

## S05 – SIMPLer Billing SIMPLer Banking Manual

Azotel Technologies Ltd,  
3<sup>rd</sup> Floor, River House,  
Blackpool Park,  
Cork,  
Republic of Ireland.

Azotel Canada Inc.  
325 Vulcan Avenue  
NS B1P 5X1  
Sydney  
Canada

Azotel Poland  
PLAC Powstancow  
Slaskich 17A/222  
53-329  
Wroclaw  
Poland

Phone (EMEA): +353-21-234-8100  
Phone (North America): +1-312-239-0680 / +1-902-539-2665  
Phone (Poland): +48-71-710-1530  
Phone (UK): +44-20-719-3417  
Phone (South Africa): +27-11-083-6900  
Fax: +353-21-467-1699  
[info@azotel.com](mailto:info@azotel.com)

# Contents

Contents .....	2
1 Introduction .....	5
2 Section Two – Available Interfaces .....	6
2.1 Introduction.....	6
2.2 Credit Card/ACH Interfaces .....	6
2.3 Banking Modules .....	7
2.4 Mobile Modules .....	7
2.5 Online Transfer Modules .....	7
3 Section Three – Merchant Interface Details.....	8
3.1 Introduction.....	8
3.2 PayPal .....	8
3.2.1 PayPal IPN.....	8
3.3 Authorize.net.....	13
3.4 Interswitch.....	14
3.5 IP Pay .....	14
3.6 Realex .....	15
3.7 Payments Gateway.....	16
3.8 Netcash.....	17
3.9 Moneris .....	18
3.10 SagePay.....	19
3.11 First Data Global Gateway E4 .....	19
3.12 Stripe .....	20
3.13 Paydock.....	22
3.14 Remita .....	25
3.15 Converge.....	27
3.16 Paystack .....	30
4 Section Four – Banking Module Details .....	35
4.1 Introduction.....	35
4.2 Bank of Ireland .....	35
4.3 Allied Irish Bank.....	35
4.4 Ulster Bank .....	35
4.5 National Irish Bank .....	35
4.6 Eazipay.....	35
4.7 HSBC .....	35
4.8 Lloyds TSB .....	36
4.9 Smart Debit .....	36
4.9.1. Setting up API details .....	36
4.9.2. Adding Bank Account Details to Customer Account .....	37
4.9.3. Import Customer Bank Account Details via API .....	40
4.9.4. Generate and Import Charge File.....	42
4.9.5. WISP Options .....	43
4.10 Security National Bank .....	44
4.11 Bank of Montreal .....	44
4.12 CPA Standard 005.....	44
4.13 Alberta Treasury Bank.....	44
4.14 Norma 19 .....	48
4.15 Banco Santander .....	48
4.16 Netcash Debit.....	48
4.17 NACHA Format.....	49
4.18 First National Bank .....	49
4.19 SEPA Banking .....	50
4.19.1 SEPA Banking: 2016 Updates .....	54

4.20	Cajamar .....	56
4.21	GoCardless .....	58
4.21.1.	SIMPLer Setup.....	58
4.21.2.	GoCardless Settings Required .....	59
4.21.3.	Adding a Bank Account via the End User Portal .....	59
4.21.4.	Making Payments.....	62
4.21.5.	Failed Payments for GoCardless.....	63
4.21.6.	Refunds for GoCardless .....	63
4.22	Sagepay Debit .....	64
4.22.1	SagePay Debit Configuration .....	64
4.22.2	SagePay Debit – SIMPLer Configuration.....	67
4.22.3	SagePay Debit – Adding Bank Accounts .....	69
4.22.4	SagePay Debit – Creating the Debit Order File.....	69
4.22.5	SagePay Debit – Failures .....	71
4.23	Toronto Dominion (TD) Bank .....	72
4.23.1	TD Bank Configuration .....	72
4.23.2	TD Bank File Generation.....	73
4.23.3	TD Bank File Upload.....	73
4.24	FastPay .....	73
4.24.1	FastPay Configuration .....	73
5	Section Five – Features .....	74
5.1	Introduction.....	74
5.2	authorize.NET PCI DSS tokenized API integration .....	74
5.2.1.	Prerequisites .....	74
5.2.2.	Limitations .....	74
5.2.3.	Payment Gateway API Setup.....	74
5.2.4.	Payment Gateway API Setup.....	76
5.2.5.	Payment Gateway API Setup.....	77
5.3	Refunds .....	81
5.3.1.	Prerequisites .....	81
5.3.2.	Feature Outline.....	81
5.3.3.	Feature Use .....	81
6	Section Six – Mobile Interfaces .....	88
6.1	Introduction.....	88
6.2	Fortumo.....	88
6.2.1.	Setting up Fortumo Dashboard .....	88
6.2.2.	Fortumo SIMPLer Setup.....	90
6.2.2.	Fortumo Payments .....	91
6.3	ApplePay.....	93
6.3.1	SETUP: .....	93
6.3.1.1	Apple Pay Merchant Identifier.....	93
6.3.1.2	Certs between ApplePay and Authorize.NET .....	94
6.3.1.3	Certs between ApplePay and Azotel SIMPLer.....	94
6.3.1.4	Domain registration and verification .....	94
6.3.1.5	Azotel help.....	94
6.4	Google Pay.....	95
6.4.1	<a href="#">AUTHORIZE.NET</a> :.....	96
6.4.2	GOOGLE: .....	96

Annex A: References.....	97
A.1 Document References .....	97
A.2 Link References .....	97
Annex B: Definitions and abbreviations .....	98
B.1 Definitions.....	98
B.2 Abbreviations.....	98
Annex C: Merchant Error Codes.....	100
C.1 IPPAY General & CC Response Codes.....	100
C.2 IPPAY ACH Response Codes .....	101
C.3 IPPAY DLL Response Codes .....	102
C.4 AVS Codes.....	103
C.5 ELAVON Codes .....	104
Annex D: Change history .....	105



---

# 1 Introduction

The purpose of this document is to outline the various payment interfaces supported by SIMPLer and to guide operators on the functions and use of each of these modules.

## 2 Section Two – Available Interfaces

### 2.1 Introduction

This section will supply a general outline of the credit card and direct debit/ACH interfaces supported by SIMPLer and will give some basic details on in what capacity these are supported.

### 2.2 Credit Card/ACH Interfaces

Merchant Interface	Credit Card module available	ACH/Echeck module available	Token Credit Card module available	Token ACH/Echeck module available	Refunds	Availability
Paypal	YES	NO	NO	NO	NO	Paypal Standard: Worldwide. Paypal Pro: U.S.A, Canada, U.K.
Authorize.net	YES	YES	YES	YES	YES	U.S.A Canada Puerto Rico
First Data	NO	NO	YES	NO	YES	U.S.A
Interswitch (via access bank plc)	NO	NO	NO	NO	NO	Bank Branch only (Nigeria)
Interswitch	YES	NO	NO	NO	NO	Nigeria
IP Pay	YES	YES	YES	YES	YES	U.S.A (CC and ACH), Canada (CC), Europe (CC)
Realex_redirect_realv ault	Tokenized	NO	YES	NO	NO	Europe
PaymentsGateway	YES	YES	YES	NO	NO	U.S.A
Moneris	YES	NO	NO	NO	NO	Canada
Moneris (Vault)	NO	NO	YES	NO	YES	Canada
SagePay	YES	NO	NO	NO	NO	South Africa
Redsys	YES	NO	NO	NO	NO	EUP Hotspot only
Stripe	NO	NO	YES	YES	YES	Australia, Canada, Denmark, Finland, U.K, Ireland, Norway, Sweden, U.S.A
GoCardless	NO	NO	NO	YES	YES	United Kingdom, Ireland, Belgium, France, Netherlands, Germany, Spain, Sweden
Paydock	NO	NO	YES	YES	YES	<a href="https://paydock.com/features/api/">https://paydock.com/features/api/</a>
Remita	YES	NO	NO	NO	NO	Nigeria: <a href="https://www.remita.net/">https://www.remita.net/</a>
Converge	NO	NO	YES	NO	NO	
Paystack	YES	NO	YES	NO	NO	Nigeria <a href="https://paystack.com/">https://paystack.com/</a>

**Fig. 2.2-1: Credit Card/ACH Interfaces**

## 2.3 Banking Modules

Banking Module	Availability	Notes
Bank of Ireland	Ireland	<a href="http://www.bankofireland.com">www.bankofireland.com</a>
Allied Irish Bank (AIB)	Ireland	<a href="http://www.aib.ie">www.aib.ie</a>
Ulster Bank	Ireland	<a href="http://www.ulsterbank.ie">www.ulsterbank.ie</a>
National Irish Bank	Ireland	<a href="http://www.nationalirishbank.ie">www.nationalirishbank.ie</a>
Eazipay	United Kingdom	<a href="http://www.eazipay.co.uk">www.eazipay.co.uk</a>
HSBC	United Kingdom	<a href="http://www.hsbc.com">www.hsbc.com</a>
Lloyds TSB	United Kingdom	<a href="http://www.lloydstsb.com">www.lloydstsb.com</a>
Smart Debit	United Kingdom	<a href="http://www.smartdebit.co.uk/">http://www.smartdebit.co.uk/</a>
Security National Bank	U.S.A	<a href="http://www.securitynationalbank.com">www.securitynationalbank.com</a>
Bank of Montreal	Canada	<a href="http://www.bmo.com">www.bmo.com</a>
CPA Standard 005	Canada	<a href="http://www.cdnpay.ca">www.cdnpay.ca</a>
Alberta Treasury Branches	Canada	<a href="http://www.atb.com">www.atb.com</a>
Norma 19	Spain	
Banco Santander	Spain	<a href="http://www.santander.com">www.santander.com</a>
Netcash Debit (replaced by SagePay Debit 2016)	South Africa	<a href="https://sagepay.co.za/">https://sagepay.co.za/</a>
NACHA Format	U.S.A	
First National Bank	South Africa	
SEPA	Ireland	Common banking scheme across Ireland – soon to be Europe Wide
CajaMar	Spain	Excel file
Bank National of Canada	Canada	
Toronto Dominion Bank (TD Bank)	Canada	<a href="https://www.tdbank.com/">https://www.tdbank.com/</a>
Fastpay	U.K	

**Fig. 2.3-1: Banking Modules**

## 2.4 Mobile Modules

Mobile Module	Availability	Notes
Fortumo	Available in 94 countries – see website for further details	<a href="https://fortumo.com/">https://fortumo.com/</a>

**Fig. 2.4-1: Mobile Modules**

## 2.5 Online Transfer Modules

Mobile Module	Availability	Notes
Remita	Nigeria	<a href="https://www.remita.net/">https://www.remita.net/</a>

---

## 3 Section Three – Merchant Interface Details

### 3.1 Introduction

This section will provide details of configuration and use of the interfaces outlined in section 2.2.

### 3.2 PayPal

Azotel SIMPLer has integrated with two different options in PayPal:

- **PayPal Standard:** PayPal standard allows customers to be redirected to the PayPal site from the SIMPLer End User Portal and pay off their invoices from there. This option is available widely across the world.
- **PayPal Pro:** Only available in the U.S.A and in the U.K at present.

#### Configuration

**Step One:** Sign up for a PayPal account by contacting staff at PayPal and selecting a suitable package.

<https://www.paypal.com/webapps/mpp/paypal-payments-pro>

<https://www.paypal.com/webapps/mpp/paypal-payments-standard>

**Step Two:** Once your account has been created, PayPal will send you some administrative details. You will need to keep these safe.

**Step Three:** Contact Azotel support ([support@azotel.com](mailto:support@azotel.com)) with the following details, previously supplied by PayPal:

1. PayPal Account: (email format)
2. Signature: (code)
3. Username: (website form)

Alternatively you can enter these details to SIMPLer on the settings -> payment gateways page in SIMPLer. Be sure to select PayPal and choose the correct availability (all, End User Portal, SIMPLer, etc)

**Step Four:** Test your payment gateway by generating a test invoice on a test account in SIMPLer. Enter your own credit card details on the account and process the payment:

- a) Via the End User Portal.
- b) Via SIMPLer “pay online” button.

Verify that the payment has been registered both in SIMPLer and in PayPal by viewing the “cc/Echeck transaction log” located on your invoices tab in SIMPLer.

**Step Five:** If automated payment will be used, please contact Azotel support to set this up.

#### 3.2.1 PayPal IPN

So far Azotel EUP was integrated with PDT, depending on the customer / customer browser to

redirect back to the EUP and send payment variables back to the server hosting EUP. To make the solution more robust PayPal IPN method has been implemented within Azotel EUP (since 2016 Q1). This method provides asynchronous payment confirmation to be sent directly to the payment listener hosted on the SIMPLer server instead of relying on the customer browser. Payment Listener processes the incoming information and closes the transaction. That means that after making a payment, without affecting the overall transaction, the customer can:

- a) redirect back to the EUP and wait for the payment confirmation / denial to arrive
- b) or close the browser before returning to the EUP

To set up with IPN implementation PDT must be disabled. This ensures that the customer browser redirects back with the internal variables (instead of PayPal PDT variables) to check the transaction status.

Follow the steps below to migrate from PDT to IPN:

- a) In the SIMPLer system, go to the Settings -> Payment Gateways and enable IPN functionality. Make sure there is a correct REDIRECTION\_LINK entered. Format of REDIRECTION\_LINK is:

[https://<server\\_name>/CustomerPortel/paymentSecondStage.pl](https://<server_name>/CustomerPortel/paymentSecondStage.pl)

OR

[https://<server\\_name>/CP/paymentSecondStage.pl](https://<server_name>/CP/paymentSecondStage.pl)

where <server\_name> is SIMPLer server domain address.

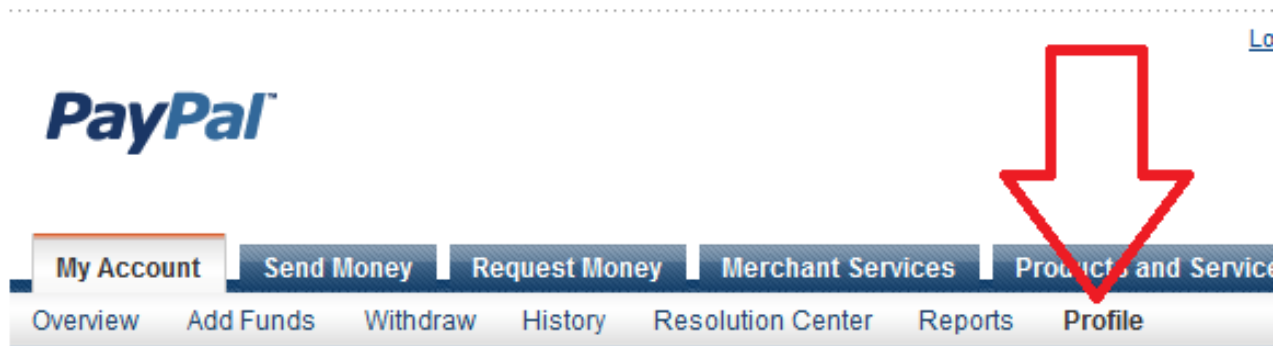
This is depending on the SIMPLer server. If you are unsure about the correct REDIRECTION\_LINK, please contact azotel support (support@azotel.com) to help with the setup.

ID	Name	Availability	Label	Module Settings
41	PayPal <a href="#">View Log</a>	All	PayPal&reg	<div> <div>AUTH_TOKEN</div> <div>CANCEL</div> <div>IPN</div> <div>PASSWORD</div> <div>PAYPAL_ACCOUNT</div> <div>REDIRECTION_LINK</div> <div>SANDBOX</div> <div>SIGNATURE</div> <div>USERNAME</div> </div> <div> <div></div> <div></div> <div>1</div> <div>123456789</div> <div>test@paypal.com</div> <div>https://84.203.220.160/CustomerPortal/payn</div> <div></div> <div>qwerty</div> <div>test</div> </div>

**Fig. 3.2.1-1: Payment Gateways**

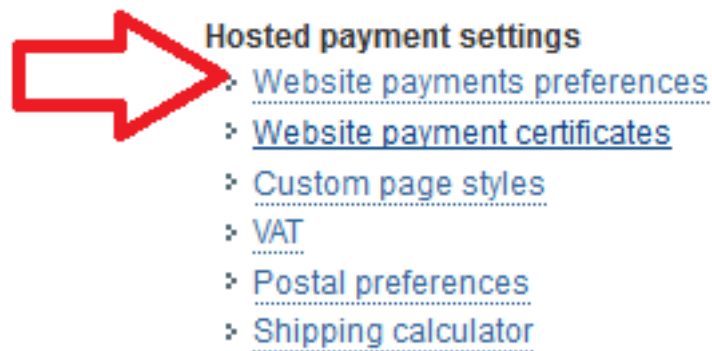
2) Under the PayPal Account:

a) Go to the Profile:



**Fig. 3.2.1-2: PayPal Profile**

b) Scroll down to the “Hosted payment settings” section and click on “Website payments preferences” link



**Fig. 3.2.1-3: Hosted Payment Settings**

c) On “Website payments preferences” page make sure that:

- Auto – Return is ON
- Return URL can be the same as entered in point (1). It will get overwritten by the URL entered in point (1)
- Payment Data Transfer must be OFF
- At the bottom of the page click “Save” button

## Website Payment Preferences

### Auto Return for Website Payments

Auto Return for Website Payments brings your buyers back to your website immediately after payment completion. This feature applies to all PayPal Website Payments, including Buy Now, Donations, Subscriptions, and Shopping Cart. [Learn More](#)

Auto Return: ☒ On  
☐ Off

**Return URL:** Enter the URL that will be used to redirect your customers upon payment completion. This URL must meet the requirements for a valid URL. [Learn More](#)

Return URL:

**Return URL Requirements:** The following items are required in order to set up Auto Return.

**Fig. 3.2.1-4: Website Payment Preferences**

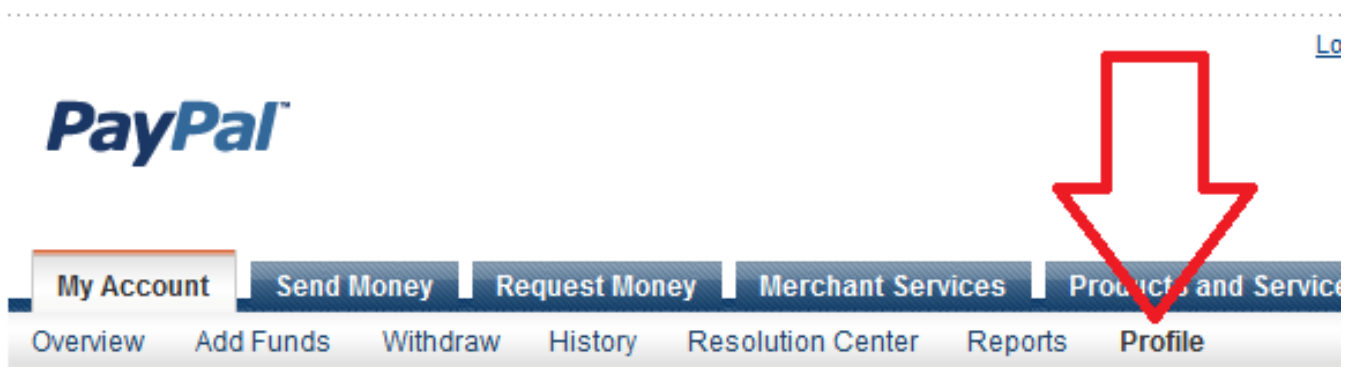
### Payment Data Transfer (optional)

Payment Data Transfer allows you to receive notification of successful payments as they are made. The use of Payment Data Transfer depends on your [system configuration](#) and your Return URL. Please note that in order to use Payment Data Transfer, you **must** turn on Auto Return.

Payment Data Transfer: ☐ On  
☒ Off

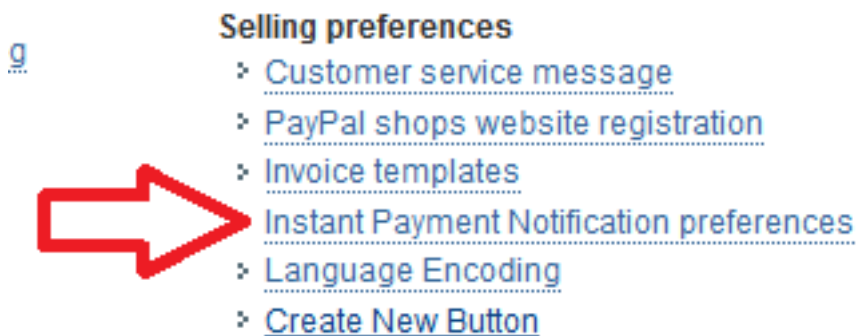
**Fig. 3.2.1-5: Payment Data Transfer**

- d) Go to “Profile” again



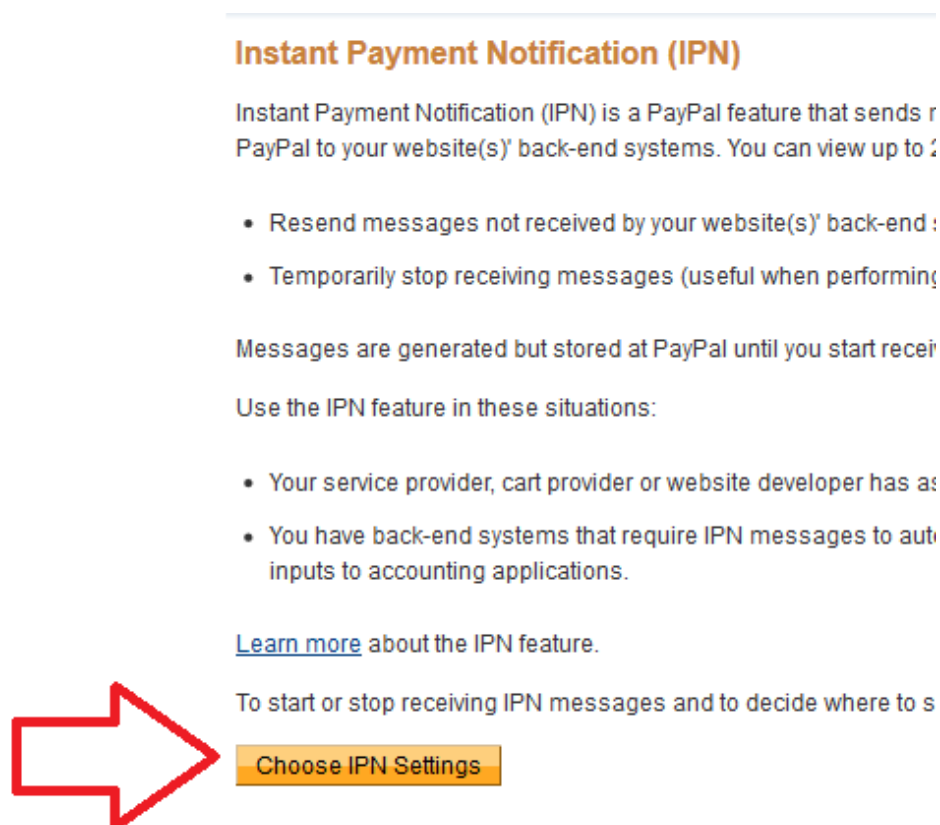
**Fig. 3.2.1-6: Profile (2)**

- e) Scroll down to the “Selling preferences” section and click “Instant Payment Notification” preferences link



**Fig. 3.2.1-7: Instant Payment Notification Preferences**

f) On the “Instant Payment Notification” page click “Choose IP Settings” button



**Fig. 3.2.1-8: Choose IPN Settings**

g) In the “Notification URL” field enter the following link:

[https://<server\\_name>/API/payments/paymentListener.pl](https://<server_name>/API/payments/paymentListener.pl)

where <server\_name> is SIMPLer server domain address.

Under “IPN messages” select “Receive IPN messages (Enabled)” option and click Save button



### Edit Instant Payment Notification (IPN) settings

PayPal sends IPN messages to the URL that you specify below.

To start receiving IPN messages, enter the notification URL and select **Receive IPN message** messages, select **Do not receive IPN messages** below. PayPal continues to generate and st IPN messages again (or turn off IPN).

Notification URL

`https://pentest.azotel.com/API/payments/paymentListener.pl`

IPN messages

- ☒ Receive IPN messages (Enabled)  
☐ Do not receive IPN messages (Disabled)

Save

Cancel

**Fig. 3.2.1-9: Save**

## 3.3 Authorize.net

Azotel have integrated with Authorize.net for both tokenized (credit card only) and non-tokenized interfaces using both credit card and ACH options:

Configuration:

For each type of configuration, the following details will be required:

- Merchant API Login
- Merchant API Transaction Key.

Both will be provided on sign up with authorize.net and can be configured either by the operator on the settings -> payment gateways tab, or by azotel support team.

Test your payment gateway by generating a test invoice on a test account in SIMPLer. Enter your own credit card details on the account and process the payment:

- Via the End User Portal.
- Via SIMPLer “pay online” button.

Verify that the payment has been registered both in SIMPLer and in Authorize.net by viewing the “cc/Echeck transaction log” located on your invoices tab in SIMPLer.

If automated payment will be used, please contact Azotel support to set this up.

### 3.4 Interswitch

Interswitch is a payment gateway available in Nigeria. It is available for credit card processing but currently does not have direct debit/ACH support. End users will be redirected from the Azotel portal to the Interswitch interface to add their credit card details. Once the transaction is processed the customer will be directed back to the SIMPLer End User Portal to continue browsing through their invoices and account details.

As credit cards will not be stored in SIMPLer, auto payment is not an option available for this interface so payments can be made solely on the End User Portal.

To set add your Interswitch account in SIMPLer please visit the Settings – Payment Gateways Section and choose InterSwitchNg as the name of your payment gateway. Enter the following information and click “update payment gateways”.

- 1) Interswitch Currency Code
- 2) Mac Key
- 3) Payment Item ID
- 4) Paydirect Product ID
- 5) Processing Server
- 6) XML Server

To test a payment, log in to the End User Portal and try to pay off an outstanding invoice with your credit card using the “pay online” button.

### 3.5 IP Pay

Azotel have integrated with IP Pay for both tokenized and non-tokenized interfaces using both credit card and ACH options:

Configuration:

For each type of configuration, the following details will be required:

- a) Terminal ID.

This will be provided on sign up with IP Pay and can be configured either by the operator on the settings -> payment gateways tab, or by Azotel support team. Usually IP Pay will contact Azotel directly with this information.

This interface can be used in the following way:

1. Customers can add credit cards/bank accounts to the End User Portal and pay off their invoices from there.
2. Operators can manually charge a customer’s credit card/bank account via SIMPLer.
3. Operators can have auto payment enabled and credit cards/bank accounts can be automatically changed on a daily/weekly, monthly basis.

4. Operators can process refunds via SIMPLer to push them directly to IP Pay. See: <http://wiki.azotel.com/2013-4q-v001-billing-refunds-via-payment-gateway>

## 3.6 Realex

Realex is a payment gateway for Credit Cards that is widely used across Ireland, the UK and parts of mainland Europe.

Realex provides a tokenized interface.

### Configuration

**Step One:** Sign up for a Realex account by contacting staff at Realex and selecting a suitable package. (<http://www.realexpayments.ie/>)

**Step Two:** Once your account has been created, Realex will send you some administrative details. You will need to keep these safe.

