to be removed. Press Next to continue.
- Press Finish button to complete the uninstallation process.

2. Windows XP

- Go to control panel

- Click **Add or Remove Programs**, scroll down to EasyV Terminal and press Uninstall button.
- A popup box will appear for confirmation.
- Click Yes button to uninstall.

3. Linux

- Delete the YESEFT folder. No further action is required as the EVT installation for Linux is created by extracting from a zip file.

Post Version 3.4.1.4:

1. Windows 7/8/8.1

- Go to control panel
- Click **Programs and Features**: you can search the EVT application on the right side top corner: type “Easy” to find the EVT application
- Select EasyV Terminal and press Uninstall button.
- A screen will appear which displays the version of EasyV Terminal selected to be removed. Press Next to continue.
- Press Finish button to complete the uninstallation process.

2. Windows XP

- Go to control panel
- Click **Add or Remove Programs**, Scroll down to EasyV Terminal and press Uninstall button.
- A screen will appear which displays the version of EasyV Terminal selected to be removed. Press Next to continue.
- Press Finish button to complete the uninstallation process.

3. Linux

- Go to YESEFT\Uninstall folder.
- Double click on UnInstallEasyV.sh.
- A screen will appear which displays the version of EasyV Terminal selected to be removed. Press Next to continue.
- Press Finish button to complete the uninstallation process.

2.2 PA-DSS 1.1.5 requires

Examine the software vendor’s procedures for troubleshooting customers’ problems and verify the procedures include:

- Collection of sensitive authentication data only when needed to solve a specific problem
- Storage of such data in a specific, known location with limited access
- Collection of only a limited amount of data needed to solve a specific problem
- Encryption of sensitive authentication data while stored
- Secure deletion of such data immediately after use

Implementation in IPC

Not applicable.

Troubleshooting might require that the merchant upload the YESEFTTransactionLog file to a secure area in Worldpay. For the IPC application, this file no longer contains sensitive authentication data. Worldpay will never request to collect sensitive authentication data for troubleshooting purposes.

2.3 PA-DSS 2.1 requires

The following must be provided for customers and integrators/resellers:

- Instruction that cardholder data exceeding the customer-defined retention period must be securely deleted.
- A list of all locations where payment application stores cardholder data, so that customer knows the locations of data that needs to be deleted.
- Instruction that customers need to securely delete cardholder data when no longer required for legal, regulatory, or business purposes.
- How to securely delete cardholder data stored by the payment application, including data stored on underlying software or systems (such as OS, databases, etc.).
- How to configure the underlying software or systems (such as OS, databases, etc.) to prevent inadvertent capture or retention of cardholder data.

Implementation in IPC

Instructions

Merchants must be aware that any cardholder data exceeding the merchants own retention periods defined in their policy must be securely deleted.

Under some scenarios cardholder data is stored in the local YESEFT/conf folder (or the respective conf folder of each instance) in files with filename beginning with "YESEFTTransactionLog".

The first scenario where IPC stores cardholder data locally is if the EPOS system loses connectivity to the Worldpay Payment Hub (WPH). A daemon process continuously checks connectivity and if the connectivity is restored then IPC will start uploading all the locally stored transactions automatically. The cardholder data will thereby be automatically deleted. No further action will be required by the merchant.

The second scenario is when the YESEFTTransactionLog file is corrupted. IPC will create an automatic backup of this file renaming the corrupted file while saving it (adding the date to the file name) and generate a new YESEFTTransactionLog file.

If the merchant/integrator is not able to restore connectivity within 48 hours or the file is corrupted then the stored encrypted data:

- should be securely retrieved from the system
- uploaded to Worldpay's Secure FTP (sFTP) site for processing

The details of the secure FTP site can be obtained from the Worldpay helpdesk. The Worldpay helpdesk should be contacted before uploading any file so that the files can be processed without delay. Once the

contents of the conf folder are sent to Worldpay then files, with filenames beginning “YESEFTTransactionLog” in the corresponding conf folder, should be deleted **securely** ([Appendix C](#)) from all the locations.

Should any integrators, resellers and partners obtain cardholder data from any other source, they should be aware of their requirements under PCI DSS 1.3, ensuring that they do not store data in Internet accessible systems.

If IPC is in offline mode then transaction data is stored in the conf folder. PA-DSS permits backups of this data provided these are controlled according to PA-DSS and PCI DSS in line with the merchant’s security policies.

However, it is possible that automatic backup process running on the system could create inadvertent or accidental backups of this data. All backups on the system should be reviewed to ensure that any file, with a file name beginning with “YESEFTTransactionLog” in the conf folder, is not part of any backup process **where such backup was not intended**. For example, review whether these files should be omitted from operating system backup processes (System Restore, Auto Backup, System Image) to prevent accidental storage of cardholder data.

In Windows please launch the Backup & Restore application and check whether the backup is configured or not. If yes, then review if all YESEFTTransactionLog files should be omitted.

For Linux platforms, the **rsync** utility is used to back up the files/folder/Drives. If rsync (or similar tool) is being used to create a backup of the system then review whether all YESEFTTransactionLog files should be omitted.

Hibernation and Memory Paging can also lead to inadvertent data storage on a PC. Merchants are recommended to either encrypt the Hard Drive or not to put the PC on Hibernate and disable Memory Paging, but please be aware that disable Memory Paging could be a resulting impact on PC performance. In Windows OS, Memory Paging can be disabled via the following steps

- Right-click on My Computer
- Click on properties
- Click on Advanced system settings
- Go to the Advanced tab, click on Settings button under performance box
- Go to Advance tab, click on Change button under Virtual memory box
- Uncheck Automatically manage paging file size for all drives
- Select No paging file, and click on Set button
- Select OK to allow and restart.

In the event IPC is being removed or uninstalled from a system, the files with file name beginning with “YESEFTTransactionLog” in the conf folder should be deleted using a secure deletion program like SDelete/Shred.

2.4 PA-DSS 2.2 requires

The following must be provided for customers and integrators/resellers:

- Details of all instances where PAN is displayed, including but not limited to POS devices, screens, logs, and receipts.
- Confirmation that the payment application masks PAN by default on all displays.

- Instructions on how to configure the payment application such that only personnel with a legitimate business need can see the full PAN.

Implementation in IPC

The list of PAN output is as follows:

- **EPOS application:** Only the first six and last four digits of the PAN are provided back to the EPOS application
- **Printed receipts:** only the last four digits of the PAN are printed
- **IPC User Interface:** When a referral (manual authorisation) is processed the first six and last four digits of encrypted PAN are displayed on the IPC Terminal user interface. In all other cases the PAN is not displayed.

IPC does not provide configuration options to change the display of PANs from the above described displays.

2.5 PA-DSS 2.3 requires

Details of any configurable options for each method used by the application to render cardholder data unreadable, and instructions on how to configure each method for all locations where cardholder data is stored by the payment application (per PA-DSS Requirement 2.1).

- A list of all instances where cardholder data may be output for the merchant to store outside of the payment application, and instructions that the merchant is responsible for rendering PAN unreadable in all such instances.

Implementation in IPC

The PAN is rendered unreadable via truncation in the printable receipts and transaction response file or message. The PAN is rendered unreadable via encryption for storing offline transactions in the YESEFTTransactionLog file.

IPC does not provide any configurable options for the encryption of the YESEFTTransactionLog file. There are no further actions for the merchant.

The YESEFTTransactionLog file, or the data contained within it, is not provided in any output response.

Instance	Description and how protected
output.txt temp.txt	PAN number is truncated. Only the first six and last four digits of the PAN are provided back to the EPOS application and this cannot be configured for full PAN.
Offline YESEFTTransactionLog file	YESEFTTransactionLog file may contain the PAN Number but the file is encrypted by AES/CBC encryption method.
a) EVTMerchantReceipt.txt b) EVTCustomerReceipt.txt c) MainReceipt.txt d) CustomerReceipt.txt	Only last four digits of the PAN are provided on the receipts and these cannot be configured for full PAN.

2.6 PA-DSS 2.4 requires

The following instructions must be provided for customers and integrators/resellers:

- Restrict access to keys to the fewest number of custodians necessary.
- Store keys securely in the fewest possible locations and forms.

Implementation in IPC

IPC does not expose any encryption key to the merchant. Key management is fully automated and transparent.

The cryptographic keys are securely kept only in a Bouncy Castle keystore file:

YESEFT/properties/jce.BKSkeystore

2.7 PA-DSS 2.5 requires

The following must be provided for customers and integrators/resellers:

- Instructions on how to securely generate, distribute, protect, change, store, and retire/replace encryption keys, where customers or integrators/resellers are involved in these key-management activities.
- A sample Key Custodian Form for key custodians to acknowledge that they understand and accept their key-custodian responsibilities.
- Provide instructions for customers and integrators/resellers on how to perform key-management functions including:
 - Generation of strong cryptographic keys.
 - Secure cryptographic key distribution.
 - Secure cryptographic key storage.
 - Cryptographic key changes for keys that have reached the end of their crypto period.
 - Retirement or replacement of keys as deemed necessary when the integrity of the key has been weakened or keys are suspected of being compromised.
 - Split knowledge and dual control for any manual clear-text cryptographic key-management operations supported by the payment application.
 - Prevention of unauthorized substitution of cryptographic keys.

Implementation in IPC

Encryption technologies are used in order to protect card data within the IPC. The encryption keys used in this process are generated and exchanged between the IPC and the Worldpay Payment Hub. This is performed automatically when the IPC first initialises at start, with a request for a new key sent to by the IPC and the Hub responding with a new AES 256-bit Key.

Under normal circumstances, the merchant/reseller/integrator has no involvement in this process, nor is any involvement required in replacing encryption keys, as this is instigated by Worldpay. The key management process is all automated.

2.7.1 Key Retirement and Replacement

From time to time, the encryption keys within the IPC will be replaced by Worldpay. This is normal and follows good industry practice. In such circumstances, a key replacement process is initiated by Worldpay

by setting specific flags within the Worldpay Payment Hub, namely <keychangerequired> and <Initialized>. This triggers all online IPC instances to change their existing keys to newly generated values.

Under normal circumstances, this is an automated process where there is no need for the merchant, integrator or reseller to perform any manual activity on the IPC. However, key replacement is not possible unless the IPC client is online. As such, all offline clients need to be restarted & brought online by the merchant, integrator or reseller, in order to instigate the automated initialisation process and thus make the key replacement effective.

In order to ensure that offline clients are brought online in order to fetch a new key, merchants/resellers will be contacted and advised to restart relevant IPC installations. Merchant communications are issued by WorldPay's Technical Service Desk (TSD) detailing all steps to be performed by the merchant or reseller.

Retired encryption keys are automatically removed securely within the key replacement process by zeroing the secure cryptographic device.

2.7.2 Key Change in Emergency / Compromised Situation

Although unlikely to ever occur, situations may arise where encryption keys are considered as compromised. In such circumstances, it will be necessary to instigate a key replacement with immediate effect. This process is similar to that described in the previous section and can be invoked upon all terminals or upon specific terminals, as needed. However, due to the risk of card data being exposed in such scenarios, the way in which the key replacement is managed differs slightly. In such situations;

- The TID will be suspended by within the Worldpay Payment Hub. This will be performed by Worldpay and temporarily prohibits transaction acceptance so as to prevent associated card data from being exposed. This will be done by setting up a flag for particular TID within the Worldpay Payment Hub.
- The key replacement process will be initiated, as described in the previous section, and new keys will be pushed to terminal remotely by autonomous means.
- During this process, the Worldpay Technical Service Desk will contact the relevant merchants/resellers and instruct them;
 - Not to accept any transaction from affected terminal/s.
 - Send an offline transaction file to the Worldpay Operations team for processing.
 - Restart the terminal once key exchange is done.
 - Reinstall the IPC client (if applicable or required)*

The Worldpay Technical Service Desk ensures the merchant/reseller has executed these steps and provides the necessary assistance, in case of any difficulties. The process is tracked by the Worldpay Technical Service Desk to ensure that acknowledgements and process results are completed successfully for all effected terminals.

- Replacement encryption keys become effective once the IPC terminal is restarted. This is validated by the Technical Service Desk via the checking of the TID/MID & index values subsequently set within the Worldpay Payment Hub.
- Once successful key replacement has been confirmed, the suspend flag is removed and the terminal is then permitted to accept transactions.

2.8 PA-DSS 2.6 requires

The following must be provided for customers and integrators/resellers:

- Procedures detailing how to use the tool or procedure provided with the application to render cryptographic material irretrievable.
- Instruction that cryptographic key material be rendered irretrievable whenever keys are no longer used and in accordance with key-management requirements in PCI DSS.
- Instructions on how to re-encrypt historic data with new keys, including procedures for maintaining security of clear-text data during the decryption/re-encryption process.

Implementation in IPC

IPC does not provide options for the merchants to render cryptographic material unreadable, to render cryptographic keys irretrievable, or to encrypt historic data with new keys as all those processes are automated by the application.

2.9 PA-DSS 3.1 requires

The following must be provided for customers and integrators/resellers:

- Directions on how the payment application enforces strong authentication for any authentication credentials (for example, users, passwords) that the application generates or manages, by:
- Enforcing secure changes to authentication credentials by the completion of installation per PA-DSS requirements 3.1.1 through 3.1.11.
- Enforcing secure changes to authentication credentials for any subsequent changes (after installation) per PA-DSS requirements 3.1.1 through 3.1.11.
- That, to maintain PCI DSS compliance, any changes made to authentication configurations would need to be verified as providing authentication methods that are at least as rigorous as PCI DSS requirements.
- Assign secure authentication to default accounts (even if not used), and disable or do not use the accounts.
- How to change and create authentication credentials when such credentials are not generated or managed by the payment application, per PA-DSS Requirements 3.1.1 through 3.1.11, by the completion of installation and for subsequent changes after installation, for all application level accounts with administrative access or access to cardholder data.

Implementation in IPC

IPC does not require user accounts and therefore there is no need for integrators, resellers or merchants to change IPC application passwords, enforce strong passwords or assign administrators or end user accounts.

IPC relies entirely on the underlying supported OS features for authentication and access control to the payment application.

The following set of guidelines provides mechanisms to implement access control on the target system:

- Administrative accounts should not be used for application logins.
- Strong passwords should be assigned to the default accounts (even if they are not used) and then disable or do not use the account. All default user accounts should be disabled.
- Strong passwords should be assigned to applications and systems whenever it is possible.

The PCI standard requires the following password complexity for compliance (often referred to as using “strong passwords”):

- Do not use group, shared, or generic user accounts (8.5).

- Passwords must be changed at least every 90 days (8.2.4).
- Passwords must be at least 7 characters (8.2.3).
- Passwords must include both numeric and alphabetic characters (8.2.3).
- New passwords should not be same as any of the last 4 passwords. Security policies should be defined in the system so that a user is not able to re-use any of the last 4 passwords (8.2.5).
- If an incorrect password is provided 6 times the account should be locked out (8.1.6).
- Account lock out duration should be at least 30 min, or until an administrator resets it (8.1.7).
- Sessions idle for more than 15 minutes should require re-entry of username and password to reactivate the session (8.1.8).

Note: These password controls are not intended to apply to employees who only have user access to facilitate transactions. These controls are applicable for access by employees with administrative capabilities, for access to servers with cardholder data, and for access controlled by the application.

However, the merchant/integrator should ensure that each employee who uses the system has a unique login ID. This information gets logged in the system log, which is helpful for forensic investigation if any fraud happens.

Administrative functions that are covered by the PCI guidelines, such as configuration of the payment application, or edits to employee security configuration, require a secure, complex administrative password. Any employee who has access to these functions will be prompted to create an Administrative password and will need to enter this password to save changes in these areas. This administrative password follows all the security guidelines for complexity as specified above.

Such functions include:

- Saving changes to security configuration for those security settings related to PCI (payment application configuration, security set up, edit employees)
- Saving changes to employee workgroup settings where these changes give the employee access to a secure function.

2.10 PA-DSS 3.2 requires

Instruct customers and integrators/resellers to use unique user names and secure authentication to access any PCs, servers, and databases with payment applications and/or cardholder data, per PA-DSS requirements 3.1.1 through 3.1.11.

Implementation in IPC

IPC does not provide any user authentication to use IPC. IPC relies entirely on the underlying supported OS features for authentication and access control to use IPC. It is advised to the merchants and integrators/resellers to use unique user names, passwords and secure authentication to access to the PCs where IPC is installed.

Please find more information in PA-DSS 3.1 section.

2.11 PA-DSS 4.1

Provide instructions for implementing automated audit trails to include:

- How to install the application so that logs are configured and enabled by default upon completion of the installation process.
- How to set PCI DSS-compliant log settings, per PA-DSS Requirements 4.2, 4.3 and 4.4, for any logging options that are configurable by the customer after installation.
- Logs must be enabled, and disabling the logs will result in non-compliance with PCI DSS.
- How to configure PCI-compliant log settings for any third-party software components packaged with or required by the payment application, for any logging options that are configurable by the customer after installation.
- Provide a description of which centralized logging mechanisms are supported, as well as instructions and procedures for incorporating the payment application logs into a centralized logging server.

Implementation in IPC

No extra installation steps are required to enable the application logs as these are enabled by default. Refer to [Appendix A](#) for installation steps.

The merchant has the option to configure IPC to facilitate some of PCI DSS requirement of 10. IPC does not directly facilitate PCI DSS requirement 10.5: IPC generates a configurable number of logs file (20 to 999) and stores them in the YESEFT/logs directory.

As per PCI DSS requirement 10:

- Requirement 10.5.3, it is the merchant's responsibility to copy the log file to a central log server.
- Requirement 10.5.2, it is the merchant's responsibility protect the log file from modification, promptly back them up.
- Requirement 10.7, it is the merchant's responsibility to ensure 12 months of logs are kept any time.

To achieve this merchant can take a backup of log files at regular intervals, or the number of application log files retained can be configured from 20 to 999. The required number of log files can be evaluated by following steps:

- Identify the average number of transactions performed in a day on a single terminal.
- Find the projected yearly total of transactions by multiplying the average transactions by the number of trading days in a year.
- Divide the yearly total figure by 40, as 1 log file contains approximately 40 transactions.

Log levels are implemented in Easy Terminal

Log level 1 – Standard logging

Log level 2 – Detail logging

By default the log level set is 1 and should not be changed. Level 2 is used to enable detailed logging for IPC when troubleshooting is required. The Worldpay Support help desk can provide instructions if required.

Logging level zero (0) will disable the log and disabling the log will result in non-compliance with PCI DSS.

No sensitive information is logged into the IPC logs. No sensitive data is required by Worldpay in troubleshooting any problems with the payment application. All required information is contained in the Worldpay log files, and these do not contain any cardholder information. It is the responsibility of the

integrator and the merchant to ensure that sensitive cardholder data is not recorded and transmitted by any other means.

2.12 PA-DSS 4.2.1 requires

Verify all individual access to cardholder data through the payment application is logged.

Implementation in IPC

In IPC the only storage of cardholder data is in the offline transaction log file (YESEFTTransactionLog). This file is encrypted. Opening the file would not allow access to plain cardholder data. It is the merchant's responsibility to ensure that the underlying OS logging mechanism logs any access to the transaction log file. Please refer to [Appendix D](#) to enable OS logging.

2.13 PA-DSS 4.2.2 requires

Verify actions taken by any individual with administrative privileges to the payment application are logged.

Implementation in IPC

IPC does not have an administrative account or any other account therefore requirement 4.2.2 is not applicable. However all the individual or administrative privileges access to the payment application must be logged on an OS level system log. This is helpful for forensic investigation if any fraud happens.

2.14 PA-DSS 4.2.3 requires

Verify access to application audit trails managed by or within the application is logged.

Implementation in IPC

IPC does not provide a feature to facilitate this requirement. It is the merchant's responsibility to ensure that access to the yescps.log file is logged via the underlying OS logging mechanism or the central log server. To alert on audit logs being changed the merchant must implement file integrity monitoring under PCI DSS requirement 10.5.5.

2.15 PA-DSS 4.2.4/5 requires

Verify invalid logical access attempts are logged. Verify use of and changes to the payment application's identification and authentication mechanisms (including but not limited to creation of new accounts, elevation of privileges, etc.), and all changes, additions, deletions to application accounts with root or administrative privileges are logged.

Implementation in IPC

IPC does not have an administrative account nor any other account therefore requirement 4.2.4 is not applicable.

2.16 PA-DSS 4.2.6 requires

Verify the following are logged:

- Initialization of application audit logs
- Stopping or pausing of application audit logs.

Implementation in IPC

1. Windows 7/8/8.1

IPC writes the initialisation and closing of application audit log files (yescps.log) to the underlying OS system event process. IPC also writes information on transactions performed to the system event logs and this information must be sent to centralized log servers. Please refer to PA-DSS requirement 4.4 for guidance on configuring the syslog agent client.

2. Linux

IPC writes the initialisation and closing of application audit log files (yescps.log) events into file /var/log/YESEFT/YESEFT.log. IPC also writes information on transactions performed to the YESEFT.log file and this information must be sent to centralized log server. Please refer to PA-DSS requirement 4.4 for guidance on configuring the client to send YESEFT.log data.

No configuration option is provided for Stopping and pausing the audit log.

2.17 PA-DSS 4.2.7 requires

Verify the creation and deletion of system-level objects within or by the application is logged.

Implementation in IPC

IPC does not create or delete system level objects.

2.18 PA-DSS 4.3 requires

Payment application must record at least the following audit trail entries for each event:

- User identification
- Type of event
- Success or failure indication
- Origination of event
- Identity or name of affected data, system component, or resource

Implementation in IPC

All the points defined in the above requirement are applicable only if the payment application implements any user account. IPC does not have an administrative or any other account therefore requirement 4.3 is not applicable.

2.19 PA-DSS 4.4 requires

Verifying that customers and integrators/resellers are provided with:

- A description of which centralized logging mechanisms are supported

- Instructions and procedures for incorporating the payment application logs into a centralized logging environment.

Implementation in IPC

All merchants and resellers/integrators should implement a centralized logging environment. Centralized Log Management systems that can import system events can be used to implement this feature. This is primarily to facilitate monitoring, analysis and archiving of the logs. For more details please refer to section 6.3 of [Appendix D](#).

2.20 PA-DSS 5.5.4 requires

A description of the vendor's published versioning methodology, and include guidance for the following:

- Details of versioning scheme, including the format of the version scheme (number of elements, separators, character set, etc.).
- Details of how security-impacting changes will be indicated by the version scheme.
- Details of how other types of changes will affect the version.
- Details of any wildcard elements that are used, including that they will never be used to represent a security-impacting change.

Implementation in IPC

- Number of Elements: There are three elements used for the version number format i.e. Major, Minor and Wildcard/Maintenance Release. The precedence of the elements is determined from left to right.
- Numbers of digits used for each element:
 - Major: Two digits are used for the Major i.e. first element.
 - Minor: Two digits are used for the Minor i.e. second element.
 - Wildcard/Maintenance Release: Three digits are used for the Wildcard/Maintenance Release i.e. third element.
- Format of separators used between elements: Dot operator being used as separator.
- Character set used for each element: It must be Numeric.

A normal version number MUST take the form XX.YY.ZZZ where X, Y and Z are non-negative integers and MUST NOT contain leading zeroes e.g. use 1 not 01. XX is the Major version element, YY is the Minor version element and ZZZ is the Wildcard/Maintenance release element. Each element MUST increase numerically. Once a versioned package has been released, the contents of that version must not be modified. Any modification must be released as a new version e.g. Version 1.0.0 defines the public API. The way in which the version number is incremented after this release is dependent on this public API and how it changes.

Major/High Impact Changes: The initial value of the first element must be 1, a non-negative integer and change in increasing incremental order. If changes to the Payment Application meet any of the following criteria, the Payment Application must undergo a full PA-DSS Assessment:

- Four or more high-level PA-DSS Requirements are affected, not including Requirements 13 and 14.
- Half or more of all PA-DSS Requirements/sub-Requirements are affected, not including Requirements 13 and 14.

- Half or more of the Payment Application's functionality is affected, or half or more of the Payment Application's code-base is changed
- Addition of tested platform/operating system to include on the List of Validated Payment Applications.
- The change is otherwise ineligible for treatment as a Low Impact change.

Minor/Low Impact Changes: The initial value of the second element must be 0, a non-negative integer and change in increasing incremental order. The version number of the second element **MUST** be reset to 0 when a Major version is released/first element is incremented. Low Impact changes are limited to changes to the Payment Application where all of the following conditions are met:

- Three or fewer high-level PA-DSS Requirements are affected, not including Requirements 13 and 14
- Less than half of all PA-DSS Requirements / sub-Requirements are affected, not including Requirements 13 and 14.
- Less than half the Payment Application's functionality is affected and less than half the Payment Application's code-base is changed.

Please Note: Low Impact and No Impact changes to listed Payment Applications may be eligible for partial re-assessment, or "delta" assessment. However please note that a delta assessment must be performed by PA-QSA Company that performed the last Full Assessment and validation of the application.

Wildcard/Maintenance release: The initial value of the third element **MUST** be 0, a non-negative integer and change in increasing incremental order. The version number of third element **MUST** be reset to 0, when Major/Minor version is released i.e. the first/second element is incremented. Wildcard/Maintenance releases can optionally be used to represent a non-security impacting change. The Wildcard/Maintenance Release element is the only variable element of Worldpay's version scheme, and is used to indicate there are only non-security-impacting changes between each version represented by the Wildcard/Maintenance Release element. The use of the Wildcard/Maintenance Release element is permitted subject to the following:

- The Wildcard/Maintenance Release element may only be used for No Impact changes, which have no impact on security and/or any PA-DSS Requirements. The Wildcard/Maintenance Release element may only be substituted for elements of the version number that represent non-security impacting changes; the use of the Wildcard/Maintenance Release element for any change that has an impact on security or any PA-DSS requirements is prohibited.
- The use of the Wildcard/Maintenance Release element is limited to the rightmost (least significant) element of the version number. For example, 1.1.x where x is the Wildcard/Maintenance release - represents acceptable usage. A Wildcard/Maintenance Release element followed by a non-Wildcard/Maintenance Release element is not permitted. For example, 1.x.1 and 1.1.y.1 represent usage that is not permitted.
- All security-impacting changes must result in a change to the non-Wildcard/Maintenance elements (i.e. the Major/Minor elements) of the application version number and will therefore result in an update to the version number listed on the Worldpay Website.
- The Wildcard/Maintenance Release element must not precede version elements that could represent security-impacting changes.
- All Wildcard/Maintenance Release element usage must be consistent with that validated by the PA-QSA Company as part of the PA-DSS Assessment of the Payment Application.

2.21 PA-DSS 6.1,6.2 and 6.3 requires

Payment applications developed for use with wireless technology, the following instructions must be provided for customers and integrators/resellers:

- Instruction that the payment application enforces changes of default encryption keys, passwords and SNMP community strings at installation for all wireless components controlled by the application.
- Procedures for changing wireless encryption keys and passwords, including SNMP strings, anytime anyone with knowledge of the keys/passwords leaves the company or changes positions.
- Instructions for changing default encryption keys, passwords and SNMP community strings on any wireless components provided with, but not controlled by, the payment application.
- Instructions to install a firewall between any wireless networks and systems that store cardholder data.
- Details of any wireless traffic (including specific port information) that the wireless function of the payment application would use.
- Instructions to configure firewalls to deny or (if such traffic is necessary for business purposes) permit only authorized traffic between the wireless environment and the cardholder data environment.

Implementation in IPC

It is the merchants' /partner's responsibility to ensure that all aspects of PCI DSS compliance are adhered to with respect to the use of wireless networks (IEEE 802.11g networks).

This section provides guidance for the PA-DSS requirement under the section 6 (Protect wireless transmissions). If the merchant is using wireless networking and fails to implement the requirements, this will result in non-compliance with PCI DSS.

IPC does not depend on the wireless network; it works on any IP based network. All merchants and resellers/integrators must be aware that, if wireless technology is used with in the payment processing environment, the wireless vendor default settings including but not limited to default wireless encryption keys, passwords and SNMP, SSID community strings must be changed as per PCI DSS Requirement 2.1.1. The following list of procedures should be followed to maintain a PCI DSS compliant wireless network.

- Encryption keys are changed from default at installation and are changed anytime anyone with knowledge of the keys leaves the company or changes positions.
- Default SNMP community strings on wireless devices were changed.
- Firmware on wireless devices is updated to the latest version supporting strong encryption for authentication and transmission over wireless networks (for example – WPA/WPA2, not WEP)
- Install a firewall between any wireless networks and systems that store cardholder data, and configure firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.
- Other security-related wireless vendor defaults, if applicable.
- Where passwords are used ensure they are strong (alpha-numeric, lower and upper case) minimum of seven digits (recommended 12 or higher where supported).

2.22 PA-DSS 7.2.3 requires

Provide instructions for customers about secure installation of patches and updates.

- How to access and install patches and updates in a manner that maintains the integrity of the patch and update code.

Implementation in IPC

It is merchant's responsibility to check Integrity of Patch/Installer before installing IPC software. IPC provides SHA2 (SHA 512) hash value along with the installer in a readme.txt file. Merchant should verify the integrity of installer/Patch provided by Worldpay before installation. See section 3.1 for more details.

2.23 PA-DSS 8.2 requires

Document all required protocols, services, components, and dependent software and hardware that are necessary for any functionality of the payment application.

Implementation in IPC

System requirement for IPC version 1.0.x:

Hardware

- Windows 7, Windows 8, Ubuntu(12.04), SUSE Linux(11) , Cent OS(6.5)
- 1024 MB of RAM minimum, 1536 MB or higher recommended. IPC requires approximate 45 MB to run each instance.
- 1200 MB of available hard-disk space. A default installation of IPC requires approximate 32 MB and each additional instance requires approximate 400 KB.

Software

- It is strongly recommended that JRE version 1.8.0_111 or above should be used.
- MSXML parser needs to be installed. It applies only to Windows OS and only if IPC is printing the transaction receipt.

Protocols

- TCP/IP network connectivity.
- Pin Pads Supported – Ingenico iPP350,iWL250,Vx820-7816,Miura M010.
- Firewall needs to allow IPC Terminal URLs and ports:
 - <https://primary.yes-pay.net/soap/servlet/rpcrouter>
 - <https://www.yes-pay.net/soap/servlet/rpcrouter>
 - <https://www.yes-pay.net/downloads>
 - Port number 443

Components

An Epos application is required to send the input request to IPC application.

2.24 PA-DSS 9.1 requires

The following instructions must be provided for customers and integrators/resellers:

- Instructions not to store cardholder data on public-facing systems (for example, web server and database server must not be on same server).
- Instructions on how to configure the payment application to use a DMZ to separate the Internet from systems storing cardholder data.

- A list of services/ports that the application needs to use in order to communicate across two network zones (so the merchant can configure their firewall to open only required ports).

Implementation in IPC

IPC is a single tier application without a database and webserver. Installation of IPC is done on a POS/till and the POS/till must be in the internal network. IPC does not rely on DMZ.

IPC Socket Mode:

If the EPOS and IPC run on the same machine no firewall configuration, other than that to allow the IPC ports and URLs detailed in section 2.22, is required. If IPC and POS are running on different machines and a firewall is in between then the tcp socket ports configured as outlined in the IPC Configuration Guide ([Appendix B](#)) must be opened.

IPC File Mode:

If file mode is used IPC and POS must be installed on the same machine.

IPC /IP-PEDs:

IPC can communicate with a maximum of 100 IP PEDs configured as outlined in the IPC Configuration Guide in [Appendix B](#). In case the merchant makes use of this configuration option and has a local firewall installed on the IPC host machine, one port per PED must be opened.

IPC /RS232 or USB PEDs:

Merchant must connect IPC machine with PED and configure IPC in accordance to the IPC Configuration Guide in [Appendix B](#).

2.25 PA-DSS 10.1 requires

Provide the following for customers and integrators/resellers:

- Instruction that all remote access originating from outside the customer's network to the payment application must use two-factor authentication in order to meet PCI DSS requirements.
- Describe the two-factor authentication mechanisms supported by the application.
- Instructions on how to configure the application to support two-factor authentication (two of the three authentication methods described in PA-DSS Req. 3.1.4).

Implementation in IPC

Partners/Merchant are reminded of their obligations under PCI DSS requirement 8.3. If the systems are accessed remotely then all network connectivity should be performed using two-factor authentication (user ID and password and an additional authentication item such as a token). Two factor authentication is required for remote access to the network by employees, administrators and third parties.

IPC does not require two factor authentication hence no configuration is available. Once two-factor authentication based access has been achieved into the merchants cardholder data environment IPC does not require additional two factor authentication.

2.26 PA-DSS 10.2.1 requires

If payment application updates are delivered via remote access into customers' systems, provide the following:

- Instructions for activation of remote-access technologies for payment application updates only when needed for downloads, and turning access off immediately after download completes, per PCI DSS Requirement 12.3.9.
- Instructions that, if computer is connected via VPN or other high-speed connection, receive remote payment application updates via a securely configured firewall or personal firewall per PCI DSS Requirement 1.

Implementation in IPC

10.2.1 is not applicable to IPC as there are no application updates delivered through remote access. Auto upgrade is performed through a secure connection between IPC and WPH.

IPC application checks the WPH server for the availability of updates every time it starts up. IPC will send the update request to a trusted host only as held in the trust-store.

WPH will provide the software update/ update for POI device only if the terminal ID is configured for software download and a new update is available.

The process for applying patches and updates is detailed below for information purposes.

If present, IPC requests the update details and WPH returns the following;

- URL from where the update is to be downloaded
- Name of the file
- Size of the file
- Checksum of the file

IPC then downloads the file from the URL. IPC checks the file size and checksum from the information it has previously received from WPH.

If all details match then the patch is applied.

2.27 PA-DSS 10.2.3 requires

Instructions for all the remote access to the payment application must be implemented securely.

Implementation in IPC

The merchant/ integrators/resellers must consider the following instructions when setting up a remote access tool to be used by internal administrators, partners and vendors.

Below is a list of required remote access software security configuration:

- Change default settings in the remote access software (for example, change default passwords and use unique passwords for each merchant).
- Allow connections only from specify (known) IP/MAC addresses.
- Use strong authentication or complex passwords for logins.
- Enable encrypted data transmission.
- Enable account lockout after a certain number of failed login attempts.
- Enable logging function.
- Restrict access to merchant environment to authorized reseller/integrator personnel.

- All non-console administration should use strong cryptography using technologies such as SSH, VPN or TLS for encryption of non-console administrative access.
- Establish customer passwords according to PCI DSS requirements 8.1, 8.2 and 8.5.

2.28 PA-DSS 11.1 requires

If the payment application sends, or facilitates sending, cardholder data over public networks, include instructions for implementing and using strong cryptography and security protocols for secure cardholder data transmission over public networks, including:

- Required use of strong cryptography and security protocols if cardholder data is ever transmitted over public networks.
- Instructions for verifying that only trusted keys and/or certificates are accepted.
- How to configure the payment application to use only secure versions and secure implementations of security protocols.
- How to configure the payment application to use the proper encryption strength for the encryption methodology in use.

Implementation in IPC

IPC encrypts all sensitive data using TLS 1.2 128 bit encryption. This is in-line with the PCI DSS Requirements 4.1 & 4.2; ensure use of strong cryptography and security protocol like TLS or IPSEC to safeguard sensitive cardholder data during transmission over open and public networks.

IPC is configured to connect to only trusted host systems. IPC consist of a trust-store that contains trusted server certificates. This trust-store is referred for every TLS/secure connection to the WPH server.

Installation of IPC involves a step to input WPH merchant ID and the terminal ID numbers. IPC uses these details to authenticate itself to the WPH server. The WPH server will not download any configuration or allow transactions from IPC if the merchant ID and the terminal ID combination is not valid on WPH.

WPH does not allow any weak cipher suites: the cardholder data is always encrypted with TLS 1.2 128 bit or more encryption.

IPC does not provide configuration options regarding the encrypted communication between IPC and WPH. The encryption settings are auto configured via the IPC installer.

2.29 PA-DSS 11.2 requires

If the payment application facilitates sending of PANs by end-user messaging technologies, include instructions for implementing and using a solution that renders the PAN unreadable or implements strong cryptography, including:

- Procedures for using the defined solution to render the PAN unreadable or secure the PAN with strong cryptography.
- Instruction that PAN must always be rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.

Implementation in IPC

IPC does not allow or facilitate transmission of Cardholder Data using end user messaging technologies like email or instant messaging. All cardholder data is transmitted encrypted under strong cryptography.

2.30 PA-DSS 12.1 requires

If the payment application facilitates non-console administrative access, include instructions on how to configure the application to use strong cryptography (such as SSH, VPN, or SSL/TLS) for encryption of all non-console administrative access to payment application or servers in cardholder data environment.

Implementation in IPC

IPC does not have administrative accounts but does require admin rights to install. Access to the files of IPC depends of the policy settings of the accounts configured on the merchant's Windows or Linux machines.

Worldpay recommends generating accounts on Linux and Windows to install and run IPC on a need to know basis depending on the size and organisational structure of the merchant.

The merchant should always use strong cryptography using technologies such as SSH, VPN or TLS for encryption of non-console administrative access.

2.31 PA-DSS 12.2 requires

Include directions for customers and integrators/resellers to use multi-factor authentication.

Implementation in IPC

Multi-factor authentication is not provided with the payment application. Nonetheless appropriate multi-factor authentication must be used for all personnel with non-console administrative access to the CDE.

2.32 IPC Monitoring/change detection Instruction

Monitoring/Change detection falls under PCI DSS requirement 11. It is recommended that the IPC application should be monitored by change detection tools to prevent any malicious change in the application. However, monitoring all the IPC files could generate unnecessary alerts as IPC updates some critical files during initialisation and transaction processing. The following static folder/files of YESEFT should be monitored by change detection/FIM tool.

- CommonFiles
- jvt.jar
- yespay-cps.jar
- installupdate.jar
- StartPOSServer
- Properties/eftdataset-api-client.properties
- Properties/epos-api-client.properties
- Properties/yespay-cps-interface.properties

Critical dynamic files that are changed by IPC are given below. It is up to the merchant how they entertain the alerts generated for these files

- Truststore
- jce.BKSkeystore
- YESEFTTransactionLog.xml
- evtkm.properties

An example of change detection is the TripWire tool. For installation and configuration details of TripWire or similar tools, please read the vendor manual.