**Step Three:** Contact Azotel support ([support@azotel.com](mailto:support@azotel.com)) with the following details, previously supplied by Realex:

For Realex Redirect RealVault (Tokenized):

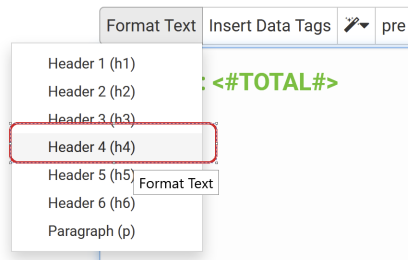
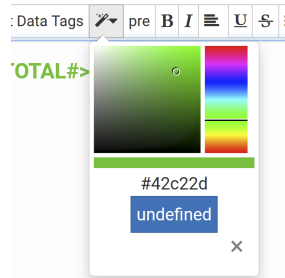
- 1) Merchant\_API\_ID
- 2) Merchant\_API\_Secret
- 3) Merchant\_ID
- 4) Merchant\_Secret
- 5) Return\_URL (this can be discovered by Azotel)

Alternatively, you can enter these details to SIMPLer on the settings -> payment gateways page in SIMPLer. Be sure to select the correct gateway name and choose the correct availability (all, End User Portal, SIMPLer, etc)

For Realex Global Payment Portal to allow for the simplification of payments go to the Realex / Global Payments Portal and make the following changes:

1. Click on **CLIENT SETTINGS**
2. Under **REDIRECT TEXT CONFIGURATION**, select the subaccount
3. Once the sub account is selected (the one where the transaction is to be processed over), you will need to click Insert data tags and select <#TOTAL#> from the dropdown menu, as per Fig. 3.9.1-1  
Should you wish to change the colour, for ease of visibility, of the amount to be paid please take a look at Fig. 3.9.1-2 and 3.9.1-3
4. Once you are happy with the message click save at the bottom of the screen
5. Please note this could take a few minutes for the change to take place

## REDIRECT TEXT CONFIGURATION

**Fig. 3.9.1-1: Redirect Test Configuration****Fig. 3.9.1-2: Format Text****Fig. 3.9.1-2: Format Text Colour**

**Step Four:** Test your payment gateway by generating a test invoice on a test account in SIMPLer. Enter your own credit card details on the account and process the payment:

- c) Via the End User Portal.
- d) Via SIMPLer “pay online” button.

Verify that the payment has been registered both in SIMPLer and in Realex by viewing the “cc/Echeck transaction log” located on your invoices tab in SIMPLer.

**Step Five:** If automated payment will be used, please contact Azotel support to set this up.

## 3.7 Payments Gateway

There is a regular interface available for credit cards and e-checks. There is also a tokenized version available for Credit Cards.

Configuration:

For the Credit Card Interface, the following details are required:

- 1) Merchant\_API\_Login\_ID
- 2) Merchant\_API\_Transaction\_Key
- 3) Merchant\_ID

- 4) Transaction
- 5) Transaction\_Password.
- 6) Client (URL to Client Services)
- 7) Merchant (URL to Merchant Services)

For the E-check interface the following details are required:

- 1) Merchant\_ID.
- 2) Transaction\_Password.

Test your payment gateway by generating a test invoice on a test account in SIMPLer. Enter your own credit card details on the account and process the payment:

- a) Via the End User Portal.
- b) Via SIMPLer “pay online” button.

Verify that the payment has been registered both in SIMPLer and in the merchant account by viewing the “cc/Echeck transaction log” located on your invoices tab in SIMPLer.

If automated payment will be used, please contact Azotel support to set this up.

## 3.8 Netcash

**NOTE: Netcash Credit card module will be replaced by SagePay at the end of August 2014. See section 3.10 for more details. Netcash Direct Debit will be replaced in summer 2016 by Sagepay Direct Debit model. See section 4.22.**

SIMPLer has integrated with Netcash for two processes:

- a) Credit Card interface.
- b) Direct Debit Module. (Explained in Section 4.16)

### **Credit Card Interface:**

To activate the credit card interface, please firstly contact Netcash and set up an account, if this has not already been done. Once the account has been set up in Netcash, please send the following details to Azotel support to be configured on your instance:

- e) Terminal ID
- f) Username
- g) Pin
- h) Password

Once these have been configured by Azotel support (or alternatively by yourself via the settings -> payment gateways) you should generate a test invoice on a test account and test the payment of this invoice by adding credit card details to a customer’s account.

Check the status of the payment in both SIMPLer and Netcash to verify that all is working correctly.

## 3.9 Moneris

Used primarily in Canada for credit card processing only.

The following details are required to communicate between SIMPLer and Moneris:

1) For non-tokenized interfaces (Moneris):

- API Token: To be obtained from Moneris.
- Store ID: To be obtained from Moneris.

c) For tokenized interfaces (Moneris – Token Based or Moneris Vault):

- API Token: To be obtained from Moneris on initially setting up the Vault Account. This code can be obtained from within the Moneris account.
- Language: Must be either en-ca (for English speakers) or fr-ca (for French speakers)
- Merchant API Login ID: To be obtained from Moneris. It is actually known as “red\_id” in Moneris and must be set up on the “hosted vault configuration” page.
- Transaction Key: To be obtained from Moneris. It is actually known as “red\_key” in Moneris and must be set up on the “hosted vault configuration” page.
- Store ID: To be obtained from Moneris on initially setting up the Vault account.

The operator must also configure some things on the “Hosted Vault Configuration” page:

- 1) Response Method: Set the response method to “Sent to your server as a POST” per Fig. 3.9.1-1.
- 2) Response URL: This should be set as [https://yourserverhere.azotel.com/API/payments/Realex\\_Redirect\\_RealVault.pl](https://yourserverhere.azotel.com/API/payments/Realex_Redirect_RealVault.pl) per Fig. 3.9.1-1

**Hosted Vault Configuration**

res\_id: [redacted]  
res\_key: [redacted]

**Basic Configuration**

**Response Method**

Please specify how the transaction response should be handled.

**Response Method:**

☒ Sent to your server as a POST  
☐ Sent to your server as a GET

**Response URL:**   
URLs must start with http or https and must be a registered domain. IP addresses are not supported.

**Hosted Vault Page Appearance**

Specify what will be displayed on the Hosted Vault Page.

Fig. 3.9.1-1: Hosted Vault Configuration

There is also a “security features” subpage where you can configure the settings as per Fig. 3.9.1-2.

The checkbox must be checked for “enable transaction verification” and the “Displayed as key/value pairs on our server” should also be selected.

Fig. 3.9.1-2: Security Features Configuration

## 3.10 SagePay

Used primarily in South Africa.

### Credit Card Interface:

To activate the credit card interface, please firstly contact SagePay and set up an account, if this has not already been done. Once the account has been set up in SagePay, please send the following details to Azotel support to be configured on your instance:

- a) Service Key

Next, you will need to request the accept & decline URL from Azotel that you can enter into your SagePay account.

Both the “Credit Card Accept URL” and the “Credit Card Decline URL” will need to be filled out with [https://<your\\_server\\_here>/CustomerPortal/paymentSecondStage.pl](https://<your_server_here>/CustomerPortal/paymentSecondStage.pl)

Once these details (service key) have been configured by Azotel support (or alternatively by yourself via the settings -> payment gateways) you should generate a test invoice on a test account and test the payment of this invoice by adding credit card details to a customer’s account.

Check the status of the payment in both SIMPLer and SagePay to verify that all is working correctly.

## 3.11 First Data Global Gateway E4

Used primarily in the U.S.A. This interface is a tokenized credit card interface. Refunds are supported via this payment Gateway.

### Credit Card Interface:

To activate the credit card interface, please firstly contact FirstData and set up an account, if this has not already been done. Once the account has been set up in First Data, please follow the steps outlined below:

- 1) Use ECOMM terminal
- 2) Provide Gateway ID & Password
- 3) Enter Transarmor Token (obtained by contacting a First Data representative)
- 4) Under API details tab get and provide Key ID and HMAC key
- 5) Create Payment Page – on the Receipt page settings page (ask Azotel if you are unsure of the settings required).

- 6) Set HMAC calculation to MD5 and provide HMAC transaction key to Azotel.
- 7) For Payments, select appropriate terminal from the list on the Credit Card Payments page.

Once these have been configured in the relevant systems, you should generate a test invoice on a test account and test the payment of this invoice by adding credit card details to a customer's account. Check the status of the payment in both SIMPLer and First Data to verify that all is working correctly.

## 3.12 Stripe

Azotel SIMPLer has integrated with two different options in Stripe:

- **Credit Card Payment Interface**
- **ACH Payment Interface**

As this is a tokenized interface, you will need to make sure your instance has tokenization enabled. Ask Azotel Support at [support@azotel.com](mailto:support@azotel.com) to check this for you.

### Payment Gateway Configuration

**Step One:** Sign up for a Stripe account by contacting staff at Stripe and selecting a suitable package. <https://stripe.com/contact/sales>

**Step Two:** Once your account has been created, Stripe will send you some administrative details. You will need to keep these safe.

**Step Three:** Contact Azotel support ([support@azotel.com](mailto:support@azotel.com)) with the following details, previously supplied by Stripe:

1. **CHECKOUT\_LINK:** This field will populate automatically in SIMPLer.
2. **DATA\_IMAGE:** A link to the logo on your portal, i.e. <https://<servername>/PortalImages/<WISPID>>
3. **ENDPOINT\_URL:** This field will populate automatically in SIMPLer.
4. **DEFAULT\_AUTO\_PAY\_ON:** Entering 1 to this field means when a customer adds a CC / bank account for the first time it will automatically be enabled for auto payment. Entering 0 to this field means it will not be enabled for auto pay unless the operator / customers select to do so manually.
5. **PUBLIC\_KEY:** Code provided by Stripe
6. **SECRET\_KEY:** Code provided by Stripe
7. **STRIPE\_JS\_LINK:** This field will populate automatically in SIMPLer.

Alternatively you can enter these details to SIMPLer on the settings -> payment gateways page in SIMPLer. Be sure to select:

- Stripe – CC: For Credit Card payments
- Stripe – EFT: For ACH transactions

Choose the correct availability (all, End User Portal, SIMPLer, etc)



- All: Available for customers to pay independently on the portal, for operators to pay in SIMPLer using the custom payment options or “pay online” buttons, AND for auto payment.
- EUP: Available for customers to pay independently on the portal
- SIMPLer: Available for operators to pay in SIMPLer using the custom payment options or “pay online” buttons.

ID ?	Name ?	Availability ?	Label ?	Module Settings ?
new	Stripe - CC	All	Pay Online	<div>CHECKOUT_LINK</div> <div>DATA_IMAGE</div> <div>ENDPOINT_URL</div> <div>HOSTED_PAGE_EUP_DEFAULT_AUTO_PAY_ON</div> <div>PUBLIC_KEY</div> <div>SECRET_KEY</div>
				<div>https://checkout.stripe.com/checkout.js</div> <div></div> <div>api.stripe.com</div> <div>1</div> <div></div> <div></div>

**Fig. 3.12-1: Stripe – CC Payment Gateway**

ID ?	Name ?	Availability ?	Label ?	Module Settings ?	Redirect
new	Stripe - EFT	All	Pay Online	<div>DATA_IMAGE</div> <div>ENDPOINT_URL</div> <div>HOSTED_PAGE_EUP_DEFAULT_AUTO_PAY_ON</div> <div>PUBLIC_KEY</div> <div>SECRET_KEY</div> <div>STRIPE_JS_LINK</div>	paymentSecondStage.p
				<div></div> <div>api.stripe.com</div> <div>1</div> <div></div> <div></div> <div>https://js.stripe.com/v2/</div>	

**Fig. 3.12-2: Stripe – CC Payment Gateway**

**Step Four:** Test your payment gateway by generating a test invoice on a test account in SIMPLer. Enter your own credit card details on the account and process the payment:

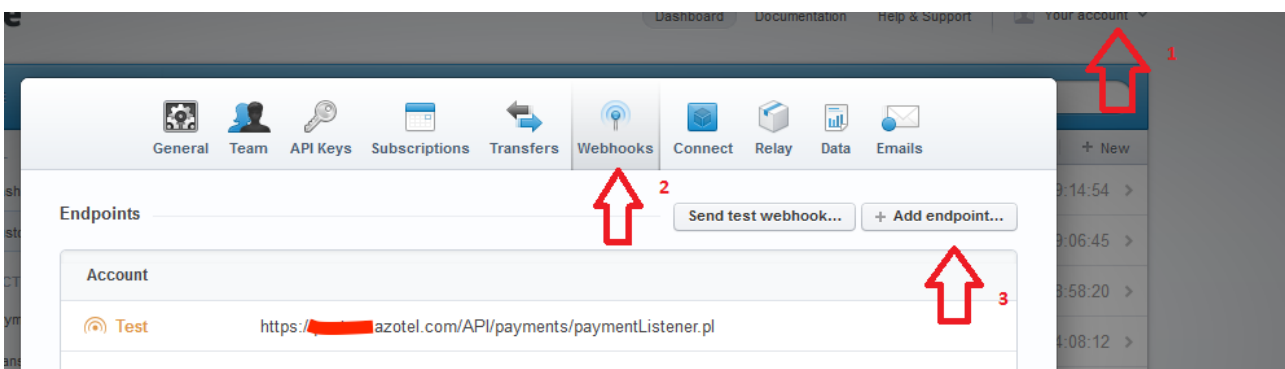
- Via the End User Portal.
- Via SIMPLer “pay online” button.

Verify that the payment has been registered both in SIMPLer and in Stripe by viewing the “cc/Echeck transaction log” located on your invoices tab in SIMPLer.

**Step Five:** If automated payment will be used, please contact Azotel support to set this up

### Additional Features

- Webhooks:** By enabling webhooks in Stripe for EFT it will be easier to confirm failures / success / refunds. To enable webhooks in the Stripe portal the operator will need to go to the webhooks page on Stripe and click “Add endpoint”. Here the operator should enter the link (items in the <brackets> depend on your SIMPLer server)  
[https://<server\\_name>/API/payments/paymentListener.pl](https://<server_name>/API/payments/paymentListener.pl)



**Fig. 3.12-3: Webhooks**

**2. Bank Account Verification:** If a customer adds a bank account it must be verified. The verification process involves entering two small deposits that will automatically be sent to your account by Stripe within 1-2 business days. The description of these deposits on your statement will be “VERIFICATION”. There is a limit of 10 failed verification attempts.

**Note:** After adding the bank account, it needs to be verified. Verification is done via two small deposits into the bank account that will be automatically send. These deposits will take 1-2 business days to appear on your online statement. The statement description for these deposits will be VERIFICATION. You need to enter those deposits under appropriate bank account on 'Personal Information' page and click 'Verify'. When accepting these values, be sure to note that there is a limit of 10 failed verification attempts. Once this limit has been crossed, the bank account will be unable to be verified.

**Enter Bank Account Details**

<input type="text" value="110000000"/>	<input type="text" value="000123456789"/>
<small>Routing Number</small>	<small>Bank Account Number</small>
<input type="text" value="test"/>	<input type="text" value="individual"/>
<small>Name on Account</small>	<small>Account Holder Type</small>

[Add Bank Account](#)

**Fig. 3.12-4: Verification**

## 3.13 Paydock

Azotel SIMPLer has integrated with two different options in Paydock:

- **Credit Card Payment Interface**
- **ACH Payment Interface**

As this is a tokenized interface, you will need to make sure your instance has tokenization enabled.

Ask Azotel Support at [support@azotel.com](mailto:support@azotel.com) to check this for you.

### Payment Gateway Configuration

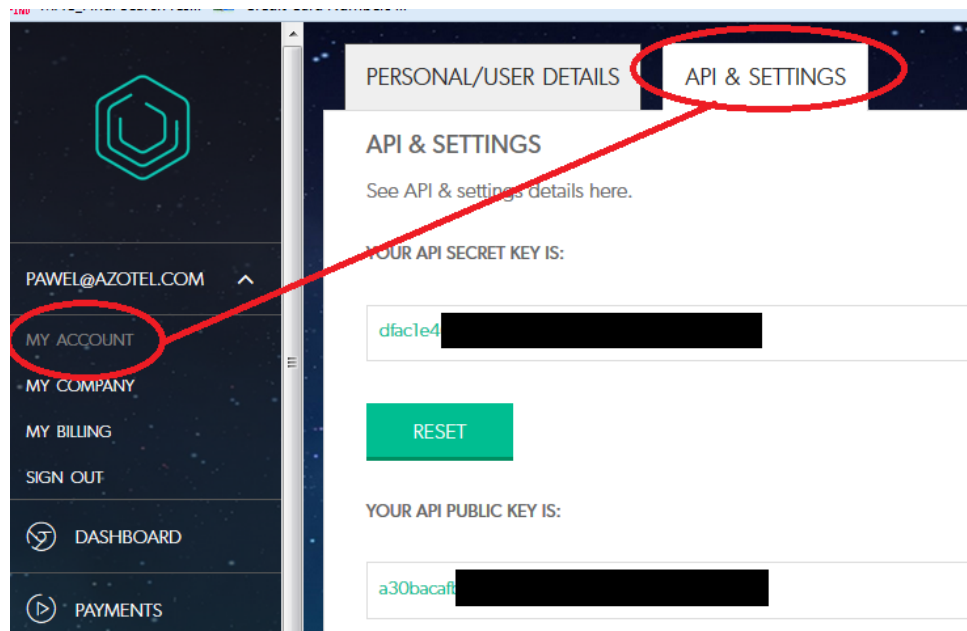
**Step One:** Sign up for a Paydock account by contacting staff at Paydock and selecting a suitable package.

**Step Two:** Once your account has been created, Paydock will send you some administrative details. You will need to keep these safe.

**Step Three:** Contact Azotel support ([support@azotel.com](mailto:support@azotel.com)) with the following details, previously supplied by Paydock:

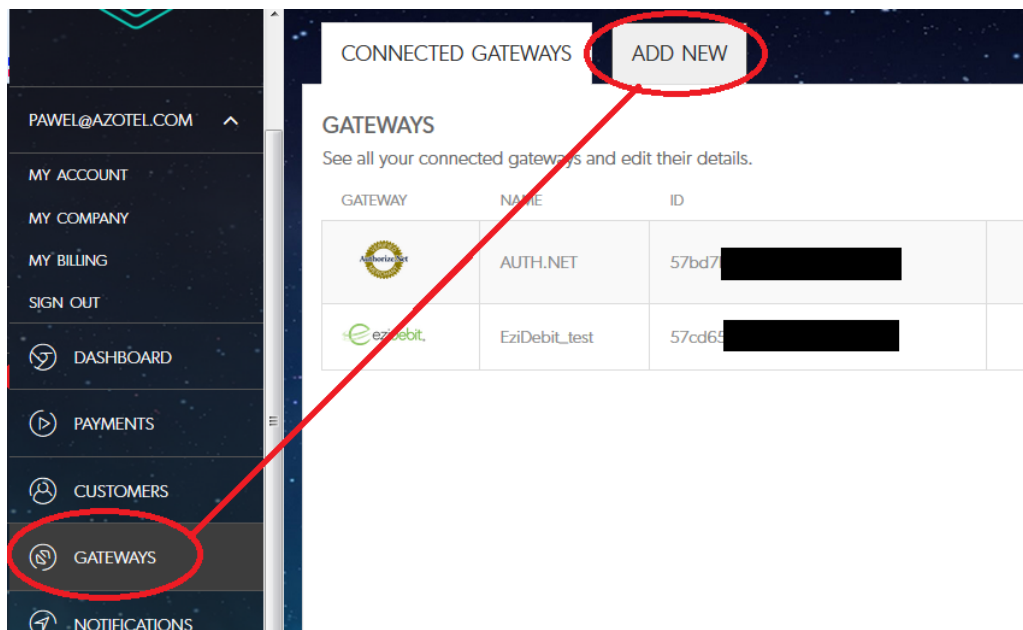
1. **Public Key:** This field is available from the API & Settings tab, on the My Account section. (See fig. 3.13-1).
2. **Secret Key:** This field is available from the API & Settings tab, on the My Account section. (See fig. 3.13-1).

3. **Gateway ID:** Available on the “Gateways” tab on the Paydock interface.



**Fig. 3.13-1: Paydock: My Account**

If you have not already set up a gateway you can do this on the “Gateways” tab and click “Add new” per Fig. 3.13-2.



**Fig. 3.13-2: Paydock: Gateways**

Alternatively, you can enter these details to SIMPLer on the settings -> payment gateways page in SIMPLer. Be sure to select:

- Paydock: For Credit Card payments

- Paydock Echeck: For ACH (bank account) transactions

Choose the correct availability (all, End User Portal, SIMPLer, etc)

- All: Available for customers to pay independently on the portal, for operators to pay in SIMPLer using the custom payment options or “pay online” buttons, AND for auto payment.
- EUP: Available for customers to pay independently on the portal
- SIMPLer: Available for operators to pay in SIMPLer using the custom payment options or “pay online” buttons.

ID	Name	Availability	Label	Module Settings	Redirect	Token Based	E-check Module
72	paydock_echeck <a href="#">View Log</a>	All	Pay Online	API_PUBLIC_KEY: a30bac... API_SECRET_KEY: dfac1e4... ENDPOINT: api-sand... GATEWAY_ID: 57cd65... SANDBOX: 1	paymentSecondStage.pl	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Fig. 3.13-3: Paydock– Payment Gateway**

**Step Four:** Test your payment gateway by generating a test invoice on a test account in SIMPLer. Enter your own details on the account and process the payment:

- a) Via the End User Portal.
- b) Via SIMPLer “pay online” button.

Verify that the payment has been registered both in SIMPLer and in Stripe by viewing the “cc/Echeck transaction log” located on your invoices tab in SIMPLer.

**Step Five:** If automated payment will be used, please contact Azotel support to set this up.

### Payment Collection

Payment collection can occur in the following ways:

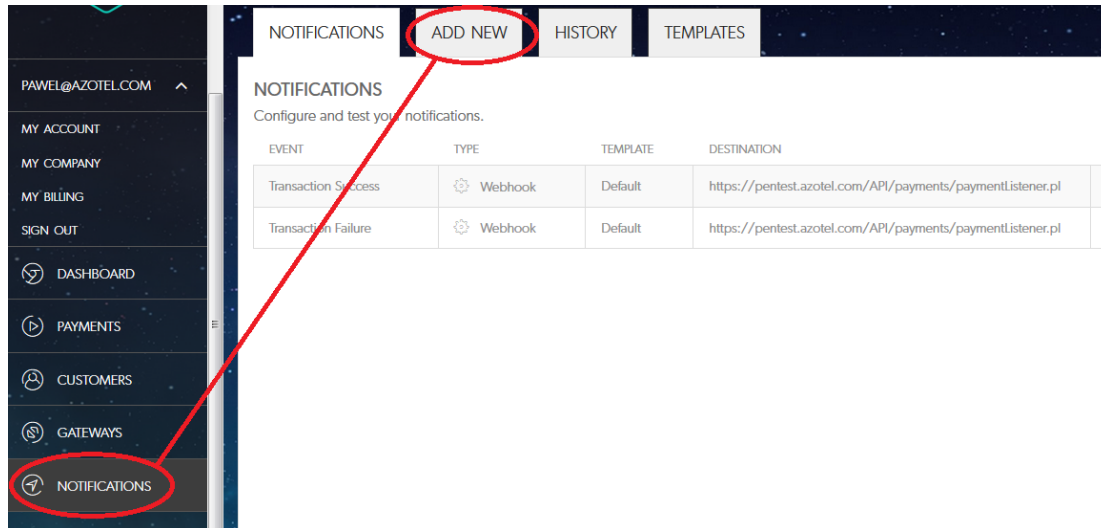
- 1) The customer can pay off an invoice independently on the customer portal.
- 2) The operator can process payments manually in SIMPLer by clicking on the “pay online” button beside an outstanding invoice.
- 3) The operator can choose to set up auto payment for certain customers and have scripts run overnight from the Settings – Cron Jobs section of SIMPLer.

### Additional Features

SIMPLer has also integrated with some additional features such as the following:

- 1) Notifications: Notifications for successful and failed payments
- 2) Refunds processed through SIMPLer that will hit the payment gateway successfully. (See Section 5.3)

On the notifications tab the operator can enter new notifications for successful transactions and for failures. The only information required is the destination address which is [https://<simpler\\_server>/API/payments/paymentListener.pl](https://<simpler_server>/API/payments/paymentListener.pl) where <simpler\_server> must be replaced by the actual SIMPLer server name.



**Fig. 3.13-4: Paydock– Notifications**

#### Final Comments

Integration makes the customer browser to connect directly to the Paydock server to add a credit card / bank account or make once-off payment. In case customer is disconnected the following URLs should be whitelisted in the firewall of the controlling NAS:

app.paydock.com 52.62.127.243

code.jquery.com 94.46.159.28

Your SIMPLer server IP (depends on the operator).

### 3.14 Remita

Azotel SIMPLer has integrated with two different options in Remita:

- **Credit Card Payments on the End User Portal**
- **Online Transfer Facilitation on the End User Portal**

To configure your instance of SIMPLer for use with Remita please Navigate to the Settings Tab of SIMPLer and Click on Payment Gateways (per Fig. 3.14-1).



**Fig. 3.14-1 Settings – Payment Gateways**

On the next page please click “Add Blank Row” and select the gateway name “Remita” from the drop-down menu, and the availability “End User Portal” as per Fig. 3.14-2.

**Fig. 3.14-2 Remita Payment Gateway**

Fill out the following details and click “Update Payment Gateways”.

- API Key: Request this information from Remita.
- Merchant ID: Request this information from Remita.
- Payment Status Server: Remita will provide this information once you complete their testing process.
- Response URL: <https://YOURSIMPLERSERVERHERE/CustomerPortal/paymentSecondStage.pl>
- Server Post URL: Remita will provide this information once you complete their testing process.
- Service Type ID: Request this information from Remita.

Finally, on the Remita side you must configure the payment listener URL, which should be <https://YOURSERVERHERE/API/payments/paymentListener.pl>

To pay by credit card the customer can log on to the “End User Portal” and click the “pay online” button, follow through with payment on the Remita site and the response will be sent back to SIMPLer.

To avail of the “online transfer” option you must click “online transfer” on the End User Portal. This will request a CODE from Remita. You must use this code when making payments at the bank, and the bank will query SIMPLer for the transaction and pay it off is successful.

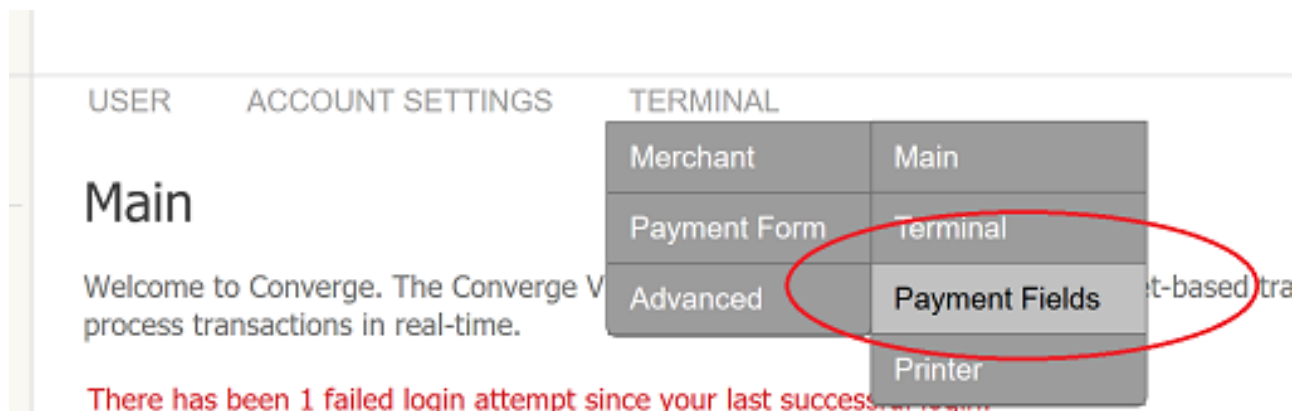
### 3.15 Converge

Azotel SIMPLer has integrated with Converge for CREDIT CARD payments only. To set up this payment gateway please follow the instructions below.

- (1) Please firstly ask Azotel Support to enable tokenization on your instance of SIMPLer.
- (2) Navigate to the Settings – Payment Gateways section in SIMPLer. Select the type “converge” and fill out the following, as received from your payment gateway:
  - SSL\_MERCHANT\_ID
  - SSL\_PIN
  - SSL\_USER\_ID

**Fig. 3.15-1: Payment Gateway Setup**

- (3) Under your own Converge Account three fields need to be ADDED by clicking “Add New Field” under the Payment Fields menu. These are “Enable Auto Payment”, “Merchant CustID: and “Close Transaction”.



▲ ▼	TOKEN	No	ssl_token	System Field
▲ ▼	Add Token	No	ssl_add_token	System Field
▲ ▼	Add Token Response	No	ssl_add_token_response	System Field
▲ ▼	Merchant Transaction ID	Yes	ssl_merchant_txn_id	System Field
▲ ▼	Customer ID	No	ssl_customer_id	System Field
▲ ▼	Bin Number	No	ssl_bin_no	System Field
▲ ▼	Promo Code	No	ssl_promo_code	System Field
▲ ▼	Enrollment	No	ssl_enrollment	System Field
▲ ▼	Enable Auto Payment	No	auto_payment	
▲ ▼	Merchant CustId	No	custId	
▲ ▼	Close Transaction	No	closeRedirectedTransaction	
Add New Field				
▲ ▼	Shipping Address	Required	ShippingAddress	System Field
▲ ▼	Ship to Company	No	ssl ship to company	System Field

Fig. 3.15-2: Payment Fields

(4) Examples of adding these fields is in Fig. 3.15-3.

## Update Payment Field

This form is used to update a payment field. Note that all fields with an asterisk (\*) are required.

Payment Field configuration

Field Options

Name: custId

Display Name: Merchant CustId \*

Section: Order Section \*

Field Type: Text \*

Minimum Number of Characters:

Maximum Number of Characters: 100 \*

Required:

Show in Virtual Terminal:

Can be changed on Payment Form:

Show on Payment Form:

Show in Receipt:

Show in Email to Customer:

Show in Email to Merchant:

Forward on Approval:

Forward on Decline:

Show in Export Script:

Update Delete Cancel



**Payment Field configuration**

**Field Options**

**Name:** closeRedirectedTransaction

**Display Name:** Close Transaction \*

**Section:** Order Section \*

**Field Type:** Text \*

**Minimum Number of Characters:**

**Maximum Number of Characters:** 1 \*

**Required:** ☐

**Show in Virtual Terminal:** ☐

**Can be changed on Payment Form:** ☐

**Show on Payment Form:** ☐

**Show in Receipt:** ☐

**Show in Email to Customer:** ☐

**Show in Email to Merchant:** ☐

**Forward on Approval:** ☒

**Forward on Decline:** ☒

**Show in Export Script:** ☐

**Update Delete Cancel**

**Payment Field configuration**

**Field Options**

**Name:** auto\_payment

**Display Name:** Enable Auto Payment \*

**Section:** Order Section \*

**Field Type:** Checkbox \*

**Maximum Number of Characters:** 1 \*

**Required:** ☐

**Show in Virtual Terminal:** ☐

**Can be changed on Payment Form:** ☒

**Show on Payment Form:** ☒

**Show in Receipt:** ☐

**Show in Email to Customer:** ☐

**Show in Email to Merchant:** ☐

**Forward on Approval:** ☒

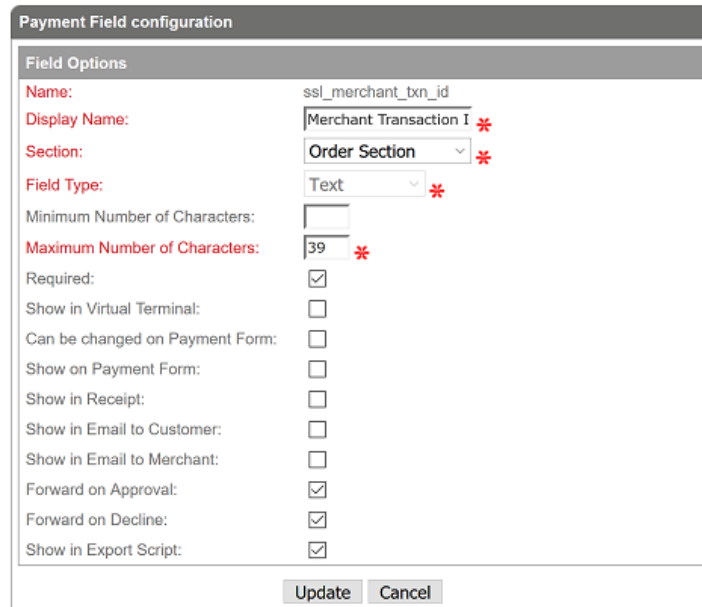
**Forward on Decline:** ☒

**Show in Export Script:** ☐

**Update Delete Cancel**

**Fig. 3.15-3: Add New Fields**

- (5) Under the Converge account please also set “ssl\_merchant”txn\_id” as shown in Fig. 3.15-4.



**Payment Field configuration**

**Field Options**

**Name:** ssl\_merchant\_txn\_id

**Display Name:** Merchant Transaction I \*

**Section:** Order Section \*

**Field Type:** Text \*

**Minimum Number of Characters:**

**Maximum Number of Characters:** 39 \*

**Required:** ☒

**Show in Virtual Terminal:** ☐

**Can be changed on Payment Form:** ☐

**Show on Payment Form:** ☐

**Show in Receipt:** ☐

**Show in Email to Customer:** ☐

**Show in Email to Merchant:** ☐

**Forward on Approval:** ☒

**Forward on Decline:** ☒

**Show in Export Script:** ☒

**Update** **Cancel**

**Fig. 3.15-4: ssl\_merchant\_txn\_id**

(6) On the Converge Account Tokenization must be enabled and DCC (dynamic currency conversion) must be disabled. Talk to Converge Support to make sure you are setup correctly.

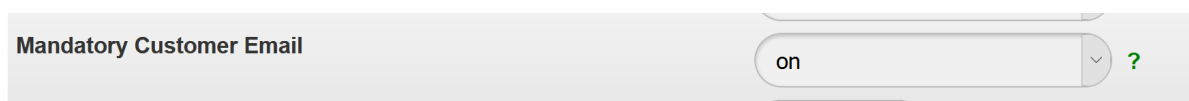
## 3.16 Paystack

Paystack is a payment gateway available in Nigeria. It is available for credit card processing but currently does not have direct debit/ACH support. End users will be redirected from the Azotel portal to the Paystack interface to add their credit card details. Once the transaction is processed the customer will be directed back to the SIMPLer End User Portal to continue browsing through their invoices and account details.

Credit cards are stored in SIMPLer so auto payment is an option available.

To configure your instance of SIMPLer for use with Paystack please do the following: -

1. Email address is a mandatory field for Paystack thus WISP Settings, within SIMPLer, need to be configured with the option "Mandatory Customer Email" enabled



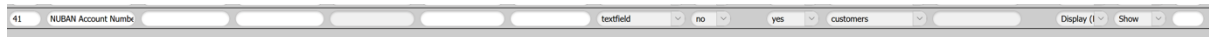
**Mandatory Customer Email**

on ?

**Fig. 3.16-1 Mandatory Customer Email**

- Under Settings => Custom Fields create a Custom Field that will be used to store the NUBAN Account Number. This field needs to be a textfield, locked and displayed under "General" TAB.

Make note of the **Custom Field ID** which will be needed in the next step.



**Fig. 3.16-2 Custom Field – NUBAN Account Number**

- Click => Settings => Payment Gateways => Add Blank Row and select Paystack under Name.

- Type in "API Public KEY" & "API Secret Key"
- Type **Custom Field ID**, from previous step, for “NUBAN Account Number Custom Field ID”

In the example above the Custom Field ID was 41 so it is entered in the appropriate field.

Make Note of the **Payment Gateway ID** which will be needed in the next step

- Enter “Redirection URL” for your instance, e.g.  
[https://<SERVER\\_NAME>/CustomerPortal/paymentSecondStage.pl](https://<SERVER_NAME>/CustomerPortal/paymentSecondStage.pl)

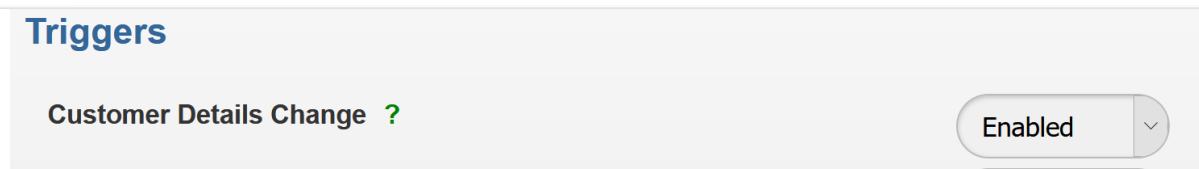
**Payment Gateways Definitions** ?

ID ?	Name ?	Availability ?	Label ?	Module Settings ?	Redirect	Token Based ?	E-check Module ?	
104	paystack <a href="#">View Log</a>	All	paystack	API_PUBLIC_KEY pk_test_b8689dbd38b30bb5a2a66447d1032 API_SECRET_KEY sk_test_2aafa6eb3e835d2ded62d2ba17530c CREATE_NUBAN 1 NUBAN_ACCOUNT_NUMBER_CUSTOM_FIELD_ID 41 NUBAN_PREFERRED_BANK  REDIRECTION_URL https://pentest.azotel.com/CustomerPortal/ URL https://api.paystack.co WEBHOOK_ALLOWED_IP_ADDRESSES 52.31.139.75 52.49.173.169 52.214.14.220	paymentSecondStage.pl	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">Delete</a>

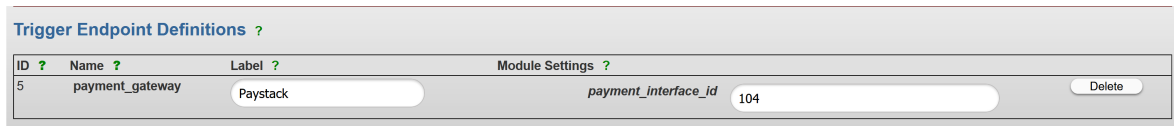
**Fig. 3.16-3 Payment Gateway**

- Click => Settings => External API (triggers) and enable "Customer Details Change". Under Trigger Endpoint Definitions add a blank row and select “payment gateway” from the dropdown list and enter in the **Payment Gateway ID** from the previous step. In the example above the **Payment Gateway ID** / Interface ID is 104.

This ensures that the Paystack Account gets created at the time the customer account is added to SIMPLer

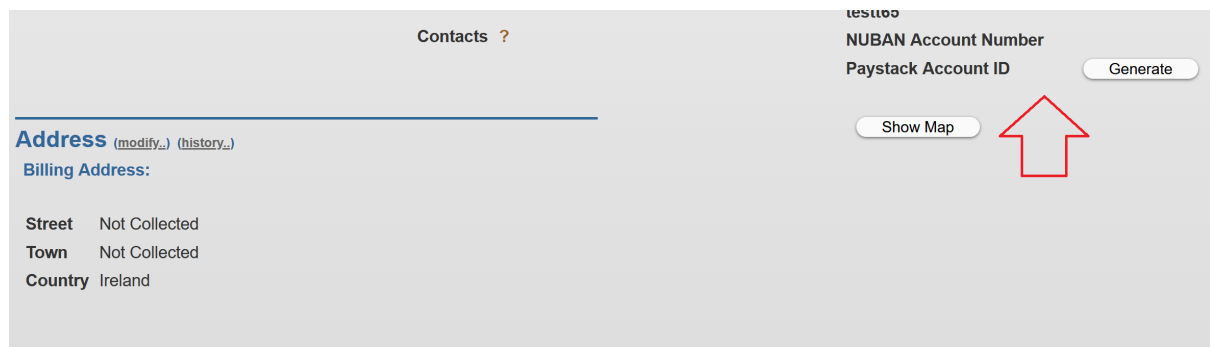


**Fig. 3.16-4 Triggers – Customer Details Change**



**Fig. 3.16-5 Trigger Endpoint Definitions**

- Under the Paystack account => webhooks configure the following endpoint - <https://<YOURSIMPLERSERVERHERE>/API/payments/paymentListener.pl> in order to receive online transfer payments.
- For an existing account or upon an unexpected error it should also be possible to create a Paystack Account from the customer details page in SIMPLer:



**Fig. 3.16-6 Create a Paystack Account from SIMPLer**

Once this is generated it will display the correct Paystack Account ID (also NUBAN Account Number should be displayed which is the Custom Field we have created)

- Once the account is created (due to security the account can and should only be created from SIMPLer) it should be good to go. The customer can start paying using "bank transfer" where the webhook will be used to capture data or make payments from the End User Portal.

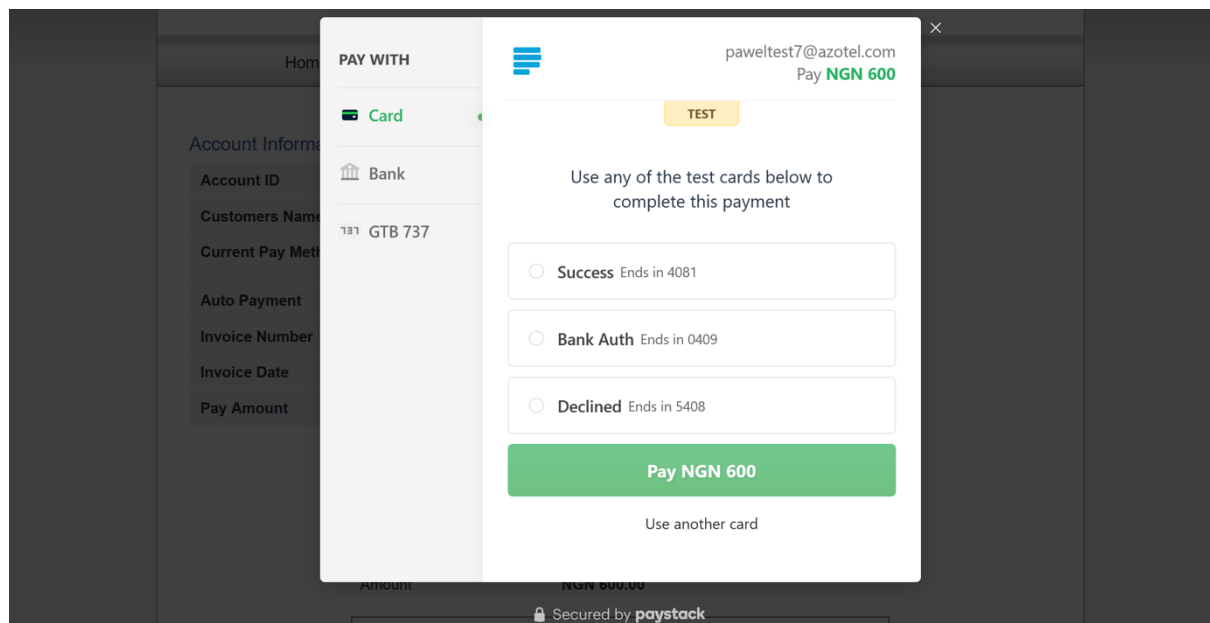
### Payment Details

Transaction Reference	<b>f754b806e63f0e8db4415745cefZ2625</b>
Invoice Number	<b>4022-66</b>
Invoice Date	<b>02 Mar 2020</b>
Amount	<b>NGN 600.00</b>

☒ Select this option to save and use the credit card information for subsequent payments.

**Pay Now**

**Fig. 3.16-7 Payment through the End User Portal**



**Fig. 3.16-8 Payment through redirection to the Paystack Portal**

8. The customer also has the option of saving their credit card details for subsequent payments so they are then able to just "charge card" to make payments.

### Payment Details

Transaction Reference      **ed4d44179862ad6088ccbb528c4Z2624**  
Invoice Number              **4022-66**  
Invoice Date                 **02 Mar 2020**  
Amount                        **NGN 600.00**

<b>Pay Now</b>	<b>Number **** * 4081</b>
<input checked="" type="checkbox"/> Select this option to save and use the credit card information for subsequent payments.	<b>Amount 600.00</b>
	<b>Charge Card</b>
	Cancel

**Fig. 3.16-9 Ability to save Credit Card Details**

---

## 4 Section Four – Banking Module Details

### 4.1 Introduction

This section will provide details of configuration and use of the banking modules outlined in section 2.3. Note that from February 2014, all Irish banking modules have been standardized and replaced by SEPA – see section 4.19.

### 4.2 Bank of Ireland

Replaced by SEPA – see section 4.19.

### 4.3 Allied Irish Bank

Replaced by SEPA – see section 4.19.

### 4.4 Ulster Bank

Replaced by SEPA – see section 4.19.

### 4.5 National Irish Bank

Replaced by SEPA – see section 4.19.

### 4.6 Eazipay

To be documented – UK banking.

### 4.7 HSBC

To be documented – UK banking.

## 4.8 Lloyds TSB

To be documented – UK banking.

## 4.9 Smart Debit

### 4.9.1. Setting up API details

Set up your SmartDebit API account. You will be provided with the following details:

- API Username
- API Password
- API PSLID
- API URL – <https://secure.ddprocessing.co.uk/api>

Provide the details to Azotel Support or enter them into “Settings->Payment Gateways Definitions” section of SIMPLer system (fig. 4.9.1 & fig. 4.9.2).

The screenshot shows the SIMPLer system interface. At the top, a navigation bar contains the following menu items: Dashboard, Map, Customers, Maintenance, Invoices, Products, Network, Hotspots, Radius, Tools, and Settings. The 'Settings' item is circled in red. Below the navigation bar, the left sidebar is divided into several sections: General (Add a new user, Add User Rights Template, Add/Modify WISP, Downloads), Customer (Groups, Custom Fields, Tracking Definitions, Post Codes), Sales Opportunities (Value Added Reseller, Master Agent, Regional Sales Manager, Sales Opportunity Types), Flexible Tax System (Tax Zones, Tax Rates), Billing (Billing Issue Types, Payment Gateways), and Templates. The 'Payment Gateways' item is circled in red. The main content area is titled 'Users' and shows a table with the following columns: User ID, Email, WISP, and Status. The table is currently empty, with a note indicating 'Results 1 - 12 of 12'.

**General:**

- Add a new user
- Add User Rights Template
- Add/Modify WISP
- Downloads

**Customer:**

- Groups
- Custom Fields
- Tracking Definitions
- Post Codes

**Sales Opportunities:**

- Value Added Reseller
- Master Agent
- Regional Sales Manager
- Sales Opportunity Types

**Flexible Tax System:**

- Tax Zones
- Tax Rates

**Billing:**

- Billing Issue Types
- Payment Gateways

**Templates:**

**Users**

Results 1 - 12 of 12

User ID	Email	WISP	Status
---------	-------	------	--------

Note:

- (1) Administrator: full access to all operators
- (2) Operator: full access to the associated WISP + can add/delete users
- (3) User: same as Operator but cannot add/delete users



**Fig. 4.9.1. Settings -> Payment Gateways**

azotel  
.....outside

WISP:  
login:  
Payment Gateways Definitions

Recently Viewed Customers

Dashboard Map Customers Maintenance Invoices Products Network Hotspots Radius

Back Reset Update Payment Gateways

Payment Gateways Definitions

ID	Name	Availability	Label	Module Settings
21				
23				
26	smartdebit View Log	SIMPLer	Pay Online	API_PASSWORD API_PSLID API_URL API_USER

Add Blank Row

[Documentation](#) | [Release Notes](#)  
copyright © Azotel Technologies Ltd. 2004 - 2013

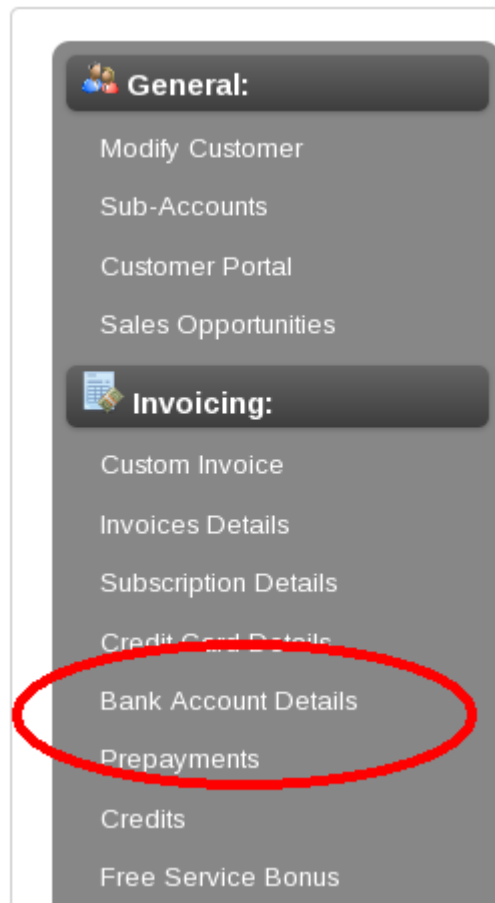
**Fig. 4.9.2. Payment Gateways Definition**

NOTE: It is important to set “Availability” flag to “SIMPLer” as this API details will only be used within “Invoices to be EFT” page of SIMPLer system.

#### 4.9.2. Adding Bank Account Details to Customer Account

It is required that customers have valid bank account details under their accounts in order to add/process their details successfully via SIMPLer – SmartDebit API.

In order to add/update customer bank account details go to the customer account and click “Bank Account Details” link on the left-hand menu (fig. 4.9.3)



**Fig. 4.9.3. Customer Account -> Bank Account Details**

On the “Bank Account Details” page enter correct bank account information (fig. 4.9.4).

NOTE: It is very important to keep Bank Online Reference field unique in the database, i.e., each customer must have unique Bank Online Reference number.

NOTE: It is very important to have First Time Direct Debit flag set correctly. If “ON” then bank account details will be active on the “Invoices to be EFT” page to import it via API to SmartDebit. If “OFF” then bank account details will be disabled to be uploaded to SmartDebit. This flag changes itself automatically from ON to OFF if customer bank account details are imported to SmartDebit system via API.

The screenshot displays the 'outside' web interface for 'EFT details'. The top navigation bar includes 'Logout', 'Update WIB files', and a 'QuickSearch ...' field. The main menu contains 'Dashboard', 'Map', 'Customers', 'Maintenance', 'Invoices', 'Products', 'Network', 'Hotspots', 'Radius', 'Tools', and 'Settings'. The 'Customers' section is active, showing 'Customer Details' for ID 7, Name Frank Hannigan, Nickname F\_Hannigan, and Invoicing ID FHANNIG. Below this are 'Back' and 'Update' buttons. A red banner states: 'Modifications will be applied only if you press the "Update" button'. The 'Auto Payment - Processing Day of Month' is set to 'default'. The 'Customer Bank EFT table' contains one entry with columns: Preferred (checked), Bank Account Number (12345678), Bank Sort Code (123456), Bank Online Reference (REF-1234), Bank Account Name (John Doe), First Time Direct Debit (on), and a Delete button. An 'Add Row' button is at the bottom left. Footer links include 'Documentation' and 'Release Notes', with a copyright notice for Azotel Technologies Ltd. 2004 - 2013.

**Customer Details**

ID: 7  
 Name: Frank Hannigan  
 Nickname: F\_Hannigan  
 Invoicing ID: FHANNIG

Back Update

Modifications will be applied only if you press the "Update" button

Auto Payment - Processing Day of Month: default ?

**Customer Bank EFT table**

Preferred	Bank Account Number	Bank Sort Code	Bank Online Reference	Bank Account Name	First Time Direct Debit	
<input checked="" type="checkbox"/>	12345678	123456	REF-1234	John Doe	on	Delete

Add Row

[Documentation](#) | [Release Notes](#)  
 copyright © Azotel Technologies Ltd. 2004 - 2013

**Fig. 4.9.4. Bank Account Details**

NOTE: Customer must have other details entered correctly in order to allow importing their details to SmartDebit. Those details are:

- Address – Street 1
- Customer Name
- Address – City/Town
- Address – ZIP / Post code

If any of the above is missing SIMPLer will refuse to import customer bank account details to SmartDebit via API. Those details can be updated under main “Modify Customer” Page (fig. 4.9.5)

**Customer Identification**

Name  \*

Invoicing ID

Nickname  \*

Value Added Reseller

---

**Customer Address Details**

**Billing Address**

- Street1

- Street2

- Town

- County

- Post Code

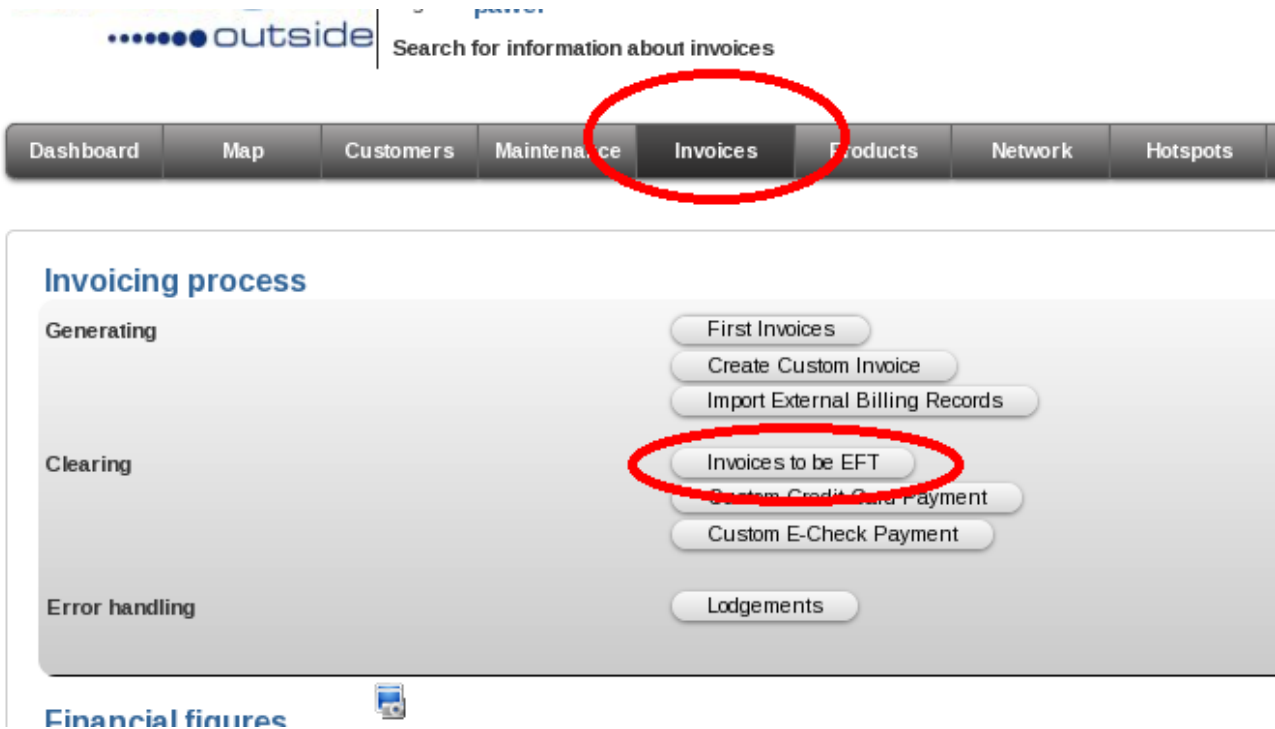
- Country

**Fig. 4.9.5. Modify Customer Details**

### 4.9.3. Import Customer Bank Account Details via API

In order to get customer accounts imported to SmartDebit via Azotel SIMPLer – SmartDebit API Interface follow the steps

1. Go to the “Invoices-> Invoices to be EFT” page (fig. 4.9.6)



**Fig. 4.9.6. Invoices -> Invoices to be EFT**

- On "Invoices to be EFT" page from "Direct Debit Module" drop-down list select "Smart Debit". Two new buttons will show up – "Download New Payer's File" and "Generate New Payer's File (nnn)". Number in parenthesis of "Generate New Payer's File (nnn)" shows information about number of bank accounts waiting to be imported to Smart Debit. This number is generated based on "First Time Direct Debit" flag. Thus nnn is a number of all bank accounts in the system that have "First Time Direct Debit" flag set to ON. If you click on "Generate New Payer's File (nnn)" button it will generate the file and automatically imports it via API to SmartDebit (fig. 4.9.7).