2.33 Changes to PA DSS requirements and changes to IPC

The regular review of this guide falls under requirements 13.1.3. WorldPay is obliged to review this guide at least at an annual basis if no changes either to the standard or to the software have taken place. Should however updates to the software or the standard occur this guide will be reviewed, updated, made available and the necessary communication sent in due course. This guide will be updated with every minor or major release. Bug fixes are covered through the readme notes distributed with the software. The standard goes through a three years major update cycle though occasionally intermittent changes are issued. No matter the nature of the change to the standard, WorldPay will review every change issues by the PCI SSC and react upon them with the necessary updates to the software as well as to this guide.

2.34 Changes to operating systems and Java

IPC depends on a the operating systems and more importantly on Java. It is essential to the security of IPC to stay in touch with security vulnerabilities identified in either of those dependencies on an ongoing basis. Worldpay operates a vulnerability and patch management process to ensure IPC is tested against any security relevant change to the OS or Java. Should an OS or Java patch or upgrade impact the functionality of IPC WorldPay's process will capture this, followed by the implementation of the necessary changes to the software and/or this guide. The relevant communications will be sent, including the updated guide and IPC patch if required, to the merchants with instruction what to do to keep their cardholder data environment secure. It is paramount for the security of the merchant cardholder data environment to stay alert and react upon patches issued by Worldpay.

2.35 Notifications

2.35.1 Critical patches

If critical patches needs to be made available to merchants, Worldpay will notify the affected merchants. The notifications will take place in form of emails sent to the merchants.

Critical vulnerabilities can be reported from various sources:

- Kernel or firmware patches for the PTS devices provided by the PTS device supplier through Worldpay
- IPC patches provided by Worldpay
- Java or Operating System patches announced industry wide with potential subsequent patches for IPC through Worldpay

Critical vulnerabilities are defined as follows:

Vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed.

2.35.2 IPC upgrades and bug fixes

It is common practice to provide regular upgrades or bug fixes for IPC in the market.

The necessary notifications are taking place in the form of emails to the affected merchants.

With every version of IPC no matter what the release type is (major, minor or bug fix release) the updated integration guide will always be packaged up with other necessary files in the installer.

2.36 Dissemination of the integration guide and installers

The integration guide is bundled with every software distribution in the installer.

The installers are made available through Dropbox.

Once a new version of IPC is available the installer will be copied to the Worldpay Dropbox folder. The Worldpay operations team or the corporate implementation team will then generate a temporary link to allow the download of the installer.

Should the merchant require a new integration guide outside of the delivery of major or minor updates or bug fixes then the Worldpay operations team should be contacted for the processing of the request.

3 Appendix A – IPC Installation Instructions

3.1 Pre-requisites

Check java version using "java -version" command on Shell-terminal/command-prompt. If it is not present, or a version below than 1.8.0_111 (latest) is installed, then please download the latest JRE (Java Runtime Environment) from

<http://www.oracle.com/technetwork/java/javase/downloads>

Please note: IPC complies with mandates to remove SSL and early versions of TLS provided that Java 1.8 or above is installed. IPC-2 will not be installed if Java version is below 1.8

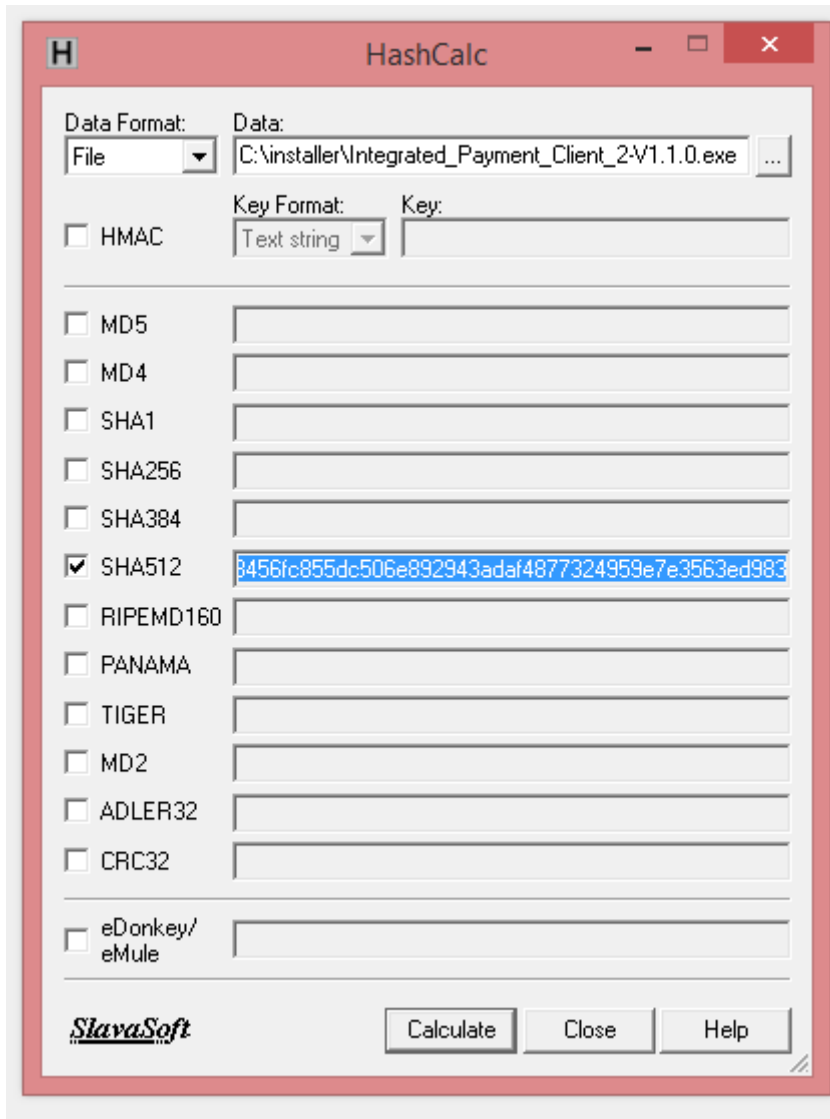
If JRE has not been installed and the JRE folder is being copied (e.g. for a reference build or 'gold' build), then the JRE path needs to be set in the JAVA_HOME variable in /YESEFT/setenv.bat(sh) file after IPC installation.

Before installing any installer (patch) verify that none of installer file has been changed.

To verify the installer, calculate the SHA-2 (SHA 512) hash value of the installer file(.exe) and compare the calculated hashvalue with one which is provided in readme.txt file.

Note :- If hashvalue doesn't match then do not install that patch/installer and contact with Worldpay Support team. This is essential as per the PA-DSS requirement 7.2.3.

See below diagram showing calculated Hash value. Using any Hash calculator tool hash value can be retrieved. Below is the example of 'HashCalc' tool, in which select .exe file from its location, select SHA512, click on calculate and tool will show you the hash value.



3.1.1 For Windows

Please download the Windows x86 Offline JRE and install it. After the installation of JRE, a popup will appear to uninstall the older java version.

If there are no other applications that are dependent on the older java then uninstall the older java application (recommended). However, if other applications are dependent on the older java then follow the instructions below

- In order to ensure availability of the older JRE path for other applications, the older JRE path needs to be added at the start of system PATH variable. For information on how to get to the system PATH variable please go to the below URL
<https://java.com/en/download/help/path.xml>
- The latest JRE path needs to be set in JAVA_HOME variable in /YESEFT/setenv.bat(sh) file after IPC installation to instruct IPC to use the latest JRE.
- **Note:** Msxml4 is required if IPC will be used to print the receipts directly to the printer. Please download and install from
<http://www.microsoft.com/en-us/download/details.aspx?id=19662>

3.1.2 For Linux

Please download the Linux x86 JRE and unzip it.

Run the commands below to set java path. replacing 'JAVA_PATH' by the location of the unzipped JRE folder.

1. `sudo update-alternatives --install "/usr/bin/java" "java" "/JAVA_PATH/bin/java" 1`
2. `sudo update-alternatives --set java / JAVA_PATH /bin/java`

3.2 IPC Terminal

- Download the installer IPC-version- 2.x.x.exe. The installer implements an integrity check that means IPC cannot be installed If the installer file has been modified or corrupted during download. Worldpay provides two separate installers for P2PE Merchants and for Non-P2PE Merchants. Installation steps are same for both the installers.
- Please refer to the below [installation steps](#) to install.
- Once IPC is installed, please refer to the [Appendix B](#) for IPC configuration details.
- Run StartPOSServer.bat/sh to start the IPC application.

3.2.1 Installation steps

Step 1

- **Windows user**

Run the installer as normal windows installer.

Note: For Windows 8/8.1

If IPC Installer gets stuck for few minutes at this stage, then please follow the below instructions

- Terminate the installation process by pressing "Cancel" button.
- Run the installer:execute the command below at the command prompt
`path\Integrated_Payment_Client_2-V1.x.x.exe-Dinstall4j.nolaf=true`

- **Linux user (Ubuntu, Suse, CentOS)**

Run `sudo sh filepath1/filename`.

¹filepath is the location where IPC is placed in the local machine.

Once the process starts, the screen below will appear on the PC.

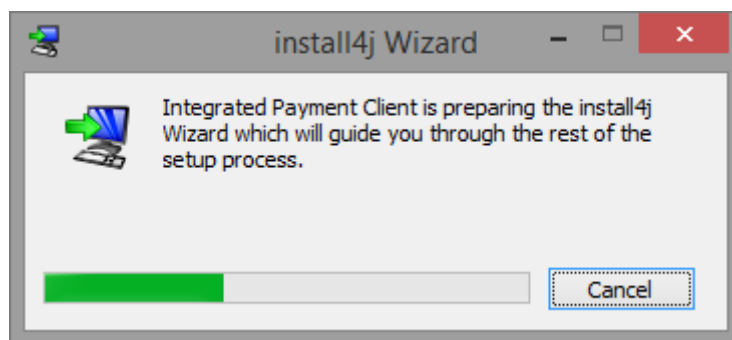


Figure 1

Step 2

After few seconds, the screen below will appear on the PC. Press Next to go ahead or cancel to terminate the installation.

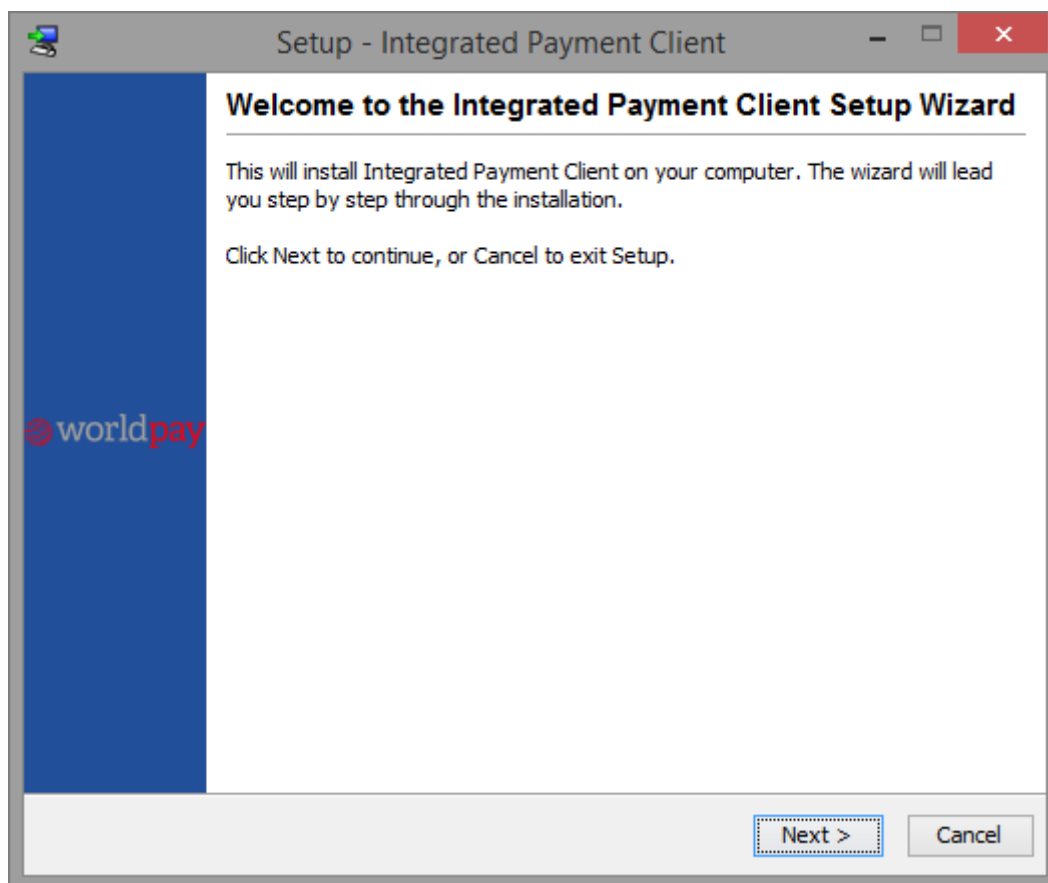


Figure 2

Step 3

After few seconds, the following screen will appear on the PC. Please select the Region from dropdown list and press Next to go ahead or cancel to terminate the installation.

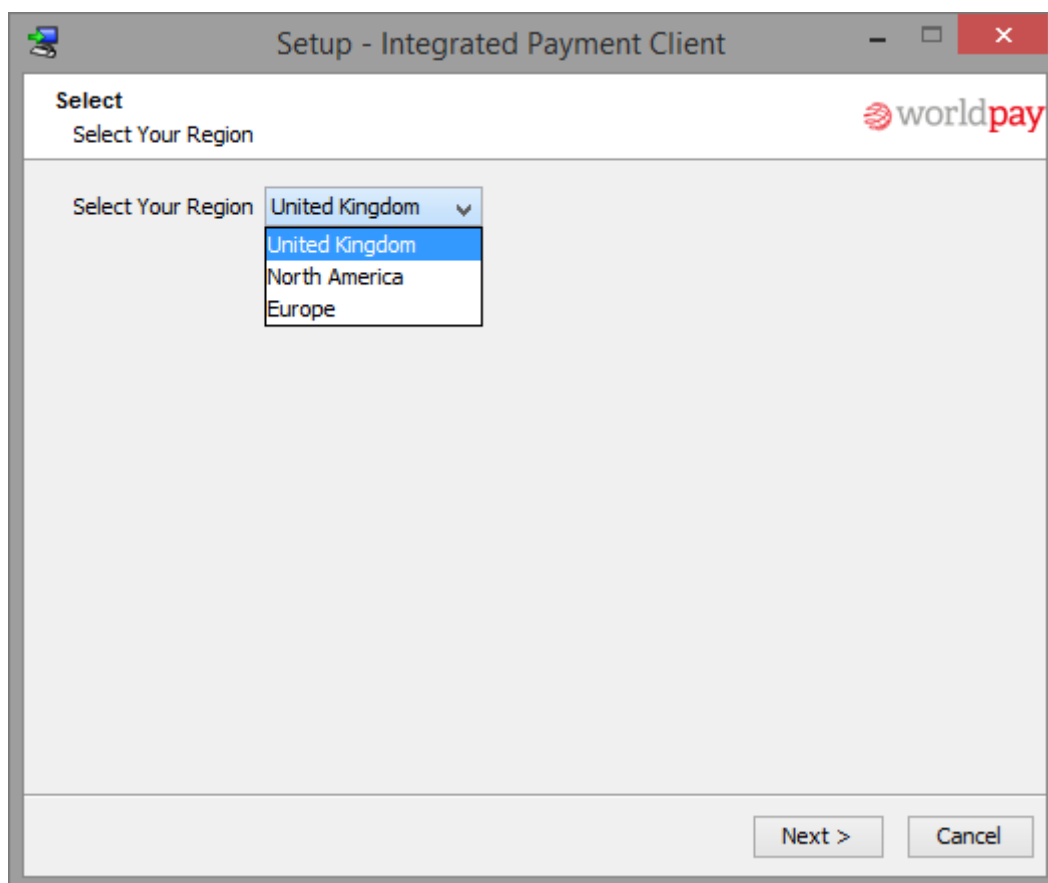


Figure 3

Step 4

The Installer will prompt to select the folder under which the application will be installed. By default, it will display C:\YESEFT. The installation directory can be changed if required to a different path, but

the folder name must always be YESEFT. For example, a valid directory would be C:\MYPOSDIR\YESEFT. Press Next to continue.

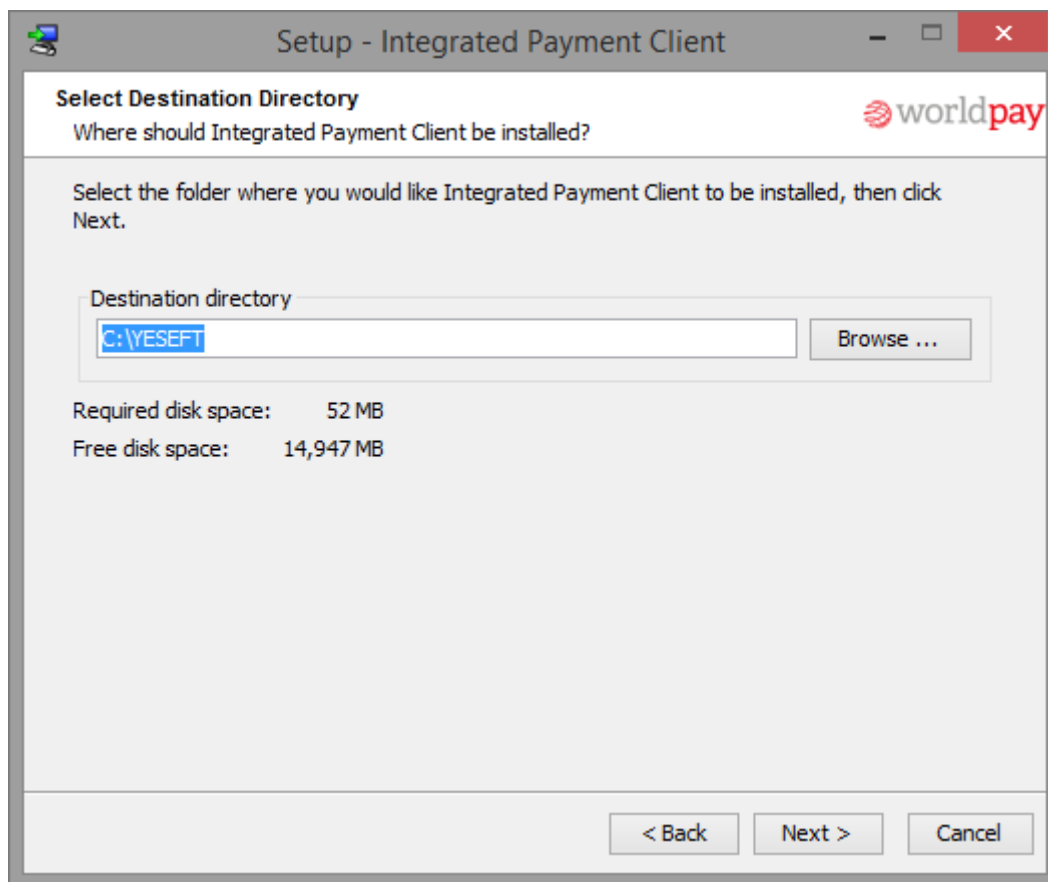


Figure 4

Step 5

The installer will now display the program name of the application (Easy V Terminal) and will create folder of Easy V terminal in start menu. Uncheck “Create a Start Menu folder” to avoid shortcut in Start Menu. Press Next to continue.

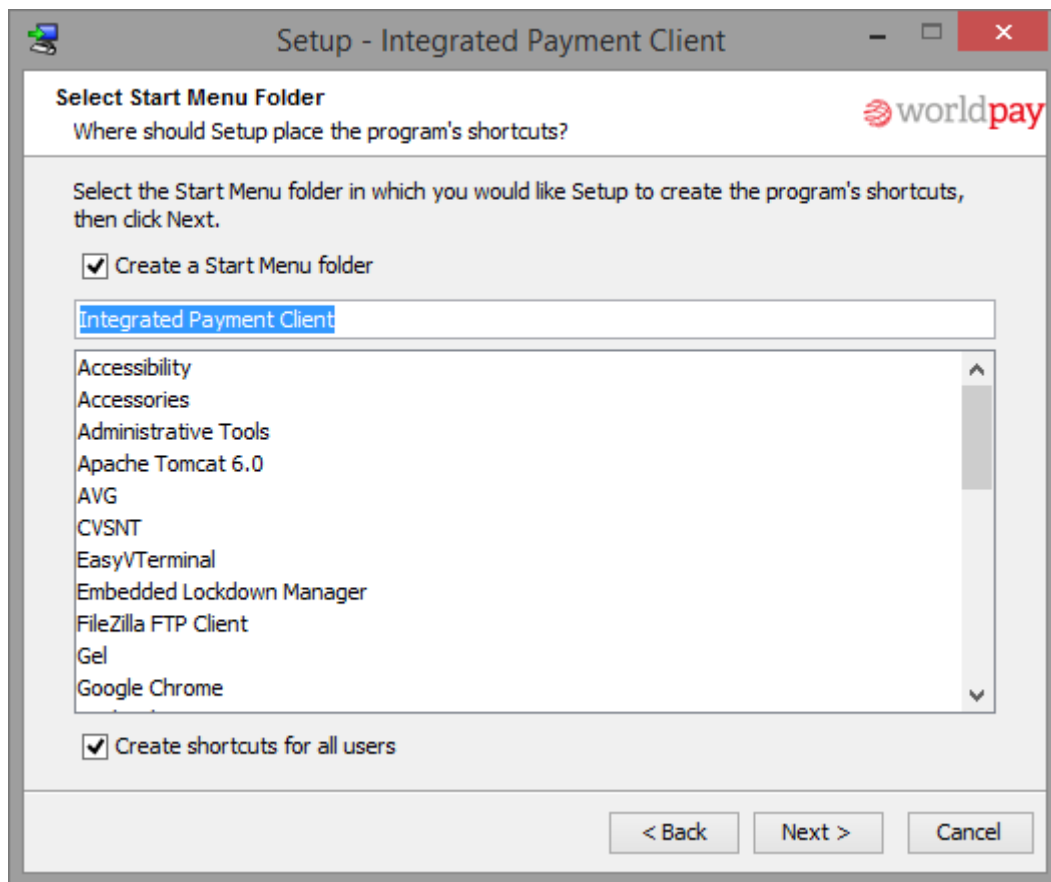


Figure 5

Then following screen will appear on PC:

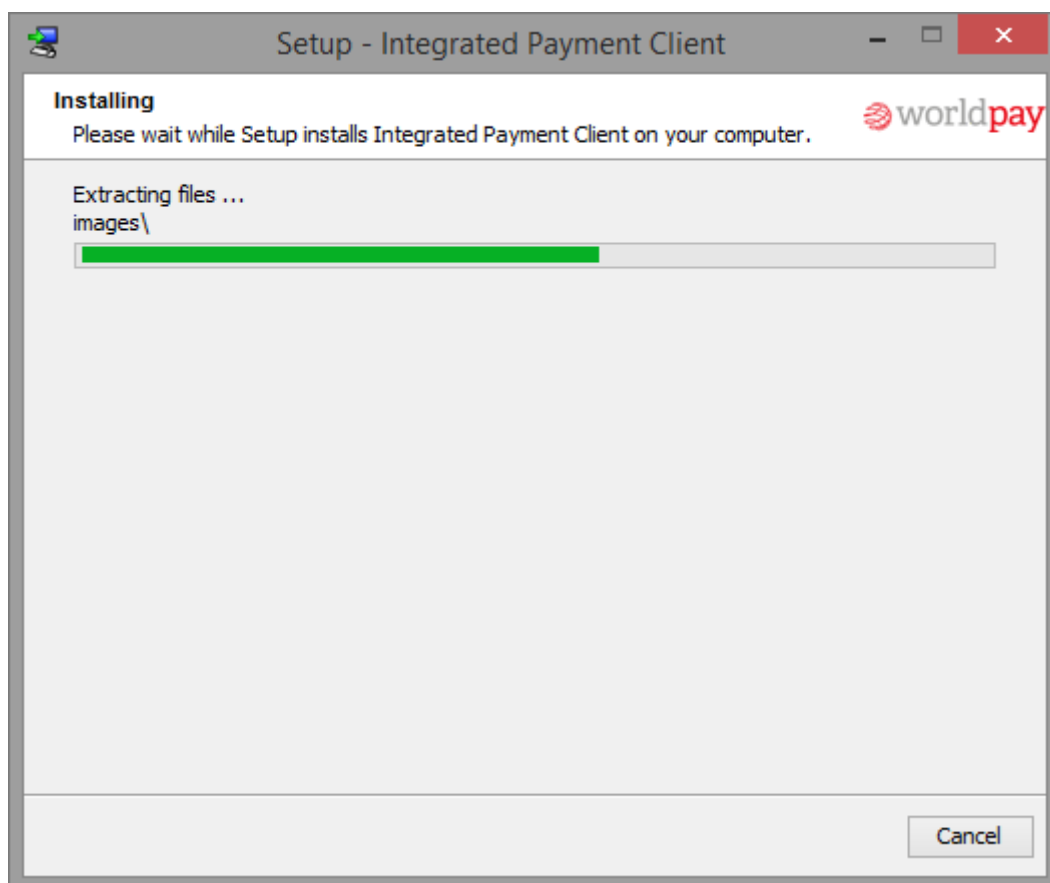


Figure 6

Step 6

Integrated Payment Client-II-Series
Implementation/Integration Guide issue 1.21 For version 2.1.6

Once the installation is complete, the screen below will appear. Click on the finish button to complete the setup process.

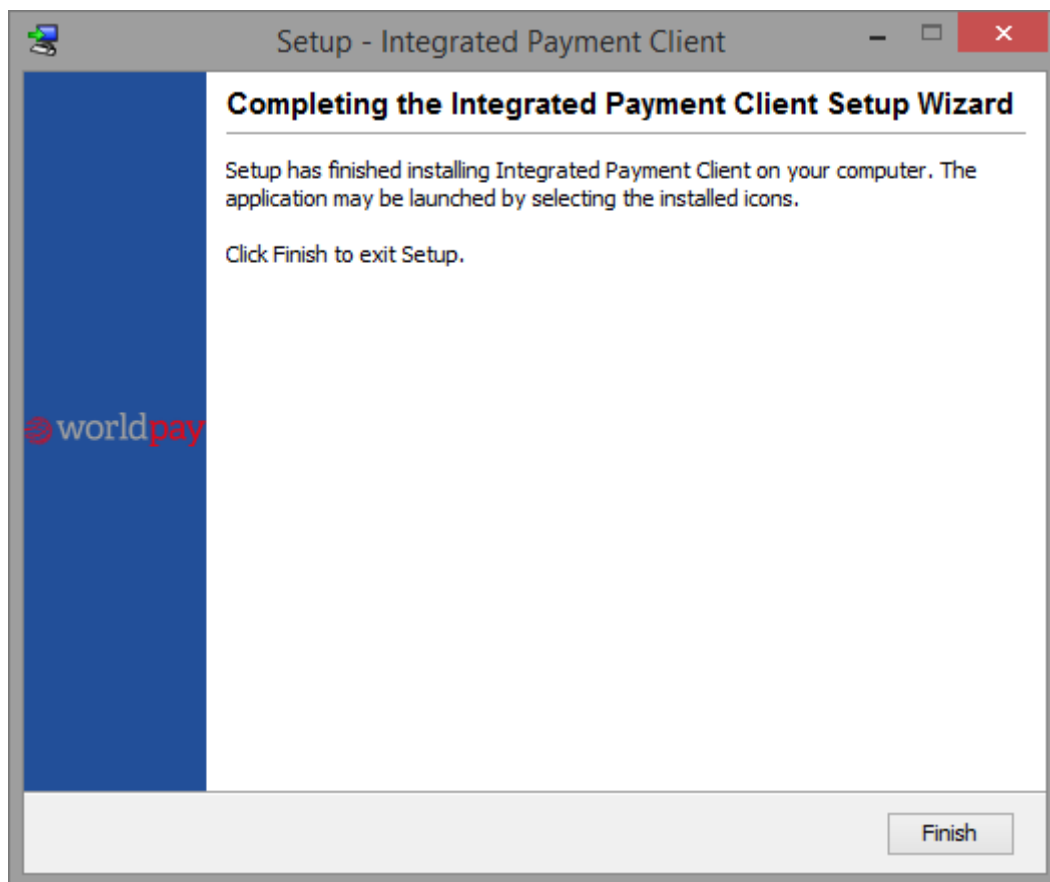


Figure 7

4 Appendix B – IPC Configuration guide

4.1 YESEFT folder contents

By default, YESEFT folder is created in the C:\ drive (Windows) or /home (Linux) of the system after running the installer of IPC:

Name	Date modified	Type	Size
.install4j	30/01/2015 06:00 PM	File folder	
bin	30/01/2015 06:00 PM	File folder	
CommonFiles	30/01/2015 06:00 PM	File folder	
conf	30/01/2015 06:00 PM	File folder	
images	30/01/2015 06:00 PM	File folder	
lib	30/01/2015 06:00 PM	File folder	
logs	30/01/2015 03:33 PM	File folder	
properties	30/01/2015 06:00 PM	File folder	
Uninstall	30/01/2015 06:00 PM	File folder	
Config-Hash	30/01/2015 06:00 PM	Windows Batch File	1 KB
ConfigHash	30/01/2015 03:33 PM	CLASS File	4 KB
EMBOSS-Setup	30/01/2015 06:00 PM	Windows Batch File	2 KB
EMBOSS-Setup-NC	30/01/2015 06:00 PM	Windows Batch File	2 KB
installUpdate	30/01/2015 03:33 PM	JAR File	26 KB
jvt	30/01/2015 03:33 PM	JAR File	989 KB
setenv	30/01/2015 06:00 PM	Windows Batch File	1 KB
StartPOSServer	30/01/2015 06:00 PM	Windows Batch File	1 KB
TakeInput	30/01/2015 03:33 PM	CLASS File	7 KB
YESEFTConfig	30/01/2015 06:00 PM	Windows Batch File	1 KB
YESEFTConfig	30/01/2015 03:33 PM	JAR File	232 KB
YEsftInterface	30/01/2015 03:33 PM	Application	76 KB
yespay_logo	30/01/2015 03:33 PM	JPEG image	5 KB
yespay_logo_hd	30/01/2015 03:33 PM	JPEG image	35 KB
yespay-cps	30/01/2015 03:33 PM	JAR File	3,275 KB

Figure 8: YESEFT Folder

A brief description of some of the important folders and files is presented below:

- **EMBOSS-Setup:** This is a batch file which can be used to set the MID and TID for a terminal.
- **MID:** This is a merchant identification number (length of 1 to 5 digits maximum) provided by Worldpay, also known as WPH MID. For testing purposes MID: 16 can be used.

- **TID:** This is a unique terminal identification number (length of 8 digits) provided by Worldpay specifically for a terminal. For testing TID: 22980012 can be used.

Run EMBOSS-Setup.bat file. You will be prompted to enter the instance number. For default instance either '0' can be entered or can be just left blank and press enter to continue further.

On the prompt to enter MID, enter the MID provided by Worldpay for the merchant (For testing MID: 16 can be used) and press enter. On the TID prompt enter the 8 digit TID provided by Worldpay for the terminal (For testing TID: 22980012 can be used).

- **StartPOSServer:** This batch file can be used to initialize IPC application after configuring the application.
- **YESEFTConfig:** This batch file can be used to configure IPC application. A complete description is provided from the next section.
- **Conf:** This folder mainly contains seven XML files.
 - YESEFTConfiguration.xml
 - YESEFTTransactionLog.xml
 - YESEFTTransactionLog-tmp.xml
 - YESEFTTransactionLogEmpty.xml
 - EFTAcquirerDataset.xml
 - EFTIssuerDataset.xml
 - EFTMerchantDataset.xml

During initialization of the application the three dataset files EFTAcquirerDataset.xml, EFTIssuerDataset.xml and EFTMerchantDataset.xml are downloaded from the WPH server and YESEFTTransactionLog-tmp.xml is generated by IPC. These files are not present by default.

- **Logs:** This folder mainly contains the audit logs which can be used for the analysis and diagnosis of any issue. This folder contains a maximum of yescps.log files if 1 MB (max) file each. All log files are in simple text format. The current log files are named as yescps.log and TerminalInitializer.log. Yescps.log contains transaction and control flow information and TerminalInitializer.log contains commands sent and responses received from the pinpad.

If the yescps.log reaches to 1MB then it is renamed automatically as yescps.log.1 and the file prior to that as yescps.log.2 and so on. The number of log files kept by IPC can be configured from 20 to 999; and once the maximum number is reached oldest log file is overwritten.

- **Common Files:** This folder contains two sub folders, conf and properties, and one brand.txt file. The conf folder contains YESEFTTransaction.log.xml and properties folder contains the files that are required for keychange process.

IPC uses both these folders when new instance is created because every new instance is set for a new TID and that requires keychange process to be completed with WPH.

- **Properties:** This folder contains most of the important properties file used by the application for specific purposes. A brief description of some important files is as provided below:
 - **eftdataset-api-client.properties:** This file contains the URL of the WPH server used by IPC to download above mentioned dataset files.

- **epos-api-client.properties:** This file contains the URL's used by IPC to communicate with the WPH server.

4.2 Minimum Configuration Required

The purpose of Section is to describe the minimum configuration required for IPC.

- Run the EMBOSS-Setup.bat/sh file. This will ask for Merchant ID and Terminal ID. Please input the merchant ID and terminal ID provided for the installation.
- Run YESEFTConfig.bat/sh to configure the minimum required parameters given below.

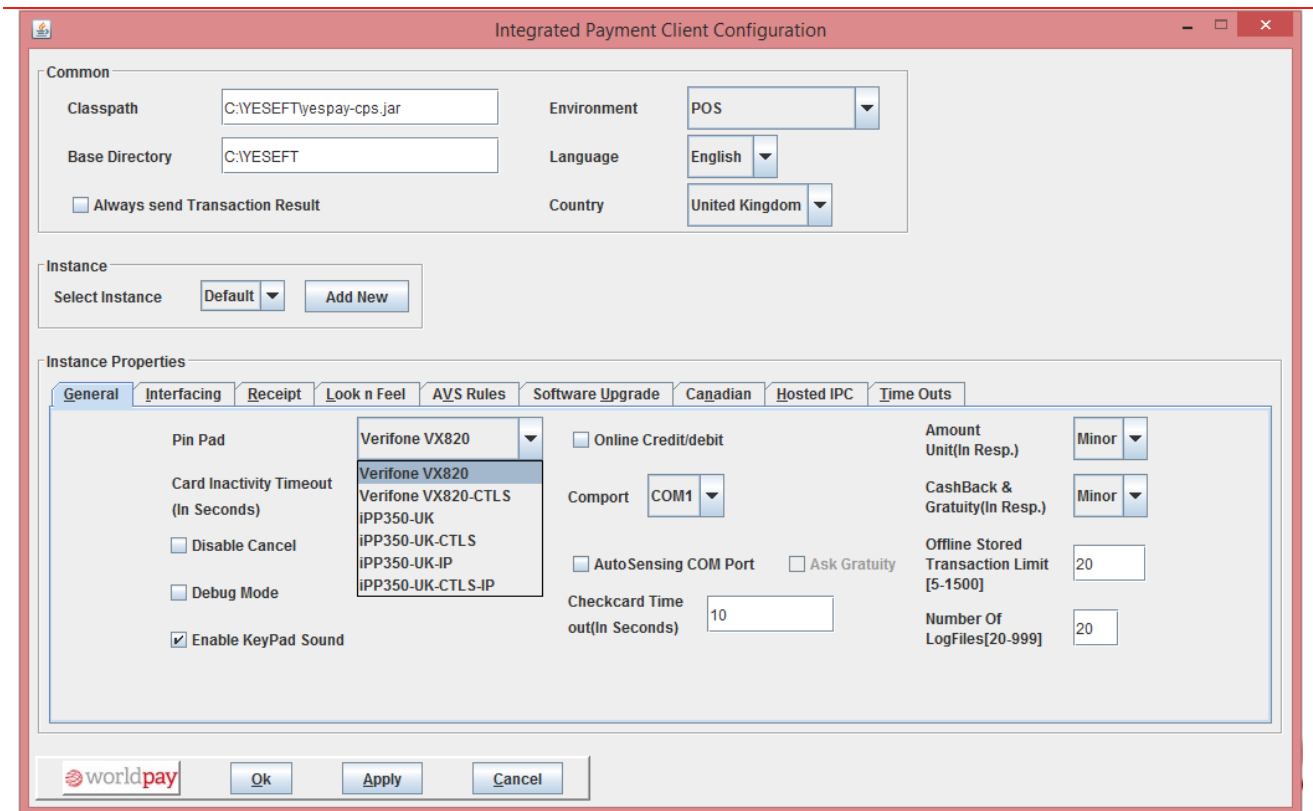
4.2.1 General Configuration

- **Environment Selection:** Select environment from environment list. This IPC application supports POS(Retail) and Semi-Attended. Based on selected environment IPC-2 will display the list of countries , languages and supported Pin Pad.

Following are the matrix of environment , countries , languages and supported Pin Pads.