**Fig. 4.9.7. "Smart Debit" Direct Debit Module**

- Generating New Payer's File can return an error if some of the details are missing or incorrect. In that case customer bank account details will not be imported to SmartDebit via API and "First Time Direct Debit" flag will not get changed from ON to OFF. You can review Error Log to find all the errors found, fix the errors, reload "Invoices to be EFT" page and click "Generate New Payer's File" again (fig. 4.9.8 and fig. 4.9.9)

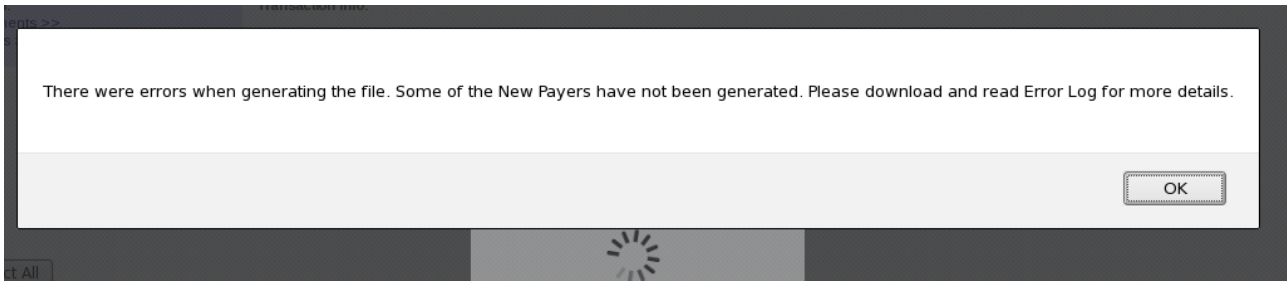


Fig. 4.9.8. Error Message

Console X

File	Created By	Created Date	Error Log
<a href="#">New Payer's File #55</a>	pawel	2013-06-10	<a href="#">Error Log #55</a>
<a href="#">New Payer's File #54</a>	pawel	2013-06-10	<a href="#">Error Log #54</a>
<a href="#">New Payer's File #53</a>	pawel	2013-06-10	<a href="#">Error Log #53</a>
<a href="#">New Payer's File #52</a>	pawel	2013-06-06	<a href="#">Error Log #52</a>
<a href="#">New Payer's File #51</a>	pawel	2013-06-06	<a href="#">Error Log #51</a>

Page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#)

Fig. 4.9.9. Generate/Import Result

#### 4.9.4. Generate and Import Charge File

If customer bank accounts details are imported you can generate/import charge file. Importing charge file via API to SmartDebit happens in the background when lodgement is generated. If some of the charges cannot be imported error message will be displayed on the summary page. If some of the charges are imported successfully and some of the charges are not imported due to errors lodgement will be created for all charges. It is required that erroneous charges are added manually to SmartDebit or they are failed in SIMPLer system. If all the charges are incorrect then charge file will not be imported at all.

In order to Generate Lodgement and Import Charge File to SmartDebit (fig. 4.9.10)

- select processing date
- select appropriate charges
- click “Generate” button

Select All	Customer ID	Invoicing ID	Name	Status	Invoice Date	Amount	Choose Bank Account	Invoice No.	Available Prepayments
<input checked="" type="checkbox"/>	Z			current	10 Jun 2013	2691.00	123456 12345678 - REF-1234	44497	0.00
<input checked="" type="checkbox"/>	Z			current	10 Jun 2013	2691.00	123456 12345678 - REF-1234	44498	0.00
<input type="checkbox"/>	Z			current	10 Jun 2013	1794.00	123456 12345678 - REF-1234	44499	0.00
<input type="checkbox"/>	Z			current	10 Jun 2013	1794.00	123456 12345678 - REF-1234	44500	0.00
<input type="checkbox"/>	Z			current	10 Jun 2013	2691.00	123456 12345678 - REF-1234	44501	0.00
<input type="checkbox"/>	Z			current	10 Jun 2013	2691.00	123456 12345678 - REF-1234	44502	0.00
<input type="checkbox"/>	Z			current	10 Jun 2013	1794.00	123456 12345678 - REF-1234	44503	0.00
<input type="checkbox"/>	Z			current	13 May 2009	97.56	123456 12345678 - REF-1234	44504	0.00
<input type="checkbox"/>	Z			current	13 Aug 2009	97.56	123456 12345678 - REF-1234	44505	0.00
<input type="checkbox"/>	Z			current	13 Nov 2009	32.52	123456 12345678 - REF-1234	44506	0.00
<input type="checkbox"/>	Z			current	13 Feb 2010	48.78	123456 12345678 - REF-1234	44507	0.00
<input type="checkbox"/>	Z			current	10 Jun 2013	2206.62	123456 12345678 - REF-1234	44508	0.00
<input checked="" type="checkbox"/>	133			current	07 May 2013	70.27	000000 12345678 - 1331000	44182	0.00
<input checked="" type="checkbox"/>	140			current	11 May 2013	120.00	000000 12345678 - 1401000	44304	0.00
<input checked="" type="checkbox"/>	154			current	16 May 2013	80.00	000000 12345678 - 1541000	44451	0.00

Fig. 4.9.10. Generate Payment

Example result of the import/lodgement is displayed on figure 4.9.11. Note the information in red colour.

General:  
Lodgements >>  
Invoices >>

**Note:**  
The A2439\_winbits\_airwave\_5652.txt file was created successfully for the customers listed below.

Lodgement Details:  
Reference: A2439 [2448]  
Narrative:  
Date: 03 Jul 2013  
Type: direct debit

[Download Winbits File](#)

Invoicing ID	Processing date	Outstanding Invoice Amount	Payment Amount
	01 Jul 2013	70.27	70.27
	01 Jul 2013	120.00	120.00
	01 Jul 2013	80.00	80.00
	01 Jul 2013	2691.00	2691.00
	01 Jul 2013	2691.00	2691.00
<b>Total Amount:</b>		5652.00	

An email was sent to pawel@azotel.com

**\*\*\*IMPORTANT\*\*\*** The following errors were found when importing winbits file via API to SmartDebit. You may want to upload those charges manually or fail the payments under the lodgement ([Open Lodgement Details](#)) created:

Line 1: Not imported: DDI "1331000" not found.  
Line 3: Not imported: DDI "1541000" not found.  
Line 4: Not imported: DDI "REF-1234" not found.

Fig. 4.9.11. Result of generating payment

## 4.9.5. WISP Options

It is required that two following options are set under “Settings->Modify WISP” to get the feature working properly:

1. Banking Details Schema is set to “UK Banking Scheme” (fig. 4.9.12).

Bank Details Schema

UK Banking Scheme

Fig. 4.9.12. Bank Details Schema

2. EFT – Consolidate multiple payment entries for each Customer processed is ON (fig. 6.2).

EFT - Consolidate multiple payment entries for each Customer processed

on



**Fig. 4.9.13. Consolidate multiple payment entries for each customer processed**

## 4.10 Security National Bank

To be documented.

## 4.11 Bank of Montreal

Firstly, under the Settings – Modify WISP page of SIMPLer, the “bank details schema” selected must be “Canadian Banking System”.

To create a file compatible with the Bank of Montreal format please visit the Invoices tab and Invoices to be EFT.

Select the bank name “Bank of Montreal” and the correct payment processing date. Enter a narrative text for your payment transaction if desired. Check off all invoices to be processed in this ACH run and click on the “generate” button. A copy of the file will be sent automatically to your accounts email but is also available to download on the Invoices – Lodgements (or Bank Deposits) page.

Log on to the Bank of Montreal Portal for direct banking for business. Choose the file transfer facility and upload the file exactly as it has been created. Click on “send” to complete the upload process.

Errors are reported within an hour or two and must be checked on the Bank of Montreal site. The error correction process must be completed on the Bank of Montreal site.

Funds should hit your bank account within a day. Payment failures may take several days to come back and are sent to the Bank of Montreal portal. Failures must be failed manually in SIMPLer.

## 4.12 CPA Standard 005

To be documented.

## 4.13 Alberta Treasury Bank

From a SIMPLer perspective the following details must be configured:

- (1) Under the Settings – Modify WISP page in the banking details section, the information must be as complete as possible. The fields circled in RED on the fig. 4.13-1 are mandatory for ATB. Those are: Originator ID, Bank Account Number, Destination Data Centre, Originator’s Long Name, Originator’s Short Name, and Currency.



## Banking details

<b>Bank Details Schema</b>	Canadian Banking Scheme ?
<b>Bank Address - Street1</b>	[Redacted] ?
- Street2	[Redacted] ?
- Town	[Redacted] ?
- Province	[Redacted] ?
- Post Code	[Redacted] ?
- Country	[Redacted] ?
<b>Originator ID</b>	[Redacted] ?
Institution ID (0BBBTTTTT) where BBB = Bank, TTTT = Bank Transit Number	
<b>Bank Account Number</b>	[Redacted] ?
Destination Data Centre	[Redacted] ?
Originator's Long Name	[Redacted] ?
Originator's Short Name may be printed on Payor's account statement	[Redacted] ?
HST Reg No	[Redacted] ?
Global HST rate	[Redacted] ?
Global Flat TAX amount	[Redacted] ?
Setup HST rate	[Redacted] ?
<b>Currency</b>	CAD ?
Invoice Billing Period Dates Shift [months]	[Redacted] ?
Email Banking Information	Off ?

**Fig 4.13-1: Banking Details**

- (2) Next the operator must make sure that:  
Customers who should be processed have bank details on file, and are set to payment method direct debit (PAD/ACH).

**Customer Billing Details** QuickSearch ...

<b>Billing Details</b> (modify) (history) <b>Invoicing Status</b> Yes <b>Payment Method</b> direct debit <b>Frequency</b> 1 month(s) <b>Credit Days</b> <b>Send Method</b> Email to Customer <b>VAT / TAX Exemption</b> No <b>Folder</b>	<b>Financial Summary</b> (statement) <b>Prepayments</b> (Amount Remaining) CAD 0.00 CR <b>Credits</b> (Amount Remaining) CAD 0.00 CR <b>Customer Balance</b> CAD 136.48 DR <b>Next Invoice Details</b> <b>Date</b> 15 Apr 2013 <b>Total Amount</b> CAD 68.24	<b>Last 5 Invoices</b> (all) <table border="1"> <thead> <tr> <th>No</th> <th>Date</th> <th>Amount</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>49</td> <td>15 Mar 2013</td> <td>68.24</td> <td>68.24 DUE</td> </tr> <tr> <td>15</td> <td>15 Feb 2013</td> <td>278.24</td> <td>68.24 DUE</td> </tr> </tbody> </table>	No	Date	Amount	Status	49	15 Mar 2013	68.24	68.24 DUE	15	15 Feb 2013	278.24	68.24 DUE	<b>Last 5 Credits</b> (all) <table border="1"> <thead> <tr> <th>Description</th> <th>Date</th> <th>Amount</th> <th>Remaining</th> </tr> </thead> <tbody> <tr> <td colspan="4">No credit has been added yet</td> </tr> </tbody> </table>	Description	Date	Amount	Remaining	No credit has been added yet			
No	Date	Amount	Status																				
49	15 Mar 2013	68.24	68.24 DUE																				
15	15 Feb 2013	278.24	68.24 DUE																				
Description	Date	Amount	Remaining																				
No credit has been added yet																							

**Quick Links**

- Custom Invoice ?
- Custom Credit Card Payment ?
- Custom E-Check Payment ?
- Apply Payment To Customer ?
- Apply Payment To Invoices ?
- Consolidate Subscriptions ?
- Payment Authorization Codes ?

**Credit Card Details** (modify) (history)  
 No Credit Card Details available

**Bank Account Details** (modify) (history)

Number	Expiration Date	Holder	Type	First Name	Last Name	Address	City
No Credit Card Details available							

**Subscription Details** (modify) (history) (consolidate subscriptions)

**Fig 4.13-2: Customer Banking Details**

To generate a file the operator must visit the Invoices – Invoices to be EFT page as shown in Fig. 4.13-3.

**Dashboard** **Map** **Customers** **Maintenance** **Invoices** **Products** **Network**

**Invoicing process**

<b>Generating</b>	First Invoices Create Custom Invoice Import External Billing Records
<b>Clearing</b>	Invoices to be EFT / PAC Custom Credit Card Payment Custom E-Check Payment
<b>Error handling</b>	Lodgements

**Fig 4.13-3: Invoices to be EFT**

Next, select the module “Alberta Treasury Branches” and select the invoices to be processed and click “generate”.

**General:**  
Lodgements >>  
Invoices >>

**Transaction Info:**  
Processing date  
Bank Name  
Customer SAND Status ?  
Reference text  
Narrative Text  
Sequence Number

May 31 2017  
Alberta Treasury Branches  
All

A3

Select All

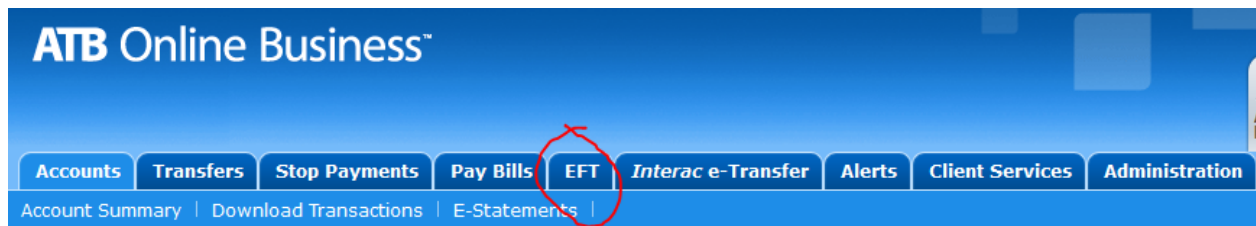
Generate	Customer ID	Invoicing ID	Name	Status	Invoice Date	Amount	Ch
<input type="checkbox"/>	1430			current	Mar 14, 2017	-118.89	
<input type="checkbox"/>	1430			current	Jun 15, 2017	304.45	
<input type="checkbox"/>	1430			current	Jun 15, 2017	57.70	

Generate

**Fig 4.13-4: Invoices to be EFT Processing**

Finally, after you generate the file, you can download it and upload it to the bank. Generation of file will also create bank deposits in SIMPLer so selected customers/invoices will be 'under EFT'. After couple of days you should get confirmation about successful / declined payment from your bank. If there will be any failures you can go to the Bank Deposits in SIMPLer, find created bank deposit and fail particular payments.

On the bank side you must log in and then click "EFT".



**Fig 4.13-5: ATB - EFT**

Click "Import EFT File" and Next.

Select the EFT file type and the option that describes the type of EFT two business days prior to the transaction due dates.

File Type: Mixed

☐ Create EFT File manually  
☐ Create EFT File from a template --- Select Template ---  
☒ Import EFT File

Next

Liquidity Balance:

**Fig 4.13-6: Import EFT File**

Browse and select the file you wish to upload (the file generated earlier). Provide a description and Import the File.

## Import Files

To import your EFT file, select the file details and the fully qualified path to the file or click Browse to locate the file, then click **Import File**.

Note: Once submitted, please ensure that you review the status of the import in the Imported Files tab.

\*Required

File Format: ☒ 96-Byte ☐ 1464-Byte ☐ CSV


Type of EFT file:

Keep receiver details after import? ☐ Yes ☒ No

File to Import: \*  No file selected.

File Description\*

**Import File**

 Review Status window on the bottom right hand corner.

**Fig 4.13-7: Browse & Import**

Once this is complete you will be taken to a processing page. It takes a few days to process.

## 4.14 Norma 19

To be documented. Spanish banking system.

## 4.15 Banco Santander

To be documented. Spanish banking system.

## 4.16 Netcash Debit

**To be replaced by Sagepay Debit in summer 2016. See section 4.22.**

SIMPLer has integrated with Netcash for two processes:

- Credit Card interface. (Explained in Section 3.8) Replaced with SagePay (Section 3.10)
- Direct Debit Module.

Note: The following details are required to use the Netcash Debit module. Please send to Azotel:

<b>CANCEL</b>	<input type="text"/>
<b>PASSWORD</b>	<input type="text" value="YOUR_API_PASSWORD_HERE"/>
<b>PIN</b>	<input type="text" value="YOUR_PIN_HERE"/>
<b>TERMINALID</b>	<input type="text" value="YOUR_TERMINALID_HERE"/>
<b>USERNAME</b>	<input type="text" value="YOUR_API_USERNAME_HERE"/>

### Direct Debit Module:

**Step One:** Please enter your bank details into the Banking Details section of “Settings -> modify WISP”.

**Step Two:** When adding customers to SIMPLer, payment method “direct debit” should be selected from the banking details tab. Bank account details need to be added also from the “bank account details” section.

**Step Three:** To process the EFT payments, please visit the Invoices -> Invoices to be EFT tab. Check off invoices to be selected. Click on the “generate” button to generate the winbits file. This will be sent to your accounts email.

**Step Four:** Visit the Netcash Portal. The exact location will be under the **debit collections** tab, under the NetFTP File upload section. If you have not already done so, you will need to ask Netcash for separate credentials to visit this page. Once you have entered this section successfully, you will go to the file upload tab. Choose the Azotel generated file. Upload the file and wait at least one minute to make sure the upload process is complete. On the Upload report tab, you will find any errors reported, such as missing bank account details. Go to the verify action date tab. The file will now be loaded to the directdebit batch, which you can authorize under point five.

**Step Five:** Authorize the batch file in the Netcash Portal under the manage debit batches tab. One day or two day payment process can be selected in the Netcash Portal.

**Step Six:** Once the Netcash payments have been submitted you should expect a report showing any failed/bounced payments within 3-4 days. These will have to be failed in SIMPLer on the invoices -> lodgements tab.

## 4.17 NACHA Format

To be documented.

## 4.18 First National Bank

**Step One:** Please enter your bank details into the Banking Details section of “Settings -> modify WISP”.

**Step Two:** When adding customers to SIMPLer, payment method “direct debit” should be selected from the banking details tab. Bank account details need to be added also from the “bank account details” section.

**Step Three:** To process the EFT payments, please visit the Invoices -> Invoices to be EFT tab. **Select the bank name “First National Bank”**. Check off invoices to be selected. Hit “generate” to generate the winbits file. This will be sent to your accounts email.

**Step Four:** Visit the First National Bank Portal. Here you must upload the winbits file. The location for uploading this file is “Collections -> from file -> import). The process should take less than five minutes.

**Step Five:** Once the FNB payments have been submitted you should expect a report showing any failed/bounced payments within a couple of days. FNB failures are reported the day after you submit the file, unless the next day is a Sunday, in which case you will receive the report the day after. Failures from other banks will arrive two days after the debit order run. These will have to be failed in SIMPLer on the invoices -> lodgements tab.

## 4.19 SEPA Banking

### Overview:

On February 1<sup>st</sup> 2014, a new direct debit payment method will come into effect across Europe. This banking method is called SEPA, (Single Euro Payments Area) and works to standardise Direct Debit payments across all banks.

SEPA works similarly to previous banking formats in that once invoices are generated in SIMPLer a file of payments must be generated and uploaded to banks for processing. The new file can be generated from the invoices tab, the section will be called “**SEPA EFT debits**”.

### Requirements:

To use the SEPA banking module the following must be complete:

**Step One:** Fill out OPERATOR banking details under Settings -> Modify WISP as shown in fig. 4.19-1 and explained in table 4.19-2.

### Customer Bank Account Details / EFT Options

Disable Default EFT Fields / EFT Module	off	?
Require Default EFT Fields	yes	?
Require Dynamic Module EFT Fields	no	?
SEPA EFT Module	on	?
SEPA: Creditor Address		?
SEPA: Creditor BIC		?
SEPA: Creditor IBAN		?
SEPA: Creditor Name		?
SEPA: Submitter OIN		?
SEPA: Submitter OIN - XML Field	PvtId	?
SEPA: Ultimate Creditor Name		?
Validate IBAN	on	?

**Fig. 4.19-1: Customer Bank Account Details / EFT Options**

Field	Description
Disable Default EFT Fields / EFT Module	To disable the old EFT fields from the previous banking scheme select “on” here. Both can co-exist during the switchover process but this should be enabled by Feb 01 2014.
Require Default EFT Fields	When enabled, if the default EFT fields are not provided – customer bank details will not be saved. Can be disabled once operators have FULLY cut over to SEPA.
Require Dynamic Module EFT Fields	When enabled, if the SEPA EFT fields are not provided – customer bank details will not be saved.
SEPA EFT Module	Setting to “on” will enable the SEPA module.
SEPA: Creditor Address	Optional – enter creditor (operator) address here.
SEPA: Creditor IBAN	Mandatory – enter creditor (operator) IBAN here.
SEPA: Creditor Name	Mandatory – Creditor (operator) name must be entered here. Must match up with bank records.
SEPA: Submitter OIN	Submitter’s OIN must be populated here. Also referred to as the submitter’s SEPA user ID. This 13 digit code will be in the format IEXXSDDZZZZZZ where XX is a check digit and ZZZZZZ is a 6 digit identification number.

	This OIN will be communicated to the customer by the bank.
SEPA: Submitter OIN – XML Field	XML field that is to be used for Submitter OIN. This will differ from bank to bank. Bank of Ireland Operators need to select “PrivId” and Allied Irish Bank operators should choose OrigId.
SEPA: Ultimate Creditor Name	Optional: Full name of Creditor can be entered here. If populated will be carried with payment.
Validate IBAN	Enables validation of any IBAN related fields.

**Fig. 4.19-2: Customer Bank Account Details / EFT Options**

**Step Two:** Make sure that SEPA EFT fields have been entered to customer accounts set up for DD payments.

Please fill in the below:

- SEPA BIC / SWIFT: Customer BIC
- SEPA Debtor Country: Default IE
- SEPA Debtor Name: Customer Bank Account name
- SEPA IBAN: Customer IBAN
- SEPA Remittance Data:
- SEPA Sequence Type: **First time Debits** should be selected for first SEPA run. It will automatically default to **Recurring debits** after the first file is generated.
- SEPA Signature Date: Date of signing mandate.

**Step Three:** Customer must have an invoice on their account and payment method set to Direct Debit.

**Step Four:** Navigate to the “Invoices” tab and click on “SEPA EFT Debits”.

Select correct Transaction Info. (See fig. 4.19-3)



**Transaction Info:**

- 1 Invoice Date To: ?
- 2 File Processing Date ?
- 3 Debit Collection Date ?
- 4 File Format ?
- 5 Sequence Type ?
- 6 Reference text ?
- 7 Narrative Text ?

**Fig. 4.19-3: Transaction Info**

1. **Invoice Date to:** This field is used to filter out unwanted invoices from the search. Mostly, operators will run a direct debit run around 14 days after the invoice date. If they wish to exclude all invoices up to this date they can modify this search parameter.
2. **File Processing Date:** Default is today's date. This is the file generation date and the date you will upload the file to the bank's portal.
3. **Debit Collection Date:** The date the monies should appear in your bank account. Note that this will need 6 working days for First Time DD, and 3 working days for Recurring Debits.
4. **File Format:** Default SEPA XML (PAIN.008)
5. **Sequence Type:** There are four types of payments: First Time Payments, Recurring Payments, Final Payments and Once Off Payments. The most commonly used will be "first time" (for all FIRST SEPA runs) and recurring. You can also choose to run "all" in the one file, but it is recommended to run all "first time" direct debits in one file and recurring debits separately. These can be filtered here by choosing each option from the drop-down.
6. **Reference Text:** SIMPLer lodgement reference.
7. **Narrative Text:** SIMPLer narrative reference.

**Step Five:** Generate SEPA file.

Select All	Customer ID	Invoicing ID	Name	Status	Invoice Date	Amount	Choose Bank Account	Invoice No.	Available Prepayments
Generate	34			current	01 Dec 2013	50.00		12010	0.00
Generate									

**Fig. 4.19-4: Generate SEPA File**

Select the relevant files by checking the appropriate boxes. The text will show in red if important details (such as banking details) are missing. Verify and generate the file.

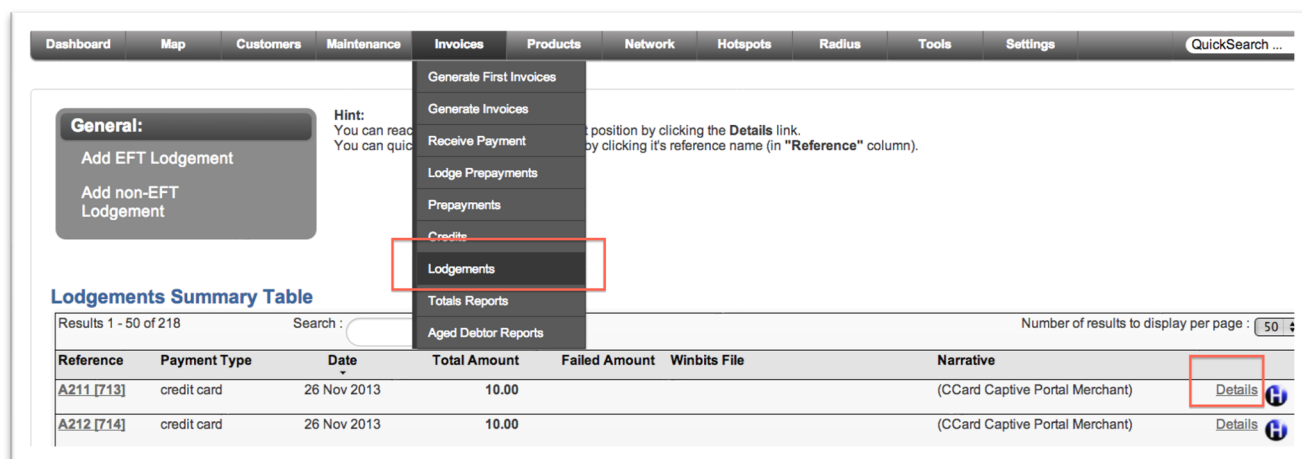
**Step Six:** Upload the file to the bank.

**Step Seven:** Await confirmation and payment.

### Logging Payment Failures in SIMPLer.

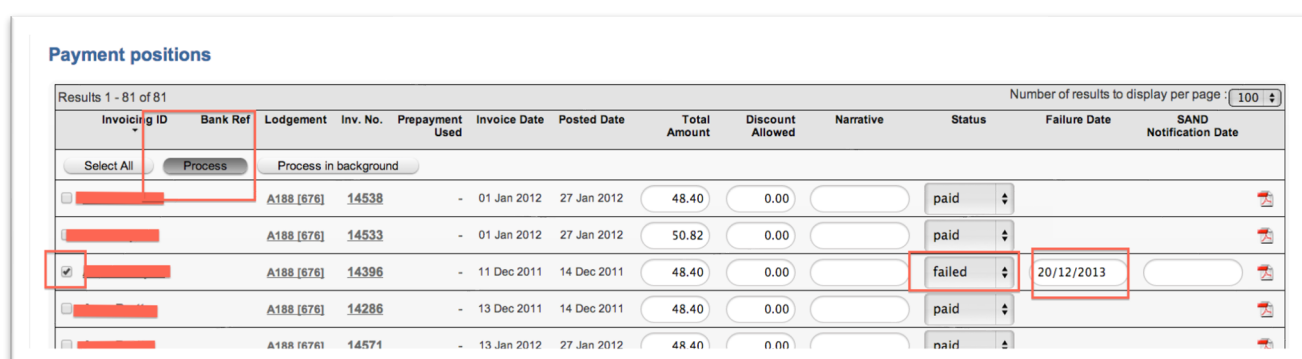
**Step One:** Navigate to Invoices -> Lodgements tab in SIMPLer.

**Step Two:** Locate the file in question and click on the “details” link.



**Fig. 4.19-5: Lodgement Details**

**Step Three:** Locate the relevant payment position. Check box. Move the payment from paid to failed. Choose appropriate failure date. Click “process”. The paid invoice will move back to unpaid and can be processed in the next banking run.



**Fig. 4.19-6: Lodgement Details**

## 4.19.1 SEPA Banking: 2016 Updates

In 2016, a number of changes have been developed as per the new SEPA requirements received from Bank of Ireland during the year. These have been documented below.