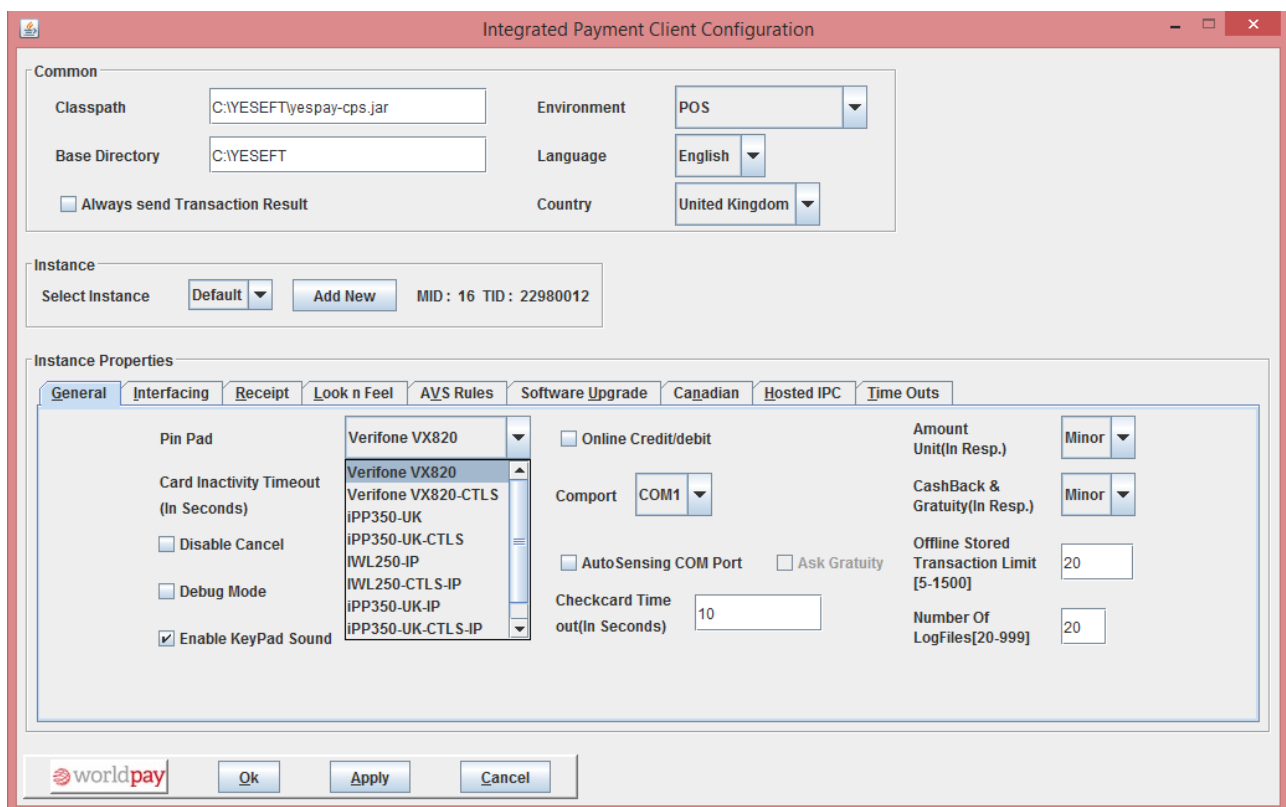
Environment	Countries	Language	Pinpad
POS	UK	English	iPP350,IWL250,Verifone VX820,Miura
	ROI	English	iPP350,IWL250,Verifone VX820
	US	English	Verifone VX820-XPI
	France	French	iPP350
Semi-Attended	UK	English	iPP350,IWL250
	ROI	English	iPP350,IWL250

- **Pin Pad Selection:** Select the pinpad from pinpad list. Pinpad list is different in P2PE and Non-P2PE installers. See below Figure 9.1 for pinpad list for P2PE Merchants and 9.2 for Non-P2PE merchants.
 - **Comport Selection:** Select the com port through which pinpad is connected to PC.
-
-



The screenshot shows the 'Integrated Payment Client Configuration' window. The 'Common' tab is active, displaying fields for Classpath (C:\YESEFT\yespay-cps.jar), Base Directory (C:\YESEFT), Environment (POS), Language (English), and Country (United Kingdom). There is a checkbox for 'Always send Transaction Result'. Below this is the 'Instance' section with a 'Select Instance' dropdown (Default) and an 'Add New' button. The 'Instance Properties' section has multiple tabs: General, Interfacing, Receipt, Look n Feel, AVS Rules, Software Upgrade, Canadian, Hosted IPC, and Time Outs. The 'General' tab is selected, showing a list of pin pads (Verifone VX820, Verifone VX820-CTLS, iPP350-UK, iPP350-UK-CTLS, iPP350-UK-IP, iPP350-UK-CTLS-IP) with 'Verifone VX820' selected. Other settings include 'Online Credit/debit' (unchecked), 'Comport' (COM1), 'AutoSensing COM Port' (unchecked), 'Ask Gratuity' (unchecked), 'Checkcard Time out(In Seconds)' (10), 'Amount Unit(In Resp.)' (Minor), 'CashBack & Gratuity(In Resp.)' (Minor), 'Offline Stored Transaction Limit [5-1500]' (20), and 'Number Of LogFiles[20-999]' (20). At the bottom are 'Ok', 'Apply', and 'Cancel' buttons.

Figure 9.1 Minimum Configuration Required (P2PE)



The screenshot shows the 'Integrated Payment Client Configuration' window. The 'Common' tab is active, displaying fields for Classpath (C:\YESEFT\yespay-cps.jar), Base Directory (C:\YESEFT), Environment (POS), Language (English), and Country (United Kingdom). There is a checkbox for 'Always send Transaction Result'. Below this is the 'Instance' section with a 'Select Instance' dropdown (Default), an 'Add New' button, and a text field showing 'MID : 16 TID : 22980012'. The 'Instance Properties' section has multiple tabs: General, Interfacing, Receipt, Look n Feel, AVS Rules, Software Upgrade, Canadian, Hosted IPC, and Time Outs. The 'General' tab is selected, showing a list of pin pads (Verifone VX820, Verifone VX820-CTLS, iPP350-UK, iPP350-UK-CTLS, IWL250-IP, IWL250-CTLS-IP, iPP350-UK-IP, iPP350-UK-CTLS-IP) with 'Verifone VX820' selected. Other settings include 'Online Credit/debit' (unchecked), 'Comport' (COM1), 'AutoSensing COM Port' (unchecked), 'Ask Gratuity' (unchecked), 'Checkcard Time out(In Seconds)' (10), 'Amount Unit(In Resp.)' (Minor), 'CashBack & Gratuity(In Resp.)' (Minor), 'Offline Stored Transaction Limit [5-1500]' (20), and 'Number Of LogFiles[20-999]' (20). At the bottom are 'Ok', 'Apply', and 'Cancel' buttons.

Figure 9.2 Minimum Configuration Required (Non-P2PE)

4.2.2 Communication Interface

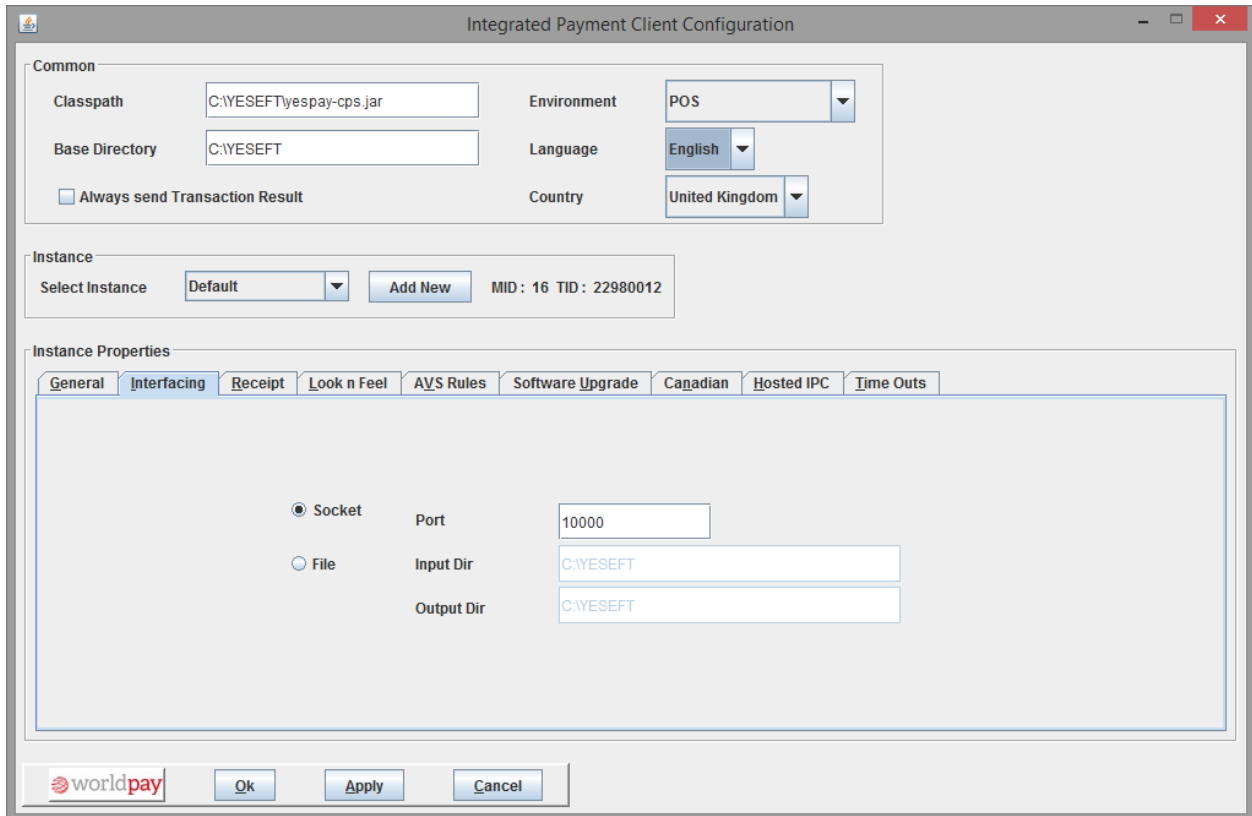
Select communication mode between IPC and EPOS application.

- **Socket:** Select this option if socket connection is going to be used by EPOS application to communicate with the IPC to send the transaction request.

By default port number is 10000

- **File:** Select this option if file is going to be used by EPOS application to communicate with the IPC to send the transaction request.

The default location for input/output directory is the absolute location of YESEFT.



The screenshot shows the 'Integrated Payment Client Configuration' window with the 'Interfacing' tab selected. The 'Common' section includes fields for Classpath (C:\YESEFT\yespay-cps.jar), Base Directory (C:\YESEFT), Environment (POS), Language (English), and Country (United Kingdom). The 'Instance' section shows 'Select Instance' set to 'Default' and 'Add New' button, with MID: 16 and TID: 22980012. The 'Instance Properties' section has tabs for General, Interfacing, Receipt, Look n Feel, AYS Rules, Software Upgrade, Canadian, Hosted IPC, and Time Outs. The 'Interfacing' tab is active, showing radio buttons for 'Socket' (selected) and 'File'. The 'Socket' section has a 'Port' field set to 10000. The 'File' section has 'Input Dir' and 'Output Dir' fields, both set to C:\YESEFT. The bottom of the window has the Worldpay logo and buttons for 'Ok', 'Apply', and 'Cancel'.

Figure 9: Interfacing Selection

4.3 Detailed Terminal Configuration

The IPC application supports a number of EMV level-2 pinpads, can support multiple terminals (instances) and has a number of configuration options as described in this section

4.3.1 Common

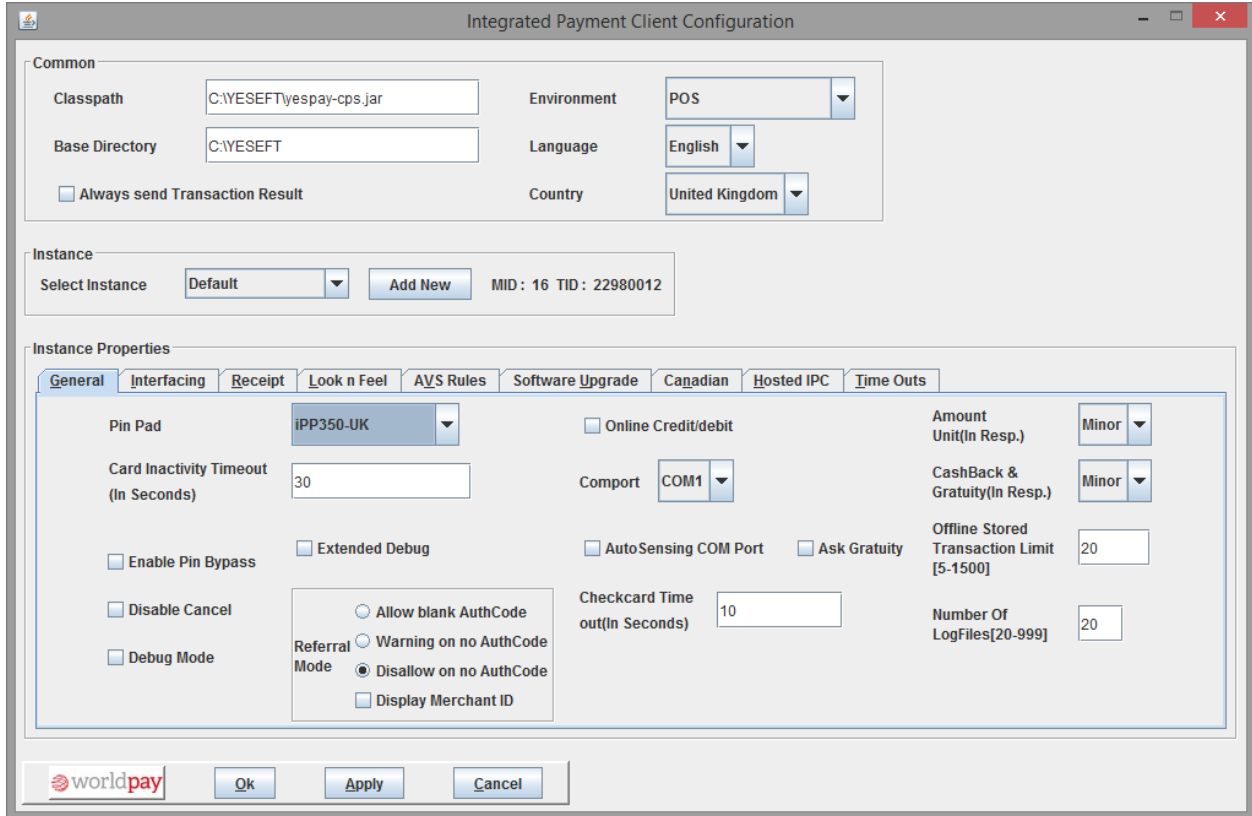


Figure 10: YESEFTConfig-Common

- **Classpath** :This configuration parameter indicates the fully qualified name of the “yespay-cps.jar” to be used by YESEFT and it must not be changed.
- **Base Directory** : The base directory should point to installation directory e.g. “C:\YESEFT”
- **Environment**: In this drop down list select appropriate environment as per the requirement.

If **POS (Retail)** is selected then IPC supports all type of transactions including Sale, Refund, CNP, PWCB and Pre-Auth, Pre Sales Completion, Cancel.

Semi-Attended environment allows only Sale transaction with Chip & Pin card.

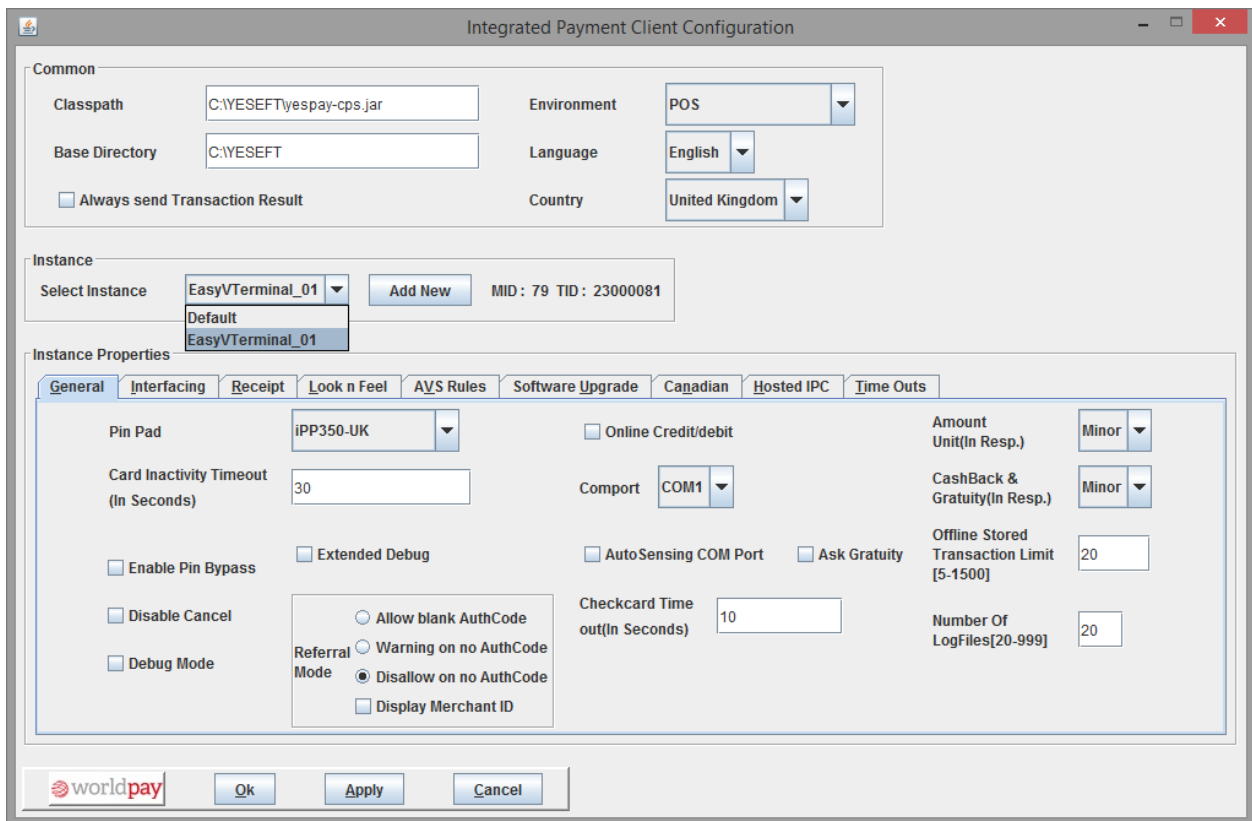
Note:-

* Petrol Station, Kiosk, Internet, Hospitality-Standalone, Hospitality and Standalone are not supported with this IPC version.

- **Always send transaction result:** If the always send transaction result option is enabled then IPC will always send transaction result field in the response to the EPOS application. It is recommended that this option is enabled.
- **Language:** This drop down can be used to select the preferred language for IPC. English and French language is supported currently.
- **Country:** This drop down can be used to configure IPC corresponding to the country or region. United Kingdom , Republic of Ireland , France and United States are supported with this IPC version.

4.3.2 Instance

Selects the instance for which the properties are set. This is useful only when configuring multiple instances of IPC. Generally in a POS environment only one instance is required and it is sufficient to keep the configuration on the default instance.



The screenshot shows the 'Integrated Payment Client Configuration' window. The 'Common' tab is active, showing fields for Classpath (C:\YESEFT\yespay-cps.jar), Base Directory (C:\YESEFT), Environment (POS), Language (English), and Country (United Kingdom). The 'Always send Transaction Result' checkbox is checked. The 'Instance' section shows a dropdown for 'Select Instance' with options 'EasyVTerminal_01', 'Default', and 'EasyVTerminal_01'. The 'Add New' button is visible. The 'Instance Properties' section is expanded, showing the 'General' tab. It includes fields for Pin Pad (iPP350-UK), Card Inactivity Timeout (30), Comport (COM1), Amount Unit (Minor), CashBack & Gratuity (Minor), Offline Stored Transaction Limit (20), and Number Of LogFiles (20). There are also checkboxes for 'Enable Pin Bypass', 'Disable Cancel', 'Debug Mode', 'Extended Debug', 'AutoSensing COM Port', 'Ask Gratuity', 'Checkcard Time out (10)', and 'Display Merchant ID'. The 'Referral Mode' section has radio buttons for 'Allow blank AuthCode', 'Warning on no AuthCode', and 'Disallow on no AuthCode' (selected).

Figure 11: YESEFTConfig-Instance

Select Instance

The instance to be used with IPC can be selected from the drop down list. A new instance can be created with “Add New” button.

For the default instance IPC uses the required property files from the properties folder. For other Instances it uses the properties folder in INSTANCE_XX folder residing in the directory specified here.

If multiple instances are configured, run the Emboss-setup.bat file as well to enter merchant ID and terminal IDs for each instance.

4.3.3 Instance Properties

General

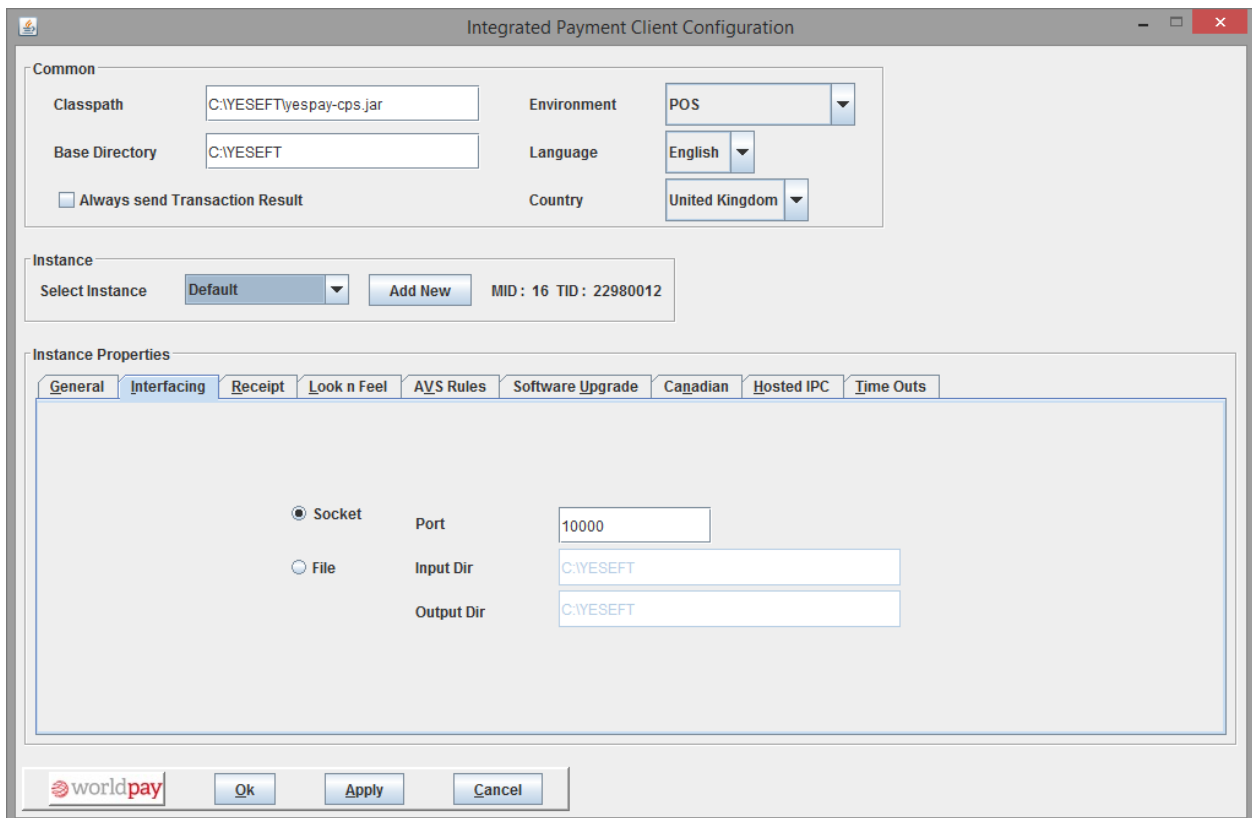
This tab provides general features of IPC.

- **Pin Pad:** This option is used to configure the pinpad to be used with IPC. If No pinpad is available then select No Card Reader from the drop down list.
- **COM Port:** Select the com port through which pinpad is connected to PC. (For IP pinpads this option will not be visible)
- **Card Inactivity Timed out:** The value in this field indicates the time in seconds after which the transaction itself gets timed out if no card is inserted to the pinpad.
- **Ask Gratuity:** This option adds a facility to prompt the cardholder for Gratuity at the time of payment.
- **Enable Pin Bypass:** If this checkbox is enabled then IPC provides an option on IPC window (GUI) to Bypass Pin for ICC transactions. If PIN is bypassed then successive card holder verification depends on the card
- **Check card Timeout:** This parameter denotes the timeout within which a transaction is cancelled after check card if no sale, pre authorisation, refund or cancel is received within that time. By default value is 10 seconds and can be set up to 30 seconds.
- **Disable Cancel:** If this checkbox is enable then the Cancel option should appear as disabled on IPC window (GUI) at the time of PIN prompt and initial card insertion state (**At present this feature is not supported**).
- **Debug Mode:** In debug mode, TVR, TSI and CVMR are printed on the receipt.
- **Extended Debug Mode:** In this mode, additional information is printed on the receipt. Examples are 9F26, 82, 9F27, 9A, 9F1A, 9F10, 9C, 9F37, 9F02, 9F03, 9F36, 5F2A, IAC ONLINE, IAC DENIAL, IAC DEFAULT, TAC ONLINE, TAC DENIAL, TAC DEFAULT.
- **Referral Mode:** This option is applicable when the transaction is seeking for manual (voice) authorisation. Any option of the following can be selected as per the requirement:
- **Allow blank Auth Code:** Provides a facility to accept a transaction without entering authorisation code.
- **Warning on no Auth Code:** Causes a warning message to pop up if no authorisation code is entered.
- **Disallow on no Auth code:** IPC does not accept any transaction without authorisation code.
- **Display Merchant ID:** Enables display of the merchant ID in the referral window. By default merchant ID display is disabled.
- **Auto Sensing COM port:** In the event that IPC is not able to detect the PED on the configured COM port, this options allows IPC to attempt to detect the pinpad on any other valid COM port.. If IPC finds a PED on another COM port, it will prompt via the GUI to allow connection via the new COM port, and change the configured com port accordingly.
- **PinPadPort:** **This option applies when an IP pinpad is selected.** This is the tcp socket port for communication between IPC and the pinpad. The Default port is 5000 for the default instance.
- **Amount Unit (In Resp.):** The Transaction amount field return in response by IPC to the EPOS application can be configured as Major (Pound) or Minor (Pence).

- **CashBack & Gratuity (In Resp.):** The CashBack & Gratuity fields returned in response by IPC to the EPOS application can be configured as Major (Pound) or Minor (Pence).
- **Offline Stored Transaction Limit [5-1500]:** This field indicates the number of offline transaction that can be stored in “YESEFTTransactionLog.xml” if Internet connectivity is not available on the IPC machine. It must be between 5 – 1500. The default value is 20. Once the stored transaction limit is reached, IPC will not process any new transaction request and will return busy status in response to the EPOS application .
- **Online Verification Of Credit/Debit:** This option applies to the Checkcard transaction request. If this check-box is enabled then IPC sends a request online to WPH for Credit/Debit card identification. If disabled, IPC will attempt to identify the card as Credit/Debit using its locally held tables, which by necessity, are not as detailed as the tables held at WPH, and hence the identification will be less accurate. If connection is not available to WPH, IPC will default to using its local tables.

4.3.4 Interfacing

This tab provides interfacing related features of IPC.



The screenshot shows the 'Integrated Payment Client Configuration' window with the 'Interfacing' tab selected. The 'Common' section includes fields for Classpath (C:\YESEFT\yespay-cps.jar), Base Directory (C:\YESEFT), Environment (POS), Language (English), and Country (United Kingdom). There is a checkbox for 'Always send Transaction Result'. The 'Instance' section shows 'Select Instance' set to 'Default' and 'Add New' button, with MID: 16 and TID: 22980012. The 'Instance Properties' section has tabs for General, Interfacing (selected), Receipt, Look n Feel, AYS Rules, Software Upgrade, Canadian, Hosted IPC, and Time Outs. Under the Interfacing tab, there are radio buttons for 'Socket' (selected) and 'File'. The 'Port' field is set to 10000. The 'Input Dir' and 'Output Dir' fields are both set to C:\YESEFT. At the bottom, there are 'Ok', 'Apply', and 'Cancel' buttons.

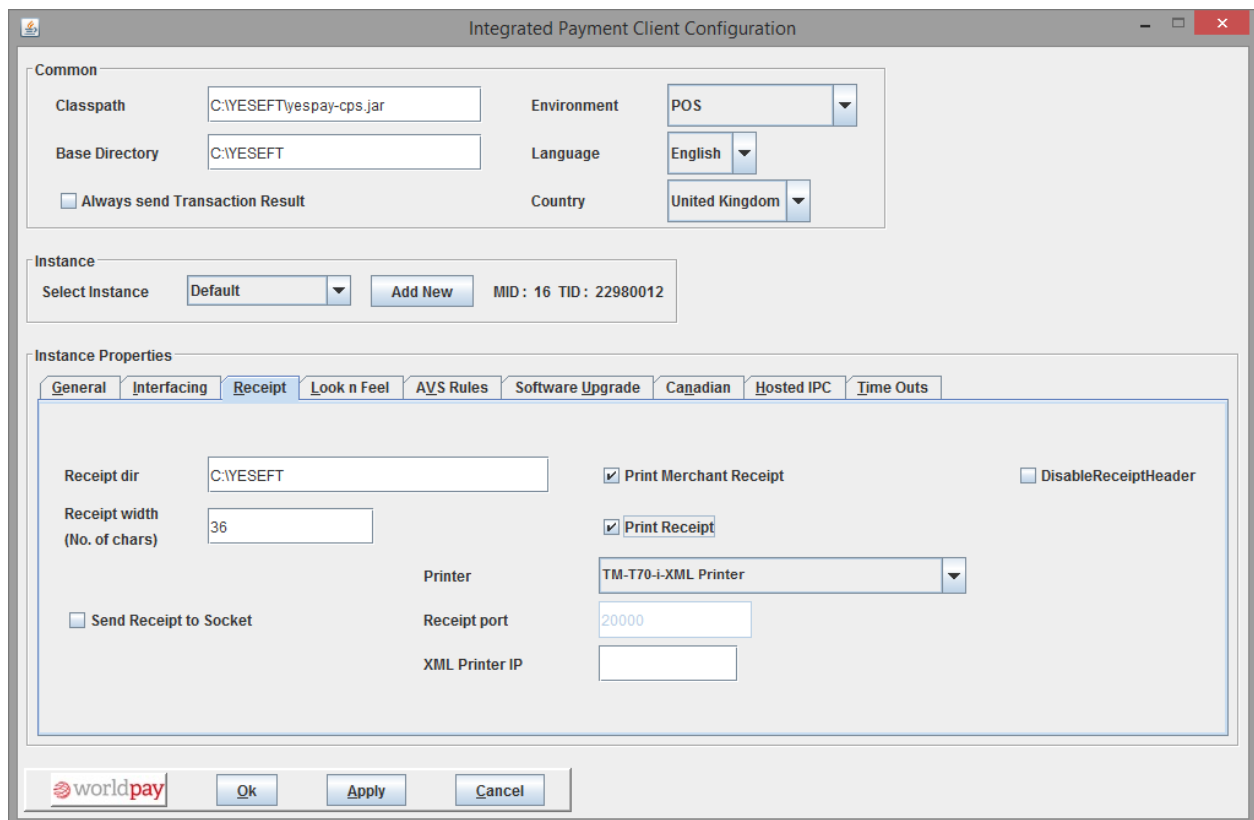
Figure 12: Interfacing

- **Socket:** Select this option if socket connection is going to be used by EPOS application to communicate with the IPC to send transaction request.
- **Port:** If socket is used as an interfacing method then the appropriate tcp port is entered in the Port field. By default it is 10000.

- **File:** Select this option if files are going to be used by EPOS application to communicate with IPC to send transaction request
- **Input Dir:** The file for communication of the input transaction request is named Input.txt. This field should contain the absolute location of Input.txt file
- **Output Dir:** The file for communication of the transaction output transaction response is named Output.txt. This field should contain the absolute location of Ouput.txt file.

4.3.5 Receipt

This tab provides transaction receipt related functionality.



The screenshot shows the 'Integrated Payment Client Configuration' window with the 'Receipt' tab selected. The 'Common' section at the top includes fields for Classpath (C:\YESEFT\yespay-cps.jar), Base Directory (C:\YESEFT), Environment (POS), Language (English), and Country (United Kingdom). Below this is the 'Instance' section with a 'Select Instance' dropdown set to 'Default' and an 'Add New' button. The 'Instance Properties' section has several tabs, with 'Receipt' currently active. This tab contains fields for 'Receipt dir' (C:\YESEFT), 'Receipt width (No. of chars)' (36), and a 'Printer' dropdown set to 'TM-T70-i-XML Printer'. There are also checkboxes for 'Print Merchant Receipt' (checked), 'Print Receipt' (checked), 'DisableReceiptHeader' (unchecked), and 'Send Receipt to Socket' (unchecked). The 'Receipt port' is set to 20000, and the 'XML Printer IP' field is empty. At the bottom of the window are 'Ok', 'Apply', and 'Cancel' buttons.

Figure 13: Receipt

- **Receipt Dir:** The transaction receipts generated by IPC are stored in this directory. By default the location is the absolute location of the YESEFT directory e.g. C:\YESEFT.
- **Print Receipt:** Enable this option to allow IPC to print receipts. Once the option is enabled IPC shows the pinpad printer check box (if applicable) or all the printers installed on machine in Printer drop down list. In Linux IPC supports only the pinpad printer and TM-T70-i-XML printer.
- **Receipt Width:** Maximum width in number of characters in each line for generated receipt. Ideal width is 36 - 40. If pinpad printer is selected for receipt printing then IPC used a default width of 42 characters, and this is not configurable by this option.
- **Send Receipt to Socket:** If this is selected the receipts are sent to the specified tcp port.

- **Receipt Port:** If “Send Receipt to Socket” is selected, then the receipts are sent to the configured port. By default the receipt port is set to 20000.
- **Printer:** IPC shows all the printer installed on the machine in the drop down list. Select a printer from the drop down list if receipt printing is handled by IPC. Drop down list is enabled only if Print Receipt option is enabled.
- **Print Merchant Receipt:** If this option is enabled then IPC will always issue the merchant receipt. However, if this is disabled then IPC will not issue the merchant receipt except where card holder signature verification is required e.g. mag. swipe cards, Chip&Signature cards.

This Option is not applicable for Semi-Attended and Kiosk environments as the Merchant receipt is not issued in these environments .

- **XML Printer IP:** Enter IP-address of XML printer If “**TM-T70-i XML printer**” is selected in printer list.
- **Disable Receipt Header:** Provide an option to remove merchant name and address information from the receipt. By default IPC includes merchant name and address information in receipt.

4.3.6 Look n Feel

This option provides facility to change the look and feel of IPC.

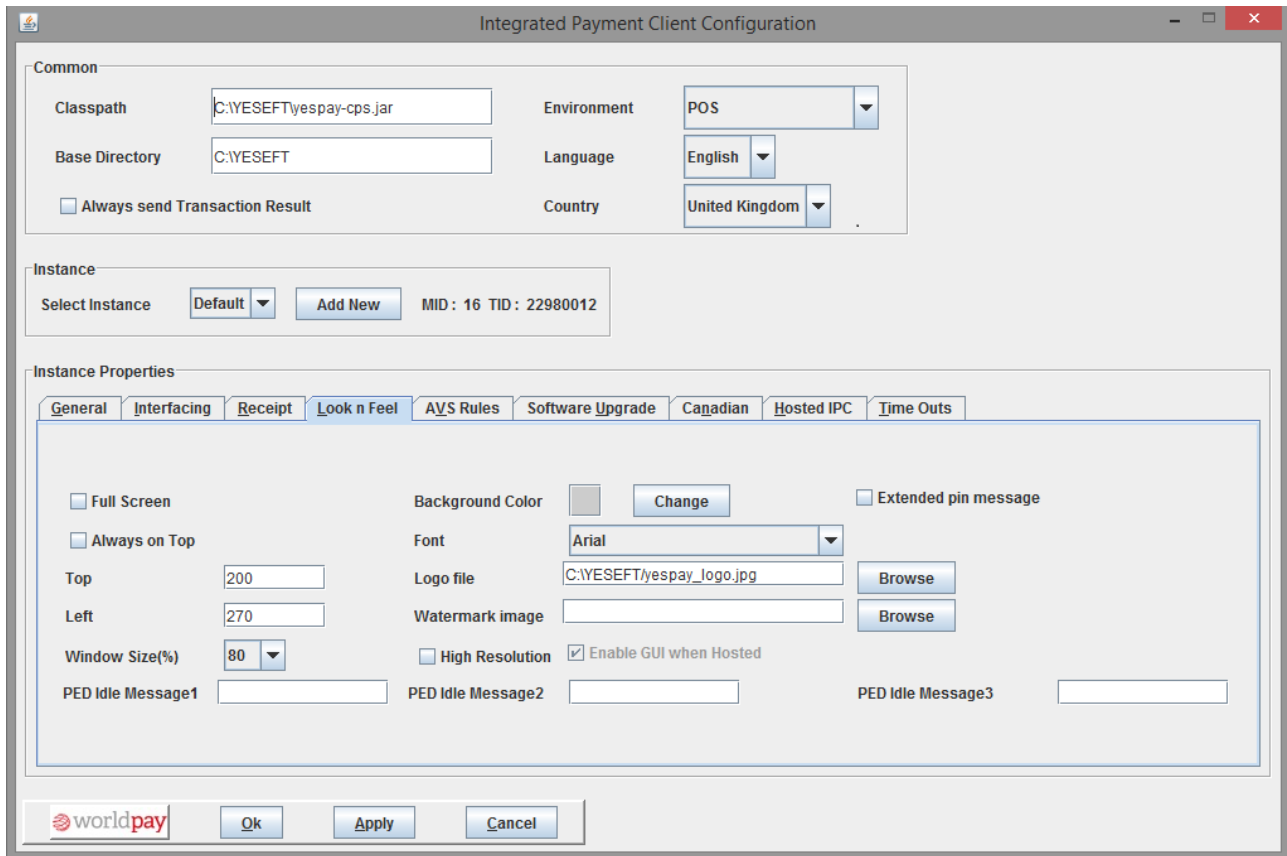


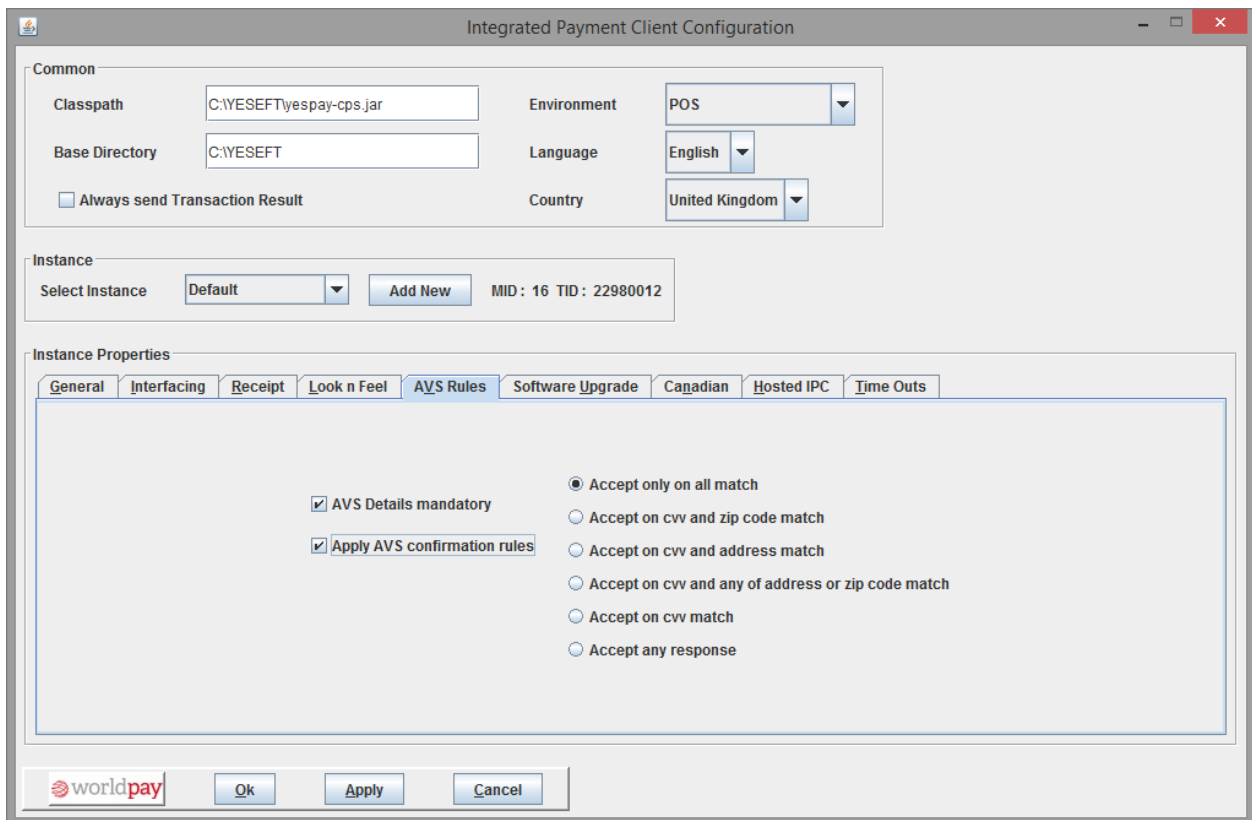
Figure 14: Look n Feel

- **Full Screen:** If this checkbox is enabled, the IPC window opens in full screen.
- **Always on Top:** IPC application always appear on top if this checkbox is enabled. If any other application is also using the same property then native APIs of OS decide which application will be displayed on top.
- **Top:** If specified, top of IPC window will be positioned at this coordinate.
- **Left:** If specified, left of IPC window will be positioned at this coordinate.
- **Background Color:** Using this option, the user can select the background colour of the IPC window. Color of fonts and user message fields will remain unchanged.
- **Font:** Using this option, the user can select the font style for the IPC window. Font setting will reflect on buttons and information displayed on user message field.
- **Logo file:** This is the fully qualified name of the logo file that appears on the top right of the IPC window.

- **Watermark Image:** Using this option, the user can select the watermark image in the IPC window.
- **Extended pin Message:** If this option is selected then additional message will appear at the time of entering pin as ENTER PIN THEN PRESS ENTER.
- **Windows Size:** This helps to resize IPC window. **This option is no longer supported.**
- **Enable GUI when Hosted:** Display of IPC window (GUI) can be configured by this option. Default value of this flag is true and it is greyed out. If **Is Hosted IPC** is selected true in Hosted IPC section then value of **Enable GUI when Hosted** will be changed to false and will be allowed to change.
- **High Resolution:** IPC GUI can be configured for a high resolution (1920 x 1086) screen.
- **PED Idle Message1 :** Using this option a custom message can be displayed on PED's available 1st line when IPC is in Idle mode. Max 16 characters can be displayed.
- **PED Idle Message2 :** Using this option a custom message can be displayed on PED's available 2nd line when IPC is in Idle mode. Max 16 characters can be displayed.
- **PED Idle Message3 :** Using this option a custom message can be displayed on PED's available 3rd line when IPC is in Idle mode. Max 16 characters can be displayed.

4.3.7 AVS Rules

This tab is applicable only for CNP (customer not present) transaction.



The screenshot shows the 'Integrated Payment Client Configuration' window. The 'Common' section includes fields for Classpath (C:\YESEFT\yespay-cps.jar), Base Directory (C:\YESEFT), Environment (POS), Language (English), and Country (United Kingdom). The 'Instance' section shows 'Select Instance' set to 'Default' and 'Add New' button, with MID: 16 and TID: 22980012. The 'Instance Properties' section has tabs for General, Interfacing, Receipt, Look n Feel, AVS Rules (selected), Software Upgrade, Canadian, Hosted IPC, and Time Outs. The AVS Rules tab contains two checkboxes: 'AVS Details mandatory' and 'Apply AVS confirmation rules', both checked. To the right, there are radio buttons for AVS rules: 'Accept only on all match' (selected), 'Accept on cvv and zip code match', 'Accept on cvv and address match', 'Accept on cvv and any of address or zip code match', 'Accept on cvv match', and 'Accept any response'. The bottom of the window has the Worldpay logo and buttons for 'Ok', 'Apply', and 'Cancel'.

Figure 15: AVS Rules

- **AVS Details Mandatory:** If this checkbox is enabled then it is compulsory to provide AVS details (CVV, Address and Postcode) in a CNP transaction.
- **AVS Details Mandatory & Apply AVS Confirmation Rules:** If both checkbox are enabled then IPC will enable AVS fields according to the selected confirmation rule. It is compulsory to provide values in AVS fields. Select confirmation rule among the following:
 - **Accept only or all match:** This option ensures that IPC accepts the CNP transaction only if all of the AVS details are matched.
 - **Accepts on CVV and Zip code Matched:** IPC accepts the CNP transaction only if CVV and Zipcode/Postcode are both matched.
 - **Accept on CVV and Address Match:** This option ensures that IPC accepts a CNP transaction only when CVV and Address are both matched.
 - **Accept on CVV and any of the address or Zip code Match:** If this is selected then a CNP transaction can be accepted upon CVV and either of address or Zipcode/Postcode match.
 - **Accept on CVV match:** If this is selected then a CNP transaction can be accepted upon CVV match.
 - **Accept any Response:** If this option is selected then a CNP transaction can be accepted on any response.
- **Apply AVS Confirmation Rules:** If only this checkbox is selected then IPC will enable AVS fields according to the selected confirmation rule. It is not compulsory to provide values in the AVS fields. But if values are entered in any enabled AVS fields then IPC will process transaction if it conforms to the selected rule, otherwise IPC will prompt to Accept/Reject the transaction based on the AVS matching. Select confirmation rules from the following:
 - **Accept only or all match:** This option ensures that IPC accepts CNP transaction only if all of the AVS details are matched.
 - **Accepts on CVV and Zip code Matched:** If CVV and Zipcode/Postcode are matched then only IPC accepts the CNP transaction.
 - **Accept on CVV and Address Match:** This option ensures that IPC accepts CNP transaction only when CVV and Address gets matched.
 - **Accept on CVV and any of the address or Zip code Match:** If this is selected then a CNP transaction can be accepted upon CVV and either of address or Zipcode/Postcode match.
 - **Accept on CVV match:** If this is selected then a CNP transaction can be accepted upon CVV match.
 - **Accept any Response:** If this option is selected then a CNP transaction can be accepted on any response.

4.3.8 Software Upgrade

This tab provides IPC software related upgrades functionality.

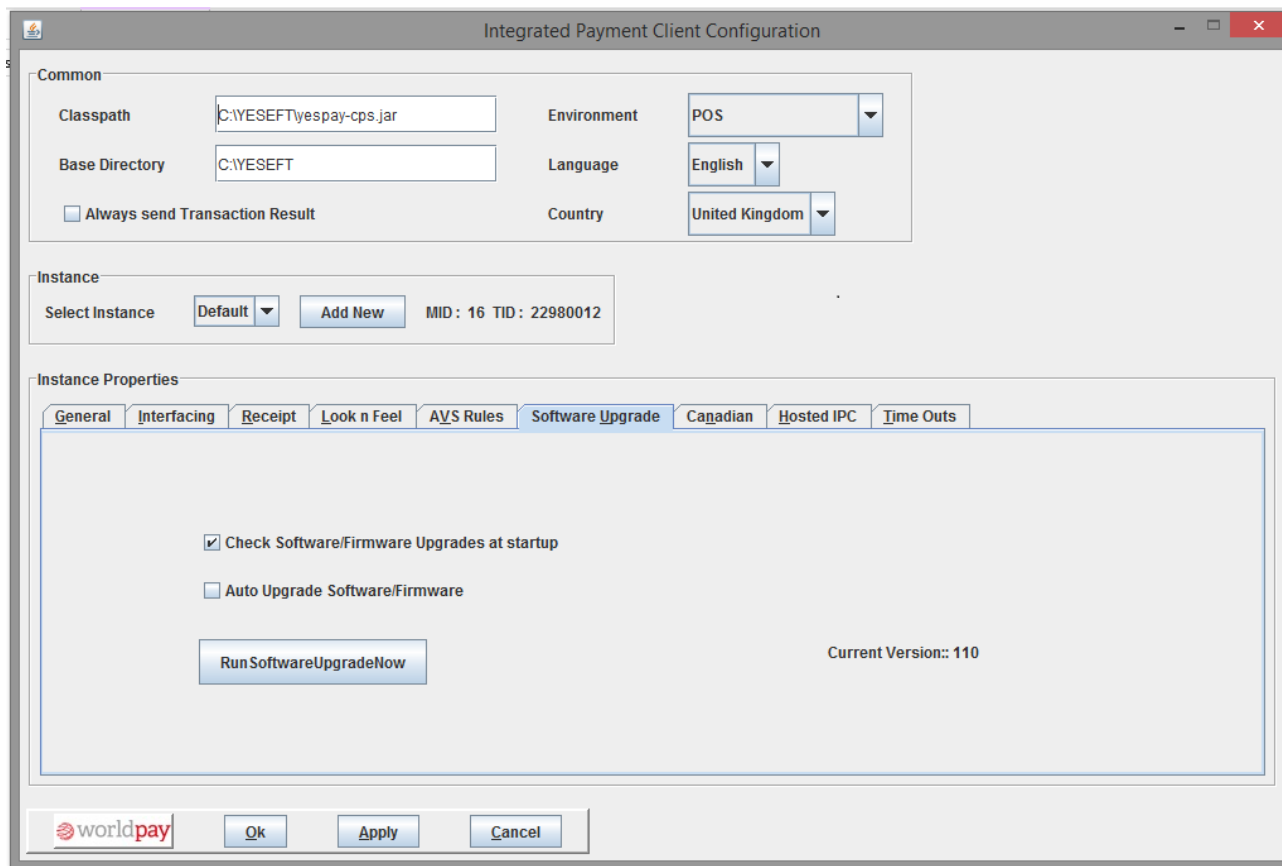
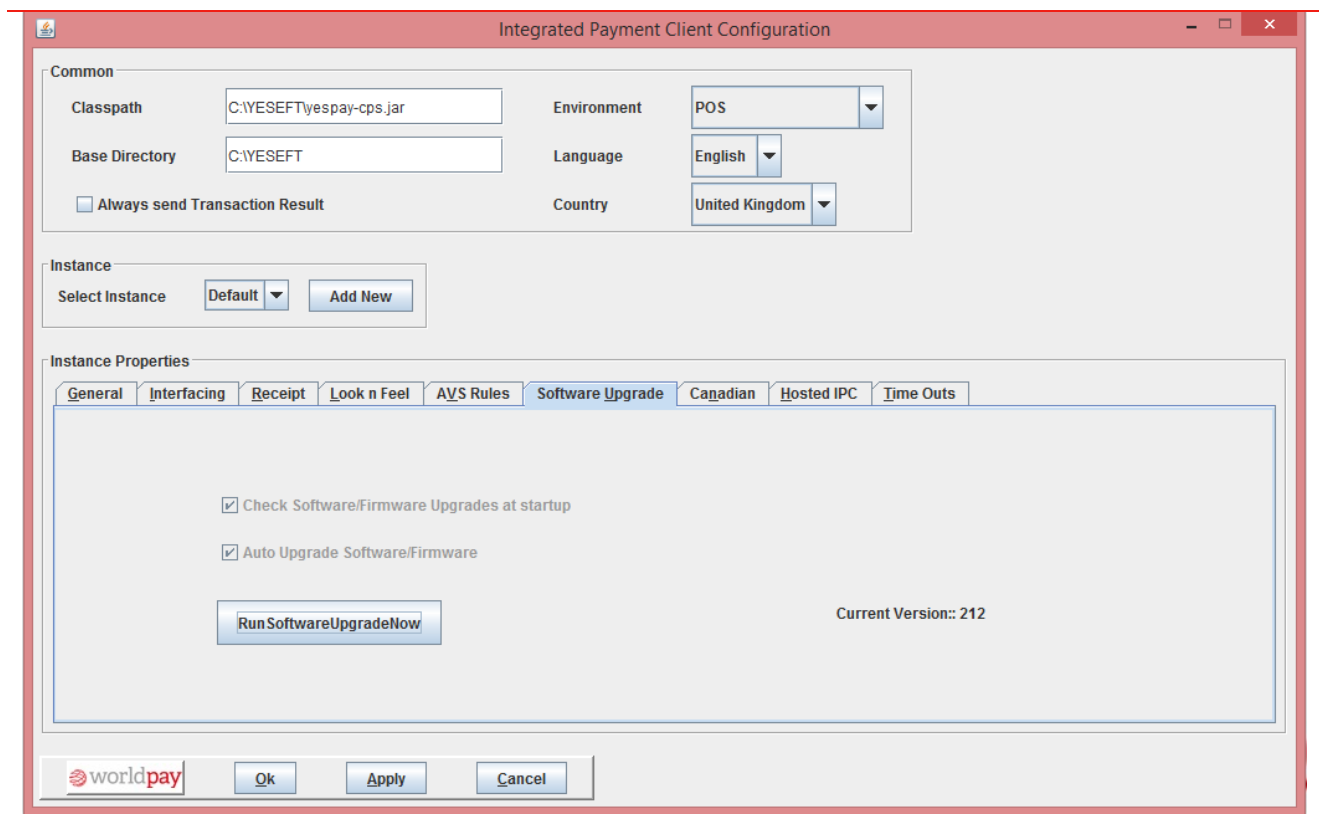


Figure 16.1: Software/Firmware Upgrade



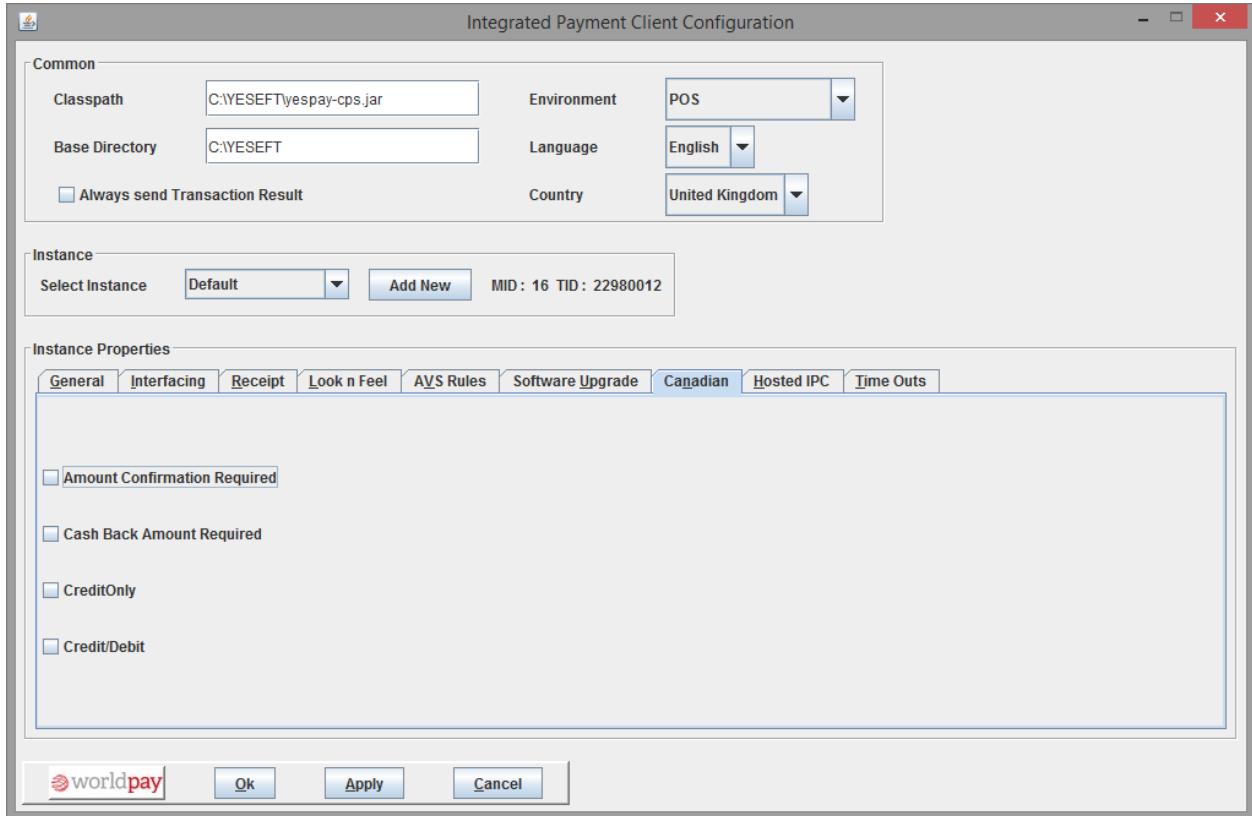
The screenshot shows the 'Integrated Payment Client Configuration' window. The 'Common' section includes fields for 'Classpath' (C:\YESEFT\yespay-cps.jar), 'Base Directory' (C:\YESEFT), 'Environment' (POS), 'Language' (English), and 'Country' (United Kingdom). There is a checkbox for 'Always send Transaction Result'. The 'Instance' section has a 'Select Instance' dropdown set to 'Default' and an 'Add New' button. The 'Instance Properties' section has tabs for 'General', 'Interfacing', 'Receipt', 'Look n Feel', 'AVS Rules', 'Software Upgrade' (selected), 'Canadian', 'Hosted IPC', and 'Time Outs'. The 'Software Upgrade' tab contains two checked options: 'Check Software/Firmware Upgrades at startup' and 'Auto Upgrade Software/Firmware'. There is a 'RunSoftwareUpgradeNow' button and a label 'Current Version:: 212'. At the bottom are 'Ok', 'Apply', and 'Cancel' buttons.

17.2 Software/Firmware Upgrade Options For P2PE

- **Check Software/Firmware Upgrades at start-up:** If this option is enabled then IPC looks for updates at start-up. By default the value of this flag is true. If a software update for IPC and or a firmware update for POI device is available a popup box will be prompted by IPC for the confirmation of new updates to be installed.
- **Auto Upgrade Software/Firmware:** If this option is enabled then at startup-up, IPC automatically downloads the updates from WPH and upgrades. There will be no pop-up to confirm installation of the updates.
- **RunSoftwareUpgradeNow:** This button can be used to upgrade the version of IPC manually, if any is available on the WPH server.
- **Current Version:** This shows the current version of IPC installed.

4.3.9 Canadian

This tab provides IPC US and Canadian related functionality.



The screenshot shows the 'Integrated Payment Client Configuration' window. The 'Common' section includes fields for Classpath (C:\YESEFT\yespay-cps.jar), Base Directory (C:\YESEFT), Environment (POS), Language (English), and Country (United Kingdom). There is a checkbox for 'Always send Transaction Result'. The 'Instance' section shows 'Select Instance' set to 'Default' and 'Add New' button, with MID: 16 and TID: 22980012. The 'Instance Properties' section has tabs for General, Interfacing, Receipt, Look n Feel, AVS Rules, Software Upgrade, Canadian, Hosted IPC, and Time Outs. The 'Canadian' tab is active, showing four checkboxes: 'Amount Confirmation Required', 'Cash Back Amount Required', 'CreditOnly', and 'Credit/Debit'. The bottom of the window has the Worldpay logo and 'Ok', 'Apply', and 'Cancel' buttons.

Figure 17: Canadian

- **Amount Confirmation Required:** If this option is enabled then IPC asks for a confirmation of the amount on the pinpad. The default value of this flag is false.
- **Cash Back Amount Required:** It is used only in the US.. If this option is enabled then IPC prompts for the cash back amount on the pinpad during the transaction.
- **Credit Only:** It is only used in Canada. If this option is enabled then only credit card transactions are supported.
- **Credit/Debit:** It is used only in the US. If this option is enabled then IPC will prompt the cardholder to choose to process the transaction as Credit or Debit if the card support both options.

4.3.10 Hosted IPC

This tab provides option to configure IPC in Hosted Mode.

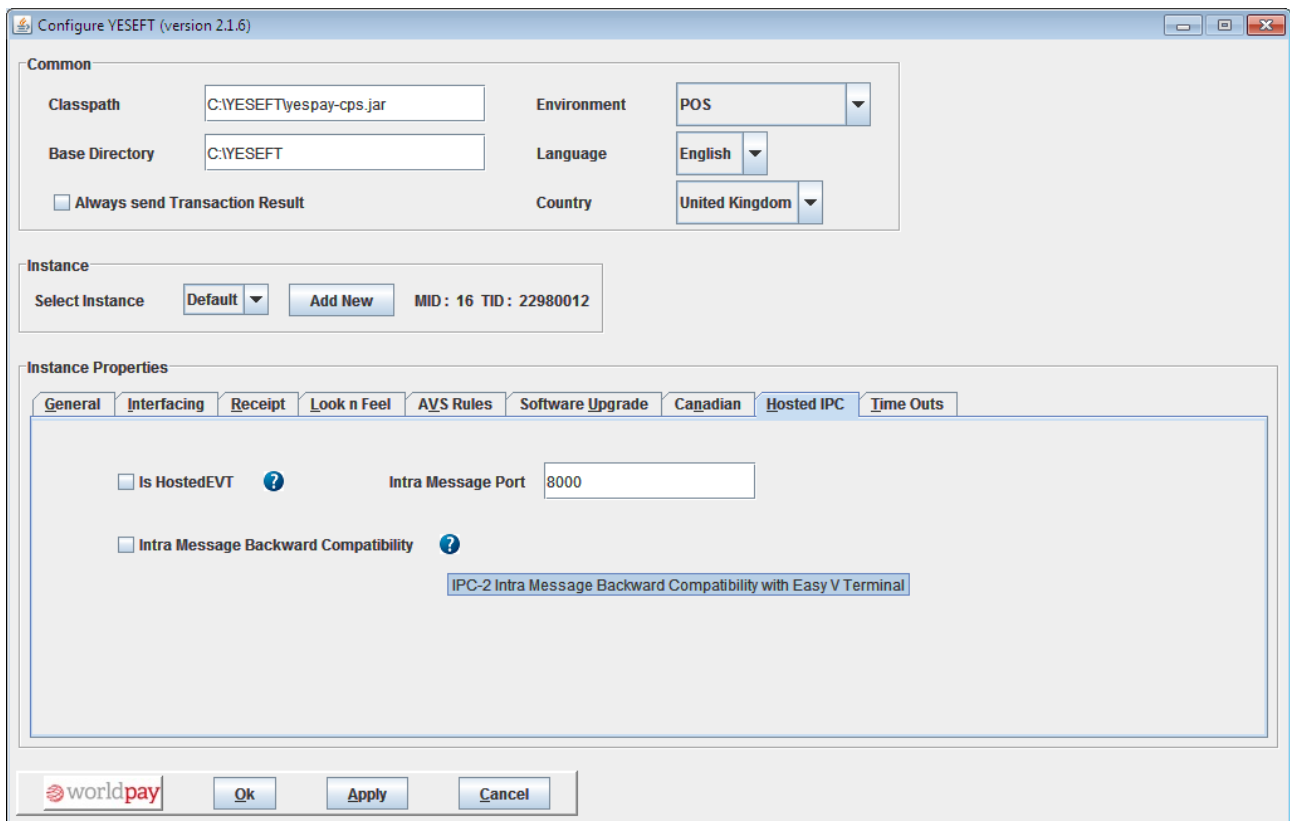
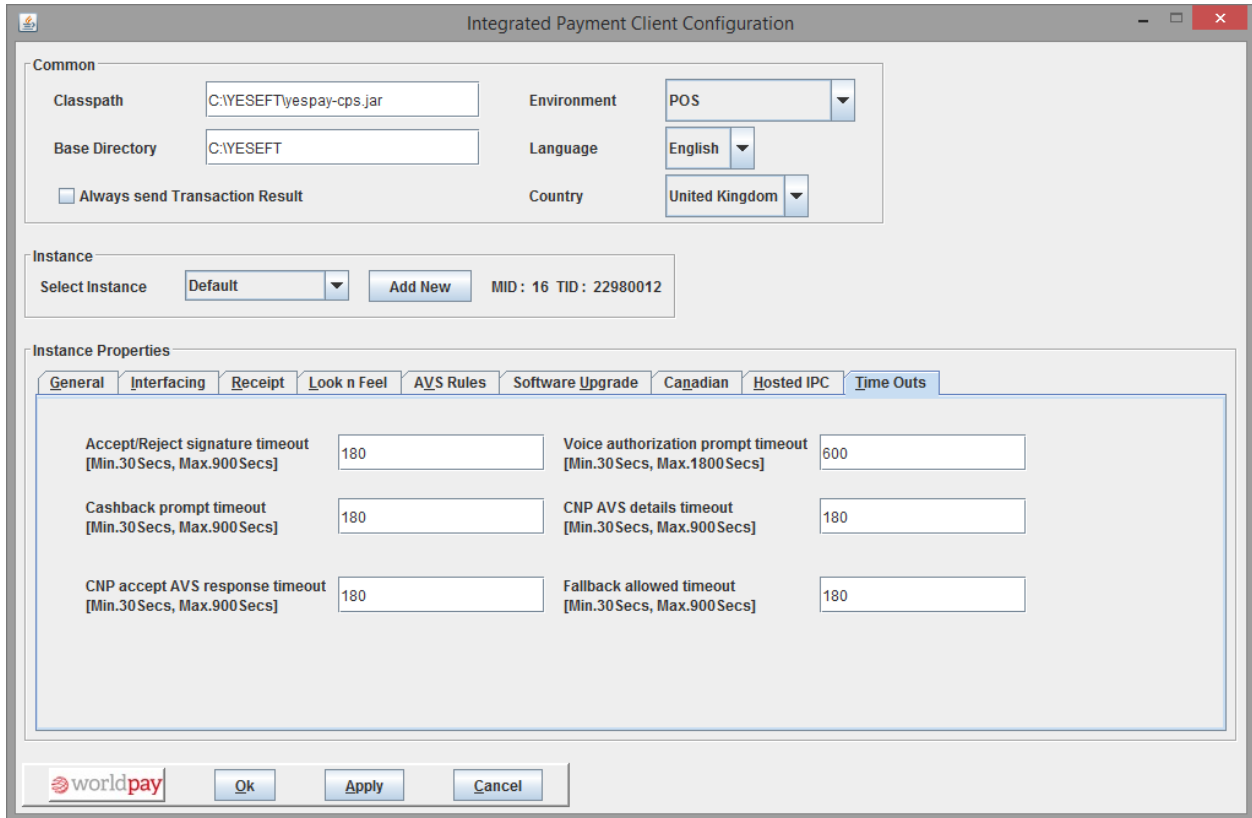


Figure 18: Hosted IPC

- **Is Hosted IPC:** This option must be enabled to use either iIPC or IntraMessage functionality. If this option is enabled then all the IPC window (GUI) messages will be sent on the IntraMessage port and the IPC GUI will not be displayed. If the merchant wishes to show the IPC GUI as well then it can be configured by enabling **Enable GUI when Hosted** option in Look n Feel tab.
- **Intra Message Port:** All IPC messages will be sent on this port.
- **Intra Message Backward Compatibility:** This option provides backward compatibility on intra messages with STS version of client software EasyVTerminal.

4.3.11 Time Outs

IPC may wait for merchant confirmation/response at different stages of the transaction for different possible reasons. This tab provides the facility to merchant to configure the timeout for each confirmation requested either on GUI or IntraMessage port.



The screenshot shows the 'Integrated Payment Client Configuration' window. The 'Common' tab is active, showing fields for Classpath, Base Directory, Environment, Language, and Country. The 'Instance' section shows a dropdown for 'Select Instance' set to 'Default' and a button for 'Add New'. The 'Instance Properties' section has several tabs, with 'Time Outs' selected. This tab contains six timeout configuration fields:

Timeout Name	Value	Range
Accept/Reject signature timeout	180	[Min.30 Secs, Max.900 Secs]
Voice authorization prompt timeout	600	[Min.30 Secs, Max.1800 Secs]
Cashback prompt timeout	180	[Min.30 Secs, Max.900 Secs]
CNP AVS details timeout	180	[Min.30 Secs, Max.900 Secs]
CNP accept AVS response timeout	180	[Min.30 Secs, Max.900 Secs]
Fallback allowed timeout	180	[Min.30 Secs, Max.900 Secs]

At the bottom of the window are buttons for 'Ok', 'Apply', and 'Cancel'.

Figure 20: Time Outs

- **Accept/Reject signature timeout:** This timeout allows the merchant to configure the time IPC will wait at the signature verification prompt. If no action is performed either via the GUI or through the IntraMessage port within the configured timeout period then transaction will be rejected.

The default value for this timeout is 180 secs and it can be configured between 30 secs to 900 secs.

- **Voice authorization prompt timeout:** This timeout allows the merchant to configure the time IPC will wait at the Voice authorisation prompt. If no action is performed either via the GUI or through the IntraMessage port then the transaction will be cancelled.

If an invalid authorisation code i.e. one containing special characters, is entered then IPC will prompt/send error message and prompt to enter a valid authorisation code 2 more times. If a valid authorisation code is not entered then the transaction will be cancelled.

The default value for this timeout is 600 secs and it can be configured between 30 secs to 1800 secs.

- **Cashback prompt timeout:** This timeout allows the merchant to configure the time IPC will wait at the Cashback prompt. If no action is performed either via the GUI or through the IntraMessage port then the transaction will be processed with the original amount.

If an invalid amount, i.e. containing special characters or greater than the allowed cashback limit, is entered, then IPC will prompt/send error message and prompt to enter a valid amount 2 more times. If a valid amount is not entered then the transaction will be processed with the original amount.

The default value for this timeout is 180 secs and can be configured between 30 secs to 900 secs.

- **CNP AVS details timeout:** This timeout allows the merchant to configure the time IPC will wait at the CNP AVS details prompt. IPC will prompt/send the request based on the AVS configuration in the AVS configuration tab. If no action is performed either via the GUI or through the IntraMessage port then the transaction will be cancelled.

if invalid detail, i.e. containing special characters, is entered, then IPC will prompt/send error message and prompt to enter valid detail 2 more times. If valid detail is not entered then the transaction will be cancelled.

The default value for this timeout is 180 secs and can be configure between 30 secs to 900 secs.

- **CNP accept AVS response timeout:** This timeout allows the merchant to configure the time IPC will wait at the AVS details confirmation prompt. If no action is performed either via the GUI or through the IntraMessage port then the transaction will be rejected.

The default value for this timeout is 180 secs and it can be configured between 30 secs to 900 secs.

- **Fallback allowed timeout:** This timeout allows the merchant to configure the time IPC will wait at the fallback confirmation prompt. If no action is performed either via the GUI or through the IntraMessage port then the transaction will be rejected.

The default value for this timeout is 180 secs and it can be configured between 30 secs to 900 secs.

Note:- For all timeouts configured in the Time Outs section where the prompt is resent following invalid entry, the timeout will be refreshed every time the prompt is sent i.e. If the CNP AVS timeout is configured to 180, and AVS details are requested by IPC, and the merchant responds with an invalid value after 150 secs, then IPC will re-prompt for CNP AVS details and wait a full 180 secs for response.

5 Appendix C – Secure delete Instructions

5.1 For Windows

SDelete can be downloaded from the URL:

<http://technet.microsoft.com/en-in/sysinternals/bb897443.aspx>

Steps to install and use SDelete:

- Download the zip file and extract sdelete.exe file on your computer.
- *SDelete* is a command line utility that takes a number of options. In any given use,

usage: sdelete.exe [-p passes] [-s] [-q] <file or directory> ...

sdelete.exe [-p passes] [-z|-c] [drive letter] ...

- a Remove Read-Only attribute
- c Clean free space
- p passes Specifies number of overwrite passes (default is 1)
- q Don't print errors (Quiet)
- s or -r Recurse subdirectories
- z Zero free space (good for virtual disk optimization)

To specify the file/folder to delete, you have two choices:

- Always type the full path to the file/folder.
- Go to the folder that contains the file/folder you want to delete. Then type file/folder name.

Example

```
C:\Software\SDelete>sdelete.exe -p 1 C:\YESEFT\MainReceipt.txt
```

SDelete is set for 1 pass.

```
C:\MainReceipt.txt...deleted.
```

```
1 files found
```

5.2 For Linux (Ubuntu, CentOS, Suse)

The Shred installation can be checked with following command.

Which shred

if it isn't installed, It can be installed as follows :

```
sudo apt-get install coreutils
```

Command

```
Shred -v -n 25 -u -z Filename
```

Example

Shred -v -n 25 -u -z /home/POS/YESEFT/MainReceipt.txt

Please go to below URL for more detail

<http://prefetch.net/blog/index.php/2006/07/25/shredding-files-on-centos-40/>

6 Appendix D – Activity Logging

IPC relies on the underlying supported OS event logging features to implement PA-DSS requirement 4 (**Log payment application activity**). Failure to implement this requirement will result in the merchant being non-compliant with PCI DSS.

Automated audit trails should be implemented to record any activity on the folder where the encrypted card details are stored.

6.1 Auditing user activity on the system

All user and application activity on the system should be audited to implement the requirements under the PCI DSS requirement 10.

For Windows, Event Logging should be enabled for System, Application and Security. Event Logs should capture –Warning, Errors, Critical audit.

- Click Start, click Control Panel
- Click System and Security (in Win7)
- Click Administrative Tools.
- Double click on Event Viewer.
- In the left pane, click on Windows Logs then right click on Application and select Filter current log or click on Filter current log.

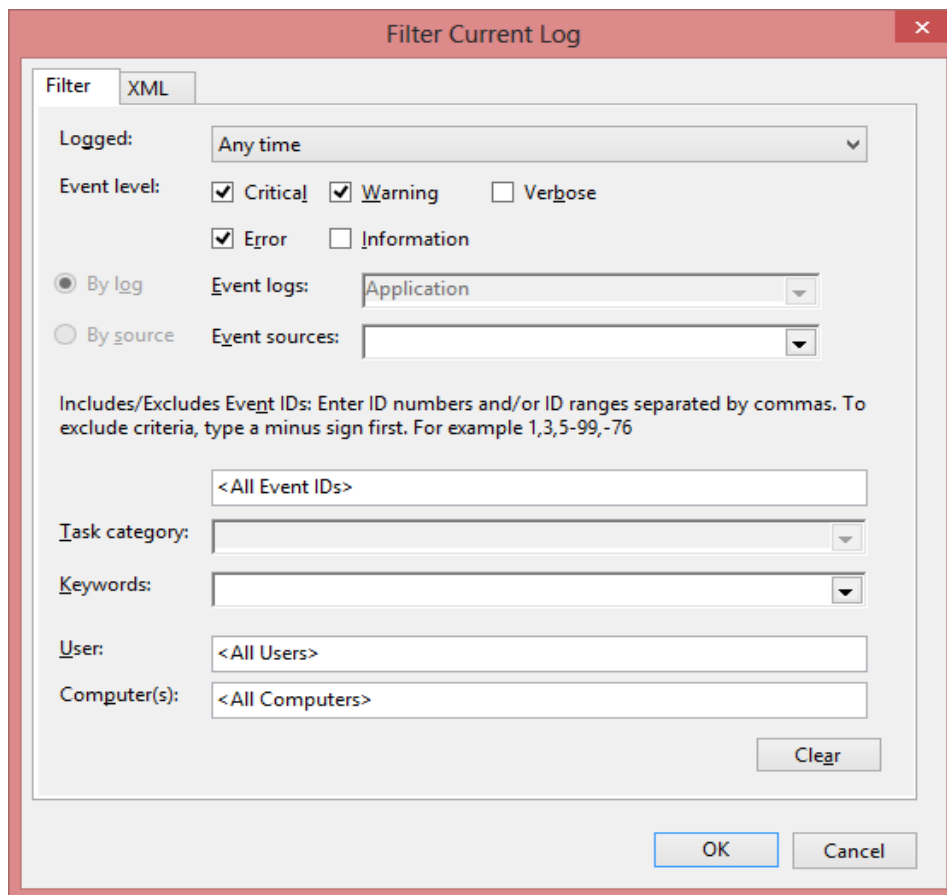


Figure 19

- Enable Warning, Error, and Critical event level in the Filter tab.
- Repeat the same process for Security and System to view event.

For Linux, all the activities of YESEFT/conf and YESEFT/properties can be traced in /var/log/audit/audit.log file.