1) Amendments to Debtor Account Details.

This covers situations where a customer mandate has been amended somewhere down the line with new bank account details without filing a new mandate. From a practical point of view, each time there will be a change made to an EFT account in SIMPLer that has already been used for processing, the system will add a dedicated amendment clause to the SEPA file.

## 2) Shorter Cycle Timelines: Bank of Ireland File Submission Date reduced to D-1 (Optional)

Previously, Bank of Ireland required operators to use a “debit collection date” that was 6 working days in advance of the “file processing date” for new debits, and three working days for recurring debits. To be safe, in the case of weekends and bank holidays, in SIMPLer we had previously defaulted the debit collection date to 10 days after the file processing date, as demonstrated in Fig. 4.19.1-1.

**Fig. 4.19.1-1: Debit Collection Date**

From now on, at least in the case of the Bank of Ireland SEPA files it is possible to submit with one day lead time, for both first time and recurring debit.

In the WISP Settings (Settings – Modify WISP) there is a new option called “SEPA: Transaction Cycle Timeline” that can be updated to set the default debit collection date in number of days after the file processing date.

**Fig. 4.19.1-2: SEPA: Transaction Cycle Timeline**

## 3) SIMPLer use of sequence types: First/Recur (Optional)

This optional update takes away the need to use the “FRST” sequence type when taking a direct debit for the first time. All debits can be processed as RCUR now. There is a new option in the WISP Settings (Settings – Modify WISP) called “SEPA: Debtor Default Sequence Type” where the operator can define what the sequence type should be. If left blank all will stay as it usually was, as this is an optional update.

SEPA: Debtor Default Sequence Type

SEPA: Debtor (Customer) BIC Field

SEPA: Debtor (Customer) Default Remittance Data

FRST  
RCUR  
OOFF  
FNAL

**Fig. 4.19.1-3: SEPA: Debtor Default Sequence Type**

- 4) Some additional options were added recently for ease of use.

SEPA: Debtor (Customer) BIC Field: This option allows operators to grey out the BIC field for customer bank accounts.

SEPA: Debtor (Customer) Default Remittance Data: Allows the operator to specify the default remittance data that should go into new bank accounts.

SEPA: Debtor (Customer) Default Signature Date: Allows the operator to specify that the signature date should default to the current date for new bank accounts. The other option is to leave the date blank.

SEPA: Debtor (Customer) BIC Field

Enabled

SEPA: Debtor (Customer) Default Remittance Data

SEPA: Debtor (Customer) Default Signature Date

Undefined

**Fig. 4.19.1-4: SEPA: New Options**

## 4.20 Cajamar

Cajamar is a bank used in Spain and can accept versions of the SEPA format, however, another method used it uploading an XLS file to the bank and having the SEPA conversion take place at the bank level.

To enable Cajamar banking in SIMPLer please visit the Settings – Modify WISP and enable the settings shown in fig. 4.20-1.

### Customer Bank Account Details / EFT Options

Cajamar Caja Rural (Spain) EFT Module

on

**Fig. 4.20-1: Cajamar WISP Setting**

Once you have invoiced the customers in SIMPLer you should be able to visit the Invoices tab and click on an option called Cajamar Bank EFT Debits as shown in Fig. 4.20-2.

Clearing

Cajamar Bank EFT Debits

Invoices to be EFT

Custom Credit Card Payment

Custom E-Check Payment

### Fig. 4.20-2: Cajamar Bank EFT Debits

Here you will see the outstanding invoices for customers with the payment method set to direct debit, and with banking details on file. Set the appropriate debit collection date and check off the customers to be processed. Click “generate” to complete the process of creating the file.

The file should be sent to your accounts email, and is also available to download under Invoices – Lodgements.

Submitting the file to the bank:

- 1) Sign in to online banking.
- 2) Click Remesas Web. (Fig. 4.20-3)

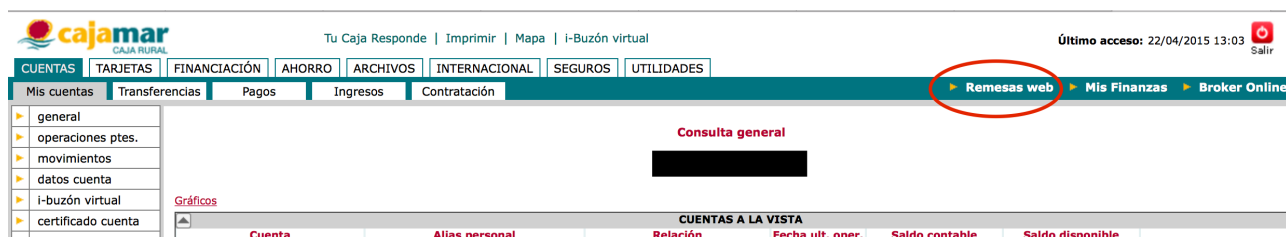


Fig. 4.20-3: Cajamar – Remesas Web

- c) Click Importar fichero (Fig. 4.20-4).



Fig. 4.20-4: Cajamar – Importar Fichero

- d) Click A partir de un fichero excel. (Fig. 4.20-5)



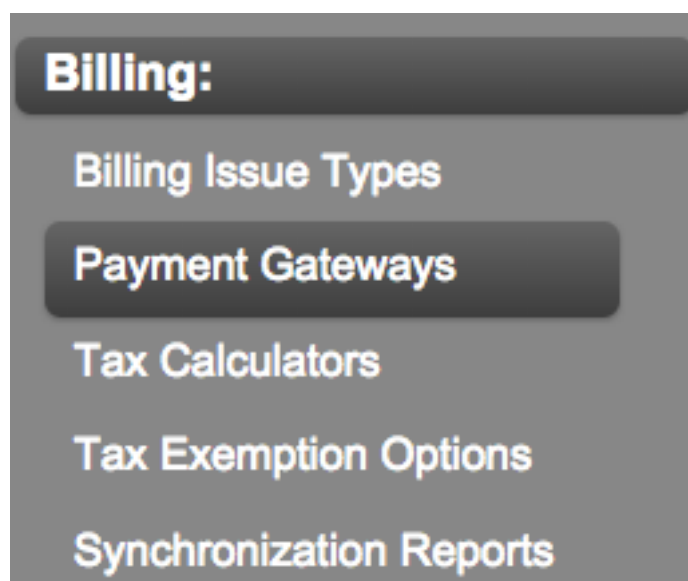
**Fig. 4.20-5: Cajamar – A partir de un fichero excel**

- e) Once this file has been loaded, you will be redirected to Fig. 4.20-3, the uploaded data can be confirmed and submitted when required.

## 4.21 GoCardless

### 4.21.1. SIMPLer Setup

To set up your GoCardless Payment Gateway in SIMPLer please navigate to the Settings – Payment Gateways page of SIMPLer as shown in figure 4.21-1.



**Fig. 4.21-1: Settings – Payment Gateways**

On the payment gateways page (Fig. 4.21-2) you will be asked for a number of different settings:

1. ACCESS\_TOKEN: The Access Token you will have generated under your GoCardless Portal.

2. ENDPOINT\_URL: For the production environment it should be api.gocardless.com
3. HOSTED\_PAGE\_EUP\_DEFAULT\_AUTO\_PAY\_ON: The value should be set as 1 or 0. If set to 1 then new bank account added will be automatically set for auto-payment when added via the End User Portal.
4. SUCCESS\_REDIRECT\_URL – this is URL where the customer should be redirected after adding a bank account. It should be always in one of the following formats, depending on the server used.
  - [https://<simpler\\_server>/CustomerPortal/closeRedirectedTransaction.pl](https://<simpler_server>/CustomerPortal/closeRedirectedTransaction.pl)
  - [https://<simpler\\_server>/CP/closeRedirectedTransaction.pl](https://<simpler_server>/CP/closeRedirectedTransaction.pl)
5. WEBHOOK\_SECRET – that is the secret code generated under GoCardless portal

42	GoCardless View Log	All	Pay Online	ACCESS_TOKEN	kq1B9hw_FlpRgi3hFoTceS4f2MR2vdR4UqBtfr
				ENDPOINT_URL	api-sandbox.gocardless.com
				HOSTED_PAGE_EUP_DEFAULT_AUTO_PAY_ON	
				SUCCESS_REDIRECT_URL	https://84.203.220.160/CustomerPortal/close
				WEBHOOK_SECRET	test1234

Add Blank Row ?

**Fig. 4.21-2: Payment Gateway Settings**

Finally, ask Azotel Support ([support@azotel.com](mailto:support@azotel.com)) to set the following settings for you:

- 1) Tokenized Modules – Add Bank Account Options
- 2) Billing – EFT token based solution

**Tokenized Modules - Add Bank Account Option**  ?

**Fig. 4.21-3: Tokenized Modules – Add Bank Account Options**

**Billing - EFT token based solution**  ?

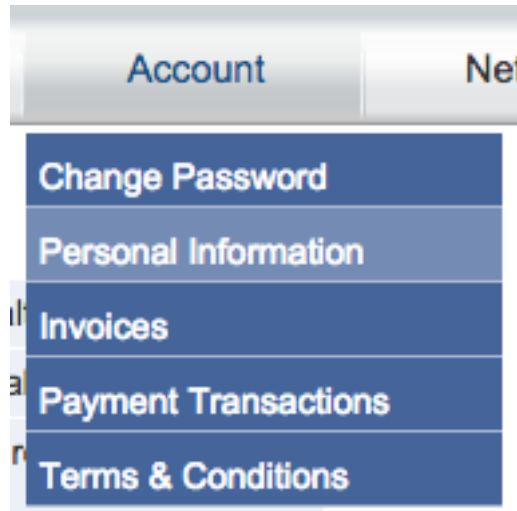
**Fig. 4.21-4: Billing – EFT token based solution**

## 4.21.2. GoCardless Settings Required

1. In GoCardless you have to setup a webhook endpoint to SIMPLer payment listener. It should always be in the format: [https://<simpler\\_server>/API/payments/paymentListener.pl](https://<simpler_server>/API/payments/paymentListener.pl)
2. Access Token: As mentioned in section 4.21.1
3. Webhook Secret: As mentioned in section 4.21.1

## 4.21.3. Adding a Bank Account via the End User Portal

Bank accounts should be added via the End User Portal. This can be done on the Account tab of SIMPLer under the personal information section as shown in Fig. 4.21-3.



**Fig. 4.21-3: Personal Information**

Customers can use the “add bank account” button to proceed to add a bank account. (Fig. 4.21-4)

 A screenshot of the 'Add Bank Account' form. On the left, there is a large grey rectangular area. A red arrow points from this area towards the 'Add Bank Account' button at the bottom. The form itself is titled 'Bank Details' and contains a table with four columns: 'Auto Payment', 'Bank Account Number', 'Bank Sort Code', and 'Bank Online Reference'. There are three rows of input fields, each with a red dot in the 'Auto Payment' column. Below the table is a blue button labeled 'Add Bank Account'.
 

Auto Payment	Bank Account Number	Bank Sort Code	Bank Online Reference
<input type="radio"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="radio"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="radio"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

**Fig. 4.21-4: Add Bank Account**

Alternatively, the customer can also add the bank account when they are on the payment page using the “add bank account” button.



Auto Payment	Enabled
Invoice Number	214
Invoice Date	07 Jan 2016
Pay Amount	7.26

Add Bank Account

Bank Account Number \*\*\*\*\*52  
Amount 7.26

Pay Now

Cancel

**Fig. 4.21-4: Add Bank Account from payment page**

Once either “add bank account” button is clicked the customer will be redirected to the GoCardless secured page and will be asked to enter their details as per Fig. 4.21-5.

SET UP A DIRECT DEBIT WITH AZOTEL

First name

Last name

Email

Or [use a company name](#)

Country  
Austria

IBAN  
E.G. AT61 1904 3002 3457 3201

Or [enter local details](#)

Set up Direct Debit

**Fig. 4.21-5: GoCardless secured page**

Once the details have been entered and finalised, the customer will be re-directed back to the End User Portal.

#### 4.21.4. Making Payments

Once the bank account has been added, SIMPLer will receive a mandate (token) for the customer. The following payment methods are available to make a payment through SIMPLer:

1. **Auto Payment:** Contact [support@azotel.com](mailto:support@azotel.com) to arrange for auto payment to take place daily, weekly, monthly, or on the days of your choice for stored tokens. (Automatically)
2. By using the “**Custom E-Check**” button in SIMPLer from the Quicklinks on the customer record, which will allow you to pay off a custom amount for that customer (Fig. 4.21-5) or from the Invoices tab which will allow you to select a customer with bank details on file and pay off a custom amount (Fig. 4.21-6) (Must be done by the CSR)
3. By clicking on the “**Pay Online**” button beside the outstanding invoice in the “last 5 invoices” section on the customer record as per Fig. 4.21-7. (Must be done by the CSR)
4. From the **End User Portal**, the customer can pay off the invoices independently. (By customer)

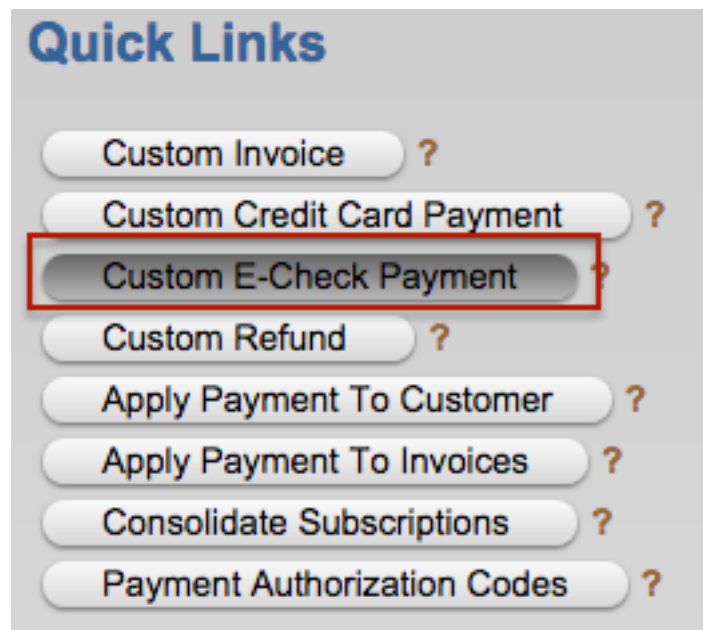


Fig. 4.21-5: Custom E-Check Button from Quick Links

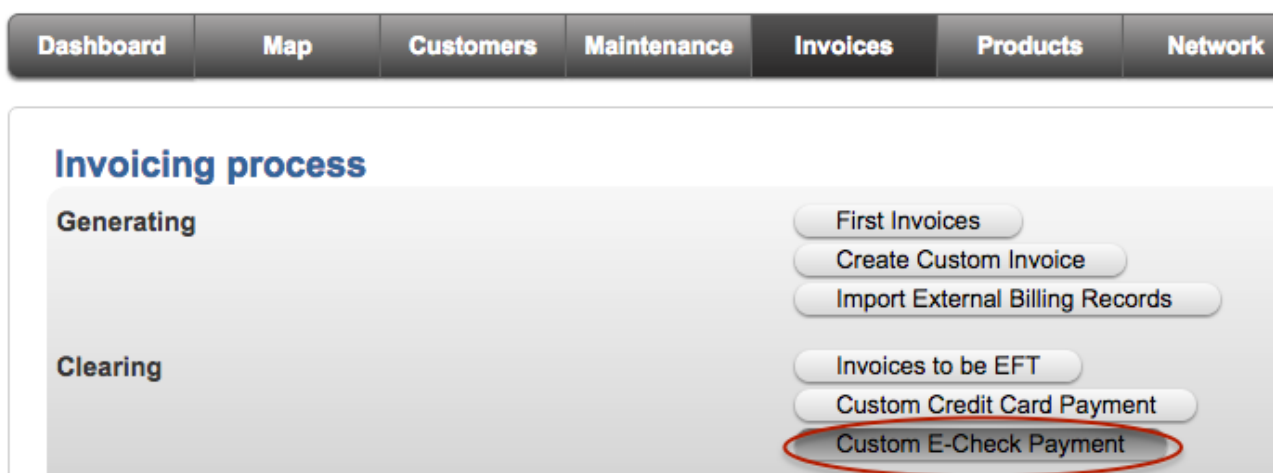


Fig. 4.21-6: Custom E-Check Button from Quick Links




























Last 5 Invoices (all..)				
No	Date	Amount	Status	
49109	01 Dec 2015	52.70	52.70 DUE	<a href="#">Pay Online</a>   
47487	01 Nov 2015	52.70	paid	     
45913	01 Oct 2015	52.70	paid	     
45104	01 Sep 2015	52.70	paid	     
42831	01 Aug 2015	52.70	paid	     

Fig. 4.21-7: Pay Online Button

Please note that the payment processed this way will end up with a status “under EFT”. This status will get changed to “paid” or “failed” whenever a successful webhook call is received and processed from GoCardless.

#### 4.21.5. Failed Payments for GoCardless

There is a payment listener running in the background, which will listen for webhooks coming in for GoCardless. Whenever a payment is paid, a paid out webhook should be sent to SIMPLer and SIMPLer should process the payment and change the status of invoice to “paid”. If a failure occurs, SIMPLer will change the payment status to “failed”.

#### 4.21.6. Refunds for GoCardless

Refunds can be processed in SIMPLer for GoCardless. The refund must be against a specific payment made and cannot be for just a specific amount. To generate a refund please click on the “R” button beside the paid invoice in SIMPLer under “last 5 invoices”. (See fig. 4.21-8)

47487	01 Nov 2015	52.70	paid	     
45913	01 Oct 2015	52.70	paid	     
45104	01 Sep 2015	52.70	paid	     
42831	01 Aug 2015	52.70	paid	     

**Fig. 4.21-8: Refund Button**

You will be re-directed to the refunds page as per Fig. 4.21-9. You can choose exactly which payment to refund against. Enter any other details such as narrative, reference, choose between customer bank accounts and click “process” to complete the refunding process.

**Customer Refund**

Refund Date ? Jan 7 2016 Recalculate

Refund Amount ? 0.11

Against Payment ? EUPCC14 [394]

Payment Interface ? GoCardless

Bank Account

Reference Text ? A18 >>

Narrative Text ?

Process Refund ?

**Fig. 4.21-9: Refund Page**

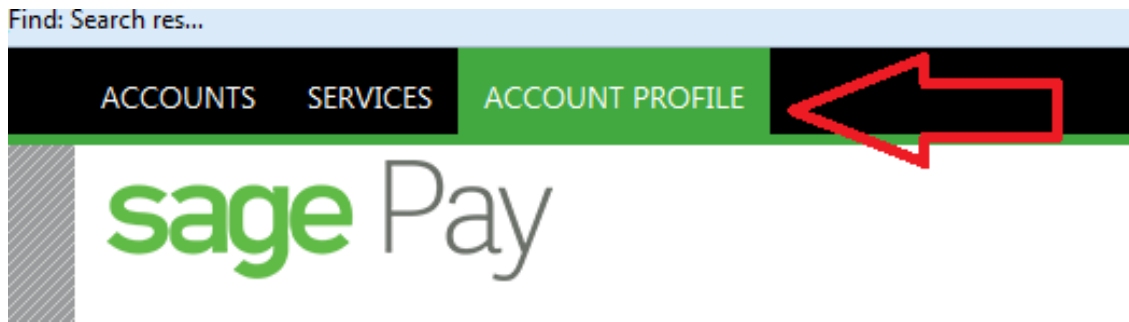
## 4.22 Sagepay Debit

Sagepay debit is a new debit order process replacing the process formerly used by Netcash in South Africa.

### 4.22.1 SagePay Debit Configuration

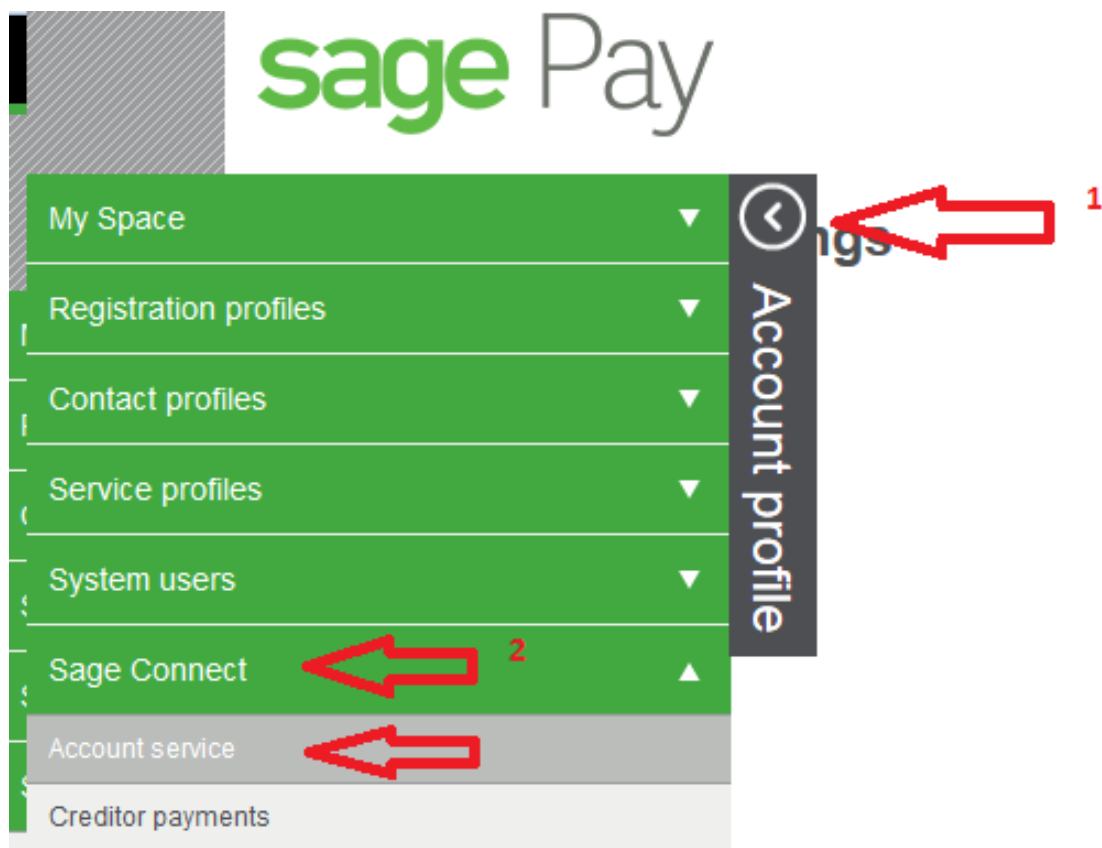
To begin enabling these features please firstly setup an account with Sagepay. Next:

- 1) Visit the portal of your Sagepay account (merchant.sagepay.co.za) and once you have logged in, navigate to the “account profile” tab as shown in Fig. 4.22.1-1.



**Fig. 4.22.1-1: Account Profile**

- 2) Expand the “account profile” tab to the left as per Fig. 4.22.1-2 and also expand the “Sage Connect” part from the menu. Finally click on “Account Service”.



**Fig. 4.22.1-2: Account Profile**

- 3) The next step is to create and activate your “service key” as per Fig. 4.22.1-3.

Active: ☒

Email:

Service key:

Postback url active: ☐

Pre-defined postback url:

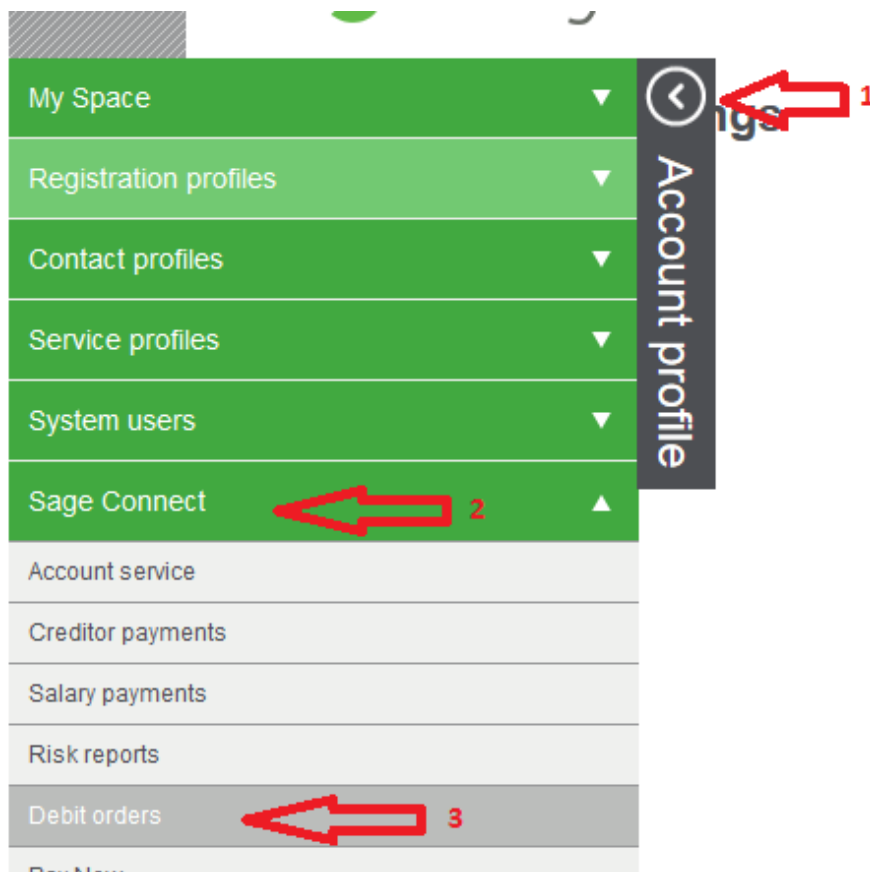
Postback url:

Statement download:

**Edit**

**Fig. 4.22.1-3: Activate Service Key**

- 4) Expand “Account Profile” to the left. Expand “Sage Connect” from the menu. Click “Debit Orders”. (Fig. 4.22.1-4).



**Fig. 4.22.1-4: Debit Orders**

- 5) On the following page create and activate your debit order service key as per Fig. 4.22.1-5.

Active: ☒

Email:

Service key:

Postback url active: ☐

Pre-defined postback url:

Postback url:

Ignore errors: ☒

Auto forward action date: ☒

Lock batch on upload: ☐

**Fig. 4.22.1-5: Debit Order Service Key**

Please note:

(a) If you check “Ignore errors” then the batch will be loaded and correct lines will be processed. Incorrect lines will not be processed and must be corrected in SIMPLer. If you uncheck “Ignore errors” then if there is at least one error, then the full batch will not be loaded and the lodgement will not get created in SIMPLer. It is recommended to check the “ignore errors” box.

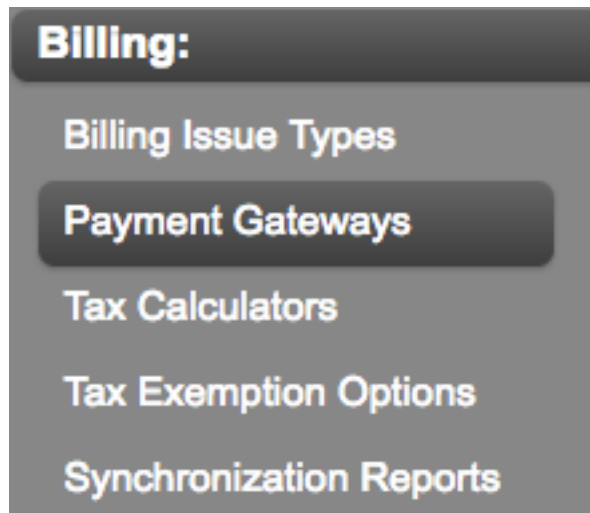
(b) If you check “auto forward action date” then if you load the batch with today’s date after 11:00 it will auto forward the batch for the next available day. Otherwise the batch will not be loaded unless you select the correct processing date in SIMPLer. It is recommended to have this option enabled.