6.2 Auditing user access to YESEFT/conf and YESEFT/properties folder

The encrypted card data is stored in the folder – YESEFT/conf, hence all access to this folder should be audited automatically. Folder YESEFT/properties contains the Keystore and the truststore file and access to this folder should be audited as well.

For Windows

The audit log appears in the Security log in Event Viewer. First to enable the auditing, audit policy should be defined in the local security settings. Below are the steps to enable this for Windows:

6.2.1 Object Access Policy on Windows

- Open Local Security Policy by clicking the Start button, typing “secpol.msc” into the search box, and then clicking secpol.
- In the left pane, double-click Local Policies, and then click Audit Policy.

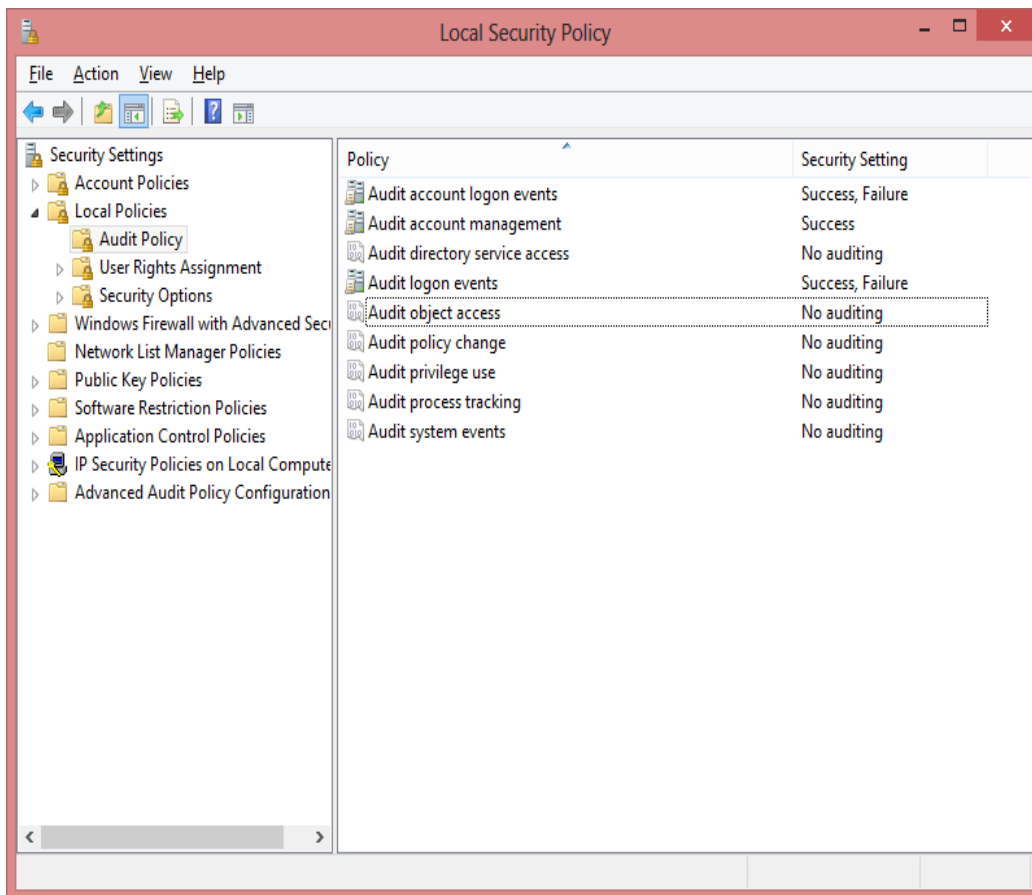


Figure 20

- Right-click on “Object Access Audit” and select Properties
- Ensure “Success” and “Failure” are both checked

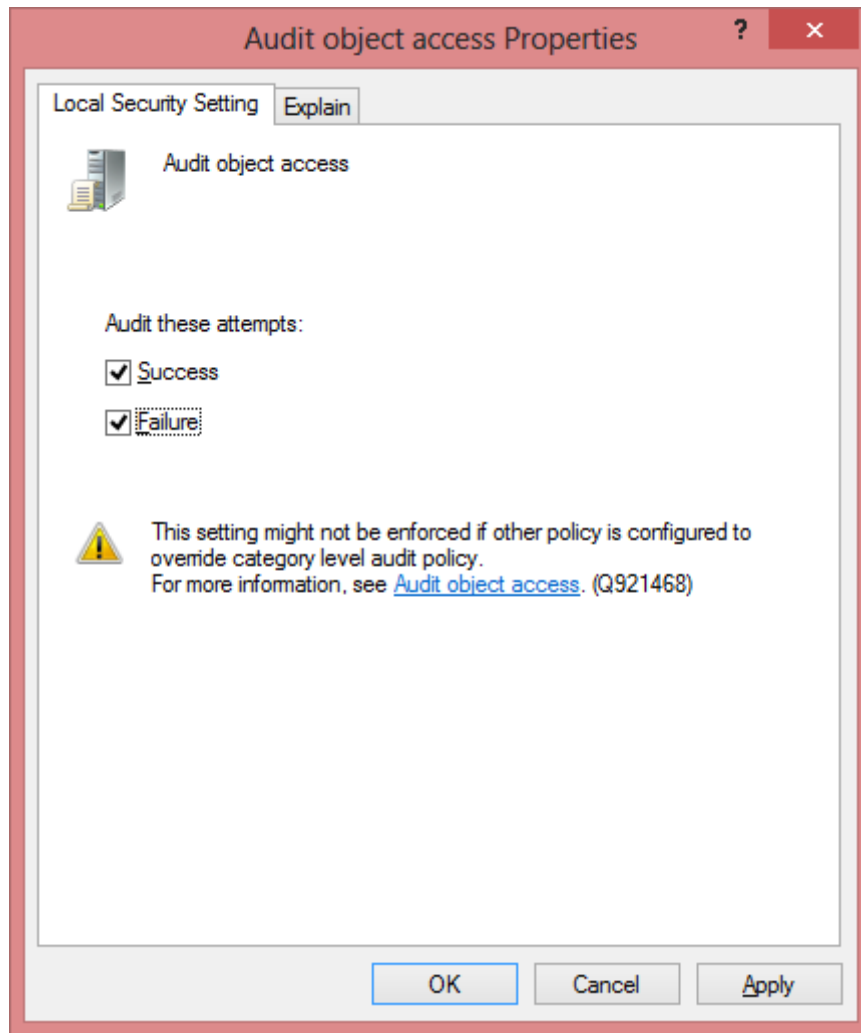


Figure 21

- Click on OK, and then close the Local Security Policy window.

Similarly define policy for the following:

- Audit Account Logon Events
- Audit Account Management
- Audit Logon Events
- Audit Privilege Use

6.2.2 Enabling Audit Trail

After enabling audit, the YESEFT/conf and YESEFT/properties folders should be specified for auditing. Please follow the below steps to enable auditing on the folder:

- Right-click the document or file that you wish to keep track of, and then click Properties.
- Click the Security tab, click Advanced, and then click the Auditing tab.
- Click Add.

- In the box 'Enter the object name to select', type the name of the user or group whose actions you wish to keep track of, and then click OK in each of the four open dialog boxes.

Note: This article assumes that you are using Windows on a domain. You must be logged on as a member of the Administrators group or you must have been granted 'Manage auditing and security log' privilege in Group Policy to perform this procedure.

- The hard disk must be formatted with the NTFS file system for auditing to work.
- If your computer is a member of a domain and the administrator has set domain-level auditing policies, those policies override these local settings.

For Linux

The audit log is /var/log/audit/audit.log.

auditd is the userspace component to the Linux Auditing System. It is responsible for writing audit records to the disk.

- Install auditd by below command

sudo apt-get install auditd

- Edit configuration file by the following command and add the full path of the YESEFT/conf and YESEFT/properties folders. In the example shown in the screenshot below the full path is /home/POS/YESEFT/conf and /home/POS/YESEFT/properties, but this could vary for your installation

sudo vi /etc/audit/audit.rules

```
# First rule - delete all
-D

# increase the buffers to survive stress events. make this bigger for busy
systems.
-b 1024

# monitor unlink() and rmdir() system calls.
-a exit,always -S unlink -S rmdir

# monitor open() system call by Linux UID 1001.
-a exit,always -S open -F loginuid=1001
# monitor write-access and change in file properties (read/write/execute) of the
following files.

#-w /etc/group -p wa
#-w /etc/passwd -p wa
#-w /etc/shadow -p wa
#-w /etc/sudoers -p wa

# monitor read-access of the following directory.
-w /home/POS/YESEFT/conf -p r
-w /home/POS/YESEFT/properties -p r
# lock the audit configuration to prevent any modification of this file.
-e 2
```

- Once you finish editing the audit configuration, restart auditd by below command.

sudo service auditd restart

- Once auditd starts running, it will start generating an audit daemon log in /var/log/audit/audit.log as auditing is in progress. You can trace the log entries relevant for the IPC folder using command below:

sudo grep -n YESEFT /var/log/audit/audit.log.

6.3 Centralized logging mechanism

6.3.1 For Windows

The Windows event log can be sent to centralized log management server using third party SyslogAgent software. This software supports only UDP port connection. Please download the Datagram SyslogAgent for your windows machine (32, 64 bit) from the URL below

<http://www.syslogserver.com/download.html>

Once the zip file is downloaded, extract it, install SyslogAgent and, as administrator, run the Syslog Agent Config tool to configure the Syslog application.

Click on Install under the Service Status section at the top (See below image).

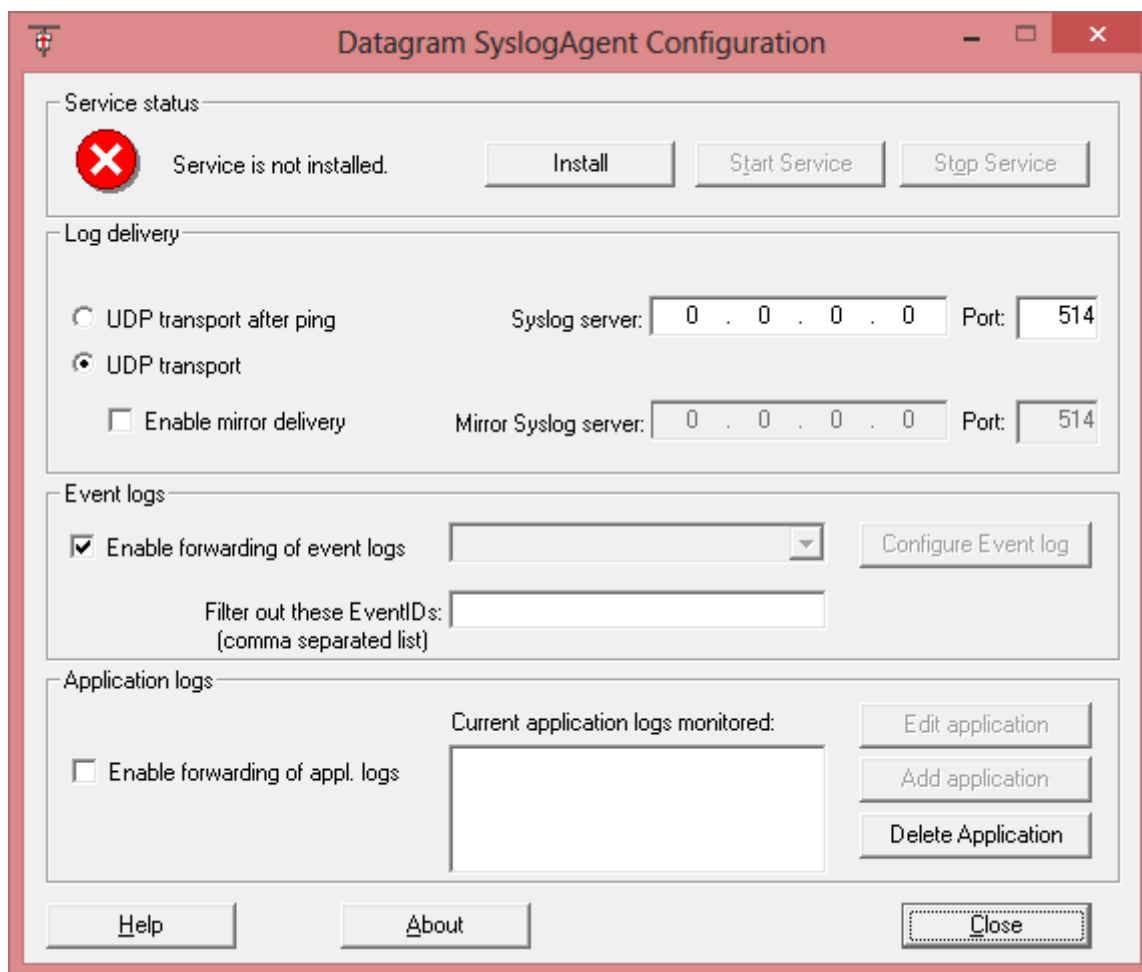


Figure 22: Installing the Syslog Agent Service

This will create the Windows service for the Syslog Agent. The minimum configuration required is:

- Syslog server IP and port
- Enable the “Enable forwarding of event logs” check box and select “Application” type.

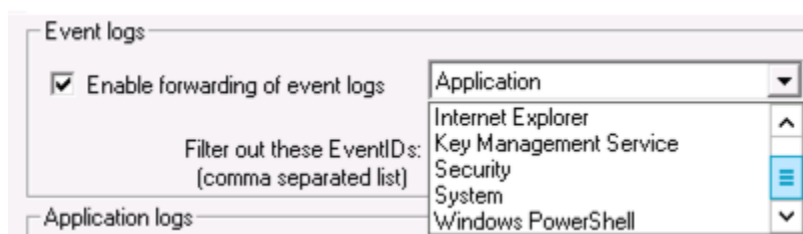


Figure 23: Selecting the Event Logs to Send to the Syslog Host

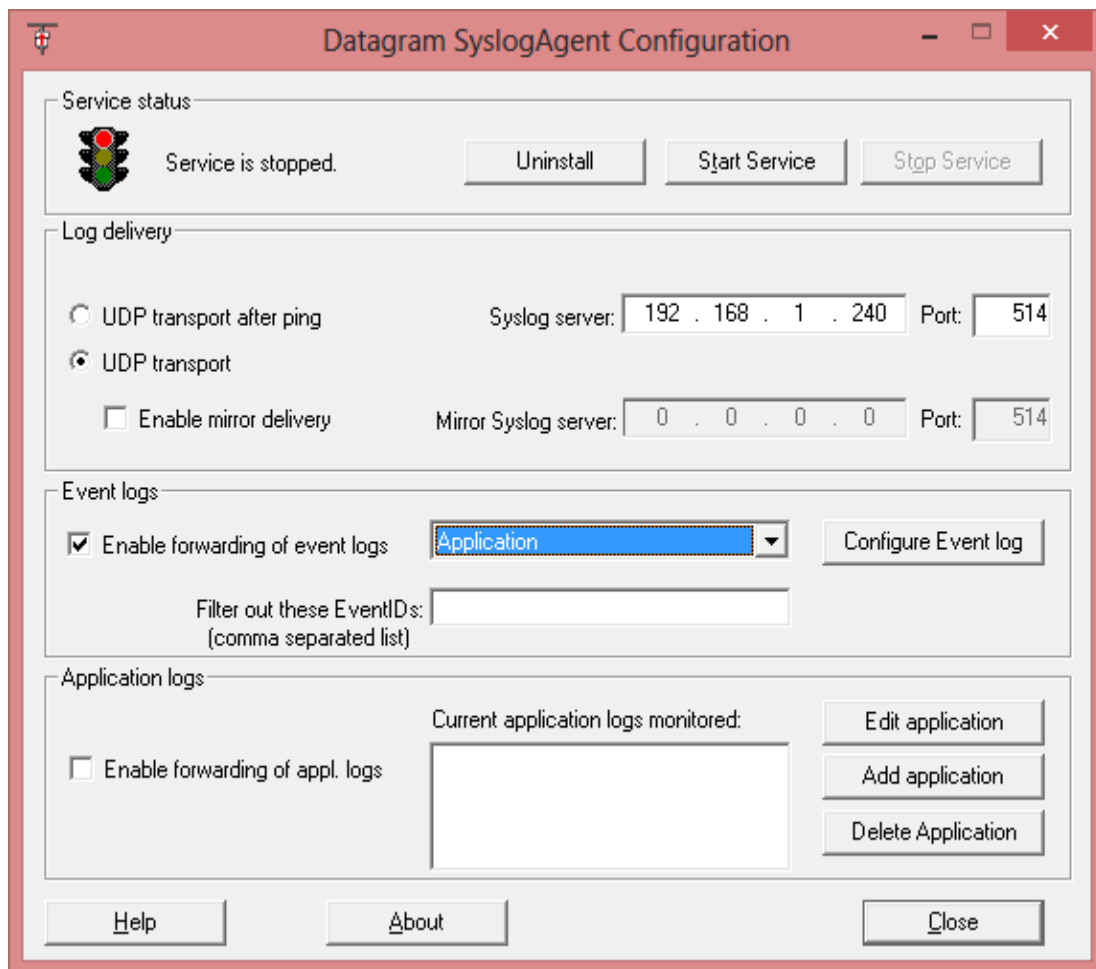


Figure 24: Syslog server IP (e.g. 192.168.1.240) and port (e.g. 514)

Optionally, you can choose to send events from specific Windows applications to the syslog host, even specifying the executable for the custom application (as you see at the bottom of Figure 2). Once configuration is complete, click Start Service.

6.3.2 For Linux

Configure the rsyslog daemon to send IPC logs to the centralized log management server. Configuration changes take effect when rsyslog is restarted.

Please note that there are separate instructions for Ubuntu, Suse and CentOS Linux – see below.

Ubuntu Linux

- **Update rsyslog.conf**

Step 1: Edit rsyslog.conf file, which is generally found in the /etc/ directory, using the command below:

```
sudo vi /etc/rsyslog.conf
```

Step 2: Copy the below Custom YESEFT Log configuration into the rsyslog.conf file (see the screenshot example below)

Note: The IP address/host name of the centralized log server should be used instead of the example address 192.168.77.8 shown below

```
##### Custom YESEFT Log Configuration #####  
$InputFileName /var/log/YESEFT/YESEFT.log  
$InputFileTag yeseft-info:  
$InputFileStateFile stat-info  
$InputFileSeverity info  
$InputFileSeverity local3  
$InputRunFileMonitor  
##### Custom YESEFT Log Configuration End #####
```

Add Server Name And File Path:

```
*.*          /var/log/YESEFT/YESEFT.log  
*.*          @192.168.77.8
```

```

root@yesdesk-95-67: /home/yespay
$umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog

#### Custome YESEFT Log ####
$InputFileName    /var/log/YESEFT/YESEFT.log
$InputFileTag yeseft-info:
$InputFileStateFile stat-info
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor

#
# Where to place spool files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf

*.debug                /var/log/messages
*.*                    /var/log/YESEFT/YESEFT.log
*.*                    @192.168.77.8

```

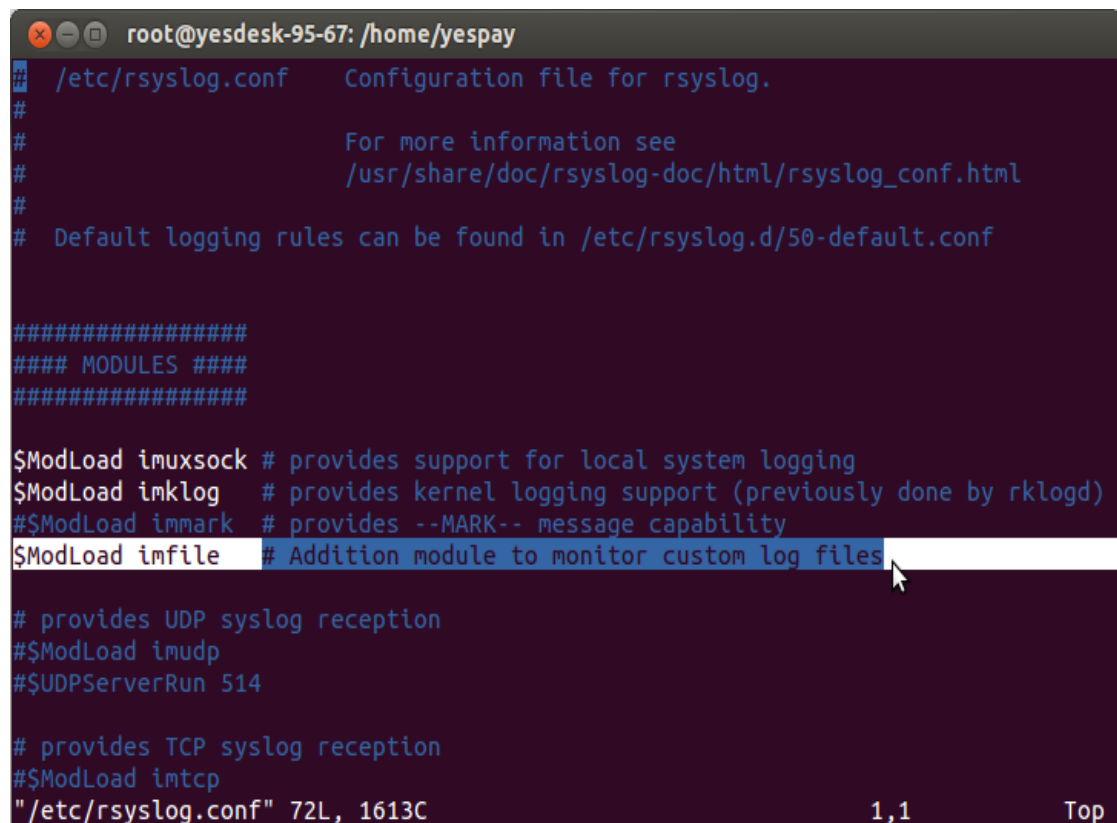
Figure 25

Step 3: Add the entry below module with other modules in the MODULES section (See the screenshot example below)

\$ModLoad imfile #Addition module to monitor custom log files

Step 4: By default the logs will be sent to UDP port 514. If the centralized log management server is listening on a different port, the port to send to can be changed by uncommenting and updating the `$UDPServerRun` tag in `rsyslog.conf` file.

e.g. `#$UDPServerRun 514` to `$UDPServerRun 515` (see the screenshot example below)



```
root@yesdesk-95-67: /home/yespay
/etc/rsyslog.conf Configuration file for rsyslog.
#
# For more information see
# /usr/share/doc/rsyslog-doc/html/rsyslog_conf.html
#
# Default logging rules can be found in /etc/rsyslog.d/50-default.conf

#####
#### MODULES ####
#####

$ModLoad imuxsock # provides support for local system logging
$ModLoad imklog    # provides kernel logging support (previously done by rklogd)
#$ModLoad immark   # provides --MARK-- message capability
$ModLoad imfile    # Addition module to monitor custom log files
#
# provides UDP syslog reception
#$ModLoad imudp
#$UDPServerRun 514
#
# provides TCP syslog reception
#$ModLoad imtcp
"/etc/rsyslog.conf" 72L, 1613C 1,1 Top
```

Figure 26

- **Update 50-default.conf file**

Step 1: Open /50-default.conf file, which is generally found in the /etc/ directory, using the command below:

```
sudo vi /etc/rsyslog.d/50-default.conf
```

Step 2: Add this line with other log facility (see the screenshot example below)

```
*.*;auth,authpriv.none,local3.none    -/var/log/syslog
```

```
root@yesdesk-95-67: ~  
# Default rules for rsyslog.  
#  
#       For more information see rsyslog.conf(5) and /etc/rsyslog.conf  
#  
# First some standard log files.  Log by facility.  
#  
auth,authpriv.*          /var/log/auth.log  
*. *;auth,authpriv.none,local3.none -/var/log/syslog  
#cron.*                  /var/log/cron.log  
#daemon.*                /var/log/daemon.log  
#kern.*                   /var/log/kern.log  
#lpr.*                    /var/log/lpr.log  
#mail.*                   /var/log/mail.log  
#user.*                   /var/log/user.log  
#  
# Logging for the mail system.  Split it up so that  
# it is easy to write scripts to parse these files.  
#  
#mail.info                /var/log/mail.info  
#mail.warn                /var/log/mail.warn  
mail.err                  /var/log/mail.err  
#  
# Logging for INN news system.  
#  
news.crit                 /var/log/news/news.crit  
news.err                  /var/log/news/news.err  
news.notice               /var/log/news/news.notice  
#  
# Some "catch-all" log files.  
#  
#*.debug;\n#   auth,authpriv.none;\n#   news.none;mail.none -/var/log/debug  
#*.info;*.notice;*.warn;\n#   auth,authpriv.none;\n#   cron,daemon.none;\n#   mail,news.none -/var/log/messages  
#  
# Emergencies are sent to everybody logged in.  
#  
*.emerg                   :omusrmsg:*  
"/etc/rsyslog.d/50-default.conf" 68L, 1667C 1,1 Top
```

Figure 27

Suse Linux

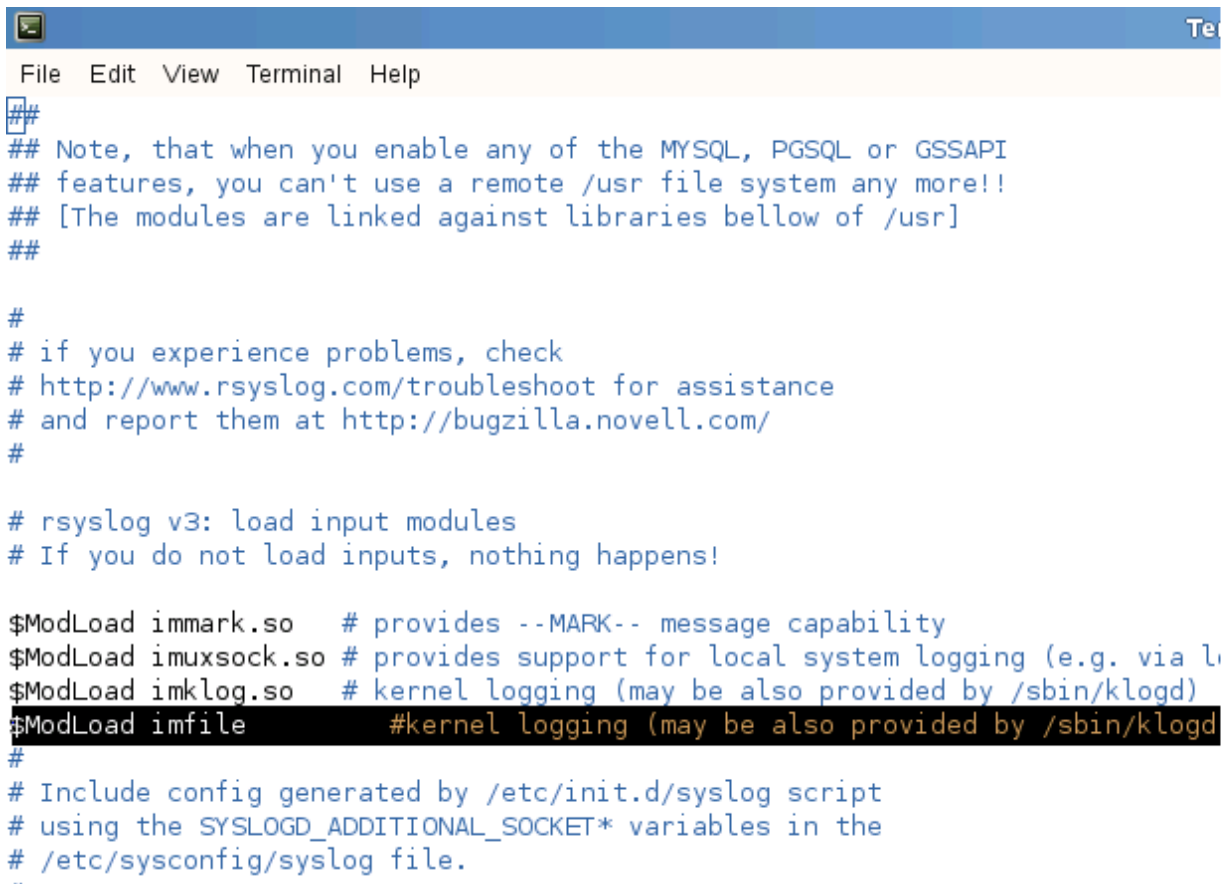
- **Update rsyslog.conf**

Step 1: Edit rsyslog.conf file, which is generally found in the /etc/ directory, using the command below:

```
sudo vi /etc/rsyslog.conf
```

Step 2: Copy the below Custom YESEFT Log configuration into the rsyslog.conf file (see the screenshot example below)

Note: The IP address/host name of the centralized log server should be used instead of the example address 192.168.77.8 shown below



```
File Edit View Terminal Help
##
## Note, that when you enable any of the MYSQL, PGSQL or GSSAPI
## features, you can't use a remote /usr file system any more!!
## [The modules are linked against libraries bellow of /usr]
##

#
# if you experience problems, check
# http://www.rsyslog.com/troubleshoot for assistance
# and report them at http://bugzilla.novell.com/
#

# rsyslog v3: load input modules
# If you do not load inputs, nothing happens!

$ModLoad immark.so    # provides --MARK-- message capability
$ModLoad imuxsock.so  # provides support for local system logging (e.g. via l
$ModLoad imklog.so    # kernel logging (may be also provided by /sbin/klogd)
$ModLoad imfile       #kernel logging (may be also provided by /sbin/klogd
#
# Include config generated by /etc/init.d/syslog script
# using the SYSLOGD_ADDITIONAL_SOCKET* variables in the
# /etc/sysconfig/syslog file.
..
```

Figure 28

```

Terminal
File Edit View Terminal Help
news.err - /var/log/news/news.err;RSYSLOG_TraditionalFileFormat
news.notice - /var/log/news/news.notice;RSYSLOG_TraditionalFileFormat
# enable this, if you want to keep all news messages
# in one file
#news.* - /var/log/news.all;RSYSLOG_TraditionalFileFormat

#
# Warnings in one file
#
#*=warning;*=err - /var/log/warn;RSYSLOG_TraditionalFileFormat
#*.crit - /var/log/warn;RSYSLOG_TraditionalFileFormat

#
# the rest in one file
#
#*.*;mail.none;news.none - /var/log/messages;RSYSLOG_TraditionalFileFormat

#
# enable this, if you want to keep all messages
# in one file
#*.* - /var/log/allmessages;RSYSLOG_TraditionalFileFormat

#### Custome YESEFT Log ####
$InputFileName /var/log/YESEFT/YESEFT.log
$InputFileTag yeseft-info:
$InputFileStateFile stat-info
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor

#
# Some foreign boot scripts require local7
#
local0,local1.* - /var/log/localmessages;RSYSLOG_TraditionalFileFormat
local2,local3.* - /var/log/localmessages;RSYSLOG_TraditionalFileFormat
local4,local5.* - /var/log/localmessages;RSYSLOG_TraditionalFileFormat
local6,local7.* - /var/log/localmessages;RSYSLOG_TraditionalFileFormat

###
*.debug /var/log/messages
#*.* /var/log/YESEFT/YESEFT.log
*.* @192.168.77.8
/var/log/YESEFT/YESEFT.log @192.168.77.8

```

Figure 29

Cent OS

- Update rsyslog.conf

Step 1: Edit rsyslog.conf file, which is generally found in the /etc/ directory, using the command below:

```
sudo vi /etc/rsyslog.conf
```

Step 2: Copy the below Custom YESEFT Log configuration into the rsyslog.conf file (see the screenshot example below)

Note: The IP address/host name of the centralized log server should be used instead of the example address 192.168.77.8 shown below

rsyslog v5 configuration file

```
# For more information see /usr/share/doc/rsyslog-*/rsyslog_conf.html
# If you experience problems, see http://www.rsyslog.com/doc/troubleshoot.html

#### MODULES ####

$ModLoad imuxsock # provides support for local system logging (e.g. via logger com
$ModLoad imklog    # provides kernel logging support (previously done by rklogd)
#$ModLoad immark   # provides --MARK-- message capability
$ModLoad imfile     #kernel logging (may be also provided by /sbin/klogd)

# Provides UDP syslog reception
#$ModLoad imudp
#$UDPServerRun 514

# Provides TCP syslog reception
#$ModLoad imtcp
#$InputTCPServerRun 514

#### GLOBAL DIRECTIVES ####

# Use default timestamp format
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# File syncing capability is disabled by default. This feature is usually not requ
# not useful and an extreme performance hit
#$ActionFileEnableSync on

# Include all config files in /etc/rsyslog.d/
$IncludeConfig /etc/rsyslog.d/*.conf

#### RULES ####

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
```

Figure 30

```
# Save news errors of level crit and higher in a special file.
uucp,news.crit                                /var/log/spooler

# Save boot messages also to boot.log
local7.*                                       /var/log/boot.log

#### Custome YESEFT Log  ###

$InputFileName                                /var/log/YESEFT/YESEFT.log
$InputFileTag                                  yeseft-info:
$InputFileStateFile                           stat-info
$InputFileSeverity                            info
$InputFileFacility                            local3
$InputRunFileMonitor

a
# ### begin forwarding rule ###
# The statement between the begin ... end define a SINGLE forwarding
# rule. They belong together, do NOT split them. If you create multiple
# forwarding rules, duplicate the whole block!
# Remote Logging (we use TCP for reliable delivery)
#
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#$WorkDirectory /var/lib/rsyslog # where to place spool files
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 1g      # 1gb space limit (use as much as possible)
#$ActionQueueSaveOnShutdown on    # save messages to disk on shutdown
#$ActionQueueType LinkedList      # run asynchronously
#$ActionResumeRetryCount -1       # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*. * @@remote-host:514
# ### end of the forwarding rule ###
*.debug                                     /var/log/messages
#*. *                                       /var/log/YESEFT/YESEFT.log
*. *                                       @192.168.77.8
/var/log/YESEFT/YESEFT.log                 @192.168.77.8
```

Figure 31

7 Appendix E – IPC Integration Guide

The purpose of this section is to provide IPC interface descriptions to integrate magnetic and EMV chip and PIN cards transaction processing within new and existing point of sale EPOS applications.

Two methods of integration are described for an EPOS application to integrate with IPC application as described in section 6.1.

7.1 IPC Integration Mode

IPC software encapsulates banking magnetic and EMV payment card processing for integrating with new and existing EPOS applications. There are two types of interfaces available for integrating with IPC.

- **IPC Socket Interface:** This interface provides a simple socket based mechanism to send transaction requests to IPC. IPC application listens on a socket for incoming transaction requests. On receiving a transaction request the IPC application provides a front-end to the attendant at the till to take chip or swiped card transactions.
- **IPC File Interface:** This interface provides a simple file based mechanism to send transaction requests to IPC. The IPC application polls an inbound directory for incoming transaction request. On receiving a transaction request the IPC application provides a front-end to the attendant at the till to take chip or swiped card transactions.

7.2 IPC Environments

The following sections describe how the IPC can be used in different environment like Retail, Hospitality, Lodging, Semi-attended & Kiosks.

7.3 IPC for Retail

IPC implements the standard transaction types for retail applications like Sale and Refunds. IPC can also be configured for cash back transactions if required. When a merchant requests the option for pay with cash back then IPC will ask for Cash Back amount if the card supports the function.

IPC provides multiple mechanisms for cancelling a previously performed Sale transaction. Available methods are Cancel and Refund.

In **UK and Ireland**, the cancel transaction should be called before the end of day settlement to the processor, which is typically mid night. A transaction cannot be cancelled if the settlement processing has completed.

WPH creates a batch for every terminal called FCR (Financial Control Record). The FCR is a logical grouping of all the transactions done by a terminal in a day. By default all the batches are closed around mid-night.

Once a batch is closed no other transactions can be added to that batch, a new batch is created for the next transaction.

IPC also provides X and Z totals reports to download the latest totals on the current batch. A Z total will close a WPH batch and can be used to report terminal activity in shifts.

7.4 IPC for Lodging

IPC implements Pre-Authorisation and Pre Sales Completion for the Lodging industry. This allows a PMS (Property Management System) to do pre-authorisation and pre sales completion to finally charge the account. The Pre Sales completion will have the reference of the pre-authorisation done on the card.

7.5 IPC for Kiosks

IPC implements the standard transaction type Sale for kiosk applications. If the merchant intends to perform refunds when the kiosk is not able to dispense then a cancel transaction can be used to stop the transaction from submission into the processor. But there are limitations in using the cancel transaction.

In **UK and Ireland**, the cancel transaction should be called before the end of day settlement to the processor, which is typically midnight. A transaction cannot be cancelled if the settlement processing has completed. In such a scenario the only other option is to refund the transaction. But as refunds are not supported for kiosk so the best option is to use the WPH HTTP POST method to perform a refund transaction.

7.6 IPC for Semi-Attended

IPC-2 implements the standard transaction type sale for semi-attended applications. Following pinpads and modes are supported for this environment.

PINPADs : IPP350,IWL250

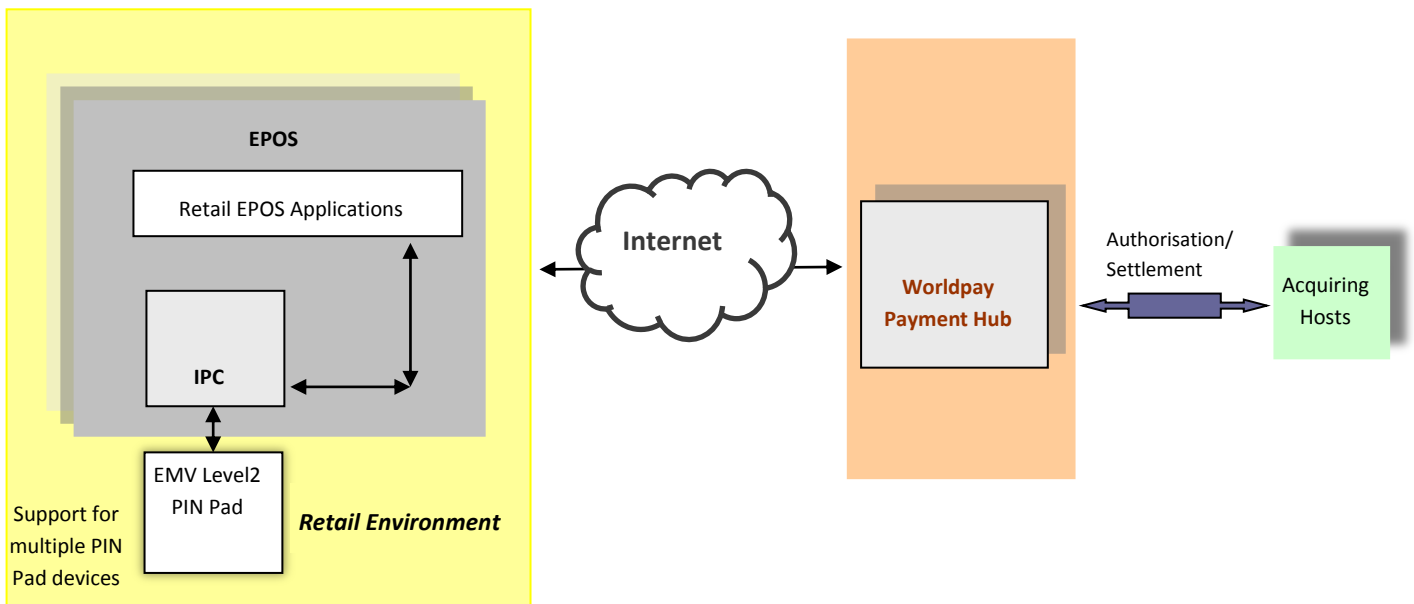
MODEs : Contact & Contactless

8 IPC INTERFACE

8.1 General

IPC is a Java based application which manages the flow-control of magnetic and smart card EMV Chip & PIN transactions by interacting with the EPOS Application over a sockets or a file interface.

IPC's purpose is to provide the User Interface for EFT processing. In this way the main EPOS application does not need to be EFT intelligent and can be merely used for initiating EFT transactions and printing the completed receipts. All EFT processing events and screens and data entry are performed through user interface screens generated by the IPC Console. (For partners who prefer not to use the IPC Console, an alternative is provided via the IntraMessage port – please see Appendix G for further information)



8.2 IPC Integration Attributes

8.2.1 Input Request Attributes

The IPC transaction request is a *Name Value* pair format. There is a name (Number) associated with all the attributes of the transaction. The EPOS application needs to send a list of attributes and their values in the request. Each attribute *Name Value* pair is separated by a *Line Feed*.

Following is the list of input attributes for a transaction:

Description	Attribute Name	Data Type	Length	Mandatory/ Conditional/ Optional
-------------	----------------	-----------	--------	----------------------------------

Description	Attribute Name	Data Type	Length	Mandatory/ Conditional/ Optional
<p>Transaction reference, which uniquely identifies the transaction with a user defined tag.</p> <p>It is recommended that Transaction Reference field should contains only characters defined in 'Data Type' however if Transaction Reference contains special characters then IPC will sanitize the Transaction Reference Filed, excluding 'Data Type' characters. IPC will use the sanitized Transaction Reference to process the transaction. IPC will send the original Transaction Reference in output response.</p> <p>For cancel, use the transaction reference of original transaction to be cancelled.</p>	1	Alpha Numeric, Hyphen(-), Underscore (_)	0-30	M

Description	Attribute Name	Data Type	Length	Mandatory/ Conditional/ Optional																																										
Transaction Type, Transaction Type indicates the type of financial transaction.	2	Integer	N/A	M																																										
<table><tr><th>Transaction Type</th><th>Description</th></tr><tr><td>0</td><td>Sale (Goods and Services)</td></tr><tr><td>1</td><td>PreAuth</td></tr><tr><td>2</td><td>Pre Sales Completion</td></tr><tr><td>3</td><td>Cancel Transaction</td></tr><tr><td>8</td><td>TaxFree Voucher (VAT Refund Voucher) for Cash Transaction ##</td></tr><tr><td>12</td><td>Sale with Token</td></tr><tr><td>13</td><td>Refund with Token</td></tr><tr><td>15</td><td>Get Territory</td></tr><tr><td>20</td><td>Returns</td></tr><tr><td>22</td><td>Printing Duplicate Merchant Receipt (Valid for Retail Mode)</td></tr><tr><td>23</td><td>Printing Duplicate Customer Receipt</td></tr><tr><td>24</td><td>Check Pinpad connection</td></tr><tr><td>25</td><td>Get total number of offline stored transactions</td></tr><tr><td>26</td><td>Get Serial number of connected Pinpad</td></tr><tr><td>30</td><td>CheckCard</td></tr><tr><td>34</td><td>CheckStatus</td></tr><tr><td>35</td><td>Last transaction result</td></tr><tr><td>36</td><td>X Report</td></tr><tr><td>37</td><td>Z Report</td></tr><tr><td>90</td><td>Hide IPC Window</td></tr></table>					Transaction Type	Description	0	Sale (Goods and Services)	1	PreAuth	2	Pre Sales Completion	3	Cancel Transaction	8	TaxFree Voucher (VAT Refund Voucher) for Cash Transaction ##	12	Sale with Token	13	Refund with Token	15	Get Territory	20	Returns	22	Printing Duplicate Merchant Receipt (Valid for Retail Mode)	23	Printing Duplicate Customer Receipt	24	Check Pinpad connection	25	Get total number of offline stored transactions	26	Get Serial number of connected Pinpad	30	CheckCard	34	CheckStatus	35	Last transaction result	36	X Report	37	Z Report	90	Hide IPC Window
Transaction Type	Description																																													
0	Sale (Goods and Services)																																													
1	PreAuth																																													
2	Pre Sales Completion																																													
3	Cancel Transaction																																													
8	TaxFree Voucher (VAT Refund Voucher) for Cash Transaction ##																																													
12	Sale with Token																																													
13	Refund with Token																																													
15	Get Territory																																													
20	Returns																																													
22	Printing Duplicate Merchant Receipt (Valid for Retail Mode)																																													
23	Printing Duplicate Customer Receipt																																													
24	Check Pinpad connection																																													
25	Get total number of offline stored transactions																																													
26	Get Serial number of connected Pinpad																																													
30	CheckCard																																													
34	CheckStatus																																													
35	Last transaction result																																													
36	X Report																																													
37	Z Report																																													
90	Hide IPC Window																																													

Description		Attribute Name	Data Type	Length	Mandatory/ Conditional/ Optional
91	Show IPC Window				
99	Close IPC application				
Transaction Amount Transaction amount is in major currency units e.g. 3=10.23 Amount must be non-zero, non negative and less than 9999999.99. Please note however that transactions above the terminal's ceiling limit will be cancelled even if they are less than 9999999.99. The Ceiling limit is defined by acquirer and varies by acquirer. Only 2 digits are allowed after the decimal point		3	Decimal	NA	M
Masked PAN, present in case of pre sales completion and cancel transaction. Required for cancel transaction unless a check card is cancelled.		5	Alpha Numeric	13-19	C1
Card Expiry Date, present in case of pre sales completion and cancel transaction in MMY format. Required for cancel transaction unless a check card is cancelled. Note: The expiry date parameter in pre sales completion and Cancel transactions has been retained for backwards compatibility, however any expiry date corresponding to MMY format is accepted.		6	Integer	4	C1
CNP indicator specifies if the transaction is cardholder not present. Value is 1 if CNP transaction otherwise 0.		12	Integer	1	C2
Transaction reference. For Pre Sales, specifies the reference of the pre sales transaction to be completed. For Cancel, specifies the reference of the transaction to be Voided. (Returned in field 28 of IPC response message. Refer response message details).		13	Alpha Numeric	12-14	C3
Keyed transaction indicator, specifies if the transaction is keyed transaction. Value is 1, if Keyed transaction otherwise 0. Keyed is allowed only for Sale and Refund transaction. Value is 2, if forced Keyed referral transaction.		18	Integer	1	O
Token Reference		19	Alpha Numeric	20	C4
Cash Tender amount Cash Tender amount is in major currency units e.g. 20=10.23		20	Decimal	NA	C5
Remove Card flag. This is Boolean field and mandatory in the request of Check Card functionality. If this field is True then IPC will ask for remove card after returning card details. If this field is False then IPC will wait for a while for transaction request.		25	Boolean	NA	M

Description	Attribute Name	Data Type	Length	Mandatory/ Conditional/ Optional
Cash transaction indicator, specifies if the transaction is cash transaction. Value must be 1.	28	Integer	1	C5
End of message indicator, values always 0.	99	Integer	1	M

- **C1 – Required for pre sales completion and cancel transaction**
- **C2 – Card not present transaction**
- **C3 – Transaction Type Sale Completion (2=2)**
- **C4 – Mandatory for Transaction Type 12 (Sale with token) & 13 (Refund with token).**
- **C5 – Mandatory for Cash Transaction.**
- **Only Alphanumeric or numbers are allowed in all the input attribute fields, except in the case of Transaction reference**
- **## - TaxFree Voucher (VAT Refund) for Cash Transaction is valid only if Merchant is enabled for TaxFree.**

8.2.2 Output Response Attributes

The IPC response message also contains transaction response in a *Name Value* pair format. There is a name (Number) associated with all the response attributes of the transaction. The IPC will send a list of attributes and their values in the response. Each attribute *Name Value* pair is separated by a *Line Feed*.

Note: Not all of the listed attributes are sent in every response. The response attributes can vary even for the same type of transaction: an example is where DCC is enabled, there are attributes detailing DCC currency, the currency conversion rate etc which will be present in the output response only if DCC was offered and accepted for the transaction. If the transaction proceeded in the home currency, these DCC attributes will not be present in the output response.

Following is the list of response attributes for a transaction:

Description		Attribute Name	Length
POS Entry Mode, card payment entry method. Please note that additional values may be added with new releases of IPC		1	2
Value	Meaning		
5	Chip transaction.		
2	Stripe transaction.		
1	Keyed transaction.		
81	Card holder not present.		
0	X & Z report and transaction type Cancel		
21	Cash transaction.		
7	Contactless chip transaction		
91	Contactless Stripe transaction		
92	Contactless On-Device transaction		

Description		Attribute Name	Length
Transaction Type. Transaction Type indicates the type of financial transaction, represented by the first two digits of ISO 8583:1987 Processing Code. Please note that additional values may be added with new releases of IPC		2	1-2
Transaction Type			
0	Sale (Goods and Services)		
3	Cancel		
9	Purchase With Cash Back		
20	Returns		

Description		Attribute Name	Length
Transaction Result. Uniquely identifies the transaction response. Please note that additional values may be added with new releases of IPC		3	1-2
Transaction Result	Description		
1	Approved Online		
2	Approved Offline		
3	Approved Manual (Referral)		
4	Declined Online		
5	Declined Offline		
9	Cancelled		
10	Transaction performed ¹		
16	Capture Card, declined online		
19	Transaction Aborted		
20	Pre sales completed		
21	Pre sales rejected		
22	Card number not matched		
23	Expiry date not matched		
24	Invalid transaction state		
25	Transaction not valid for requested operation		
26	Invalid PGTR		
27	Invalid Merchant		
28	Invalid Terminal		
29	Merchant status is not valid		
30	Invalid card number		
31	Expired Card		
32	Pre valid card		
33	Invalid issue number		
	continued....		
Integrated Payment Client-II-Series			
Implementation/Integration Guide issue 1.21 For version 2.1.6			
© Worldpay 2015. All rights reserved.	Page 94 of 163		

Description		Attribute Name	Length																						
...continued																									
<table><tr><th>Transaction Result</th><th>Description</th></tr><tr><td>34</td><td>Invalid card expiry date</td></tr><tr><td>35</td><td>Invalid start date</td></tr><tr><td>36</td><td>Card not accepted</td></tr><tr><td>37</td><td>Transaction not allowed</td></tr><tr><td>38</td><td>Cash back not allowed</td></tr><tr><td>42</td><td>Status Busy</td></tr><tr><td>43</td><td>Status Not Busy</td></tr><tr><td>44</td><td>Pinpad is not connected</td></tr><tr><td>45</td><td>Pinpad is connected</td></tr><tr><td>50</td><td>AVS details required</td></tr></table>		Transaction Result	Description	34	Invalid card expiry date	35	Invalid start date	36	Card not accepted	37	Transaction not allowed	38	Cash back not allowed	42	Status Busy	43	Status Not Busy	44	Pinpad is not connected	45	Pinpad is connected	50	AVS details required		
Transaction Result	Description																								
34	Invalid card expiry date																								
35	Invalid start date																								
36	Card not accepted																								
37	Transaction not allowed																								
38	Cash back not allowed																								
42	Status Busy																								
43	Status Not Busy																								
44	Pinpad is not connected																								
45	Pinpad is connected																								
50	AVS details required																								
Authorisation Code, holds the value generated by the issuer for an approved transaction. Present only in case of a successful transaction.		4	2-6																						
EMV Card Data Element Application Primary Account Number (PAN) holds the valid cardholder account number. Masked PAN consists of first 6 digits and last 4 digits: e.g. 492949 XXXXXX 0002		5	13-19																						
EMV Card Data Element Application Label holds the mnemonic associated with the AID according to the ISO/IEC 7816-5.		6	1-16																						
EMV Card Data Element Application Effective Date which holds date from which the application may be used. The format is DDMMYYYY.		7	8																						
Transaction Date contains local date that the transaction was authorised. The format is DDMMYYYY.		8	8																						
Transaction Time contains local time that the transaction was authorised. The format is HHMMSS.		9	6																						
EMV Card Data Element Cardholder Name indicates cardholder name according to ISO 7813.		10	4-52																						
EMV Card Data Element Cardholder Name Extended indicates the whole cardholder name when greater than 26 characters using the same coding convention as in ISO 7813.		11	54-90																						
Merchant Identifier.		12	15																						

Description		Attribute Name	Length
Terminal Identifier.		13	8
Card Verification Method		14	1-2
Please note that additional values may be added with new releases of IPC			
CVM	Description		
1	Signature verified		
2	Pin verified/ CVM performed on Consumer device in contactless transaction		
7	Cardholder not present		
8	No CVM		
9	Unknown CVM		
10	Signature and Pin verified		
Start Date, present only in case of a swiped UK Maestro/Solo card transaction.		15	8
Total Number of Sale Counts		16	NA
Total Number of Refund Counts		17	NA
Total Sale Amount.		18	NA
This amount is returned when X and Z report transaction is performed.			
Amount is returned in major currency denomination			
Total Refund Amount.		19	NA
This amount is returned when X and Z report transaction is performed.			
Amount is returned in major currency denomination			
EFT Sequence number		21	1-6
Merchant Address		22	1-140
Merchant Name		23	40
Batch Number		25	9
Referral telephone number 1		26	8-20
Referral telephone number 2		27	8-20
PGTR, Payment gateway transaction reference.		28	12-14
EMV Card Data Element Application Identifier (AID), which identifies the application as described in ISO/IEC 7816-5.		29	10-32

Description	Attribute Name	Length
PAN Sequence number or Issue Number. PAN Sequence number in case of an ICC transaction and Issue number in case of a Swiped UK Maestro/Solo card transaction.	30	2
Transaction Status Information (TSI), present only in case of an ICC transaction. Used for debug purpose only.	31	4
Terminal Verification Results (TVR), present only in case of an ICC transaction. Used for debug purpose only.	32	10
Retention reminder	33	10-100
Customer Declaration	34	240
Additional Response Data, the CVV response	35	6
Receipt Number	36	1-10
Card Expiry Date IPC returns the encrypted expiry date in case of IPP350, iWL250 and Miura PEDs. Any valid MMY date can be sent to IPC for cancel and pre sales completion transaction type.	37	4
Total Amount. Amount is returned in configured major/minor currency denomination. Total amount includes Sale Amount, Cash Back Amount (if any), Gratuity Amount (if any) and Pennies Donation Amount (if any) The default format of amount will be in minor currency.	38	NA
Cash Back Amount. Present if cash back amount is entered when requested Cash Back Amount is returned in configured major/minor currency denomination. The default format of amount will be in minor currency.	39	NA
Gratuity Amount Gratuity Amount is returned in configured major/minor currency denomination. The default format of amount will be in minor currency.	40	NA
This field indicates Card type, If card is fuel card it returns 1 else 0.	41	1
A field of 40 zeros(0) is returned to maintain the backward compatibility (earlier SHA1 hash value for the PAN number was returned in response	59	40

Description				Attribute Name	Length
<p>Card Issuer Code, this is the 3 digit WPH card issuer code. Should be used to identify the type of the card.</p> <p>Following is the current list of issuer codes for UK & Europe :</p> <p>Please note that additional values may be added with new releases of IPC</p>				60	3
Code	Description	Name abbreviation	Comments		
000	Not In Use	NOT ISSUED	Not in use		
001	VISA DEBIT	DELTA			
002	UK Electron	UKELECTRON			
003	Visa Purchasing	VISA			
004	Visa	VISA			
005	MasterCard	MASTER			
006	UK Maestro	UK MAESTRO			
007	Solo	SOLO	Not in use		
008	JCB	JCB			
009	Maestro	MASTER			
010	VISA ATM	VISA ATM			
011	ARVAL PHH	ARVALPHH			
012	Amex	AMEX			
013	Diners Club	DINERS			
014	Laser	LASER	Not in use		
015	DUET	DUET	Not in use		
016	HN Mastercard	MASTER			
017	HN PLCC	PLCC			
018	Tesco Clubcard	CLUBCARD			
019	DANKORT	DANKORT			
020	Discover	DISCOVER			
021	US Debit	USDEBIT			
022	Debit	MASTER			
023	MasterCard	MASTER			
024	Bank of America	BANAMER			
080	YESpay Virtual	FLEXCASH	Not in use		
081	Flexecash Love 2	FLEXECASH			
090	YESpay Gift Card	YESPAY	Not in use		
Token Reference: This will be 20 characters long and alphanumeric field.				61	20

Description	Attribute Name	Length
Credit/Debit card identification with online/offline indicator will be returned only in Check Card response. Only four values are possible, D Online C Online D Offline C Offline	64	9-10
Acquirer Name will be returned in this field only in get territory response.	65	1-40
Converted currency name for DCC transactions like HKD – HK Dollar.	70	NA
Amount converted into accepted currency for DCC transactions.	71	NA
Currency conversion rate.	72	NA
Pennies Donation Amount: This field will be present only in the response of Pennies Donation transaction. Pennies Donation Amount is returned in major currency.	74	NA
Total number of offline stored transactions.	75	1-4
Serial number of connected pinpad.	76	6-9
Available offline spending amount	77	NA
Retrieval Reference Number. It is a copy of receipt number.	80	12
Transaction reference. This field will be present in the response of a transaction if field 1 is present in transaction request.	98	1-30
End of message indicator, values always 0.	99	1

Note:

1. The Transaction result 10 in field 3 is valid for non-financial transactions, these transaction types are 22,23,25,26 and 27. Also these transaction types are available for UK.
2. Now for only **Contactless EMV refund transaction** full ICC data will be send in capture request for both IPP350 and VeriFone 7816 PED. Since VeriFone does not understand HVC refund processing instead of IPP350 so value for PEM will be reflect in output.txt which is mentioned in below table against CVM value for refund EMV contactless transaction.

PINPAD	CVM Method (14 =)	PEM (1 =)
IPP350 Contactless	8	7
IPP350 HVC	2	92

VeriFone 7816 Contactless	8	7
VeriFone 7816 HVC	8	7

8.3 IPC Socket Interface

IPC application listens on a TCP/IP port number for transaction requests . IPC application can send the receipt data and GUI (Window) message to TCP/IP port. IPC application opens all sockets in Server mode. The EPOS application should open the relevant sockets in Client mode. Please refer the [Appendix G](#) for GUI messages on TCP/IP port

The EPOS application should first establish a connection with the IPC application (e.g. request port 10000) and then send a transaction request.

IPC responds on the same connection to the transaction request e.g. if the transaction request is sent on socket 10000 to IPC by the EPOS application, IPC will send the transaction response back on the same socket.

The request message has the same format as the *INPUT.TXT* file and similarly the response message has the same format as the *OUTPUT.TXT* file.

8.4 Typical Transaction Requests and Responses

This section lists the typical transaction requests to IPC and responses from the IPC.

Please note that

- The response message can vary according to the circumstances of the transaction, and not all fields shown in the example will be returned at all times. An example of this is the Checkcard transaction, where the response message is very different according to whether a valid card is read, or if the card was invalid e.g. a loyalty card from other merchant, unknown card. (In this case the definition of a valid card is one that falls into the bin ranges of payment cards, gift cards etc. that IPC is aware of)
- It is possible for IPC to refuse to entertain a request because it is busy with another activity e.g. IPC is still completing its startup processing. In this case IPC will not respond to the request with a busy status (see transaction Checkstatus for more details)

8.4.1 Transaction Type Sale

Request

1=2211

2=0

3=10.99

99=0

Response

7=01042002

29=A0000000031010

6=VISA BARCLAYCARD

5=492949XXXXXX2008

4=729945
10=BMSTESTCARDG6091/G
14=2
1=5
22=Checknet House, I53 East Barnet Road, Barnet EN4 8QZ
12=6818780
23= Worldpay Retail
28=PGTR13513393
13=22980045
8=07092009
3=1
21=1
9=172748
2=0
34=PLEASE DEBIT MY ACCOUNT
33=PLEASE KEEP THIS RECEIPT FOR YOUR RECORDS
36=5
37=0101
38=1099
41=0
30=0
31=F8 00
32=40 00 00 80 00
59=00
60=004
98=2211
99=0

8.4.2 Transaction Type Refund

Request

1=123
2=20
3=10
99=0

Response

7=30121899
6=Maestro
5=679999XXXXXXXXX0919
4=10025
14=8
1=2
22=153 Checknet House East Barnet Road Barnet Herts EN4 8QZ
12=21249872
23=YESpay Demo

[illegible]

8.4.3 Transaction Type Sale CNP

Request

1=2214
2=0
3=10.99
12=1
99=0

Response

7=01082004
6=Visa
5=492949XXXXXX2008
4=831842
14=7
1=81
22=Checknet House 153 East Barnet Road Barnet Hertfordshire EN4 8QZ
12=6818780
23= Worldpay Retail
28=PGTR73221377
15=0804
13=22980045
8=07092009
3=1
21=3
9=125044
2=0

34=PLEASE DEBIT MY ACCOUNT
33=PLEASE KEEP THIS RECEIPT FOR YOUR RECORDS
35=422800
36=14
37=0101
38=1099
41=0
59=00
60=004
98=2214
99=0

8.4.4 Transaction Type Refund CNP

Request

1=2214
2=20
3=10.99
6=0314
12=1
99=0

Response

7=30121899
6=Visa
5=492949XXXXXX2008
4=10017
14=7
1=81
22=Checknet House 153 East Barnet Road Barnet Hertfordshire EN4 8QZ
12=6818780
23= Worldpay Retail
28=PGTR73222021
13=22980045
8=07092009
3=1
21=1
9=125351
2=20
34=PLEASE CREDIT MY ACCOUNT
33=PLEASE KEEP THIS RECEIPT FOR YOUR RECORDS
36=15
37=0101
38=1099
41=0
59=00

60=004
98=2214
99=0

8.4.5 Transaction Type Pre-Authorisation

Request

1=2217
2=1
3=10.99
99=0

Response

[illegible]

8.4.6 Transaction Type Pre Sales Completion

This transaction type is used to charge a previously performed pre-authorisation. Request should have the Masked PAN, Expiry date and PGTR number of the pre-authorisation.

Request

```
1=2218
2=2
3=10.99
5=492949XXXXXX2008
6=0314
13=PGTR61734250
99=0
```

Response

[illegible]

8.4.7 Transaction Type Cancel

The Cancel request can be used to stop a previously authorised transaction from being charged to the card. The Cancel request is only successful if the transaction is not yet settled by WPH.

Request

```
1=52
2=3
5=492949XXXXXX2008
6=0314
13=PGTR73222788
```

99=0

Response

1=0

13=22980045

3=1

2=3

41=0

98=5

99=0

8.4.8 Transaction Type Keyed

The Keyed request can be used to perform Keyed Sale and Keyed Refund transaction. IPC allows entry of card details only from the pinpad (supported with iPP350, iWL250). Once the below transaction request is received by IPC, the pinpad will prompt for card details.

Request for Keyed Sale

1=123456

2=0

3=10.00

18=1

99=0

Response for Keyed Sale

7=30121899

6=Visa

5=478825XXXXXX8291

4=096708

14=1

1=1

22=Checknet House 153 East Barnet Road Barnet Herts EN4 8QZ

12=000700000200136

23= Worldpay Retail

28=PGTR1753554

13=23000017

8=28012010

3=1

21=1

9=121702

2=0

34=PLEASE DEBIT MY ACCOUNT

33=PLEASE KEEP THIS RECEIPT FOR YOUR RECORDS

36=131

37=1210

38=1000

41=0

[illegible]

Request for Keyed Refund

```
1=123456
2=20
3=10.00
18=1
99=0
```

Response for Keyed Refund

[illegible]

8.4.9 Transaction Type Forced Keyed Referral

Please note that this transaction is available only with Worldpay US acquirer using the Vx820 pinpad.

This transaction type can be used to send pre-approved referral transaction information to WPH. It is intended for situations where the store has been through a period of manual trading, using zip-zap machines and calling the bank for voice authorisation, because of e.g. power loss in the store. Once the payment service is restored, this transaction can be used to capture the details of the manually approved transactions via IPC.

Request

1=123456
2=0
3=10.00
18=2
99=0

After placing this request, IPC will prompt for the card details via the UI or the IntraMessage port. Once the card details are provided, IPC will prompt for the previously obtained Authorisation code. If the Auth. code is provided and the transaction accepted, IPC will return a transaction response of 'Approved Manual' (3=3) , and the capture will be sent to WPH if IPC is online, or stored locally if it is offline. If the transaction is rejected IPC will return a cancelled response message and the capture will not be sent or stored.

Response

[illegible]

8.4.10 Transaction Type CheckCard

This transaction type can be used to read the card details. If the card is not accepted by IPC, then the transaction is cancelled and response send back to EPOS application. In the response only the first 6 and last four digits for the card number are returned. The digits in between the first 6 and the last four are all zeroed out (replaced by 0).

There are two ways of using Checkcard depending on the value of 'Remove Card' flag. If this field is true then IPC will ask the cardholder to remove the card after returning card details. If this field is False then IPC will wait for a transaction request using the same card i.e., the cardholder is not prompted to remove the card unless the next request does not arrive within the configurable timeout period (default 10 seconds).

Request

```
1=2216
2=30
25=true
99=0
```

Response

[illegible]

Response field 64 will have a pipe separated value where the first part of pipe separated value indicates whether card is Credit or Debit (C-Credit, D-Debit) and second part indicates verification is done online or offline (using local card bin ranges).

To perform the check card transaction followed by, for example, a sale, or break request, implement the following steps

Check card Request

```
1=123
2=30
25=false
99=0
```

On receiving this request IPC will prompt the cardholder to Insert/swipe card. After insertion or swipe of the card IPC will return a response to the EPOS application and wait for the next transaction request for a configurable time (default 10 sec).

At the Checkcard stage IPC does not prompt Cardholder Verification i.e. the cardholder is **not** prompted for PIN entry or signature. Any cardholder verification required will be prompted when proceeding on to the payment transaction stage.

IPC handles fallback within the Checkcard without interaction with the EPOS application i.e. if the Chip is not readable, IPC will cause the PED to prompt for a Card Swipe; if a Magnetic Swipe card fails on card swipe, IPC will cancel the transaction and send the transaction response back to the EPOS application.

Please note therefore that there is no fallback to keyed entry when using Checkcard.

Also note, There are no IntraMessage port messages during the fallback event.

If the EPOS application wishes to continue the financial transaction with the tendered card then the request below should be sent

Sale Request

1=123 (This must be same as check card request)
2=0
3=10.00
99=0

If the EPOS application wishes to break or exit immediately from waiting state then a 'Sale' or any other request can be sent with a different transaction reference number to the one used in 'Check Card' request. This will cause the Check Card process to terminate immediately and prompt the cardholder to remove their card

Break Transaction Request

1=124
2=0
99=0

Response

13=23000081
3=10
2=14
8=29072014
9=111913
98=123
99=0

8.4.11 Transaction Type CheckStatus

The CheckStatus request can be used to check the IPC status. There are only two states, which may be returned in the result: Status Busy and Status Not Busy.

Request

1=1234

2=34

99=0

Response

3=43

99=0

8.4.12 Transaction Type Check Pinpad Connection

The Check pinpad connection request can be used to check the pinpad is connected with IPC or not. There are only two states which are returned in the result, they are the pinpad is connected (45) and pinpad is not connected (44).

Request

1=12345

2=24

99=0

Response

2=24

3=45

13=22980045

98=12345

99=0

8.4.13 Transaction Type Print Duplicate Merchant Receipt

The Printing Duplicate Merchant can be used to print Merchant Receipt of the last transaction available to IPC. If IPC has been restarted since the last transaction there will be no transaction available to IPC and below response will be returned by IPC. The response message is as shown below. Please note that for this transaction the value of attribute 1, Transaction Reference, has no significance and any value can be used: IPC always references the last transaction performed.

Request

1=121

2=22

99=0

Response

2=22

3=10

13=22980045

98=121

99=0

8.4.14 Transaction Type Print Duplicate Customer Receipt

The Printing Duplicate Customer can be used to print Customer Receipt of the last transaction available to IPC. If IPC has been restarted since the last transaction there will be no transaction available to IPC and below response will be returned by IPC. The response message is as shown below. Please note that for this transaction the value of attribute 1, Transaction Reference, has no significance and any value can be used: IPC always references the last transaction performed.

Request

1=1234
2=23
99=0

Response

2=23
3=10
13=22980045
98=1234
99=0

8.4.15 Transaction Type Get Number of Offline Stored Transactions

The Get Number of Offline Stored Transactions can be used to get total number of offline stored transactions. The status returned in the result will have one of two values: successful, in which case the total number of offline stored transactions is returned in field 75; or failure, if the transaction log file is corrupted.

Request

1=1010
2=25
99=0

Response

2=25
3=10
13=22980045
75=5
98=1010
99=0

8.4.16 Transaction Type Get Pinpad Serial Number

The Get Pinpad Serial number Transaction can be used to get serial number of connected pinpad with IPC.

Request

1=111

2=26

99=0

Response

2=26

3=10

13=22980045

76=123456789

98=111

99=0

8.4.17 Transaction Type Get Territory

The Get Territory Transaction can be used to get Acquirer Name.

Request

1=111

2=15

99=0

Response

98=1234

2=15

13=23000081

65=WorldPay US Test

8=29072014

9=111913

3=10

99=0

8.4.18 Transaction Type Cash transaction

If merchant is taking payment in Cash, It can be recorded to WPH server by Cash transaction request and can be viewed on merchant portal.

Cash tender amount (Field 20) must be equal to or greater than Goods amount (Field 3).

Request

1=113

2=0

3=35.50 (Goods amount)

20=50.00 (Cash tender)

28=1

99=0

Response

5=000000XXXXXX0000

1=21
22=Kinetic Business Centre Theobald Street Elstree Hertfordshire WD6 4PJ
12=6818780
23= Worldpay HSBC Agent
13=22980045
8=02012014
3=2
21=2
9=100126
2=0
36=129
38=3550
41=0
98=113
99=0

8.4.19 Transaction Type Close IPC

The close IPC request can be used to close IPC if it is running. There is no response is generated for this request.

Request

1=1200
2=99
99=0

8.4.20 X Report

The X Report returns the current totals in the terminal batch in an XML format. This is an online function only. If the network is not available then the transaction will be cancelled and no report data will be returned in response.

Request

1=2217
2=36
3=0
99=0

Response

1=0
2=36
13=22980045
41=0
19=47959
18=245099
17=8

16=71

25=541505

```
48=<BatchReport><FCR>541505</FCR><ReportDate>15102007</ReportDate><Report><CardScheme>Delta</CardScheme><CreditCount>0</CreditCount><CreditTotals>0</CreditTotals><DebitCount>3</DebitCount><DebitTotals>900</DebitTotals></Report><Report><CardScheme>Visa</CardScheme><CreditCount>7</CreditCount><CreditTotals>47264</CreditTotals><DebitCount>33</DebitCount><DebitTotals>203726</DebitTotals></Report><Report><CardScheme>MasterCard</CardScheme><CreditCount>1</CreditCount><CreditTotals>695</CreditTotals><DebitCount>35</DebitCount><DebitTotals>40473</DebitTotals></Report></BatchReport>
```

98=2217

99=0

8.4.21 Z Report

The Z Report returns the current totals from the terminal batch in an XML format and also closes the terminal batch. This is an online function only. If network is not available then transaction will be cancelled and no report data will be returned in response.

Request

1=2218

2=37

3=0

99=0

Response

1=0

2=37

13=22980045

41=0

19=47959

18=245099

17=8

16=71

25=541505

```
48=<BatchReport><FCR>541505</FCR><ReportDate>15102007</ReportDate><Report><CardScheme>Delta</CardScheme><CreditCount>0</CreditCount><CreditTotals>0</CreditTotals><DebitCount>3</DebitCount><DebitTotals>900</DebitTotals></Report><Report><CardScheme>Visa</CardScheme><CreditCount>7</CreditCount><CreditTotals>47264</CreditTotals><DebitCount>33</DebitCount><DebitTotals>203726</DebitTotals></Report><Report><CardScheme>MasterCard</CardScheme><CreditCount>1</CreditCount><CreditTotals>695</CreditTotals><DebitCount>35</DebitCount><DebitTotals>40473</DebitTotals></Report></BatchReport>
```

98=2218

99=0

8.4.22 Tokenization Of Card Numbers

IPC provides a Tokenization mechanism for card numbers.

The WPH system can create a unique Token reference for an IPC card present transaction if the merchant is configured on WPH for token creation.

The WPH token references the customer's card details to enable payment through the card by the merchant at a later date, without a requirement to retrieve the PAN, or to have the cardholder present. Examples are CCA (Continuous Charge Authority) payments for hire-purchase type transactions.

The merchant application can use IPC transaction types 12 or WPH HTTPS POST method to charge a card using the token reference.

Below is the attribute returned by IPC for a Token in the Response:

Description	Attribute Name
Token Reference (e.g.: 532931432DB44ABB5)	61

8.4.23 Sample Request for Charging a Token

Transaction type 12 can be used for charging a token through IPC. Mandatory elements required are Token Reference and amount.

Request

1=3101
2=12
3=10.00
19=532931432DB44ABB5
99=0

Response

7=30121899
4=005872
14=7
1=81
22=Kinetic Business Centre Theobald Street Elstree Hertfordshire WD6 4PJ
12=79808991
23=YESpay HSBC Agent
28=PGTR281978350
13=22980071
8=10102014
3=1
9=082141
2=12
34=PLEASE DEBIT MY ACCOUNT

33=PLEASE KEEP THIS RECEIPT FOR YOUR RECORDS
36=121
38=1000
41=0
61=532931432DB44ABB5
59=00
98=3101
99=0

8.4.24 Sample Request to Refund a Token

Transaction type 13 can be used for refunding to a token through IPC. A refund via the token can be performed for a previously completed sale transaction or a sale performed with a token

Mandatory elements required for the requests are Amount, PGTR of previously completed sale transaction & token reference.

Multiple refunds can be done for the previously completed sale transaction but the sum total of all the refunds have to be equal to or less than the sale amount.

Request

1=3101
2=13
3=5.00
13=PGTR61734250
19=532931432DB44ABB5
99=0

Response

7=30121899
4=05017
14=7
1=81
22=Kinetic Business Centre Theobald Street Elstree Hertfordshire WD6 4PJ
12=79808991
23=YESpay HSBC Agent
28=PGTR697126959
13=22980071
8=10102014
3=1
21=1
9=082320
2=13
34=PLEASE CREDIT MY ACCOUNT
33=PLEASE KEEP THIS RECEIPT FOR YOUR RECORDS
36=122
38=500

[illegible]

8.4.25 Sale with Dynamic Currency Conversion (DCC)

IPC supports DCC transactions to provide merchants a service that allows card holders to pay for goods and services internationally with their local currency.

Request

1=231234
2=0
3=50
99=0

Response

7=01042002
29=A0000000031010
6=VISA
5=492949XXXXXX2008
4=729945
10=BMSTESTCARDG6091/G
14=2
1=5
22=Checknet House, 153 East Barnet Road, Barnet EN4 8QZ
12=6818780
23= Worldpay Retail
28=PGTR13513393
13=22980045
8=07092009
3=1
21=1
9=172748
2=0
34=PLEASE DEBIT MY ACCOUNT
33=PLEASE KEEP THIS RECEIPT FOR YOUR RECORDS
36=5
37=0101
38=1099
41=0
60=004

70=HKD

71=905.83

72=12.0777

98=231234

99=0

8.4.26 Transaction Type Last Transaction Result

To find out the result of last transaction, transaction type 35 can be used. If the IPC instance has been restarted since the last transaction, there will be no result available and the IPC response message indicates this as below. Please note that for this transaction the value of attribute 1, Transaction Reference, has no significance and any value can be used: IPC always references the last transaction performed.

Request

1 = 231224

2 = 35

99 = 0

Response (When Last transaction response is present in IPC)

7=01042002

29=A0000000031010

6=VISA BARCLAYCARD

5=492949XXXXXX2008

4=729945

10=BMSTESTCARDG6091/G

14=2

1=5

22=Checknet House, I53 East Barnet Road, Barnet EN4 8QZ

12=6818780

23= Worldpay Retail

28=PGTR13513393

13=22980045

8=07092009

3=1

21=1

9=172748

2=0

34=PLEASE DEBIT MY ACCOUNT

33=PLEASE KEEP THIS RECEIPT FOR YOUR RECORDS

36=5

37=0101

38=1099

$$\begin{aligned} 1 &= 0 \\ 2 &= 0 \\ 41 &= 0 \\ 99 &= 0 \end{aligned}$$

8.4.27 Transaction Type TaxFree Voucher for Cash Transaction

TaxFree voucher generation is a mechanism to generate TaxFree Voucher for a cash transaction. It will be applicable only if merchant is enabled for TaxFree Voucher. The TaxFree voucher text will be generated in a file (VATRefundVoucher.txt) under \YESEFT folder. Each text line of VATRefundVoucher.txt file is preceded by formatting character which is used for printing. The formatting character details are given in the APPENDIX (H).