I “Lock batch on upload” means that the batch cannot be tampered with after it gets uploaded i.e. you will not be able to edit the batch at all once it is listed in the sage pay account.

You must validate your settings to create the service key.

## 4.22.2 SagePay Debit – SIMPLer Configuration

- 1) To configure this payment gateway in SIMPLer first please navigate to Settings – Payment Gateways as per Fig. 4.22.2-1.



**Fig. 4.22.2-1: Debit Order Service Key**

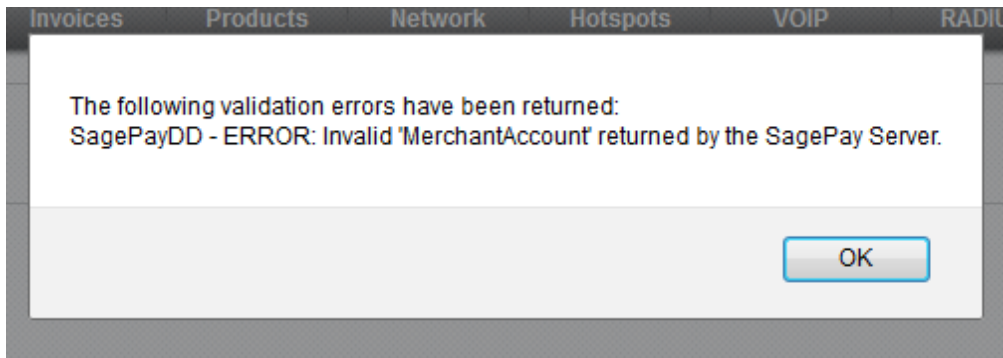
- 2) On the payment gateways page select the payment gateway type “SagePay – Debit Order”, and fill out the following, as per Fig. 4.22.2-2.
- ACCOUNT\_SERVICE\_KEY – the key from “Account Service” tab in SagePay
  - DEBIT\_ORDER\_SERVICE\_KEY – the key from “Debit Orders” tab in SagePay
  - MERCHANT\_ACCOUNT – your merchant ID
  - SERVICE\_ID – always 1
  - SOFTWARE\_VENDOR\_KEY – always “24ade73c-98cf-47b3-99be-cc7b867b3080”

ACCOUNT_SERVICE_KEY	
DEBIT_ORDER_SERVICE_KEY	
MERCHANT_ACCOUNT	
SERVICE_ID	1
SOFTWARE_VENDOR_KEY	24ade73c-98cf-47b3-99be-cc7b867b3080
VALIDATED	1

**Fig. 4.22.2-2: SIMPLer Configuration**

- 3) The account must be validated before it gets added completely. The validation should happen automatically when you click the “Update Payment Gateways” button. If the incorrect keys were provided, the VALIDATED field will show as 0 and the payment gateway will not get added to the database, an error message will be displayed, like in Fig. 4.22.2-3.





**Fig. 4.22.2-3: Validation Error**

### 4.22.3 SagePay Debit – Adding Bank Accounts

- 1) In SIMPLer or in the End User Portal (of SIMPLer) when adding a bank account, there is a feature provided by SagePay to enter the correct branch code and change the account type automatically based on the branch code or account number provided and validate the bank account. See Fig. 4.22.3-1.

Modifications will be applied only if you press the 'Update' button

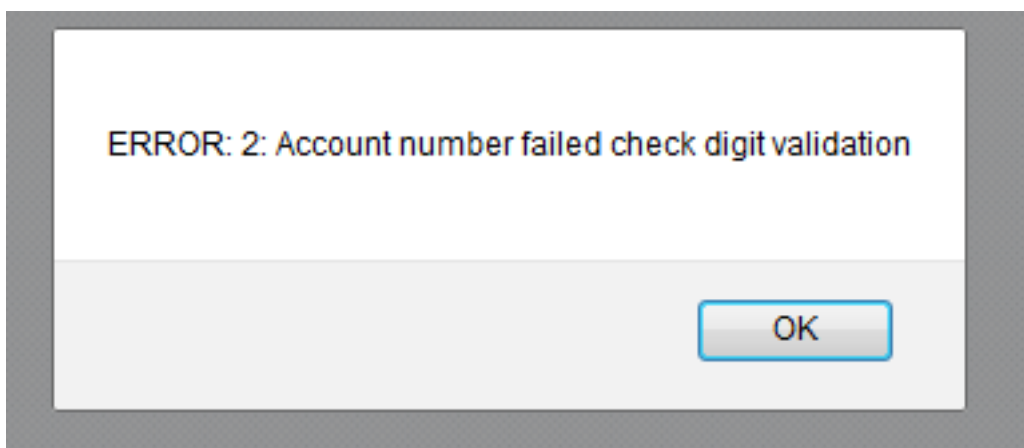
**Customer Bank EFT table**

ID	Preferred	Bank Account Number	Bank Sort Code	Bank Online Reference	Bank Account Name	Bank Account Type
115	<input checked="" type="radio"/>	123456789	051001	tt	df	Current/Cheque
	<input type="radio"/>	2222	Select Bank: Nedbank (South Africa) 198765			Savings

Add Row Update

**Fig. 4.22.3-1: Validate Bank Account**

- 3) An example of an error from an invalid bank account is shown in Fig. 4.22.3-2.



**Fig. 4.22.3-2: Bank Account Validation Error**

### 4.22.4 SagePay Debit – Creating the Debit Order File

- 1) As a first step, navigate to the Invoices tab in SIMPLer and click on “Invoices to be EFT” per Fig. 4.22.4-1.



Fig. 4.22.4-1: Invoices to be EFT

- 2) Make sure to select the “SagePay – Debit Orders” bank name from the drop-down menu and select the transactions you would like to process and click “generate”. The file will be created and uploaded automatically via the API. See Fig. 4.22.4-2.

### Transaction Info:

Processing date

Bank Name

Instruction

Fig. 4.22.4-2: File Creation

- 3) In case of any errors they will be displayed in the SIMPLer system. An example is provided in Fig. 4.22.4-3.

#### Note:

The AUTOEFT3\_winbits\_devel\_2747.txt file was created successfully for the customers listed below.

#### Lodgement Details:

Reference: AUTOEFT3 [498]

Narrative:

Date: 05/21/16

Type: direct debit

[Download Winbits File](#)

Invoicing ID	Processing date	Outstanding Invoice Amount	Payment Amount
	05/19/16	13.01	13.01
	05/19/16	14.46	14.46
		<b>Total Amount:</b>	27.47

\*\*\*IMPORTANT\*\*\* The following errors were found when importing winbits file via API. You may want to upload those charges manually or fail the payments under the lodgement ([Open Lodgement Details](#)) created:

###BEGIN BATCH-116 REF-AUTOEFT3 SUCCESSFUL WITH ERRORS 10:11 AM R27.47 20160525

Acc Ref :PDURCZYN Line :3 Bank account name has incorrect length (min 4, max 30 characters)

###END 10:11 AM

Fig. 4.22.4-3: File Errors

Once you have clicked “generate” the file is automatically submitted to SagePay via the API, and you will receive an email to this effect (per Fig. 4.22.4-4). Please note that you still must “authorize” the file in SagePay in order for it to process properly.

Original message  
From: Sage Pay Support [mailto:[support@sagepay.co.za](mailto:support@sagepay.co.za)]  
Sent: 15 June 2016 11:37  
To: [REDACTED]  
Cc: [log@sagepay.co.za](mailto:log@sagepay.co.za)  
Subject: 102 Validation return from Sage Pay [REDACTED]

All the data in the file you submitted has been validated successfully.

Your batch has been loaded.

Please note, the batch will still need to be authorised on the Sage Pay system before it can be processed.

[REDACTED]

Please do not reply to this mail as it has been sent from an automated mailbox.  
Please contact [support@sagepay.co.za](mailto:support@sagepay.co.za) for assistance.

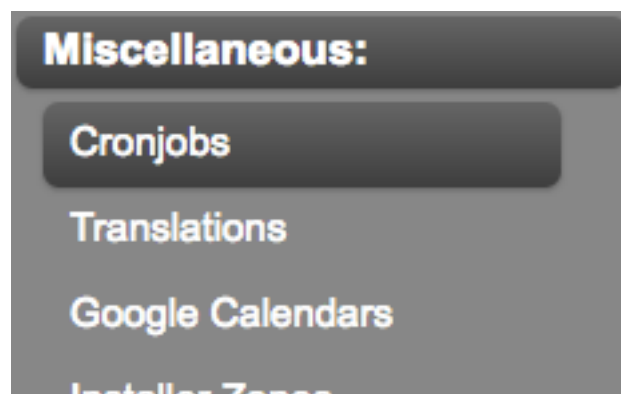
Yours faithfully  
The Sage Pay Team

**Fig. 4.22.4-4: Submission Email**

## 4.22.5 SagePay Debit – Failures

SagePay debit also supports notifying the system about failures that occur to the transactions. The process is that SIMPLer runs a script every weekday to query SagePay debit for their “daily statement”. If any failures are reported in that statement they can be automatically marked as “failed” in SIMPLer.

You can configure these auto failures under the Settings – Cron Jobs section in SIMPLer as shown in Fig. 4.22.5-1.



**Fig. 4.22.5-1: Settings – Cron Jobs**

Choose the script called “auto failures” and select the days and times you would like it to run. See Fig. 4.22.5-2. It should run Monday to Friday sometime after 12pm.

The screenshot shows the 'Automated Scripts' configuration window. The 'Name' field is set to 'Auto Failures'. The 'Hour' is 13, 'Minute' is 0. The 'Day of Month' is 'Every day'. The 'Month' is 'All'. The 'Weekday' is 'Monday' to 'Friday'. The 'Optional' field is 'Payment Gateway: sagepay - ID: 33'. There is a 'Delete' button.

**Fig. 4.22.5-2: Auto Failures Script**

Please be aware that if you fail to “authorize” the file in SagePay on time it will expire in SagePay, but it will still be marked as paid in SIMPLer, so you would need to FAIL the payment in SIMPLer and then re-do the file generation, so it sends a fresh file over to SagePay.

## 4.23 Toronto Dominion (TD) Bank

Toronto Dominion Bank is a bank used in Canada for uploading payment files.

### 4.23.1 TD Bank Configuration

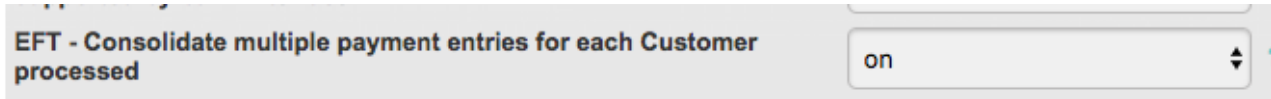
To successfully create and upload files for TD bank the operator must:

- (1) Have filled out the banking details under the WISP Settings (Settings – Modify WISP) per Fig. 4.23.1-1. If these are not filled out correctly the file will be rejected. The destination data centre field is required.

The screenshot shows the 'Banking details' form. The 'Bank Details Schema' is set to 'Canadian Banking Scheme'. The form includes fields for Bank Address (Street1, Street2, City, County, Zip Code, Country), Originator ID, Institution ID (0BBBTTTT), Bank Account Number, Destination Data Centre, Originator's Long Name, Originator's Short Name, TAX Reg No, Global TAX rate, Global Flat TAX amount, Setup TAX rate, Currency (CAD), Invoice Billing Period Dates Shift [months], and Email Banking Information (On). A large black redaction box covers the middle section of the form.

**Fig. 4.23.1-1: Bank Details**

- (2) Next, the operator must have banking details set for each customer under the “bank details” section of their record. The payment method for these customers should be “direct debit” or “PAC”.
- (3) The setting from Settings – Modify WISP called “EFT – Consolidate multiple payment entries for each Customer processed” (see Fig. 4.23.1-2) must be enabled, as TD bank will reject any “duplicate” lines in the file from the same customers.



**Fig. 4.23.1-2: Consolidate Multiple Payments**

## 4.23.2 TD Bank File Generation

To generate the file, please navigate to the Invoices tab and click “Invoices to be EFT”. From the drop-down menu select “TD Commercial Bank”. Select all items to appear on the file. Click generate. The file will be emailed to your accounts department and is also available under Invoices – Bank Deposits (Lodgements).

## 4.23.3 TD Bank File Upload

TBD

## 4.24 FastPay

FastPay is a banking system used in the U.K for uploading payment files.

### 4.24.1 FastPay Configuration

TBD

---

## 5 Section Five – Features

### 5.1 Introduction

This section will provide details of any additional features available with the payment gateways available in SIMPLer.

### 5.2 authorize.NET PCI DSS tokenized API integration

This section outlines the steps to setup the integration of authorize.NET API with PCI compliance.

#### 5.2.1. Prerequisites

The following API options must be enabled on the authorize.NET account to be able to use the integration:

- CIM – Customer Information Manager – see: <http://developer.authorize.net/api/cim/>

Please contact authorize.NET support centre to make sure that your authorize.NET account has the above options enabled.

Existing WISP operators who plan to migrate to authorize.NET tokenized PCI compliant model are advised to contact [support@azotel.com](mailto:support@azotel.com) to get the steps outlined for the migration.

#### 5.2.2. Limitations

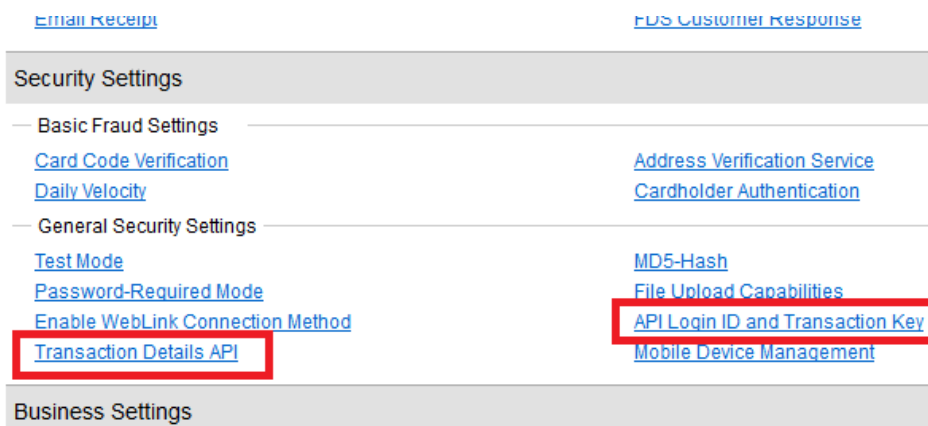
While simplifying PCI DSS compliance this integration has the following limitations due to authorize.NET API limitations:

- Credit card information returned is limited to the number last 4 digits. It does not return credit card type or credit card expiration date. Due to this limitation, it is not possible to use a script to notify customers that their credit card is due to expire.
- The operator cannot add credit card / bank account details directly into the SIMPLer system as this would break PCI compliance. Options to add credit card / bank account details should be disabled on the instance level. These options can be disabled under the Settings – Modify WISP section of SIMPLer. “Add Credit Card option and Add bank account option are the options in question. The only way to add a credit card / bank account would be by using authorize.NET secure pages (available under the EUP (End User Portal))
- While theoretically the Operator’s instance could have an unlimited number of different payment gateways it is no longer possible in the case of a PCI compliant solution. Credit cards are added directly to the authorize.NET portal and are not being passed through the SIMPLer server thus the SIMPLer server cannot redistribute credit cards to a different payment gateway.

#### 5.2.3. Payment Gateway API Setup

The following actions are required in the authorize.net interface:

1. Login to your authorize.NET portal account using the credentials received from authorize.net.
2. Go to the Account -> Settings (as shown in Fig. 5.2.1)



**Fig. 5.2.1. Authorize.NET portal settings**

- a. Under “Security Settings” -> “General Security Settings” make sure that “Transaction Detail API” is enabled and also generate (unless it was generated before) and keep note of “API Login ID and Transaction Key” as this will be needed to setup SIMPLer interface as detailed below.

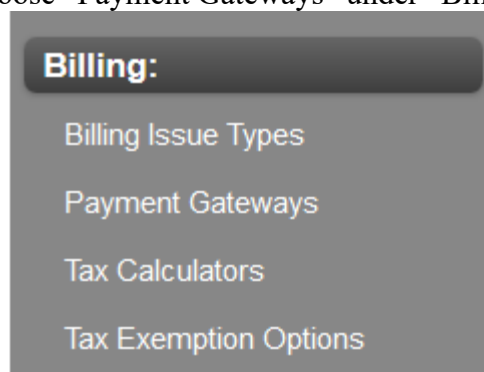
The following actions are required in the SIMPLer interface:

1. Login to your SIMPLer system instance.
2. Go to the Settings tab (Fig. 5.2.2)



**Fig. 5.2.2. SIMPLer Settings**

3. On the left-hand menu choose “Payment Gateways” under “Billing” (Fig. 5.2.3)



**Fig. 5.2.3. Billing -> Payment Gateways**

4. Click “Add Blank Row” twice to have two positions generated. From the list of available payment gateways select “authorize.NET – EFT Token” and “authorize.NET – Token Based” for EFT and CC payments respectively.
5. Enter the following module settings (Fig. 5.2.4):

16	authorizeNet_Echeck_token View Log	All	Pay by EFT	ECHECK_TYPE	PPD
				HOSTED_PAGE_RETURN_URL_TEXT	Save Details & Return To Payment Page
				MERCHANT_API_LOGIN_ID	MERCHANT_API_LOGIN_ID
				MERCHANT_API_TRANSACTION_KEY	MERCHANT_API_TRANSACTION_KEY
				MERCHANT_MD5_HASH	MERCHANT_MD5_HASH
				PCI_DSS	1
				RETURN_URL	n/CustomerPortal/paymentSecondStage.pl
				SERVER	https://test.authorize.net/gateway/transact.d
17	authorizeNet_token View Log	All	Pay Online	HOSTED_PAGE_RETURN_URL_TEXT	Save Details & Return To Payment Page
				MERCHANT_API_LOGIN_ID	MERCHANT_API_LOGIN_ID
				MERCHANT_API_TRANSACTION_KEY	MERCHANT_API_TRANSACTION_KEY
				MERCHANT_MD5_HASH	MERCHANT_MD5_HASH
				PCI_DSS	1
				RETURN_URL	https://demo.azotel.com/CustomerPortal/pa
				SERVER	https://test.authorize.net/gateway/transact.d

Fig. 5.2.4 Payment Gateway Settings

6. Authorize.NET – EFT Token
  - a. **ECHECK\_TYPE** – PPD
  - b. **HOSTED\_PAGE\_RETURN\_URL\_TEXT** - any text, e.g. “Save Details & Return To Payment Page”
  - c. **MERCHANT\_API\_LOGIN\_ID** – API Login ID from authorize.NET portal – see subsection 3.1
  - d. **MERCHANT\_API\_TRANSACTION\_KEY** – API Transaction Key from authorize.NET portal – see subsection 3.1
  - e. **MERCHANT\_MD5\_HASH** – MD5\_HASH from authorize.NET portal – see previous section.
  - f. **PCI\_DSS** – 1
  - g. **RETURN\_URL** – [https://<server\\_name>/CustomerPortal/paymentSecondStage.pl](https://<server_name>/CustomerPortal/paymentSecondStage.pl)
  - h. **SERVER** – <https://secure.authorize.net/gateway/transact.dll>  
(<https://test.authorize.net/gateway/transact.dll> when testing in sandbox environment)
7. Authorize.NET – Token Based
  - a. **HOSTED\_PAGE\_RETURN\_URL\_TEXT** - any text, e.g. “Save Details & Return To Payment Page”
  - b. **MERCHANT\_API\_LOGIN\_ID** – API Login ID from authorize.NET portal – see previous section.
  - c. **MERCHANT\_API\_TRANSACTION\_KEY** – API Transaction Key from authorize.NET portal – see subsection 3.1
  - d. **MERCHANT\_MD5\_HASH** – MD5\_HASH from authorize.NET portal – see subsection 3.1
  - e. **PCI\_DSS** – 1
  - f. **RETURN\_URL** – [https://<server\\_name>/CustomerPortal/paymentSecondStage.pl](https://<server_name>/CustomerPortal/paymentSecondStage.pl)
  - g. **SERVER** – <https://secure.authorize.net/gateway/transact.dll>  
(<https://test.authorize.net/gateway/transact.dll> when testing in sandbox environment)

## 5.2.4. Payment Gateway API Setup

In order to keep the instance PCI compliant some of the options must be disabled. Presented below are the options that must be disabled under global WISP settings.

- 1) Tokenized Modules – Add Bank Account Option (See Fig. 5.2.4)
- 2) Add Credit Card Option (See Fig. 5.2.5)

Tokenized Modules - Add Bank Account Option	off	?
---	-----	---



**Fig. 5.2.4: Add Bank Account Option**

**Credit Card Details Settings ?**

Add Credit Card Option	off ?
Auto Payment Attempts	3 ?
Credit Card Auto Billing Option	on ?
Credit Card Billing Address	off ?
Credit Card Expiration Date	off ?
Credit Card Holder	on ?
Credit Card Number	on ?
Credit Card Type	off ?
Credit Card Types	<input type="checkbox"/> American Express ? <input type="checkbox"/> Visa ? <input type="checkbox"/> Discover ? <input type="checkbox"/> MasterCard ? <input type="checkbox"/> other ?

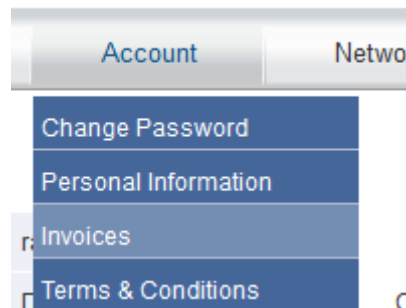
**Fig. 5.2.5 Options to be disabled on the Operator to level to make sure Operator instance is PCI compliant and works properly with authorize.NET integration**

### 5.2.5. Payment Gateway API Setup

There are two sections of interest in the EUP (End User Portal):

1. Payment Interface Page – to communicate with authorize.NET interface (Add Credit Card, Edit Credit Card, Add Bank Account, Edit Bank Account, make a payment with saved payment profile, make a once off payment etc)
2. Personal Details Page – to review / refresh all personal details including credit card / bank account details & to switch Auto-Payment flag between different credit cards and/or bank accounts

To access the Payment Interface Page go to the Account -> Invoices

**Fig. 5.2.6 Account -> Invoices**

Enter a “Payment Amount” under “Make a Custom Payment” subsection and click on one of the available Payment buttons (“Pay Online”, “Pay by EFT” etc. – note those names may differ depending on the operator setup and preferences). Or click on the Payment Buttons alongside the particular invoice.

### Make a custom payment

Outstanding Invoices	NGN 0.00
Available Credit	NGN 0.00
<b>Amount Due</b>	<b>NGN 0.00</b>
Payment Amount	<input type="text" value="10"/>

[Pay by EFT](#)
[Pay Online](#)

**Fig. 5.2.7 “Make a Custom Payment” subsection**

The next page presented will display all of the available options

[Home](#)
[Account](#)
[Network](#)
[Hotspot](#)
[Support](#)

#### Account Information

Account ID	radiuscustomer
Customers Name	Demo RADIUS Customer / Hotspot Recurring Customer
Current Pay Method	<input type="text" value="Credit Card - 1815"/>
Auto Payment	Enabled
Pay Amount	63.00

[Add Credit Card](#)
[Update Credit Card](#)

Number \*\*\*\* \* 1815

Amount 63.00

[Pay Now](#)

Copyright © 2014 Emma Testing. All rights reserved


Powered by AZOTEL

**Fig. 5.2.8 Payment Options**

Customers can:

- Make a direct payment by clicking on the “Pay Now” button. It will use the currently selected card for payment.
- Add a New Credit Card for auto-payment by clicking “Add Credit Card”. Secure authorize.NET hosted page will be presented to allow the customer to add a new credit card (Fig. 5.2.9)

---

**Add a New Payment Method** 

☒ Credit Card ☐ Bank Account (USA only)

Card Number:  \*

Expiration Date:  \* (mm/yy)

Card Code:  [What's this?](#)

**Billing Information**

First Name:

Last Name:

Company:

Address:

City:

State:  Zip:

Country:

Phone:

Fax:

**Fig. 5.2.9. Secure Page to Add Credit Card Details**

- Update current credit card by clicking “Update Credit Card”. Secure authorize.NET hosted page will be presented that will allow the customer to edit their credit card info (Fig. 5.2.10)

**Edit Payment Information**

Card Number:  \*

Expiration Date:  \* (mm/yy)

Card Code:  [What's this?](#)

**Edit Billing Information**

First Name:

Last Name:

Company:

Address:

City:

State:  Zip:

Country:

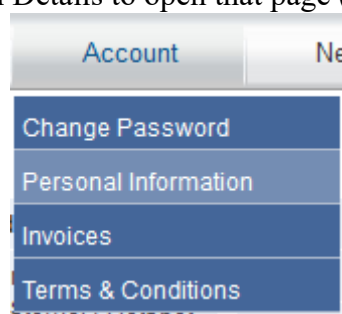
Phone:

Fax:

**Fig. 5.2.10 Secure Page to Edit Credit Card Information**

Note that the same options are available for the bank accounts as well when it is chosen to make a payment using bank account.

As mentioned above all credit card / bank account details can be reviewed under “Personal Details” page. Go to the Account -> Personal Details to open that page (Fig. 5.2.11)



**Fig. 5.2.11 Account -> Personal Information**

If a customer has added/updated/deleted a credit card / bank account in authorize.NET and it is not displayed in the End User Portal, the customer can click on “Refresh” to synchronise the SIMPLer system with authorize.NET system. There is also an option also to switch the account that should be used for auto-payment (Fig. 5.2.12).

Bank Details

Auto Payment	Bank Account Number	Bank Sort Code	Bank Online Reference	Bank Account Name	Account Type	Refresh
No Bank details available						
Add Bank Account						

Credit Card Details

Auto Payment	Number	Holder	Refresh	
	*****1815	Demo RADIUS Customer / Hotspot Recurring Customer	Edit	Delete
	*****2827	Demo RADIUS Customer / Hotspot Recurring Customer	Edit	Delete
Add Credit Card				

Auto-Payment Switch:

Credit Card - 1815

Fig. 5.2.12. Bank / Credit Card Details in EUP

## 5.3 Refunds

This section will describe the option to refund money to a customer from SIMPLer and through detected payment gateways.

### 5.3.1. Prerequisites

Direct refunds are available through certain payment gateways. To avail of this feature, you must have an account with one of the following payment gateways:

1. IP Pay (See section 3.5)
2. First Data (See section 3.11)
3. GoCardless (See section 4.21.6)
4. PayDock (See section 3.13)

### 5.3.2. Feature Outline

There are three ways of using the feature:

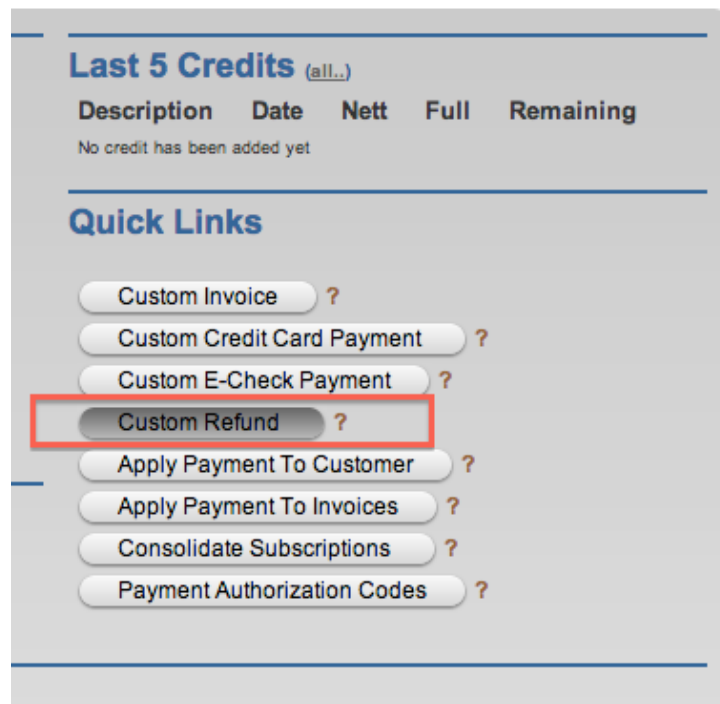
1. **Custom Refund.** By defining a refund product in SIMPLer, operators can choose to refund a custom amount through SIMPLer and push this refund directly via IP Pay.
2. **Refund button for negative invoices.** Some operators may already have some negative invoices generated in SIMPLer. If they need to physically refund this money, a [refund](#) link has been created to make the process easier.
3. **Prorated Refund for paid invoices.** A refund button has been created beside paid invoices. If not the entire amount is to be refunded, dates can be manipulated to only partially refund the invoice in question. (**Note:** only applied to single paid invoices)

### 5.3.3. Feature Use

#### f) Custom Refund Option

**Step One:** Create a product in SIMPLer that you will use for refunds.

**Step Two:** Visit the subscriber record of the customer you wish to refund. Scroll to the **customer billing details** section. See the quick links on the right-hand-side and click on **custom refund** as per fig. 5.3.1.