Request:

1=2345

2=8

3=50.50

99=0

Response:

1=0

22=153 East Barnet Road Barnet Hertfordshire Hertfordshire EN4 8QZ

12=6818780

23=First Retailer Site

13=22980046

8=13052010

3=1

9=105700

2=8

41=0

98=2354

99=0

8.5 IPC Updates

IPC Software and PED firmware updates are provided from the WPH. The IPC software manages the process of downloading and deploying its software upgrades, and the firmware upgrades for the connected PED.

8.5.1 Connections to enable Upgrade

The software and firmware upgrade components are downloaded from url www.yes-pay.net/downloads via https connection. Connection via TLS is supported, however SSL connection is not supported.

The certificate that enables the https connection is based on the domain name www.yes-pay.net.

For networks that do not support DNS, please ensure that you create an entry in the `hosts` file of the IPC host machine to map the domain name www.yes-pay.net to its ip address. This will allow the ip address to be resolved to the domain name and allow the https handshake to succeed

Hosts file entries

1. Go to below location

Windows: - C:\Windows\System32\Drivers\etc

Linux: - /etc/

2. Open the file called hosts and add below entries at the end of the file.

194.72.158.227 primary.yes-pay.net

80.69.5.198 www.yes-pay.net

Note 1: on some Windows systems, similar changes might be needed in file `lmhosts`

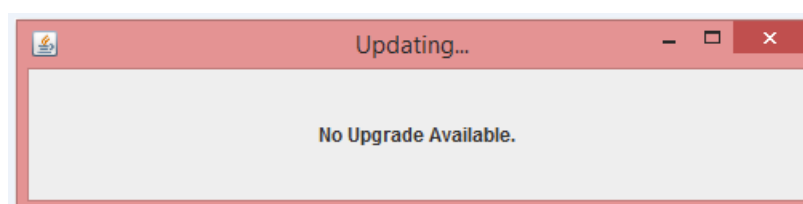
Note 2: If it is necessary to define entries in hosts file as described above please be aware that these might need to change in future if the ip address of the WPH domains change. Worldpay will advise in advance if such ip address changes are planned.

8.5.2 Software Upgrade

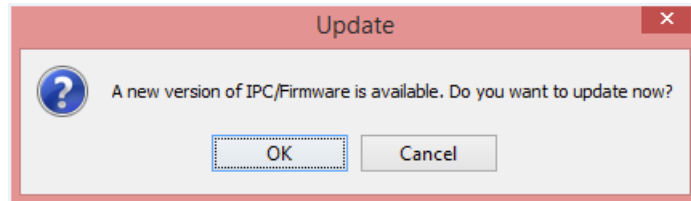
Step 1

At the time of initialisation a check is made by IPC with the WPH for availability of software and firmware updates.

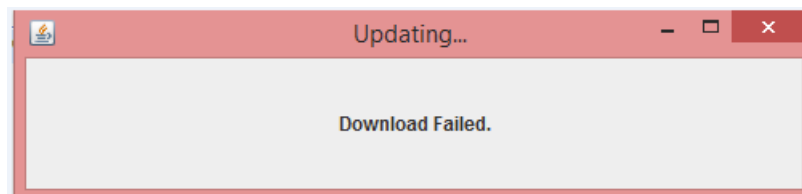
If no software upgrade is available, or the IPC software version is already updated to the latest version, the message below is shown



If an upgrade is available IPC will commence the upgrade process. Depending on the the setting of the Auto Upgrade flag in IPC configuration, Software Upgrade (see section 4.3.8), IPC will prompt for the upgrade to be accepted before proceeding

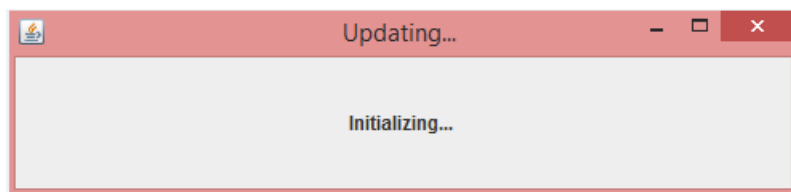


If any problem occurs during the installation of the software upgrade IPC will show the message below.



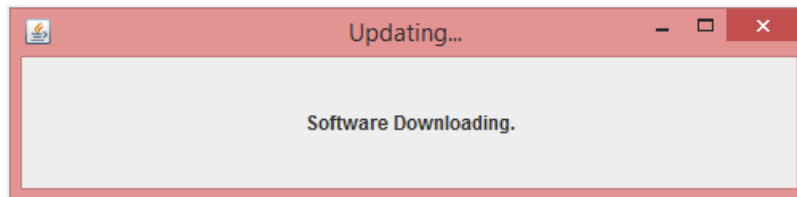
Step 2

The message below appears at the time of Initializing Software Upgrade component



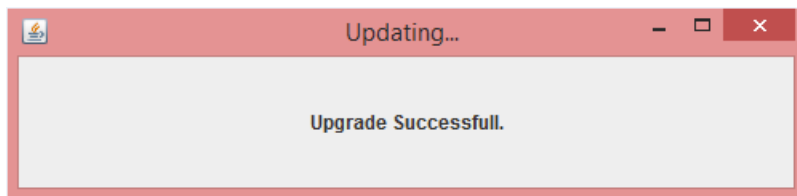
Step 3

When Software Download from Server begins the message below appears



Step 4

On completion of the IPC software upgrade the message below will be shown

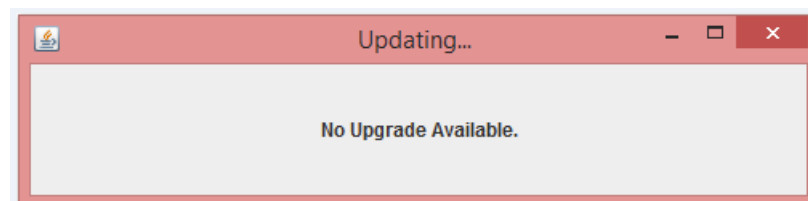


8.5.3 Firmware Upgrade

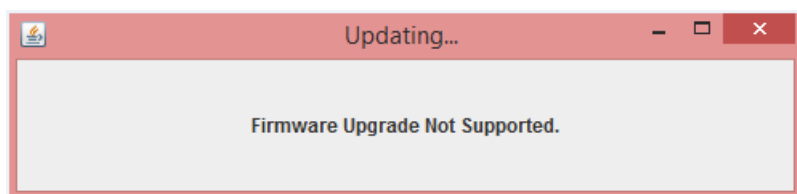
Step 1

At the time of initialisation a check is made by IPC with the WPH for availability of software and firmware updates.

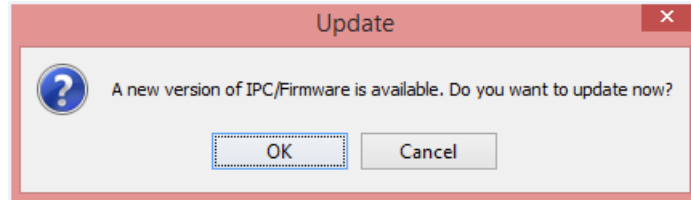
If no firmware upgrade is available, or the IPC firmware version is already updated to the latest version, the message below is shown



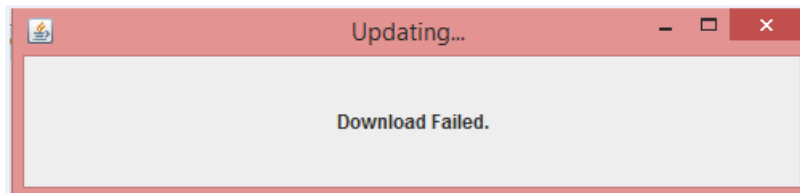
The firmware upgrade functionality is supported with IPP350 and Vx820-7816 PED. If any other PED device is configured IPC will display an error message



If an upgrade is available IPC will commence the upgrade process. Depending on the the setting of the Auto Upgrade flag in IPC configuration, Software Upgrade (see section 4.3.8), IPC will prompt for the upgrade to be accepted before proceeding

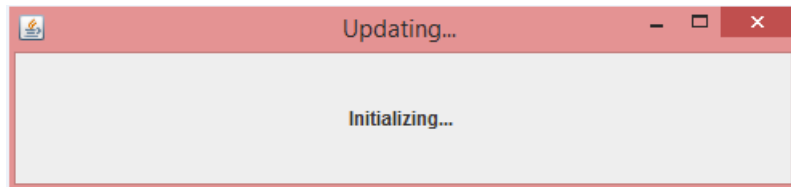


If any problem occurs during the installation of the firmware upgrade IPC will show the message below.



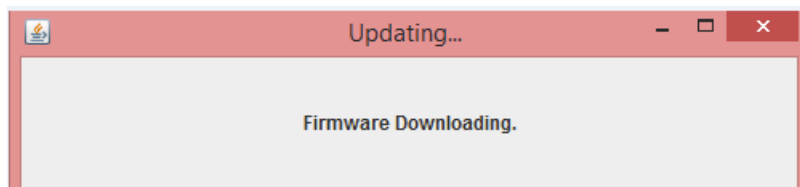
Step 2

The message below appears at the time of Initializing the PED Firmware Upgrade component



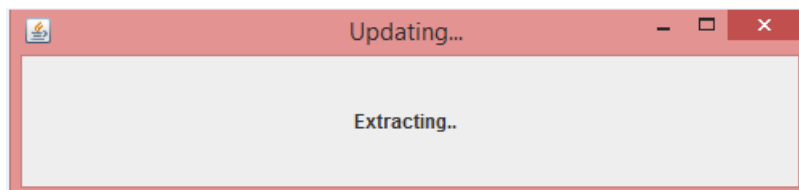
Step 3

When the PED Firmware Download from Server commences the prompt below appears



Step 4

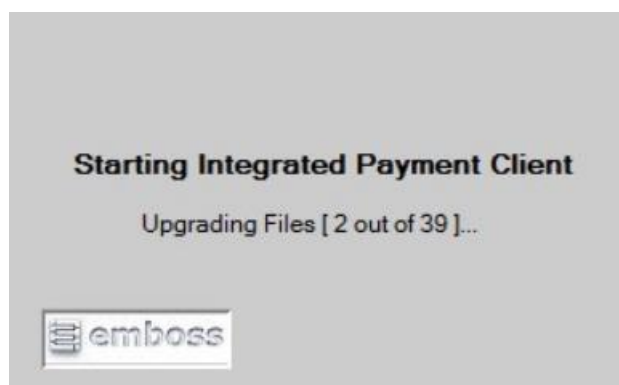
Upon successful download, the firmware patch is extracted into FirmwareUpgrade folder of YESEFT. The message below is shown



Step 5 & 6 are applicable for Ingenico PEDs and step 7 to step 17 are applicable for Verifone Vx820-7816 PED.

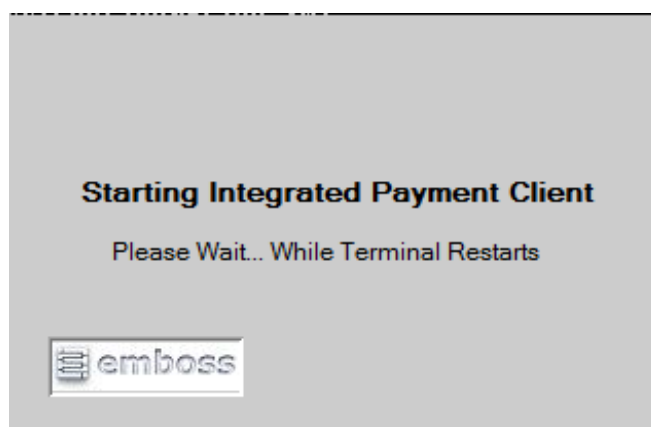
Step 5

Once the extraction of the firmware patch is complete the upgrade process begins and the message below appears

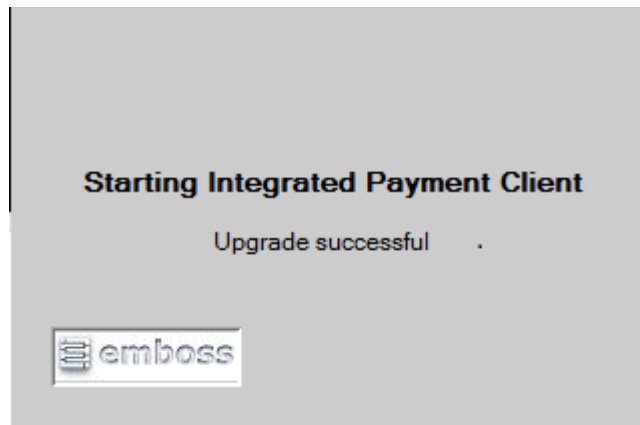


Step 6

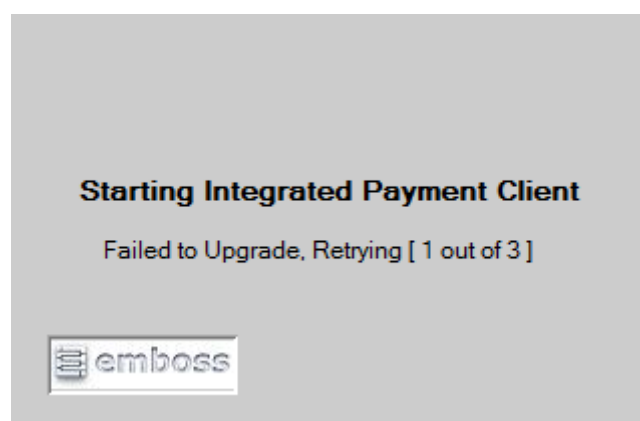
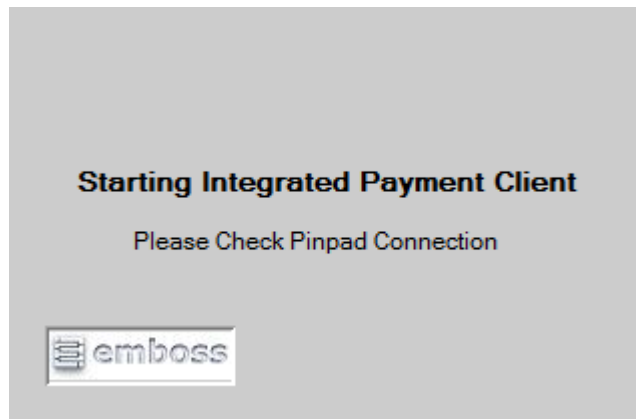
When all the files download successfully into the PED, the PED restarts and displays the prompt below.



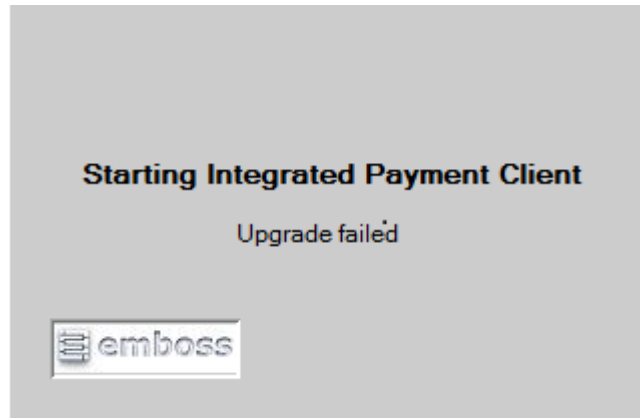
After successful upgrade below prompt is displayed.



If the Firmware Upgrade process should fail, which could happen due to communication failure between IPC client and PED, then IPC displays the prompt below and retries 3 times to download firmware files into PED.



If after 3 attempts the firmware upgrade has not been successful, IPC displays the prompt below and exits from the upgrade process.



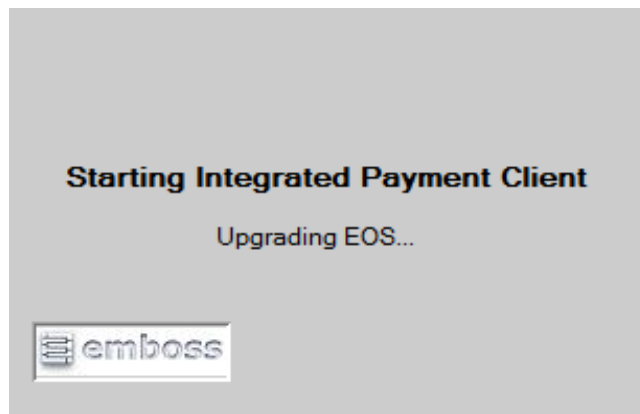
Step 7

Firmware Upgrade process for Vx820-7816

There are five components to upgrade pin-pad software of Vx820-7816 which are:- EOS -> OS -> CTLS -> VIPA->Whitelist.

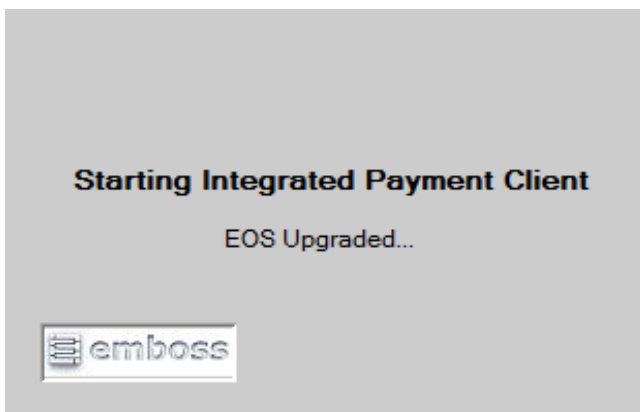
For Vx820-7816 firmware upgrade process step 1 to step 4 is same as above section 8.5.1. Below are the further steps.

Once the extraction of the firmware patch is complete the upgrade process begins and below message appears with EOS upgrade.



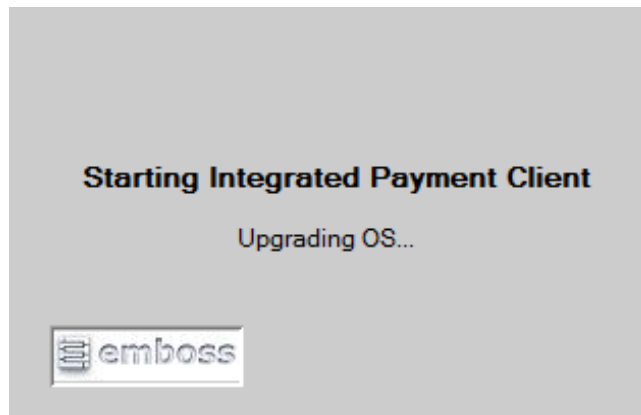
Step 8

As EOS process completes below message will be appear .



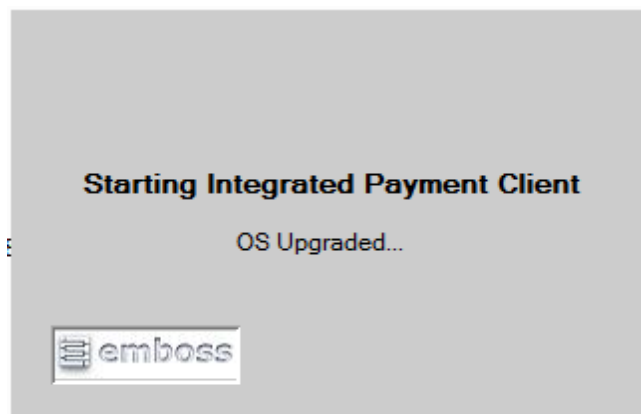
Step 9

After successful EOS completion, OS process begins & below message appears.



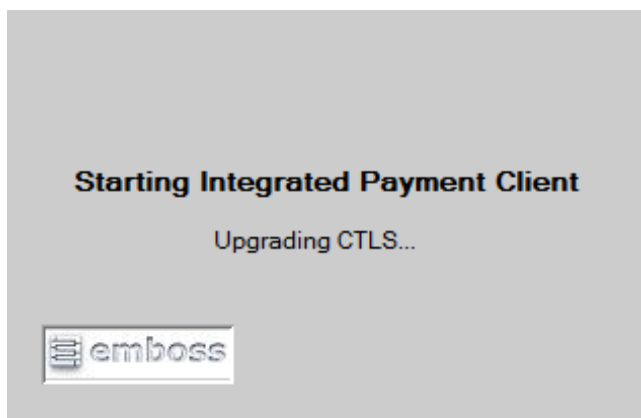
Step 10

As OS process completes below message will be appear.



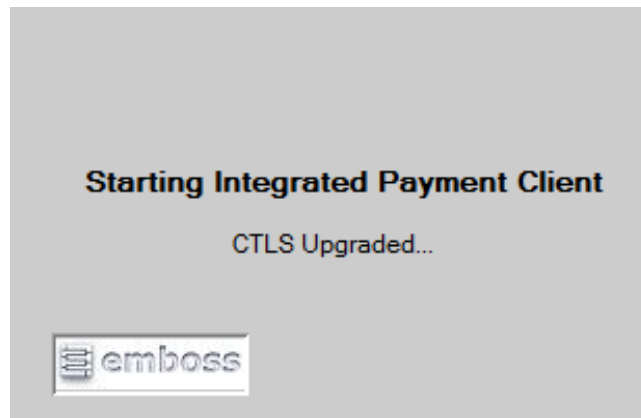
Step 11

After successful OS completion, CTLS process begins & below message appears.



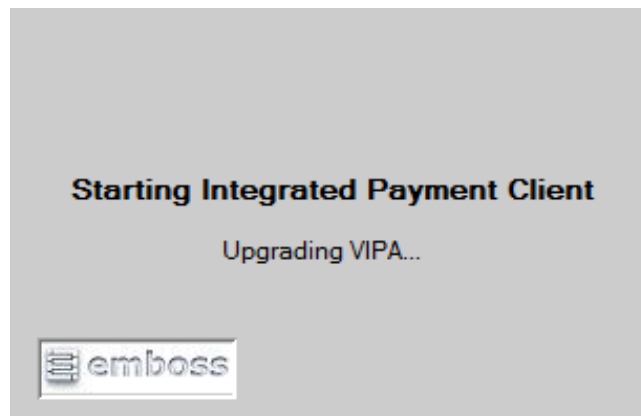
Step 12

As CTLS process completes below message will be appear.



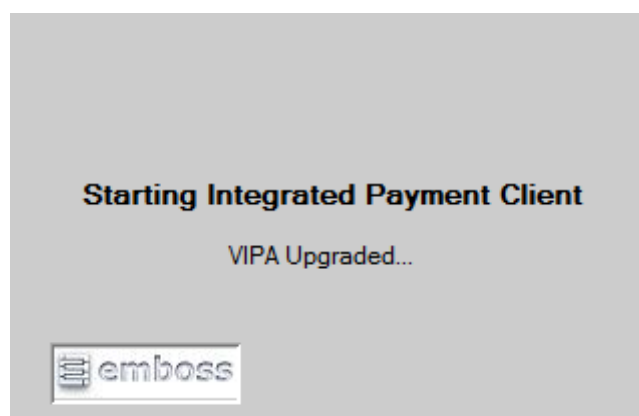
Step 13

After successful CTLS completion, VIPA process begins & below message appears.



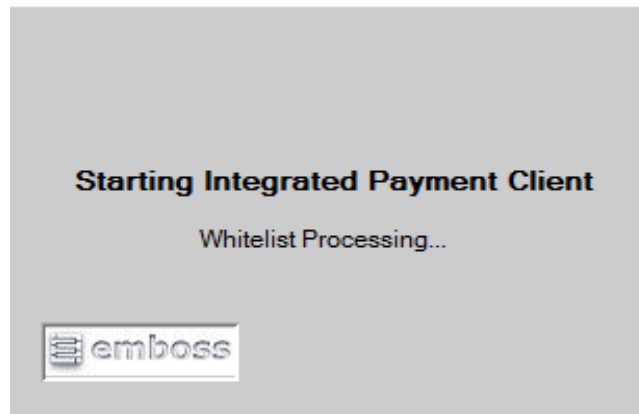
Step 14

As VIPA process completes below message will be appear.



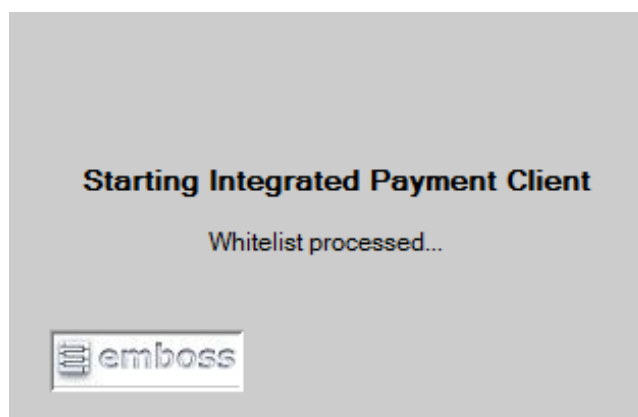
Step 15

After successful VIPA completion, Whitelist downloading process begins & below message appears.



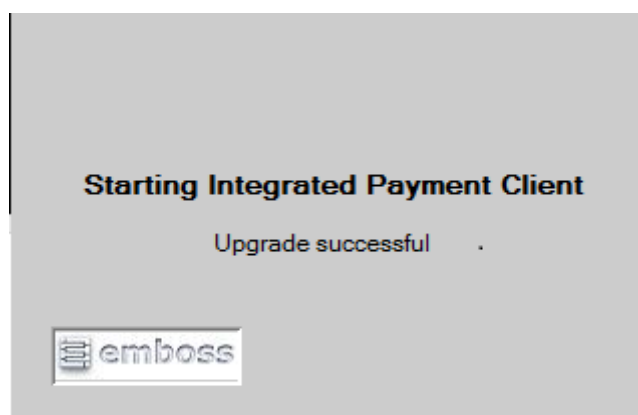
Step 16

As Whitelist download completes into the PED below message will be appear.



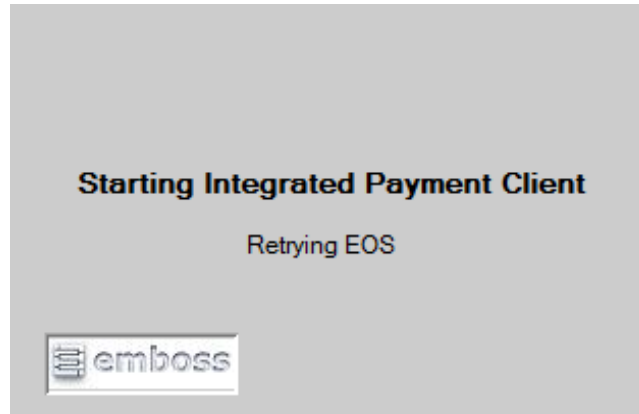
Step 17

When all the components upgraded successfully into the PED. PED restarts and after successful upgrade below prompt is displayed.



If Firmware Upgrade process fails at any component due to fail in command API process into PED then IPC retry once again that running component.

For ex: If upgrade is failed at EOS then below message appears.



Rollback of firmware Upgrade :- Ingenico PEDs has capability to rollback automatically to original firmware version but Vx820-7816 PED doesn't have.

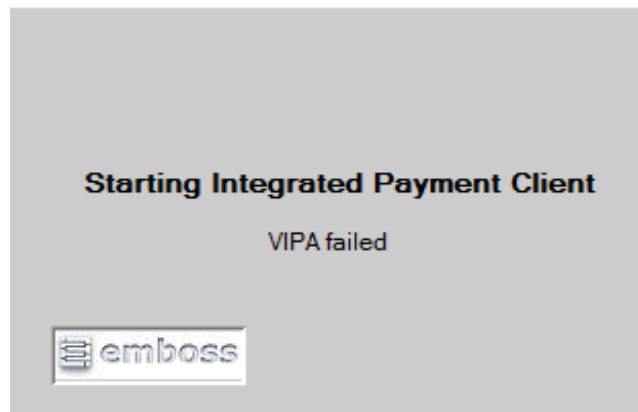
IPC have capability to roll back or downgrade Vx820-7816 PED to its previous version. Firmware Upgrade folder contains 3 sub folders which are :-

upload whitelist, VIPA_4056 & VIPA_4056to4057, VIPA_4056to4057 for upgrade and VIPA_4056 for downgrade.

Following are the steps for downgrade :-

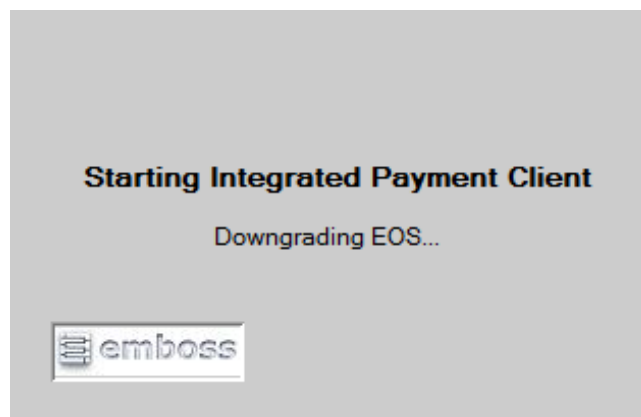
Step 1

If VIPA failed in between then below message appears then IPC downgrade all four components starts from EOS, OS, CTLS to VIPA.



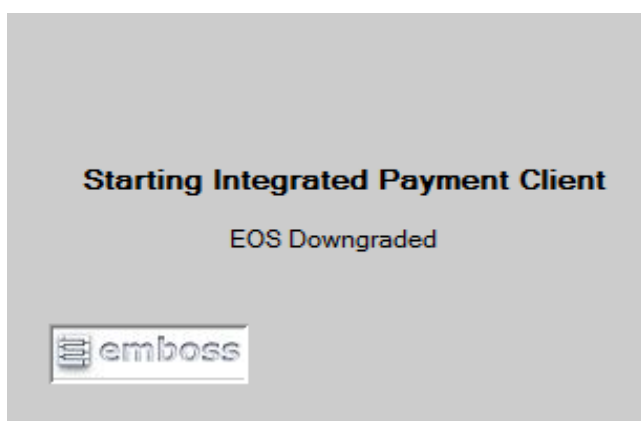
Step 2

IPC starts to downgrade EOS & below message appears.



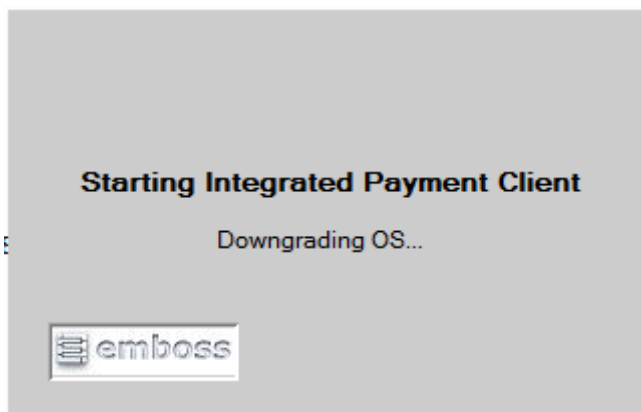
Step 3

As EOS downgrade successful then below message appears.



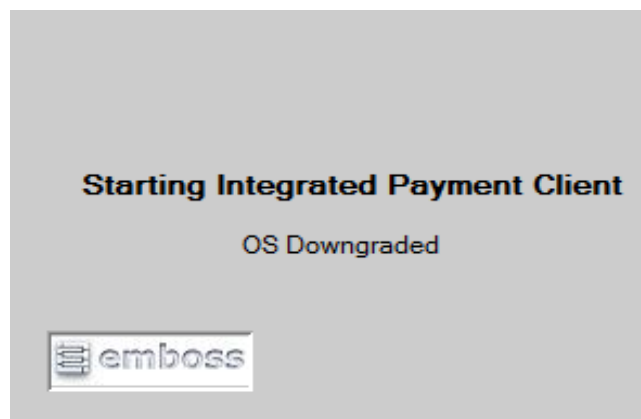
Step 4

After successful downgrade of EOS, IPC starts to downgrade OS and below message appears.



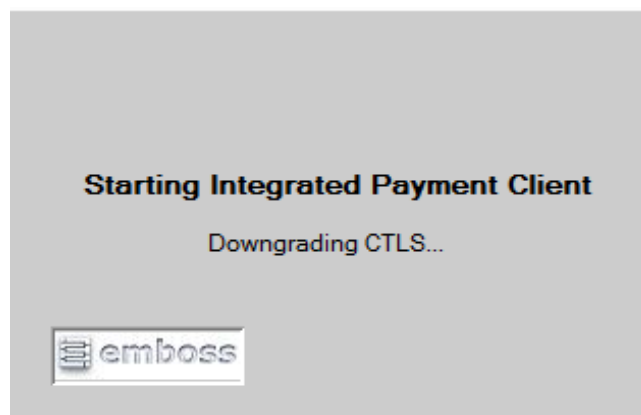
Step 5

As OS downgrade successful then below message appears.



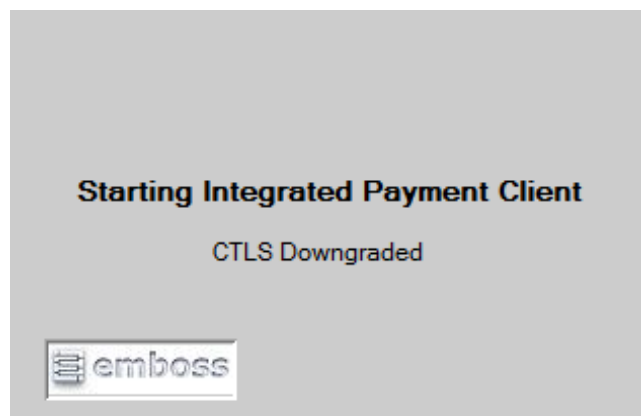
Step 6

After successful downgrade of OS, IPC starts to downgrade CTLS and below message appears.



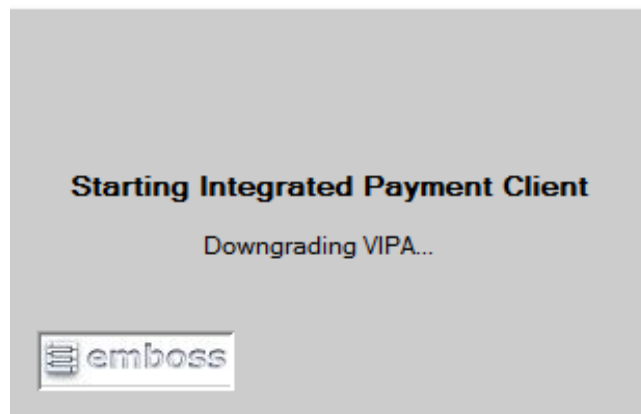
Step 7

As CTLS downgrade successful then below message appears.



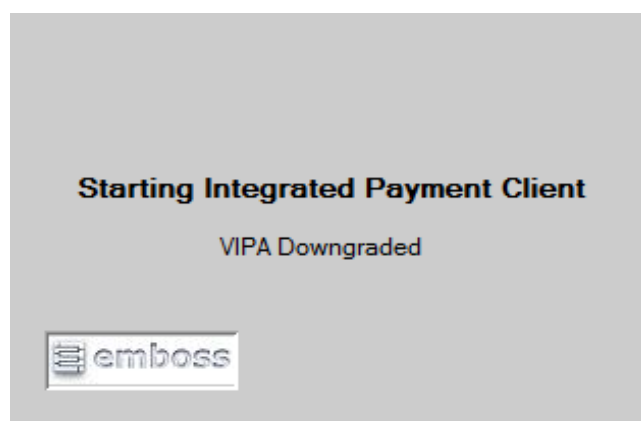
Step 8

After successful downgrade of CTLS, IPC starts to downgrade VIPA and below message appears.



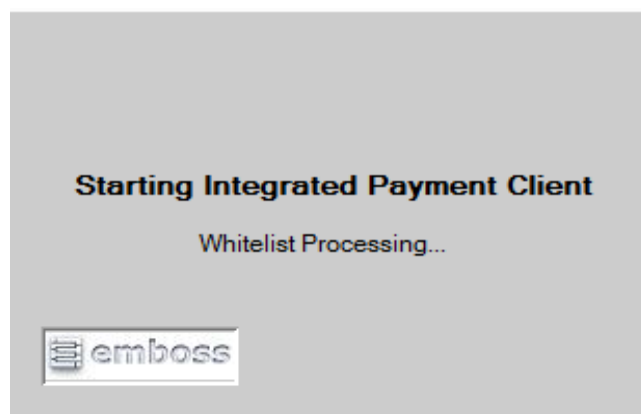
Step 9

As VIPA downgrade successful then below message appears.



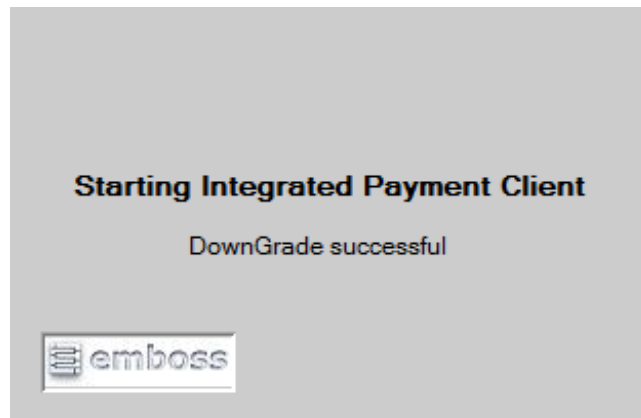
Step 10

After successful downgrade of VIPA, IPC starts to update whitelist file into PED and below messages appear.



Step 11

After successful downgrade below messages appear.



8.6 Proxy Settings for IPC

IPC also supports use of http/https Proxy Server. To enable IPC to work through a proxy server the Proxy Host address and Proxy port are entered in the ProxySetting properties file.

This file resides in YESEFT/properties folder. The File name is ProxySetting.properties. Below is the required entry that should be present in the file :

proxyhost= 'Enter proxy host here'

proxyport= 'Enter proxy port here'

8.7 Customer Image/Logo Display

IPC allow customers to load their logo on home screen of Verifone Vx820-7816 PED and image or SlideShow onto the home screen of Ingenico IPP350 PED.