**Fig. 5.3.1: Custom Refund**

**Step Three:** (See fig. 5.3.2)

- Choose your product.
- Enter price and correct tax.
- Verify amount is correct.
- Verify correct credit card and gateway have been selected.
- Process Refund.

Fig. 5.3.2: Process Refund

**Step Four:** Verify your action as per fig. 5.3.3.

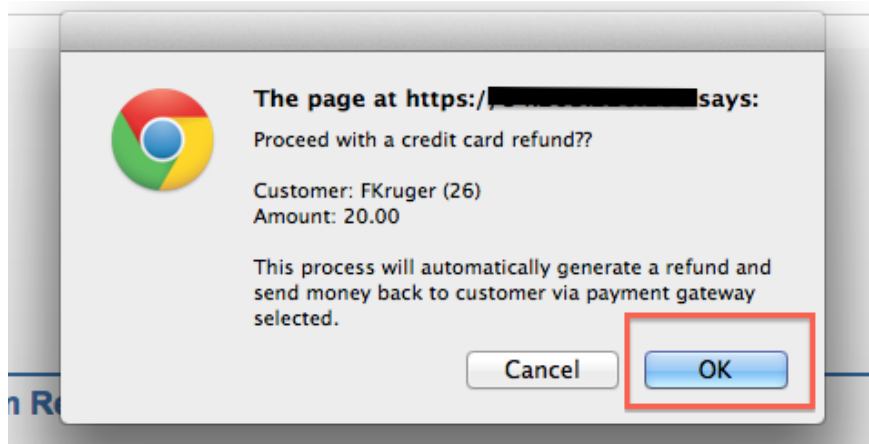
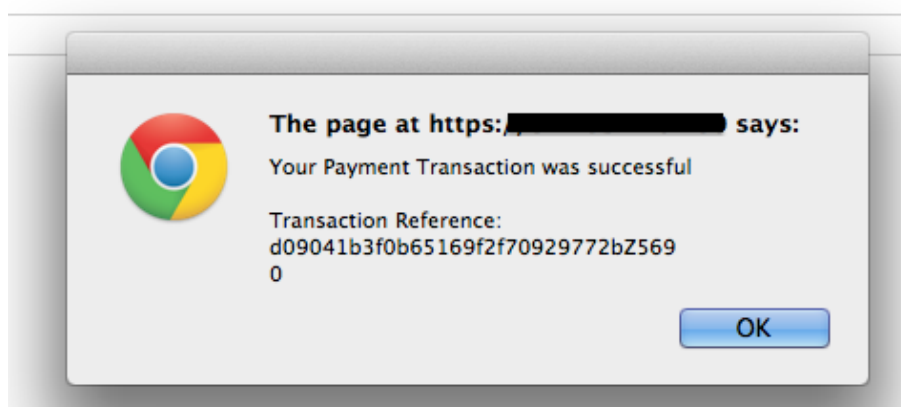


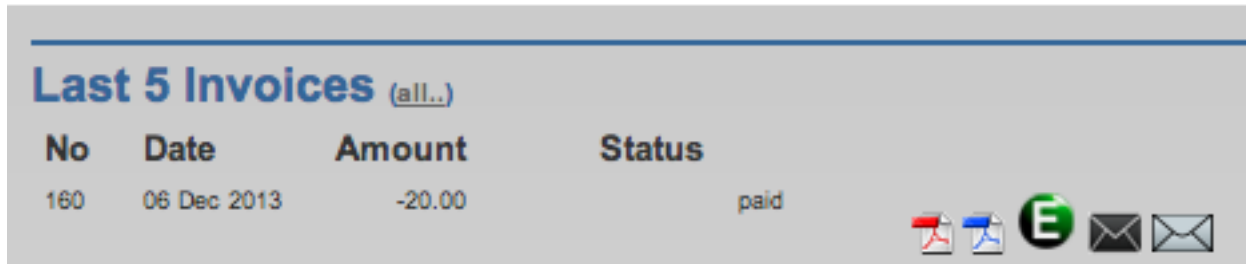
Fig. 5.3.3: Verify Refund

**Step Five:** You will receive a transaction reference as per fig. 5.3.4.



**Fig. 5.3.4: Transaction Reference**

**Step Six:** Verify that your refund has been logged successfully in SIMPLer as per fig. 1.5, and in your IP Pay portal.



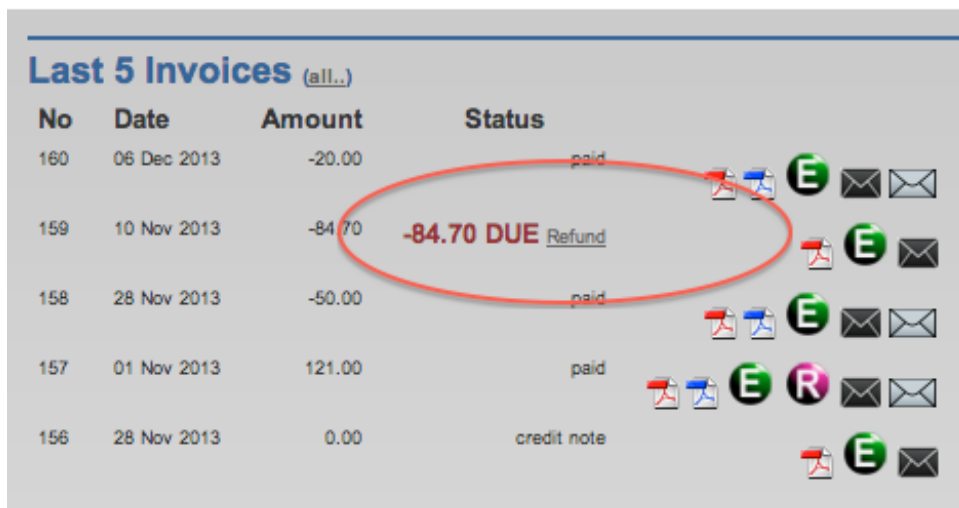
No	Date	Amount	Status
160	06 Dec 2013	-20.00	paid

**Fig. 5.3.5: View refund ref in SIMPLer**

g) Refund Negative Invoice Option

**Step One:** You will have previously created a negative invoice in SIMPLer but have not yet pushed the monies back to the customer's account via the payment gateway.

**Step Two:** Visit the subscriber record in question. Locate the negative invoice under “last five invoices” as per fig. 5.3.6.



No	Date	Amount	Status
160	06 Dec 2013	-20.00	paid
159	10 Nov 2013	-84.70	<b>-84.70 DUE Refund</b>
158	28 Nov 2013	-50.00	paid
157	01 Nov 2013	121.00	paid
156	28 Nov 2013	0.00	credit note

**Fig. 5.3.6: Locate Refund**

**Step Three:** Click on the refund link beside the amount as highlighted in fig. 5.3.6.

**Step Four:** See fig. 5.3.7.

- Verify the details of the products being refunded.
- Verify amount, date, credit card, payment gateway, reference and narrative.
- Process Refund.



**Customer Details**

ID: 26  
Name: Freddy Kruger  
Nickname: fgn000214  
Invoicing ID: FKruger

---

**Customer Refund**

Refund Date: Dec 6 2013 **b**

Refund Amount: 84.70

Payment Interface: IPay\_token

Credit Card: \*\*\*\*\*7365 (Visa) - Freddy Kruger

Reference Text: A136

Narrative Text: **c**

**Process Refund**

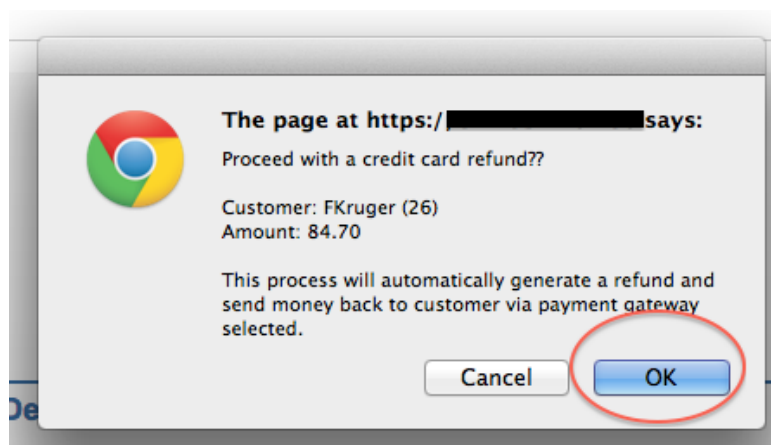
**Refund Details**

Description	Nett Amount	TAX rate	TAX amount	Tax Mode	Tax Zone
Emma Test Upgrade Product - Refund [10 Nov 2013 - 01 Dec 2013]	-70.00	21.00	-14.70	Fixed / Default TAX Rate System	-

**a**

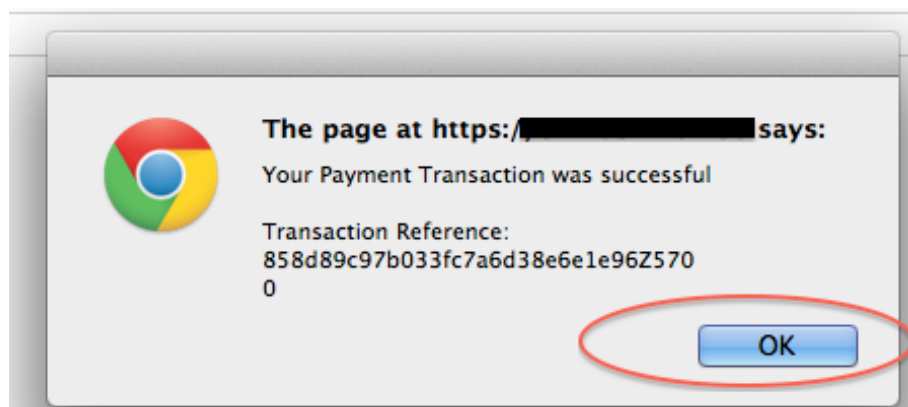
**Fig. 5.3:7 Verify and Process Refund**

**Step Five:** Verify refund and click ok. (See fig. 5.3.8)



**Fig. 5.3.8: Verify Refund**

**Step Six:** View transaction code. (See fig. 5.3.9)



**Fig. 5.3.9: Transaction Reference**

**Step Seven:** Verify subscriber record balance.

### h) Calculate and Process Refund Option (paid invoices)

**Scenario:** The customer has received an invoice on November 1<sup>st</sup> for \$121.00. The invoice has been fully paid. The customer cancels service on November 8<sup>th</sup>. You need to refund money from this date.

**Step One:** Go to the last five invoices section of your subscriber record. Locate the paid invoice in question and click on the R button as per fig. 5.3.10.

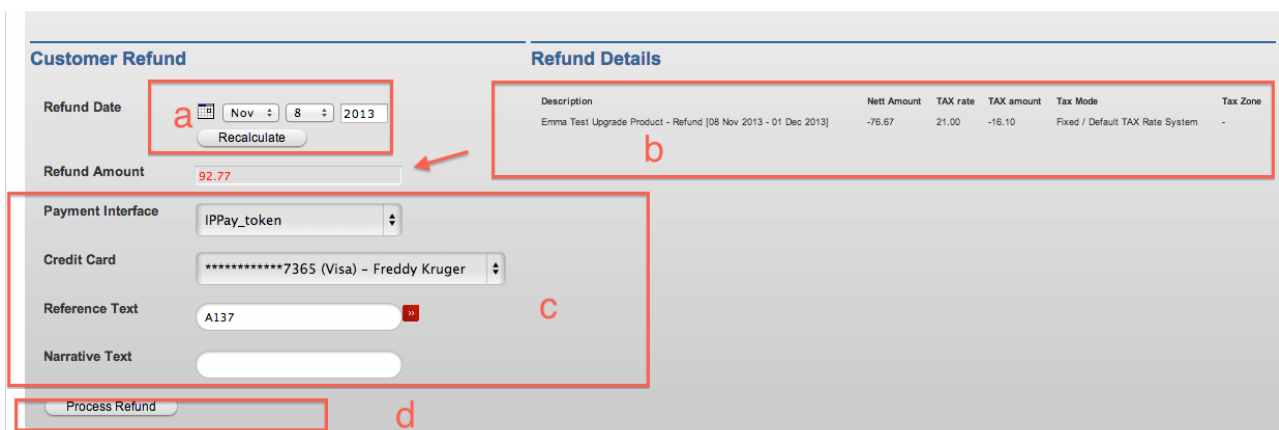


No	Date	Amount	Status
160	06 Dec 2013	-20.00	paid
159	10 Nov 2013	-84.70	paid
158	28 Nov 2013	-50.00	paid
157	01 Nov 2013	121.00	paid
156	28 Nov 2013	0.00	credit note

**Fig. 5.3.10: Refund Button**

**Step Two:** See fig. 5.3.11.

- Choose the appropriate date for refund to begin and select “recalculate”
- Verify the refund details and final amount.
- Verify the credit card and interface and reference.
- Select “process refund”



### Customer Refund

Refund Date

Nov

8

2013

Recalculate

Refund Amount

92.77

Payment Interface

IPPay\_token

Credit Card

\*\*\*\*\*7365 (Visa) - Freddy Kruger

Reference Text

A137

Narrative Text

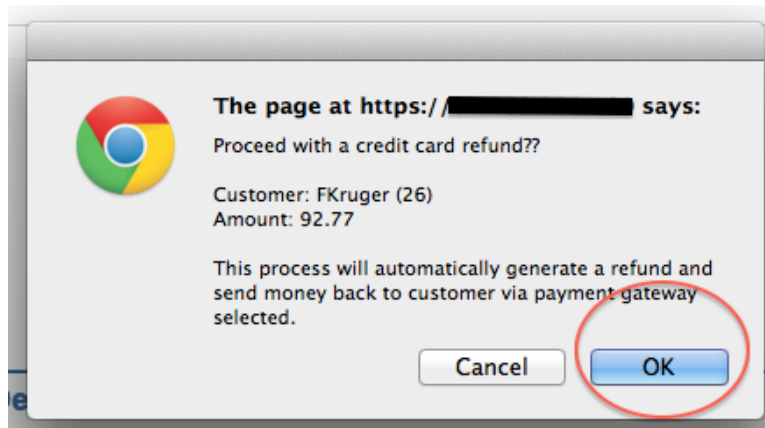
Process Refund

### Refund Details

Description	Nett Amount	TAX rate	TAX amount	Tax Mode	Tax Zone
Emma Test Upgrade Product - Refund [08 Nov 2013 - 01 Dec 2013]	-76.67	21.00	-16.10	Fixed / Default TAX Rate System	-

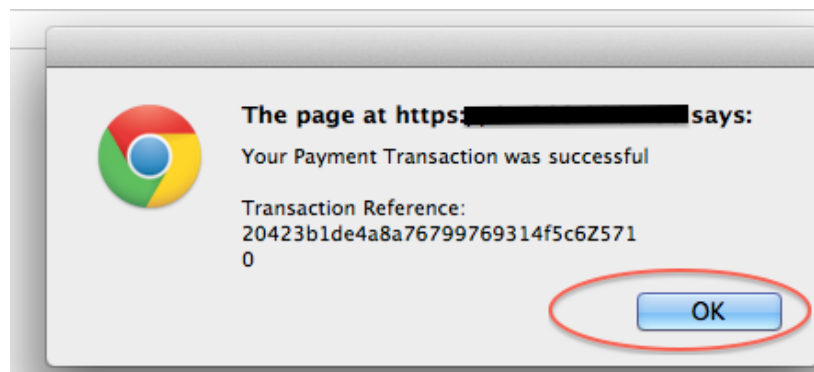
**Fig. 5.3.11: Verify and Process Refund.**

**Step Three:** Verify details once more and click OK. (Fig. 5.3.12)



**Fig. 5.3.12: Verify Refund**

**Step Four:** Acknowledge Transaction Reference. (Fig. 5.3.13)



**Fig. 5.3.13: Transaction Reference**

**Step Five:** Verify customer balance looks ok in SIMPLer and refund has been processed in IP Pay.

## 6 Section Six – Mobile Interfaces

### 6.1 Introduction

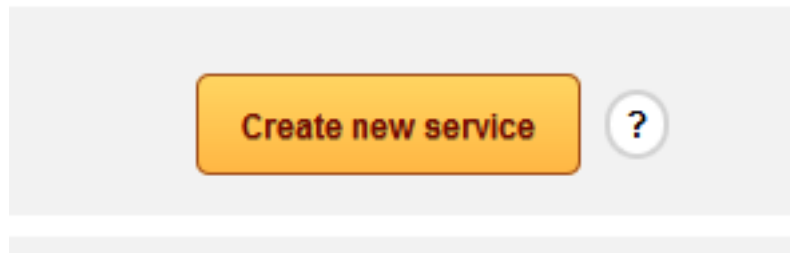
This section will provide details of configuration and use of the interfaces outlined in section 2.4.

### 6.2 Fortumo

This section outlines the steps to setup the integration with Fortumo,

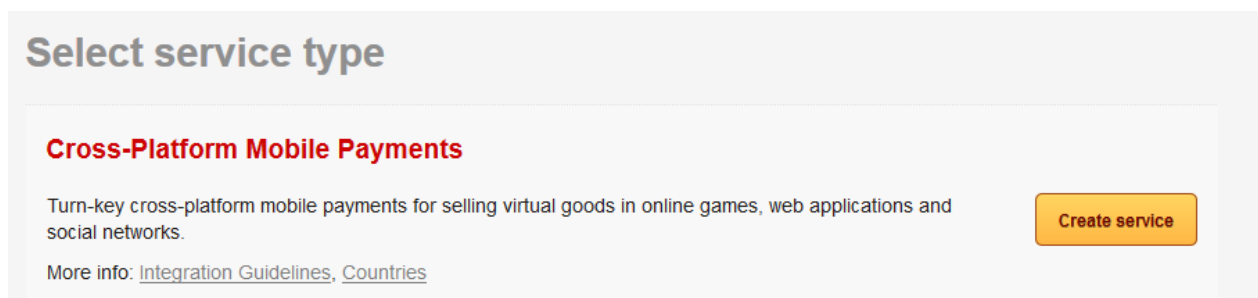
#### 6.2.1. Setting up Fortumo Dashboard

Firstly, on the Fortumo dashboard, you must click on “create new service” as shown in Fig. 6.2.1-1.



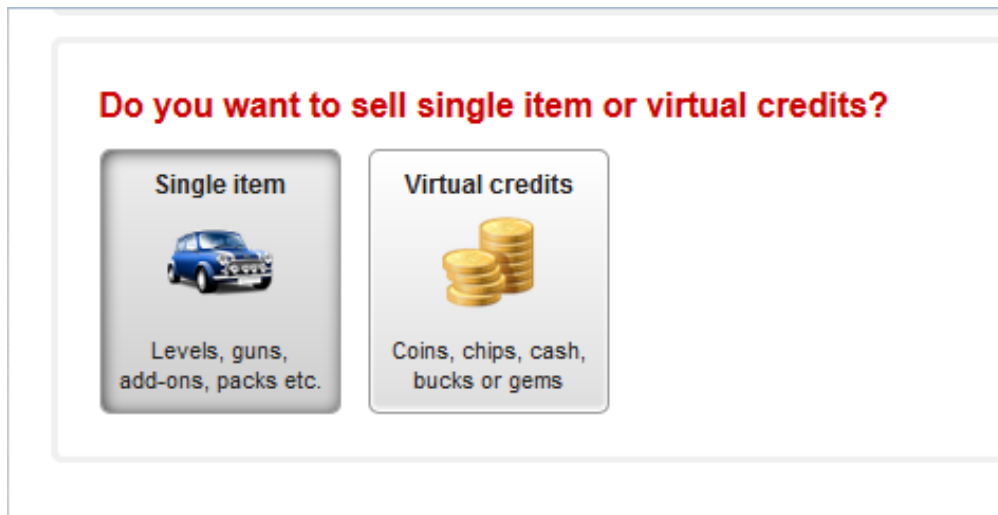
**Fig. 6.2.1-1: Create New Service**

Next, select a service type. It must be “cross platform mobile payments” as shown in Fig. 6.2.1-2.



**Fig. 6.2.1-2: Select Service Type**

Next, select if you would like to sell single item or virtual credits. Here, “single item” must be selected as shown in Fig. 6.2.1-3.



**Fig. 6.2.1-3: Single Item Sales**

Next, you will define the price of your service. Please note that each service will also require setting up a new payment gateway line item in SIMPLer. Creating a service price in Fortumo is displayed in Fig. 6.2.1-4.

COUNTRY	END-USER PRICE	REVENUE SHARING
Poland	2.46 PLN ~ 2.46 PLN	42%

**Fig. 6.2.1-4: Defining a Service Price**

On the next screen, you will be asked for the name of the service you are creating, and the name of the application where the service will be used, and also for to links:

- To which URL will your payment requests be forwarded to? The URL will be [https://<server\\_name>/API/payments/paymentListener.pl](https://<server_name>/API/payments/paymentListener.pl) where <server\_name> will be replaced by the name of your SIMPLer server.
- Where to redirect the user after completing the payment? The URL will be [https://<server\\_name>/CustomerPortal/paymentSecondStage.pl?checkStatusOnly=1&transaction=CUID](https://<server_name>/CustomerPortal/paymentSecondStage.pl?checkStatusOnly=1&transaction=CUID) where <server\_name> will be replaced by the name of your SIMPLer server.

There are other informational fields to be completed, but they are unimportant from the point of view of the integration with SIMPLer.

Once the service is created you will receive the Service ID and Secret, which will be required when you are creating the payment gateway in SIMPLer. An example is shown in Fig. 6.2.1-5.

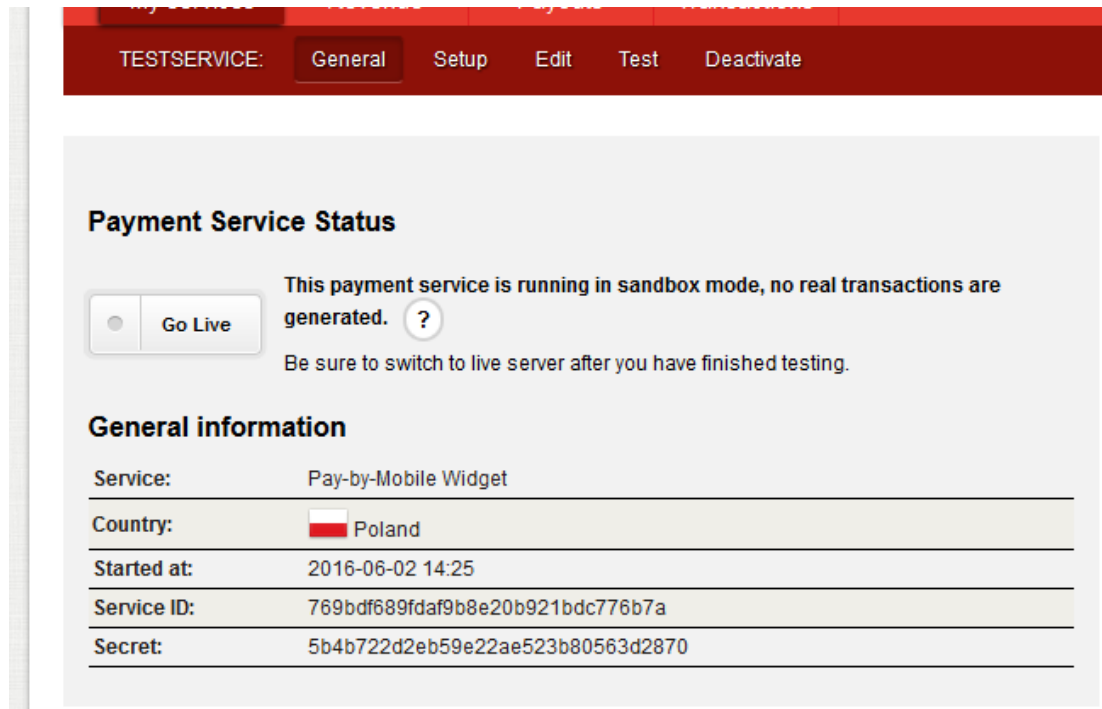


Fig. 6.2.1-5: Service ID and secret

## 6.2.2. Fortumo SIMPLer Setup

In SIMPLer, the first step is to navigate to the Settings – Payment Gateways section of SIMPLer, as shown in Fig. 6.2.2-1.

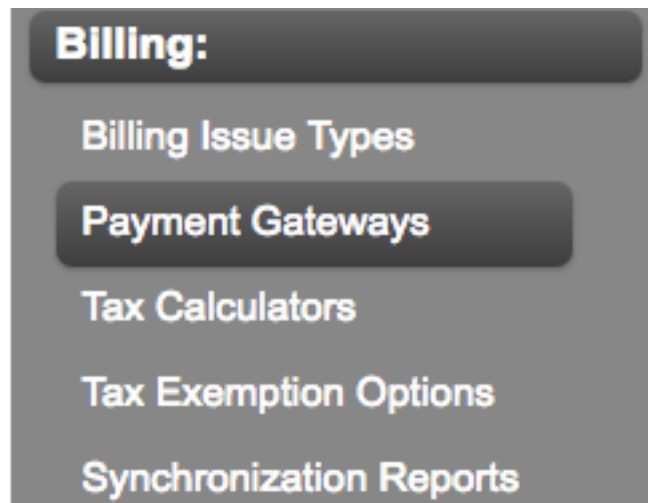


Fig. 6.2.2-1: Settings – Payment Gateways

On the next page, you will be given the option to select the appropriate payment gateway, which is “fortumo” and set the appropriate settings as per Fig. 6.2.2-2.

1. Secret: Enter the secret provided by Fortumo as discussed in section 6.3.
2. Service ID: Enter the service ID provided by Fortumo as discussed in section 6.3.
3. Label: The label should describe the service the customer is paying for as it will show up as a button on the portal.

4. Availability: You should enter the credentials once under “End User Portal” and once under “Hotspot”. Two lines would be required for each set of credentials.

Back
Reset
Update Payment Gateways ?

Payment Gateways Definitions ?

ID ?	Name ?	Availability ?	Label ?	Module Settings ?	Redirect	Token Based ?	E-check Module ?	
62	fortumo View Log	All	Pay by Phone - 2.46	SECRET SERVICE_ID 5b4b722d2eb59e22ae523b80563d2870 769bdf689fdaf9b8e20b921bdc776b7a	paymentSecondStage.pl	<input type="checkbox"/>	<input type="checkbox"/>	Delete
66	fortumo View Log	All	Pay by Phone - 11.07	SECRET SERVICE_ID ab2b78b226ed982e74f05bc387ab5729 15055d13f60dc3b6320e64b5fef81b74	paymentSecondStage.pl	<input type="checkbox"/>	<input type="checkbox"/>	Delete

Add Blank Row ?

**Fig. 6.2.2-2: Payment Gateway Configuration**

Please note that if you have created multiple services as described in Section 6.3 you will need to add a payment gateway per each service.

## 6.2.2. Fortumo Payments

Fortumo payments will be made on the End User Portal or hotspot portal. For hotspots, the user will be presented with the home page and an option to buy a token. The options “pay by phone – 11.07” and “pay by phone – 2.46” in the Fig. 6.2.3-1 represent the two available payment gateways in this test environment.

### Account Information

Account ID	pa1testes2
Customers Name	test test
Current Pay Method	Credit Card
Auto Payment	

### Hotspot Tokens

Token	Status	Details	Password
pa1testes3	active	Show	Change
pa1testes4	active	Show	Change

### Buy Additional / Recharge Hotspot Token:

#### Purchase Option:

Buy Additional Hotspot Token ▼

#### Product:

super internet - 1 day ▼

#### Choose payment interface:

- ☒ Pay by Phone - 11.07  
☐ Pay by Phone - 2.46

Purchase

### Fig. 6.2.3-1: Purchase Options

Once the user has selected the payment option and clicked “purchase”, you will be directed to a page that allows you to verify the purchase and move on to pay, as shown in Fig. 6.2.3-2.

Home	Account	Network	Hotspot
<b>Account Information</b>			
Account ID	pa1testes2		
Customers Name	test test		
Current Pay Method	<input type="checkbox"/>		
Auto Payment			
Invoice Number	Invoice will be generated when the payment is processed successfully		
Pay Amount	4.00		
<b>Payment Details</b>			
Invoice Number	Invoice will be generated when the payment is processed successfully		
Product	super internet		
Product Price	4.00		
Amount to be paid	4.00		
<p>Note: Mobile Payments have predefined set of prices. If you pay less than the amount specified above hotspot token will not get generated but your account will be topped up for future use</p>			
<div>Pay by MOBILE </div>			

Fig. 6.2.3-2: Verification

Next, you will be re-directed to Fortumo pages where you can verify that you would like to pay, and then choose your mobile operator and phone number to use (as per Fig. 6.2.3-3).

[< Z powrotem](#)
[English](#)
×

Płatność odbywa się w trybie testowym, nie zostaniesz obciążony należnością

car za **11,07 PLN**

Opłata zostanie doliczona do Twojego rachunku za telefon komórkowy

Orange

+48

1234567890

OK

Pomoc
 Dostawca usług Azotel



### Fig. 6.2.3-3: Mobile Details

At the next stage there may be some verification process with Fortumo, including sending an SMS. Once your payment was successful you will be re-directed back to SIMPLer with a note that payment went through, per section 6.2.3-4.

## Your Payment Transaction was successful

**Transaction Reference:** 24958e170dddb783431a76249edZ1197

Dear test test ,

Please use the following details to access the internet

**Username: pa1testes6**

**Password: zx747**

Please record the username and password above or open a new browser page in order to use the hotspot.

### Fig. 6.2.3-4: Payment Successful

## 6.3 ApplePay

This section will provide details for the setup of ApplePay integration.

NOTE:

ApplePay certificates do expire - accounts have to be maintained. One has to ensure that proper certificates get regenerated and sent over to Azotel before they expire.

### PREREQUISITES

- > Apple Account
- > Payment Gateway - [Authorize.NET](https://support.authorize.net/knowledgebase/Knowledgearticle/?code=000003850)

You can check to see if your processor is supported (as not all processors use network tokenization) using the link below:

<https://support.authorize.net/knowledgebase/Knowledgearticle/?code=000003850>

### 6.3.1 SETUP:

#### 6.3.1.1 Apple Pay Merchant Identifier

Create a **Merchant Identifier** as per the link below. It will be required as part of configuration in Azotel SIMPLer.

<https://developer.apple.com/help/account/configure-app-capabilities/configure-apple-pay#create-a-merchant-identifier>

### 6.3.1.2 Certs between ApplePay and Authorize.NET

a.) under [authorize.NET](#) account create a CSR (Certificate Signing Request) as per link below: [https://developer.authorize.net/api/reference/features/in-app.html#Apple\\_Pay](https://developer.authorize.net/api/reference/features/in-app.html#Apple_Pay)

b.) under Apple account create a **payment processing certificate** as per link below (use CSR - Certificate Signing Request created in step

(a)): <https://developer.apple.com/help/account/configure-app-capabilities/configure-apple-pay#create-a-payment-processing-certificate>

### 6.3.1.3 Certs between ApplePay and Azotel SIMPLer

a.) Request CSR (Certificate Signing Request) from [support@azotel.com](mailto:support@azotel.com). Azotel will send CSR to you.

b.) under Apple account create a **merchant identity certificate** as per link below (use CSR created in step (a)): <https://developer.apple.com/help/account/configure-app-capabilities/configure-apple-pay-on-the-web#create-a-merchant-identity-certificate>

(c) Download generated certificate and send it back to Azotel

### 6.3.1.4 Domain registration and verification

a.) follow Apple instructions to register a domain. You should use EUP domain, for example: [demo.azotel.com](https://demo.azotel.com)

<https://developer.apple.com/help/account/configure-app-capabilities/configure-apple-pay-on-the-web#register-a-merchant-domain>

b.) Domain requires verification - you will get a file for verification (apple-developer-merchantid-domain-association.txt). You need to download this file and send to [support@azotel.com](mailto:support@azotel.com) so we can upload it to the server. Once it is uploaded you can process verification:

<https://developer.apple.com/help/account/configure-app-capabilities/configure-apple-pay-on-the-web#register-a-merchant-domain> - little below there under section "Verify a merchant domain"

### 6.3.1.5 Azotel help

You need Azotel help in order to get things setup on Azotel side (generating CSR, uploading certs, uploading domain verification file). We can also help in finalizing the setup under Payment Gateways:

You can let us know:

Apple Display Name - this is what gets displayed when Apple Pay Pop-Up appears

[Authorize.NET](#) Login ID / Transaction Keys - if you use the same account / credentials as for regular CC/ACH payments we can copy them over.

payment type - we suggest to create a separate payment type called "applePay" to track applePay payments in SIMPLer (this payment type will have to be created under Settings -> Payment Types in SIMPLer).

Other options we recommend to stay as they are, unless you have a specific requirements to the types of cards accepted.

<b>APPLE_DISPLAY_NAME</b>	Test Merchant
<b>APPLE_MERCHANT_ID</b>	merchant.com.azotel
<b>AUTHORIZENET_API_LOGIN_ID</b>	
<b>AUTHORIZENET_ENDPOINT</b>	https://apitest.authorize.net/xml/v1/request.e
<b>AUTHORIZENET_TRANSACTIONKEY</b>	5i
<b>GATEWAY</b>	authorizenet
<b>MERCHANT_CAPABILITIES</b>	supports3DS supportsCredit supportsDebit
<b>PAYMENT_TYPE</b>	applePay
<b>SSL_CERT_NAME</b>	.pem
<b>SSL_KEY_NAME</b>	.key
<b>SUPPORTED_NETWORKS</b>	visa masterCard amex discover

[INTERNAL COMMANDS for Azotel Engineers]

#### 1. Create CSR (Certificate Signing Request):

In data/ssl folder:

```
openssl req -new -newkey rsa:2048 -nodes -keyout <key_name>.key -out <key_name>.csr
```

#### 2. Convert CER from Apple

In data/ssl folder:

```
openssl x509 -in <cert_name>.cer -inform DER -out <cert_name>.pem -outform PEM
```

## 6.4 Google Pay

Google Pay is much easier to setup. Here are the steps involved:

#### 6.4.1 [AUTHORIZE.NET](#):

- (a) make note of Payment Gateway ID (found under Account -> User Administration)
- (b) use API Login ID / API Transaction Key that you normally use when processing payments over API

#### 6.4.2 GOOGLE:

You will need:

- (a) Google Merchant Name
- (b) Google Merchant ID

You can set it up under "Google Pay and Wallet Console"

<https://developers.google.com/pay/api/web/guides/test-and-deploy/request-prod-access>

Once you have the credentials simply send them over to Azotel to setup under your instance (Settings -> Payment Gateways)

## Annex A: References

### A.1 Document References

Azotel Supported Payment Gateways							
Part 1 - Credit Card/ACH Modules							
Merchant Interface	Credit Card	ACH/ Echeck	Token Credit Card	Token ACH/ Echeck	DD /ACH Banking	Region / Country	Notes
Paypal	Yes	No	No	No	N/A	USA/Canada (PayPal Pro) PayPal standard - worldwide.	<a href="http://www.paypal.com">www.paypal.com</a>
AuthorizeNet	Yes	Yes	Yes	No	N/A	USA	<a href="http://www.authorize.net">www.authorize.net</a>
InterSwitch (via access bank plc)	Yes	No	No	No	N/A	Nigeria	<a href="http://cipg.accessbankplc.com">http://cipg.accessbankplc.com</a>
InterSwitchNg	Yes	No	No	No	No	Nigeria	<a href="http://www.interswitchng.com">http://www.interswitchng.com</a>
IPPAY	Yes	Yes	Yes	Yes	N/A	Worldwide	<a href="http://www.ippay.com">www.ippay.com</a>
Realex	Yes				N/A	UK, Ireland, France, Mainland Europe, Worldwide	<a href="http://www.realexpayments.com">www.realexpayments.com</a>
Realex_redirect_realvault			Yes		N/A	UK, Ireland, France, Mainland Europe, Worldwide	<a href="http://www.realexpayments.com">www.realexpayments.com</a>
PaymentsGateway		Yes	Yes		N/A	USA	<a href="http://www.paymentsgateway.com/home.aspx">www.paymentsgateway.com/home.aspx</a>
Netcash	Yes				N/A	Africa	<a href="http://www.netcash.co.za">www.netcash.co.za</a>
Moneris	Yes				N/A	Across North America	<a href="http://www.moneris.com">www.moneris.com</a>
Propay	Coming soon	Coming soon	Coming soon	Coming soon	N/A	USA	<a href="http://www.propay.com">www.propay.com</a>
Part 2 - DD Banking Modules supported by SIMPLer							
Banking Modules Supported by Azotel							
Bank of Ireland (default)					Yes	Ireland	<a href="http://www.bankofireland.com">www.bankofireland.com</a>
Bank of Ireland (DD+)					Yes	Ireland	<a href="http://www.bankofireland.com">www.bankofireland.com</a>
AIB					Yes	Ireland	<a href="http://www.aib.ie">www.aib.ie</a>
Ulster Bank					Yes	Ireland	<a href="http://www.ulsterbank.ie">www.ulsterbank.ie</a>
National Irish Bank					Yes	Ireland	<a href="http://www.nationalirishbank.ie">www.nationalirishbank.ie</a>
Eazipay					Yes	UK	<a href="http://www.eazipay.co.uk">www.eazipay.co.uk</a>
HSBC					Yes	UK	<a href="http://www.hsbc.com">www.hsbc.com</a>
Lyods TSB					Yes	UK	<a href="http://www.lloydstsb.com">www.lloydstsb.com</a>
Smart Debit				Yes	Yes	UK	
authorize.NET e-check type PPD					Yes	USA	<a href="http://www.authorize.net">www.authorize.net</a>
Security National Bank					Yes	USA	<a href="http://www.securitynationalbank.com">www.securitynationalbank.com</a>
Bank of Montreal					Yes	Canada	<a href="http://www.bmo.com">www.bmo.com</a>
CPA Standard 005					Yes	Canada	<a href="http://www.cdnpay.ca">www.cdnpay.ca</a>
Alberta Treasury Branches					Yes	Canada	<a href="http://www.atb.com">www.atb.com</a>
Norma 19					Yes	Spain	
Banco Santander					Yes	Spain	<a href="http://www.santander.com">www.santander.com</a>
Netcash Debit*					Yes	GENERAL	NOTE: * Netcash Debit requires Netcash credentials to be setup under settings->payment gateways
NACHA Format					Yes	US - General	
First National Bank					Yes	GENERAL / South Africa	

### A.2 Link References

[L1] <http://www.azotel.com/>

Azotel homepage.

[L2] <https://wib.azotel.com/>

Access to SIMPLer system.

---

## Annex B: Definitions and abbreviations

### B.1 Definitions

### B.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

<b>EFT</b>	Electronic Funds Transfer (Direct Debit)
<b>WIB-C</b>	WISP in a Box – Client
<b>SIMPLer</b>	Azotel's integrated Operators platform



## Annex C: Merchant Error Codes

### C.1 IPPAY General & CC Response Codes

Visa	Mastercard	Jetpay specific	Discover
00 Successful completion	00 Approved	089 Timeout	00 Approved or completed successfully
01 Refer to card issuer	01 Refer to issuer	750 Velocity check fail	01 Refer to Card Issuer
02 Refer to card issuer, special condition	03 Invalid merchant	899 Misc. decline	02 Refer to Card Issuer's special conditions
03 Invalid merchant or service provider	04 Capture card	900 Invalid message type	03 Invalid Merchant
04 Pick up card	05 Do not honor	901 Invalid Merchant ID	04 Capture Card
05 Do not honor	08 Honor with ID	903 Debit not supported	05 Do not honor
06 Error	10 Partial Approval	904 Private Label not supported	07 Pick-up Card, special condition
07 Pick up card, special condition	12 Invalid transaction	905 Invalid Card type	08 Honor with ID
10 Partial approval	13 Invalid amount	906 Unit not active	10 Approved for partial amount
11 VIP approval	14 Invalid card number	908 Manual Card Entry Invalid	11 Approved
12 Invalid transaction	15 Invalid issuer	909 Invalid Track Information	12 Invalid transaction
13 Invalid amount	25 Unable to locate record	911 Master Merchant not found	13 Invalid amount
14 Invalid account number	27 File update field edit error	912 Invalid Card Format	14 Invalid Card Number
15 No such issuer	30 Format error	913 Invalid Transaction Type	15 Invalid Issuer
19 Re-enter transaction	41 Lost card	917 Expired Card	19 Re-enter transaction
21 No action taken	43 Stolen card	919 Invalid Entry Type	30 Format error
25 Unable to locate record in file	51 Insufficient funds	920 Invalid amount	31 Bank not supported by switch
28 File is temporarily unavailable	54 Expired card	921 Invalid message format	33 Expired Card
39 No credit account	55 Invalid PIN	923 Invalid ABA	34 Suspected fraud
41 Pick up card (lost card)	57 Transaction not permitted to cardholder	924 Invalid DDA	35 Card Acceptor contact Acquirer
43 Pick up card (stolen card)	58 Transaction not permitted to terminal	925 Invalid TID	36 Restricted Card
51 Insufficient funds	61 Exceeds withdrawal limit	926 Invalid Password	37 Card Acceptor call Acquirer security
52 No checking account	62 Restricted card	930 Invalid zipcode	38 Allowable PIN tries exceeded
53 No savings account	63 Security violation	931 Invalid Address	39 No credit Account
54 Expired card	65 Exceeds withdrawal count	932 Invalid ZIP and Address	40 Requested function not supported
55 Incorrect PIN	68 Response late	933 Invalid CVV2	41 Lost Card
57 Transaction not permitted to cardholder	70 Contact card issuer	940 Record Not Found	43 Stolen Card
58 Transaction not allowed at terminal	71 PIN not changed	941 Merchant ID error	51 Decline
59 Suspected Fraud	75 PIN tries exceeded	942 Refund Not Allowed	53 No savings Account
61 Activity amount limit exceeded	76 Invalid "to" account	943 Refund denied	54 Expired Card
62 Restricted card	77 Invalid "from" account	958 Bad Status	55 Invalid PIN
63 Security violation	78 Nonexistent account	981 Invalid AVS	56 No Card record
65 Activity count limit exceeded	79 Key exchange validation failed	987 Issuer Unavailable	57 Transaction not permitted to Issuer/Cardholder
75 Allowable number of PIN-entry tries exceeded	80 Duplicate add. action not performed	988 System error SD	58 Transaction not permitted to Acquirer/terminal
76 Unable to locate previous message	84 Invalid auth life cycle	989 Database Error	59 Suspected fraud
77 Message inconsistent with original message	85 Not declined	992 Transaction Timeout	60 Card acceptor contact Acquirer
78 Blocked, first used	87 Cash back not allowed	996 Bad Terminal ID	61 Exceeds withdrawal amount limit
80 Invalid date	89 Auth system or issuer inop	997 Message rejected by association	62 Restricted Card
81 PIN crypto error	91 Auth system or issuer inop	999 Communication failure	63 Security violation
82 Incorrect CVV	92 Unable to route transaction	994 Invalid avs hosted page	64 Original amount incorrect
83 Unable to verify PIN	94 Duplicate transmission	995 Invalid cvv hosted page	65 Exceeds withdrawal count limit
85 No reason to decline request for account or address verification	96 System error	99 Format Error	66 Card Acceptor call Acquirer's security dept
91 Issuer or switch inoperative		900 Network Error	67 Hard capture (requires ATM pick-up)
92 Destination cannot be found for routing			68 Response received too late
93 Transaction cannot be completed, violation of law			75 Allowable number of PIN tries exceeded
96 System malfunction			76 Invalid/nonexistent "to" Account specified
809 R1 Surcharge not permitted	000 Approved		77 Invalid/nonexistent "from" Account specified
805 N0 Force STP	001 Approve with ID		78 Invalid/nonexistent Account specified (general)
57 N3 Cash service not available	002 Partial Approval		91 Authorization system or Issuer system inoperative
61 N4 Cash request exceeds issuer limit	003 Approve VIP		92 Unable to route transaction
806 N7 Decline for CVV2 failure	092 Approved (Express Rewards Program)		93 Transaction cannot be completed, violation of law
0 P0 Approved: PVID missing, invalid or expired	100 Deny		94 Duplicate transmission detected
83 P1 Declined: PVID missing, invalid or expired	101 Expired Card		96 System malfunction
807 P2 Invalid biller information	103 Deny - Invalid Manual Entry		
55 P5 PIN change/unblock request denied	104 Deny - New card issued		
55 P6 Unsafe PIN	105 Deny - Account Canceled		
807 Q1 Card authentication failed	107 Please call issuer		
808 R0 Stop Payment order	109 Invalid Merchant		
808 R1 Revocation of Auth order	110 Invalid Amount		
808 R3 Revocation of all auth order	111 Invalid Account		
2 XA Forward to issuer	115 Service not permitted		
2 XD Forward to issuer	122 Invalid security code		
999 Z3 Decline: unable to go online	125 Invalid effective date		
	181 Format error		
	182 Please wait		
	183 Invalid currency code		
	187 Deny - new card issued		
	188 Deny - Account Canceled		
	189 Deny - closed merchant		
	200 Deny - pick up card		
	400 Reversal Accepted		



## C.2 IPPAY ACH Response Codes

	A	B	C	D	E
1		<b>ACH</b>			
2	C01	Approved			
3	C02	Approve with ID			
4	C03	Approve VIP			
5	C04	Approved (Express Rewards Program)			
6	C05	Deny			
7	C06	Expired Card			
8	C07	Deny - Invalid Manual Entry			
9	C09	Deny - New card issued			
0	C10	Deny - Account Canceled			
1	C11	Please call issuer			
2	C12	Invalid Merchant			
3	C13	Invalid Amount			
4	R01	Insufficient funds			
5	R02	Account closed			
6	R03	No account/unable to locate			
7	R04	Invalid account number			
8	R05	Reserved			
9	R06	Returned per ODFI's Request			
0	R07	Authorization Revoked by Customer			
1	R08	Payment stopped			
2	R09	Uncollected funds			
3	R10	Customer advises not authorized			
4	R11	Check truncation entry Return			
5	R12	Branch sold to other DFI			
6	R13	RDFI not qualified to participate			
7	R14	Representative payee deceased or unable to continue in that capacity			
8	R15	Beneficiary deceased			
9	R16	Account frozen			
0	R17	File/Record edit criteria			
1	R18	Improper effective entry date			
2	R19	Amount field error			
3	R20	Non-transaction account			
4	R21	Invalid company ID			
5	R22	Invalid individual ID			
6	R23	Credit entry Refused by Receiver			
7	R24	Duplicate entry			
8	R25	Addenda error			
9	R26	Mandatory field error			
0	R27	Trace number error			
1	R28	Transit/Routing check digit error			
2	R29	Corporate customer advises not authorized			
3	R30	RDFI not a participant in check truncation program			
4	R31	Permissible Return entry			
5	R32	RDFI - non-settlement			
6	R33	Return for XCK			
7	R34	Limited participation DFI			
8	R50	State law affecting RCK acceptance			
9	R51	Item is ineligible, notice not provided, signature not genuine, or item altered			
0	R52	Stop payment on item for which an RCK item was Received			
1	R80	Cross border coding error			
2					
3					
4					
5					

\*NOTE: All CXX series of codes for ACH are known as ROCs (Records Of Change). The ACH was processed but the information submitted is no longer valid. This DOES NOT mean the ACH was rejected, only that the receiving institution has notified us that the information in the original submission is either incorrect or has changed due to bank mergers, acquisitions, etc.

\*RXX series of codes for ACH are REJECTS.

RDFI = Receiving Depository Financial Institution  
ODFI = Originating depository financial institution

Phases of ACH Transfers	
ND	Not Done
PH1	Phase 1 - Request for funds
PH2	Phase 2 - Funds transferred to RDFI (merchant's acct)
CMP	Complete - delay times passed - transfer done

\*CMP can be changed if challenged (i.e. R10)

### C.3 IPPAY DLL Response Codes

CODE	DESCRIPTION	CAUSES						
A50	Unexpected error	Virtual Terminal Application Error						
A80	Invalid transaction type	Transaction type code is not recognized						
A81	Missing Merchant ID	Merchant ID is not present						
A82	Invalid price	Price is negative						
A83	Invalid ABA number	ABA number size problem						
A84	Missing checking account number	Account number size is zero						
A85	Missing check number	Check number size is zero						
A86	Invalid check surcharge	Surcharge is negative						
A87	Invalid credit card expiration date	The size of the expiration date is different to four digits: must be MMY						
A88	Missing credit card number	Credit card number size is zero						
A89	Invalid credit card number	The size is incorrect, or is not numeric or invalid						
A90	Invalid CVV2 number	CVV must be numeric						
A91	Missing account holder name	Account holder name size is zero						
E50	Unexpected error							
E51	No response received from JetPay Gateway							
E52	Incomplete response received from JetPay Gateway							
E53	Invalid response received from JetPay Gateway							
E54	Action code not returned from JetPay Gateway							
E55	Transaction identifier returned from JetPay Gateway did not match outbound							

\*NOTE: On several of these errors it is possible that the transaction did in fact hit the JetPay system and was approved. You may wish to contact JetPay at 1-800-834-4405 ext 2 to confirm that it did in fact not process before retrying the transaction. Specifically any of the EXX error codes where a communication error occurred, or the A50 error code could have actually gone through.

\*EXX error codes are generally caused by communication errors between the client and JetPay.

## C.4 AVS Codes

1				
2	VISA			
3	AVS resp	Addr Match	Zip Match	Inter. Only
4	A	Y	N	N
5	B	Y	X	N
6	C	X	X	N
7	D	Y	Y	Y
8	F	Y	Y	Y
9	G	X	X	Y
10	I	X	X	Y
11	M	Y	Y	Y
12	N	N	N	N
13	P	X	Y	N
14	R	X	X	N
15	S	NA	NA	NA
16	U	X	X	N
17	W	NA	NA	NA
18	X	NA	NA	NA
19	Y	Y	Y	N
20	Z	N	Y	N
21				
22				
23	MC			
24	AVS resp	Addr Match	Zip Match	
25	A	Y	N	
26	B	Y	X	
27	C	X	X	
28	D	Y	Y	
29	F	Y	Y	
30	G	X	X	
31	I	X	X	
32	M	Y	Y	
33	N	N	N	
34	P	X	Y	
35	R	X	X	
36	S	X	X	
37	U	X	X	
38	W	N	Y	
39	X	Y	Y	
40	Y	Y	Y	
41	Z	N	Y	
42				
43				
44	AMEX			
45	AVS resp	Addr Match	Zip Match	Name Match
46	A	Y	N	X
47	D	N	Y	N
48	E	Y	Y	N
49	F	Y	N	N
50	K	N	N	Y
51	L	N	Y	Y
52	M	Y	Y	Y
53	N	N	N	X
54	O	Y	N	Y
55	R	X	X	X
56	S	X	X	X
57	U	X	X	X
58	W	N	N	N
59	Y	Y	Y	X
60	Z	N	Y	X
61				
62	Discover			
63	AVS resp	Addr Match	Zip Match	
64	A	Y	Y	
65	S	X	X	
66	T	N	Y	
67	U	X	X	
68	W	X	X	
69	X	Y	Y	
70	Y	Y	N	
71	Z	N	Y	
72				
73				

## C.5 ELAVON Codes

### 16. Reason codes

#### Top retrieval request reason codes

Visa reason code	Description
28	Request for copy bearing signature
32	Cardholder does not recognise transaction
33	Fraud analysis request

Mastercard reason code	Description
6321	Cardholder does not recognise the transaction
6341	Fraud investigation

#### Top chargeback reason codes

Visa reason code	Description
60	Illegible fulfilment
75	Transaction not recognised
81	Fraud – card present environment
83	Fraud – card absent environment
71	Declined authorisation
72	No authorisation
74	Late presentment
77	Non-matching account number
80	Incorrect transaction amount or account number
82	Duplicate processing
86	Paid by other means
74	Late presentment
53	Not as described or defective merchandise
85	Credit not processed
30	Service not provided or merchandise not received

Mastercard reason code	Description
4840	Fraudulent processing of transaction
4837	No cardholder authorisation
4863	Cardholder does not recognise
4870	Chip liability shift
4847	Request authorisation not obtained
4808	Request required authorisation not obtained
4812	Account number not on file
4834	Point of interaction error
4860	Credit not processed
4853	Cardholder dispute
4855	Non-receipt of merchandise
4859	Service not rendered

## Annex D: Change history

Change history				
Date	Author	Subject/Comment	Old	New
08/07/2013	emma	Original	N/a	001
19/07/2013	emma	Updated Doc	001	002
16/09/2013	emma	Updated Doc	002	003
25/11/2013	emma	Updated Doc – FNB	004	005
20/12/2013	emma	Updated Doc – SEPA	005	006
23/12/2013	emma	Updated Doc with Maciej's comments	006	007
28/03/2014	emma	Updated Doc	007	008
18/04/2014	emma	Updated blank fields	008	009
15/07/2014	emma	Updated Interswitch Section	009	010
05/08/2014	emma	Updated doc with Bank of Montreal and SagePay information	010	011
30/11/2014	emma	Updated Netcash Debit instructions	011	012
09/12/2014	emma	Updated doc with auth.net PCI compliance	012	013
01/05/2015	emma	Updated Section 4.20	013	014
23/06/2015	emma	Updated Introductory Table	014	015
07/01/2016	emma	Added Section 4.21 – Gocardless	015	016
18/01/2016	emma	Corrections to Gocardless	016	017
08/02/2016	emma	Stripe Documentation	018	019
13/04/2016	emma	Updated Sagepay Section	019	020
23/05/2016	emma	Updated SagePay Debit Section	020	021
08/06/2016	emma	Added SagePay Failures Section	021	022
15/06/2016	emma	Clarification in SagePay Debit doc	022	023
04/07/2016	emma	Added Section on Fortumo	023	024
12/07/2016	emma	Some updated to Moneris section	024	025
25/07/2016	emma	Documented Moneris	025	026
16/09/2016	emma	Documented Paydock	026	027
23/09/2016	emma	Documented SEPA Updates	027	028
28/03/2017	emma	Documented Remita	028	029
04/04/2017	emma	Documented TD Bank	029	030
19/04/2017	emma	Updated IP Pay Availability	030	031
31/05/2017	emma	Documented section 4.13 – ATB Module	031	032
11/09/2017	emma	Documented Converge	032	033
12/05/2019	pawel	IPPAY Error Codes – Annex C	033	034
12/05/2020	heather	Updated Fig. 2.2-1: Credit Card/ACH Interfaces, added Realex / Global Payments and Paystack	034	035
23/12/2021	oharej	Updated IPPAY and Elavon Error Codes	035	036