8.7.1 Customer Image display on IPP350 PED

Images Specification -

- Supported image format - BMP with 24 bit (3 byte) bitmaps.
- Dimension - width*height – 320*240 pixels (1/4 VGA) .
- File size - 230,454 bytes max.
- Resolution - 72 x 72 dpi at maximum colour depth.

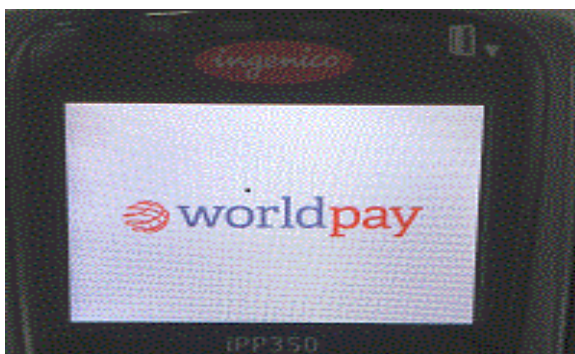
IPC-2 Manual Setup and Configuration -

- IPC-2 installer by default configure to load WorldPay image.
- Customer can manually replace their images on YESEFT/images/screensaverImages/Ingenico folder.
- The naming convention of images will be WPCTxx. Ex: - WPCT00.BMP, WPCT01.BMP, WPCT02.BMP.
- All images names should be in sequence. Ex: - WPCT00, WPCT01, WPCT02 and so on.
- Maximum number of images supported are 10 (00 to 09).
- Images can be added, modified or deleted from the folder.
- IPC-2 can be configure for idle time through configuration utility. The default is 10 seconds and it can be configure from 10 to 999 seconds.

Image display during start-up and transaction flow -

- IPC-2 will load the image on PED on two scenarios –
 3. Customer starts the IPC-2 first time.
 4. Customer modify ,add or delete images and restart IPC-2.
- Each image load on PED may take approximately 3 minutes.
- IPC-2 will display images on PED when there is no transaction is processing and then will wait for idle time out period to elapse.

WorldPay Image



Error Condition -

IPC-2 will not display any image and show an error message “Image Failed in Validation” if sequence number is incorrect or image validation fails. In this case IPC-2 will start with default ingenico screen saver or with last loaded image.

8.7.2 Customer logo display on Vx820-7816 PED

logo Specification -

- Supported image format - PNG
- Dimension - width*height – 180*33 pixels

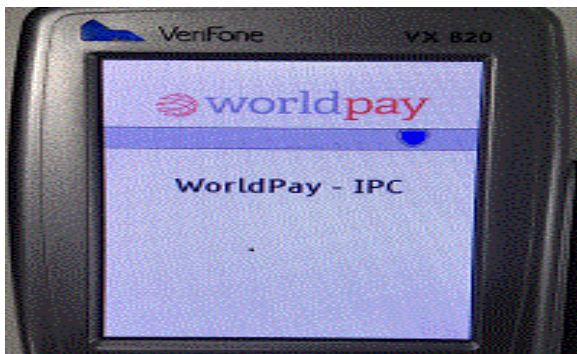
IPC-2 Manual Setup and Configuration -

- IPC-2 installer by default configure to load WorldPay logo.
- Customer can manually replace their logo on YESEFT/images/ screensaverImages/Verifone folder.
- The naming convention of logo will be vfLogo. Ex: - vfLogo.PNG.

logo display during start-up and transaction flow -

- IPC-2 will load the logo on PED on two scenarios –
 5. Customer starts the IPC-2 first time.
 6. Customer modify ,add or delete logo and restart IPC-2.
- Loading of logo on PED may take approximately 1.5 minutes.
- IPC-2 will display logo on PED after initialization and during transaction flow.

WorldPay Logo



Error Condition -

IPC-2 will not display any logo and show an error message “Image Failed in Validation” if image validation fails. In this case IPC-2 will start without logo or with last loaded logo.

9 Appendix F - IPC Receipt Generation

IPC provides formatted text only receipts either on a socket or a file. In attended mode two receipts are returned: the Merchant and the Customer receipts. In case of a Kiosk or Semi-Attended mode only a Customer receipt is returned.

Below are the attributes of an EFT receipt. Please note that these are subject to change in future releases of IPC in compliance with requirements from UK APACS.

UK APACS Receipt Format

Mandatory (APACS) Fields		Property
1	Merchant/Outlet Number	MerchantID
2	Merchant Name	MerchantName
3	Merchant Address	MerchantAddress1, MerchantAddress2, City, State, ZipCode
4	Transaction Type e.g. SALE / REFUND	TransactionType
5	Card Number (PAN) - Truncated * See Note 1 *	AppIPAN
7	Transaction Data Source e.g. ICC, SWIPE, KEYED	ChipStripeorKeyed
8	Date of Transaction	TransactionDate
9	Terminal Number (TID)	TerminalID
10	Transaction Number	TransactionSeqNo or TransactionReference
11	Transaction Response e.g. Auth Code	AuthCode
12	Amount of Transaction (Inc. currency symbol)	Amount
13	Request for Signature (not required for PIN Transactions replaced by 17)	N/A
14	Space for Signature (nor required for PIN Transactions replaced by 17)	N/A
15	Declaration e.g. Please debit my account	N/A
16	Retention Reminder	N/A
17	Amount of Cash (for Purchase With Cashback transaction)	AmountOther
18	PIN Verified Statement	N/A

Mandatory (APACS) Fields		Property
19	Application Identifier	applID
20	Gratuity Amount (where a gratuity amount is added to the original amount)	AmountGratuity
21	Diagnostic Message	N/A
23	Card Issue No / Sequence No - App PAN Sequence No for ICC Transactions	ApplPANSeqNo
24	Time of Transaction	TransactionTime
25	Application Preferred Name*	ApplPreferredName

*If the Application Preferred Name is not provided, or not readable from the card, the Application Label is provided on the receipt.

Optional		Property
1	Card Scheme Name	ApplLabel
2	Courtesy Message	N/A
3	Receipt Number (not transaction number)	N/A
4	Goods Amount	N/A
5	Goods Description	N/A
6	Hot Card File Version No	HotCardVerNo
7	Term Software Version No	TermSoftVerNo

IPC provides receipts in two text files in the receipt folder as configured in the YESEFTConfig:

MainReceipt.txt – Merchant receipt

CustomerReceipt.txt – Customer receipt

IPC also provides receipts on a socket connection, if configured via YESEFTConfig.

IPC provides a configuration option to suppress the Merchant receipts. If this option is chosen then Merchant receipts are not issued EXCEPT where signature verification is required.

In case of signature verification, the Merchant receipt is received first from IPC. There is a possibility that the EPOS application may receive another Merchant receipt if the attendant rejects the signature verification on the IPC prompt. The Customer receipt follows the Merchant receipt(s).

Below is a sequence of steps that needs to be followed for receipt printing if the EPOS application is printing the receipts.

- Check for Merchant Receipt
- On receiving Merchant Receipt, print the receipt.

- Check for Merchant Receipt or Customer Receipt.
- If Merchant Receipt, print the receipt and then wait for Customer receipt.
- If Customer receipt, print the receipt and wait for response.

The IPC transaction response is issued at the end of the transaction. There will be no more receipts after the response message is issued.

The receipts are validated as compliant EMV receipts as part of the accreditation process that IPC undergoes with the acquiring banks. All the information contained within the IPC Customer receipt should be printed by the EPOS application. The Customer receipt text should be at least 2.55mm in height and not narrower than 15 characters per inch. The EPOS application should print Customer receipts from all transactions where IPC issues such a receipt.

The examples below show typical Merchant and Customer receipts generated by IPC for a Chip&PIN transaction.

1. Receipts in Text Files *MainReceipt.txt* and *CustomerReceipt.txt*

```
CUSTOMER RECEIPT
YESPAY DEMO
153 CHECKNET HOUSE EAST BARNET ROAD
BARNET HERTS EN4 8QZ
06/11/2013 01:47:34
RECEIPT NO.: 3
MID:XXX49873                      TID:XXXX0012
AID:A0000000041010
MASTERCARD
XXXX XXXX XXXX 0020
PAN SEQ NO. : 00
ICC
SALE                               GBP100.00
TOTAL                             GBP100.00
PLEASE DEBIT MY ACCOUNT
PIN VERIFIED
PLEASE KEEP THIS RECEIPT FOR YOUR
RECORDS
AUTH CODE: 007054
```

```
MERCHANT RECEIPT
YESPAY DEMO
153 CHECKNET HOUSE EAST BARNET ROAD
BARNET HERTS EN4 8QZ
06/11/2013 01:47:34
RECEIPT NO.: 2
MID:21249872                      TID:22980012
AID:A0000000041010
MASTERCARD
XXXX XXXX XXXX 0020
PAN SEQ NO. : 00
ICC
SALE                               GBP100.00
TOTAL                             GBP100.00
PLEASE DEBIT MY ACCOUNT
PIN VERIFIED
PLEASE KEEP THIS RECEIPT FOR YOUR
RECORDS
AUTH CODE: 007054
```

2. Receipts from the Receipt Socket port

Receipts issued on the Receipt Socket port are prefixed by labels CUSTOMER: and MERCHANT: so that their start point may be readily identified in the stream of data from the socket. These labels should be removed from the receipt data and not printed.

```
CUSTOMER:CUSTOMER RECEIPT
YESPAY DEMO
153 CHECKNET HOUSE EAST BARNET ROAD
BARNET HERTS EN4 8QZ
06/11/2013 01:47:34
RECEIPT NO.: 3
MID:XXX49873 TID:XXXX0012
AID:A0000000041010
MASTERCARD
XXXX XXXX XXXX 0020
PAN SEQ NO. : 00
ICC
SALE GBP100.00
TOTAL GBP100.00
PLEASE DEBIT MY ACCOUNT
PIN VERIFIED
PLEASE KEEP THIS RECEIPT FOR YOUR
RECORDS
AUTH CODE: 007054
```

```
MERCHANT:MERCHANT RECEIPT
YESPAY DEMO
153 CHECKNET HOUSE EAST BARNET ROAD
BARNET HERTS EN4 8QZ
06/11/2013 01:47:34
RECEIPT NO.: 2
MID:21249872 TID:22980012
AID:A0000000041010
MASTERCARD
XXXX XXXX XXXX 0020
PAN SEQ NO. : 00
ICC
SALE GBP100.00
TOTAL GBP100.00
PLEASE DEBIT MY ACCOUNT
PIN VERIFIED
PLEASE KEEP THIS RECEIPT FOR YOUR
RECORDS
AUTH CODE: 007054
```

10 Appendix G - IPC console Message to socket interface

IPC provides a mechanism to emulate the IPC window (GUI) by providing a mechanism to send the IPC messages to, and take command inputs from, an EPOS application.

IPC can be configured to send the GUI messages on a TCP/IP socket called the IntraMessage port. The messages correspond to the prompts displayed to the EPOS operator via the IPC UI window.

To receive and respond to the messages, the EPOS application connects to the designated IntraMessage port in client mode. The IntraMessage port is a separate port to the Request and Receipt ports, and is configurable through the YESEFTConfig utility.

IntraMessage port messages, in common with all socket messages from IPC, are in the form of key values separated by a linefeed character (Hex. 0A). IntraMessage port messages are terminated with the characters 99=0 (Hex. 39 39 3D 30).

There are two kinds of IntraMessage port messages sent by IPC: synchronous and asynchronous mode.

10.1 Asynchronous Mode

Messages in asynchronous mode advise progress of the transaction and require no response from the EPOS application. The message is in the form of key value that can be used to look up the full message text in file YESEFT/properties/MessageBundle_en_GB.properties. The POS application can choose to display the message text from the file, or replace it with its own preferred text.

The asynchronous mode example below is for a Sale transaction

Event	Request Socket port e.g. 10000	Message port e.g. 8000	Message lookup from MessageBundle_en_GB.properties
EPOS sends sale transaction request on socket port	1=1234 2=0 3=21.99 99=0 31 3D 31 32 33 34 0D 0A 32 3D 30 0D 0A 33 3D 32 31 2E 39 39 20 0D 0A 39 39 3D 30		
PED displays 'INSERT/SWIPE CARD'		info:ClearInstruction ClearInstruction99=0 69 6E 66 6F 3A 43 6C 65 61 72 49 6E 73 74 72 75 63 74 69 6F 6E 20 0A 20 43 6C 65 61 72 49 6E 73 74 72 75 63 74 69 6F 6E 39 39 3D 30	ClearInstruction=" "

Event	Request Socket port e.g. 10000	Message port e.g. 8000	Message lookup from MessageBundle_en_GB.properties
PED displays 'INSERT/SWIPE CARD'		info:PlsInsSwpCrd99=0 69 6E 66 6F 3A 50 6C 73 49 6E 73 53 77 70 43 72 64 39 39 3D 30	PlsInsCrd=PLEASE INSERT CARD
PED displays 'PLEASE WAIT'		info:ChpWt99=0 69 6E 66 6F 3A 43 68 70 57 74 39 39 3D 30	ChpWt=CHIP : PLEASE WAIT
PED displays 'ENTER PIN'		info:EntPin ClearInstruction 99=0 69 6E 66 6F 3A 45 6E 74 50 69 6E 20 0A 20 43 6C 65 61 72 49 6E 73 74 72 75 63 74 69 6F 6E 20 39 39 3D 30	EntPin=ENTER PIN
PED displays 'PIN OK PLEASE WAIT'		info:PlsWt ClearInstruction99=0 69 6E 66 6F 3A 50 6C 73 57 74 20 0A 20 43 6C 65 61 72 49 6E 73 74 72 75 63 74 69 6F 6E 39 39 3D 30	PlsWt=PLEASE WAIT...
PED displays 'PIN OK PLEASE WAIT'		info:Connecting...99=0 69 6E 66 6F 3A 43 6F 6E 6E 65 63 74 69 6E 67 2E 2E 2E 39 39 3D 30	Connecting...= Connecting...
PED displays 'PIN OK PLEASE WAIT'		info:Authorising...99=0 69 6E 66 6F 3A 41 75 74 68 6F 72 69 73 69 6E 67 2E 2E 2E 39 39 3D 30	Authorising...= Authorising...
PED displays 'PIN OK PLEASE WAIT'		info:Finalising...99=0 69 6E 66 6F 3A 46 69 6E 61 6C 69 73 69 6E 67 85 39 39 3D 30	Finalising...=Finalising...
PED displays 'APPROVED '		info:AuthCd1 =013028 AppdOI99=0 69 6E 66 6F 3A 41 75 74 68 43 64 31 20 3D 30 31 33 30 32 38 0A 41 70 70 64 4F 6C 39 39 3D 30	AuthCd=AUTH CODE: AppdOI = APPROVED

Event	Request Socket port e.g. 10000	Message port e.g. 8000	Message lookup from MessageBundle_en_GB.properties
PED displays 'REMOVE CARD'		info:PlsRmvCrd ClearInstruction99=0 69 6E 66 6F 3A 50 6C 73 52 6D 76 43 72 64 20 0A 20 43 6C 65 61 72 49 6E 73 74 72 75 63 74 69 6F 6E 39 39 3D 30	PlsRmvCrd=PLEASE REMOVE CARD
PED displays welcome message e.g. Worldpay – IPC		info:ClearInstruction ClearInstruction99=0 69 6E 66 6F 3A 43 6C 65 61 72 49 6E 73 74 72 75 63 74 69 6F 6E 20 0A 20 43 6C 65 61 72 49 6E 73 74 72 75 63 74 69 6F 6E 39 39 3D 30	
EPOS receives IPC Response Request port	7=01012004 29=A0000000041010 6=MASTERCARD 5=541333XXXXXX0045 4=013028 10=MTIP08-2 MCD 90A 14=2 1=5 22=153 Checknet House East Barnet Road Barnet Herts EN4 8QZ 12=21249872 23= Worldpay Demo 28=PGTR640970884 13=22980012 8=17092013 3=1 21=4 9=181628 2=0 34=PLEASE DEBIT MY ACCOUNT 33=PLEASE KEEP THIS RECEIPT FOR YOUR RECORDS 36=60 37=1214 38=2199 41=0 30=3 31=E8 00 32=00 00 00 80 00 59=0000000000000000 00000000000000000000 60=005 98=1234 99=0		

10.2 Asynchronous mode messages

10.2.1 Sale

The request will have the following format

Request

1=reference number
2=0
3=amount
99=0

Message port messages

info:ClearInstruction
ClearInstruction99=0
info:PlsInsSwpCrd99=0
info:ChpWt99=0
info:EntPin
ClearInstruction 99=0
info:PlsWt
ClearInstruction99=0
info:Connecting...99=0
info:Authorising...99=0
info:Finalising...99=0
info:AuthCd1 =013028
AppdOI99=0
info:PlsRmvCrd
ClearInstruction99=0
info:ClearInstruction
ClearInstruction99=0

10.2.2 Refund

The request will have the following format

Request

1=reference number
2=20
3=amount
99=0

Message port messages

info:ClearInstruction
ClearInstruction99=0
info:PlsInsSwpCrd99=0
info:ChpWt99=0
info:EntPin

ClearInstruction 99=0
info:PlsWt
ClearInstruction99=0
info:AuthCd1 =22054
AppdOI99=0
info:PlsRmvCrd
ClearInstruction99=0
info:ClearInstruction
ClearInstruction99=0

10.2.3 Sale CNP

When using the IntraMessage port IPC allows entry of card details only from the pinpad (supported with iPP350, iWL250 and Vx820). Once the below transaction request is received by IPC, the **pinpad** will prompt to enter the card number, expiry date and CVV (if CVV is configured in AVS Details tab in YESEFTConfiguration). The remainder of the details will prompted for on the IntraMessage port based on AVS Details configured in YESEFTConfiguration. Please refer to the section [4.3.3.5](#) for detailed workflow of AVS.

The request will have the following format

Request

1=reference number
2=0
3=amount
12=1
99=0

Message port messages

info:ClearInstruction
ClearInstruction99=0
info:PlsWt
ClearInstruction99=0
info:Connecting...99=0
info:Authorising...99=0
info:Finalising...99=0
info:AuthCd1 =00452C
AppdOI99=0
info:ClearInstruction
ClearInstruction99=0
info:ClearInstruction
ClearInstruction99=0

10.2.4 Refund CNP

When we use message port then there is only option to enter card details from pinpad (supports with iPP350, iWL250 and Vx820) is valid. Once you send the below transaction request, pinpad will ask to enter the card details.

The request will have the following format

Request

1=reference number

2=20

3=amount

12=1

99=0

Message port messages

info:ClearInstruction

ClearInstruction99=0

info:PlsWt

ClearInstruction99=0

info:AuthCd1 =00026

AppdOffl99=0

info:ClearInstruction

ClearInstruction99=0

info:Finalising...99=0

10.2.5 Cancel

The request will have the following format

Request

1=reference number

2=3

5=masked card number i.e. as returned in IPC response message

6=expiry Date

13=PGTR

99=0

Message port messages

info:ClearInstruction

ClearInstruction99=0

info:ClearInstruction

ClearInstruction99=0

info:ClearInstruction

ClearInstruction99=0

10.2.6 Check Card

The request will have the following format

Request

1=reference number

2=30

25=true/false

99=0

Message port messages

info:ClearInstruction

ClearInstruction99=0

info:PlsInsSwpCrd99=0

info:ChpWt99=0

info:PlsRmvCrd

ClearInstruction99=0

info:ClearInstruction

ClearInstruction99=0

10.2.7 Last Transaction Status

No output message on message port

10.2.8 X – Report / Batch Totals

No output message on message port

Z – Report / End of Day

No output message on message port

10.3 Synchronous Mode

Messages in synchronous mode require response from the POS application. Typically these are sent by IPC so that EPOS operator can enter additional data for the transaction e.g. manual authorisation details where a card has been referred; or can influence the transaction flow.

The request from IPC is in the form of key value pairs sent on the Message port. The response from the EPOS application should be sent on the same port.

Following is the list of attributes IPC can send during transaction:

Description	Attribute Name	Data Type	Length														
<p>Request Type. Request Type indicates which type of input is required from EPOS application</p> <p>Please note that additional values may be added with new releases of IPC</p> <table><tr><th>Request Type</th><th>Description</th></tr><tr><td>400</td><td>Voice authorization</td></tr><tr><td>401</td><td>Signature verification</td></tr><tr><td>402</td><td>Fallback confirmation</td></tr><tr><td>403</td><td>CNP details confirmation</td></tr><tr><td>405</td><td>Cashback confirmation</td></tr><tr><td>407</td><td>Address, ZIP entry</td></tr></table>	Request Type	Description	400	Voice authorization	401	Signature verification	402	Fallback confirmation	403	CNP details confirmation	405	Cashback confirmation	407	Address, ZIP entry	2	Integer	3
Request Type	Description																
400	Voice authorization																
401	Signature verification																
402	Fallback confirmation																
403	CNP details confirmation																
405	Cashback confirmation																
407	Address, ZIP entry																
User Message, IPC sends the relevant message based on the state of transaction and request type	3	Alpha Numeric and Special characters	0-100														
Acquirer MID, present in case of voice authorization	11	Numeric	6-15														
Acquirer contact number, present in case of voice authorization request. Multiple contact number is separated by comma	12	Numeric	10-16														
End of message indicator, values always 0.	99	Numeric	1														

Following is the list of attributes EPOS can send during transaction:

Description	Attribute Name	Data Type	Length
Request Type. Same request type, received from IPC, must be sent back to IPC	2	Integer	NA
User, value 0 represents accept and else rejected	3	Integer	1
Authorization code, if IPC issues request for voice authorisation confirmation and auth code and, If merchant wants to accept the transaction then auth code needs to be sent in this field.	4	Alpha Numeric	6

Description	Attribute Name	Data Type	Length
Cashback Amount, if IPC issues request for cashback confirmation and cashback amount and customer wants cash back then cashback amount needs to be sent in this field	5	Decimal	NA
Address; provide address in this field if address is requested to be sent to IPC.	7	Alpha Numeric	NA
Zip; provide Zip code in this field if Zip is requested to be sent to IPC.	8	Alpha Numeric	NA

The synchronous mode example below is for a Sale transaction where IPC requests Accept/Reject Signature

Event	Request Socket port e.g. 10000	Message port e.g. 8000	Message lookup from MessageBundle_en_GB.properties
EPOS sends sale transaction request on socket port	1=1234 2=0 3=21.99 99=0 31 3D 31 32 33 34 0D 0A 32 3D 30 0D 0A 33 3D 32 31 2E 39 39 20 0D 0A 39 39 3D 30		
PED displays 'INSERT/SWIPE CARD'		info:ClearInstruction ClearInstruction99=0 69 6E 66 6F 3A 43 6C 65 61 72 49 6E 73 74 72 75 63 74 69 6F 6E 20 0A 20 43 6C 65 61 72 49 6E 73 74 72 75 63 74 69 6F 6E 39 39 3D 30	ClearInstruction=" "
PED displays 'INSERT/SWIPE CARD'		info:PlsInsSwpCrd99=0 69 6E 66 6F 3A 50 6C 73 49 6E 73 53 77 70 43 72 64 39 39 3D 30	PlsInsCrd=PLEASE INSERT CARD
PED displays 'PLEASE WAIT'		info:ChpWt99=0 69 6E 66 6F 3A 43 68 70 57 74 39 39 3D 30	ChpWt=CHIP : PLEASE WAIT
PED displays 'PLEASE WAIT'		info:Connecting...99=0 69 6E 66 6F 3A 43 6F 6E 6E 65 63 74 69 6E 67 2E 2E 2E 39 39 3D 30	Connecting...= Connecting...

Event	Request Socket port e.g. 10000	Message port e.g. 8000	Message lookup from MessageBundle_en_GB.properties
PED displays 'PLEASE WAIT'		info:Authorising...99=0 69 6E 66 6F 3A 41 75 74 68 6F 72 69 73 69 6E 67 2E 2E 2E 39 39 3D 30	Authorising...= Authorising...
IPC requests EPOS application to confirm if signature is accepted PED displays 'REMOVE CARD'		2=401 3=AUTH CODE:00492Dis Signature Ok ? 99=0 32 3D 34 30 31 0A 33 3D 41 55 54 48 20 43 4F 44 45 3A 30 30 34 39 32 44 49 73 20 53 69 67 6E 61 74 75 72 65 20 4F 6B 20 3F 0A 39 39 3D 30 0A	
PED displays 'REMOVE CARD'		info:PlsWt ClearInstruction99=0 69 6E 66 6F 3A 43 6C 65 61 72 49 6E 73 74 72 75 63 74 69 6F 6E 20 0A 20 43 6C 65 61 72 49 6E 73 74 72 75 63 74 69 6F 6E 39 39 3D 30	PlsWt=PLEASE WAIT...
EPOS applications responds that signature is accepted PED displays 'REMOVE CARD'		2=401 3=0 99=0 32 3D 34 30 31 0D 0A 33 3D 30 0D 0A 39 39 3D 30	
PED displays 'PLEASE WAIT '		info:PlsWt ClearInstruction99=0 69 6E 66 6F 3A 50 6C 73 57 74 20 0A 20 43 6C 65 61 72 49 6E 73 74 72 75 63 74 69 6F 6E 39 39 3D 30	PlsWt=PLEASE WAIT...

Event	Request Socket port e.g. 10000	Message port e.g. 8000	Message lookup from MessageBundle_en_GB.properties
PED displays 'APPROVED'		info:AuthCd1 =00492D AppdOI99=0 69 6E 66 6F 3A 41 75 74 68 43 64 31 20 3D 30 30 34 39 32 44 0A 41 70 70 64 4F 6C 39 39 3D 30	AuthCd=AUTH CODE:
PED displays 'REMOVE CARD'		info:PlsRmvCrd ClearInstruction99=0 69 6E 66 6F 3A 50 6C 73 52 6D 76 43 72 64 20 0A 20 43 6C 65 61 72 49 6E 73 74 72 75 63 74 69 6F 6E 39 39 3D 30	PlsRmvCrd=PLEASE REMOVE CARD
PED displays welcome message e.g. Worldpay – IPC		info:ClearInstruction ClearInstruction99=0 69 6E 66 6F 3A 43 6C 65 61 72 49 6E 73 74 72 75 63 74 69 6F 6E 20 0A 20 43 6C 65 61 72 49 6E 73 74 72 75 63 74 69 6F 6E 39 39 3D 30	ClearInstruction=" "

Event	Request Socket port e.g. 10000	Message port e.g. 8000	Message lookup from MessageBundle_en_GB.properties
Response received on socket port	7=01072009 29=A0000000031010 6=VISA CREDIT 5=476173XXXXXX0119 4=00492D 10=VISA ACQUIRER TEST CARD 01 14=1 1=5 22=153 Checknet House East Barnet Road Barnet Herts EN4 8QZ 12=21249872 23= Worldpay Demo 28=PGTR214582583 13=22980012 8=20092013 3=1 21=2 9=152302 2=0 34=PLEASE DEBIT MY ACCOUNT 33=PLEASE KEEP THIS RECEIPT FOR YOUR RECORDS 36=88 37=1215 38=2199 41=0 30=1 31=F8 00 32=00 00 00 80 00 59=000000000000 00000000000000 60=004 98=1234 99=0		

10.3.1 Accept/reject Signature

This request is issued by IPC on the message port when a transaction requires signature validation

Request from IPC

2=401
3= AUTH CODE:XXXXXXIs Signature Ok ?
99=0

The response from the EPOS application is in the format below

Response from EPOS

2=401

3= 0 (*Accepted*), 1 (*Rejected*)

99=0

10.3.2 Referral Request

- This request is issued by IPC on the message port when a transaction is referred by the acquiring bank and requires the EPOS application either to reject it or to supply a manual authorisation code to complete it.
- The IPC request provides the information required by the EPOS operator to contact the acquiring bank i.e. the contact numbers and the merchant id (MID) in use for the transaction

Request from IPC

2=400

3=CALL BANK Amount:xx.xx

11=MID e.g. 21249872

12=Acquirer contact numbers e.g. 02083871299,02083871295

99=0

The response from the EPOS application is in the format below

Response from EPOS

2=400

3=0 (*Accepted*), 1 (*Rejected*)

4=Authorisation Code received from bank (Present only if the above value is 0)

99=0

10.3.3 FallBack Confirmation Request

This request is issued if a transaction requires card fallback i.e. the card cannot be verified using the optimum method available on both the card and terminal. IPC issues this request when a magnetic swipe card falls back. The intention is that the sales operator may reject fallback and thereby cancel the transaction if there is any doubt about it.

Request from IPC

2=402

3= Swipe card fallback allowed ?

99=0

The response from the POS application is in the format below

Response from EPOS

2=402

3= 0 (*Accepted*), 1 (*Rejected*)

99=0

10.3.4 CNP Confirmation Request

IPC will send the below request to EPOS application for CNP Confirmation if merchant has selected AVS details Mandatory in YESEFTConfig. However, if merchant has selected AVS details Mandatory and Apply AVSRules in YESEFTConfig then IPC will not send this request to EPOS application.

Request from IPC

2=403
3=Security Code Matched, Address Matched, Zip Code Matched
99=0

The response from the POS application is in the format below

Response from EPOS

2=403
3= 0 (*Accepted*), 1 (*Rejected*)
99=0

10.3.5 CashBack Confirmation Request

Where IPC is enabled to allow cashback, and a cashback candidate card is read by the PED, IPC will send the following request to the EPOS application to confirm cashback, and the cashback amount. If the cashback amount is greater than allowed limit, IPC sends an error message and will send the cashback request 2 more times. If IPC does not receive valid amount in 3 attempts then IPC will process the transaction with original amount

Request from IPC

2=405
99=0

The response from the POS application is in the format below

Response from EPOS

2=405
3= 0 (*Accepted*), 1 (*Rejected*)
5=Cashback amount (present only if the above value is 0) e.g. 50.00
99=0

10.3.6 Address and Postcode (Zip Code) Enter Request

The Address and Postcode (Zip Code) request is issued under the following scenarios

CNP transaction

If the merchant has selected 'AVS details Mandatory' in YESEFTConfig, IPC will always send the request below to the EPOS application to prompt for entry of CNP address and postcode/Zip Code details. However, if the merchant has selected 'AVS details Mandatory and Apply AVSRules' in YESEFTConfig, this request will be sent according to the AVS confirmation rules set. Similarly, if the merchant has selected only 'Apply AVSRules' in YESEFTConfig, then IPC will send this request according to the AVS confirmation rules.

Keyed/Forced keyed Referral transaction

This request is issued on message port for Keyed/Forced keyed referral transactions if IPC is being used with Worldpay US acquirer using the Vx820 pinpad. IPC prompts for Card number, expiry date, CVV and State code on the pinpad. CVV and State code are not mandatory entries.

After these entries on the pinpad are complete, IPC will send the request below to the EPOS application for Address and Zip Code entry. If the merchant does not have the values for Address and Zip Code then both the fields can be sent empty with accept response (3=0). In the Keyed/Forced keyed scenario this message port request is not configurable through the AVS details tab.

Request format

According to the CNP rules configured, the application can prompt

- only for Address:

Request from IPC

2=407
3=Address
99=0

Expected Response from POS

2=407
3=(0=Accept 1=Reject)
7=Cardholder Address
99=0

- only for Zipcode

Request from IPC

2=407
3=ZipCode
99=0

Expected Response from POS

2=407
3=(0=Accept 1=Reject)
8=Cardholder Zipcode
99=0

- for both Address and ZipCode

Request from IPC

2=407
3=Address,ZipCode
99=0

Expected Response from POS

2=407

3=(0=Accept 1=Reject)

7=Cardholder Address

8=Cardholder Zipcode

99=0

10.3.7 Cancel Transaction Request

This request is issued by IPC on the message port after having commenced a new transaction (Sale or refund). 'Insert or Swipe Card' message is displayed on PED. To cancel the transaction request at this point, a string formed of the keyword 'Cancel' may be sent on the message port to cancel the request.

Request from IPC to begin new transaction

1=1234

2=0

3=10.00

99=0

Request from EPOS to Cancel transaction

Below string should be sent on the message port to cancel the current transaction from EPOS. The string is non case sensitive can be send in either capital or small letters.

Cancel

11 Appendix H - Print Command details for Tax Free Voucher

First two characters of each line in VATRefundVoucher.txt is the print command followed by the data to print.

Print Command:

Below are the print commands which come with every line in the VATRefundVoucher.txt file.

Code	Print Output
01	<ul style="list-style-type: none"> Print Bitmap – this will be the Premier Taxfree bitmap.
• 02	<ul style="list-style-type: none"> Print Large Bold Text followed by a carriage return
• 03	<ul style="list-style-type: none"> Print Large Underlined Text followed by a carriage return
• 04	<ul style="list-style-type: none"> Print Normal Underlined Text followed by a carriage return
• 05	<ul style="list-style-type: none"> Print Normal Text followed by a carriage return
• 06	<ul style="list-style-type: none"> Print normal sized bold text followed by a carriage return
• 07	<ul style="list-style-type: none"> Print normal sized wide text followed by a carriage return
• 08	<ul style="list-style-type: none"> Print right sided text followed by a carriage return
• 09	<ul style="list-style-type: none"> Print normal centred text followed by a carriage return
• 10	<ul style="list-style-type: none"> Print large bold centred text followed by a carriage return
• 11	<ul style="list-style-type: none"> Print Interleave 2 of 5 barcode that data passed will be encoded in the barcode
• 12	<ul style="list-style-type: none"> Print carriage return
• 13	<ul style="list-style-type: none"> Auto cut paper
• 14	<ul style="list-style-type: none"> Print normal text no carriage return
• 50	<ul style="list-style-type: none"> Load another voucher
• 51	<ul style="list-style-type: none"> Print Copy
• 61	<ul style="list-style-type: none"> The remainder of the text after the print code in this element is encrypted and in base64 string format. Decrypt it and then Print Normal Text followed by a carriage return

Sample VATRefundVoucher.txt file:

01
09Supplier: Premier Tax Free (UK)Ltd
09Merstham, Surrey, RH1 3ED
09Reg: 2076853
09Vat No: 650 1577 51
09info@uk.premiertaxfree.com
1182620100019101036449
09YesPay Test Store
09a1
09a2,a3
09a4,a5
09Vat No:809353718
05.....
06Vouch No:D-GB-826-20-100019-10103644-9
05Shop No: 100019
05Seq No:009872164
05Asst.ID: 22980046
05Asst:
05Date of Sale: 07/05/10
05.....
06A. Description of Goods.
05Qty Goods Description Price
051 TV GBP 100.00
05.....
06Price Incl Vat: GBP 100.00
05 Price Ex Vat: GBP 85.11
05 Vat: GBP 14.89
05 Admin Fee: GBP 6.99
05.....
06 Refund Amt: GBP 7.90
05.....
06B. Customers Declaration
05Permanent Home Address Outside the EC
05Sold To: (Complete in Block Capitals)
12
06Full Name : _____
12
05Street : _____
12
05Town/City : _____
12
05State : _____
12
05Zip/PostCode : _____
12
05Country : _____
12
05Passport No : _____
12
05Issued by Govt : _____

12

05Final Destination : _____

05Arrival Date Departure Date:

05____|____|____ - ____|____|____

05.....

06How do you want your Refund:

051. ☐ Cheque

052. ☐ Credit Card

12

09PRINT CARD NUMBER BELOW

08If you intend to get a cash refund do

08not write your credit card number on

08this form.

05 _____

05 _____

05 _____

053. ☐ Details for refund if different

12

05I declare that I, _____ am

05- not a resident in the EC; or

05- a non-EC resident studying or working

05- in the UK who intends to leave the EC

05 for a minimum of 12 months; or

05- an EC resident who intends to leave

05 the EC for a minimum of 12 months.

05I intend to export the goods listed in

05part A of this form from the EC by the

05last day of the third month following

05that in which they were purchased.

05Customs officials may ask to see

05evidence of your entitlement to use

05the scheme. I understand that when I

05present this form to Customs, I am

05declaring that I am exporting all of

05the goods listed in part A from the EC.

05I will delete any goods from part A

05that I decide to leave in the EC

05before I present this form to Customs.

05The information on this form is correct.

05*The purchaser hereby understands and

05confirms that the credit card nominated

05to credit the VAT refund is the same

05used for the payment of the goods

05described.*

05I agree to Premier Tax Free terms and

05conditions of sale.

12

05SIGNATURE : _____

05 DATE :07/05/10 TIME: 14:54:41

12

05.....

06:C. Retailers Declaration as Agent of :

06: Premier Tax Free :
05:THE DETAILS ON THIS FORM ARE CORRECT AND:
05:I AM SATISFIED THAT THIS CUSTOMER IS :
05:ENTITLED TO USE THE VAT RETAIL EXPORT :
05:SCHEME, THE CUSTOMER HAS COMPLETED AND :
05:SIGNED THE FORM IN MY PRESENCE :
05:I sold the goods to customer on: 07/05/10:
05: :
05:SIGNATURE : _____:
05:PRINT NAME : _____
05: :
05:.....:

06D. FOR OFFICIAL USE AT EXPORT FROM THE
06 E.C

05You must produce this form and the goods
05to customs at the point of departure
05from the EC.

12
12
12
12
12
12
12

05SIGNATURE : _____
05(Export Officer)

05WARNING. PAYMENT MAY NOT BE AUTHORISED
05IF THIS FORM IS NOT FULLY COMPLETED. IT
05IS A SERIOUS OFFENCE TO PRESENT THIS
05FORM AND MAKE AN UNTRUE DECLARATION TO
05CUSTOMS AND EXCISE IF THE GOODS ARE NOT
05EXPORTED FROM THE EC

12

09Data Protection Act 1998

05For full Terms & Conditions please see

05www.premiertaxfree.com

05Tourists, select UK, FAQ

12

09Refund Policy

05For full Terms & Conditions of the

05Premier Tax Free Refund Policy please see

12 Miura Pinpad Configuration and Supported Transactions

IPC-2 non-P2PE installer supports Miura M010 Pinpad. Following are the configuration and supported transaction type with Miura M010 in IPC-2.

Pinpad	Miura - M010
Pinpad OS version	7.7
Pinpad MPI version	1.43
System Hardware	Windows-8 Tablet
Transaction Types supported	Sale Sale with Gratuity Refund Cancel Check Status Duplicate Merchant Receipt Duplicate Customer Receipt Get number of offline stored transactions Cash transaction Close IPC X Reprot Z report Sale (Charge) Token Refund Token Last Transaction Result