# PT2 System Document

## User Manual

Version 1.0
15 July 2020
Christine Trinidad, Florida Estrella

# Contents

# Document Information

Version:            1.0
Date:               15 July 2020
Prepared by:        Christine Trinidad, Florida Estrella

**History**

| Version | Date | Notes |
|---------|------|-------|
| 1.0 | 15 Jul 2020 | Updated: Invoicing<br>Added: Background, Transaction details, Test card, Reason codes, |

# 1. Document Overview

This User Guide covers the **use of PayTabs V2 System** (V2) for following Business Units:

1. Merchant
2. PayTabs Commercial and Business Development team
3. PayTabs Customer Success team

| Portals | | |
|---|---|---|
| Merchant | : | https://merchant.paytabs.com/merchant/home |
| Developers | : | https://merchant.paytabs.com/merchant/developers |

# 2. Background

**Partners**

The system is designed to operate as a 'white-label' system, and this is controlled at a top-level using partner IDs. All data in the system is segregated at this level. It is designed such that an individual white-label system can be operated on its own infrastructure, or on infrastructure shared with other white-labels.

**Merchants**

A merchant is linked to one white-label system. The merchant record is largely a way of grouping information related to a single company, and the onboarding/underwriting process takes place at this level.

**Profiles**

Each merchant will generally have 2 profiles. One is their initial testing profile, which is automatically created when they first register. This allows for things such as integration work and getting familiar with the operation of the system to happen in parallel with their application being processed.

Once a merchant has been approved, a live profile is created. The merchant can now switch between the test and live profiles at any time, both at the merchant dashboard level and within the integration to the system. The test profile will always remain active, allowing the merchant to do any additional integration work/testing they may want at any time without affecting their live processing.

All transactions are segregated at the profile level.

A merchant may require more than one live profile, for example dealing with different brands or trading names that they operate under, but in most cases it will be one test and one live profile.

**Terminals**

Within each profile, a merchant will have one or more terminals. These are the links to the acquirers. A profile may have any number of terminals with any mixture of currencies, acquirers, payment methods etc. For example, a single profile could have a terminal that processes SAR transactions through Riyadh Bank using Cybersource, an AED link through Mashreq using MPGS, and so on.

**Accounts**

Each merchant, once accepted, will have at least one account. This manages the payments to the merchant (there is a separate accounting document which details this process). An account operates under a single trading currency. This trading currency does not need to match the transaction currency, any transaction processed in a different currency will be converted to the account currency when pushed to the accounting system (This does not affect the currency the transaction itself is processed in)

Each terminal is linked to a merchant account. All transactions through that terminal will be process and paid through the relevant merchant account. Multiple terminals can link to the same account.

**Users**

Each merchant can have more than one user (login) associated with it. Each user associated with a merchant can be given a specific role and set of permissions, which controls what that user will be able to do when they login.

For example, a user may be given a customer support type role where they can lookup transactions but would not have any access to the accounting system, the developer/integration sections. A finance role would be able to see transactions and the accounting system. There are several different roles with different abilities, and additional roles can be created if required.

In addition to a merchant being able have more than one user, a user can be linked to more than one merchant. It is possible for a user to have a different role within each merchant they are connected to.

A common example of this is merchants giving access to a third-party developer to work on integrating their systems. The merchant can invite the user to their merchant using the 'developer' role (and optionally say they can only see the test profile, not the live one). This same user may have developer links to multiple merchants, and when that user logs in can switch between these merchants at any time. The merchant can later unlink that user when they want to, and that user would then no longer have any access to that merchant.

**Block Diagram**

This shows the basic relationships between the different elements. For example, a merchant will have 1 or more profiles, and may have 0 or more accounts (test transactions are not linked to an account).
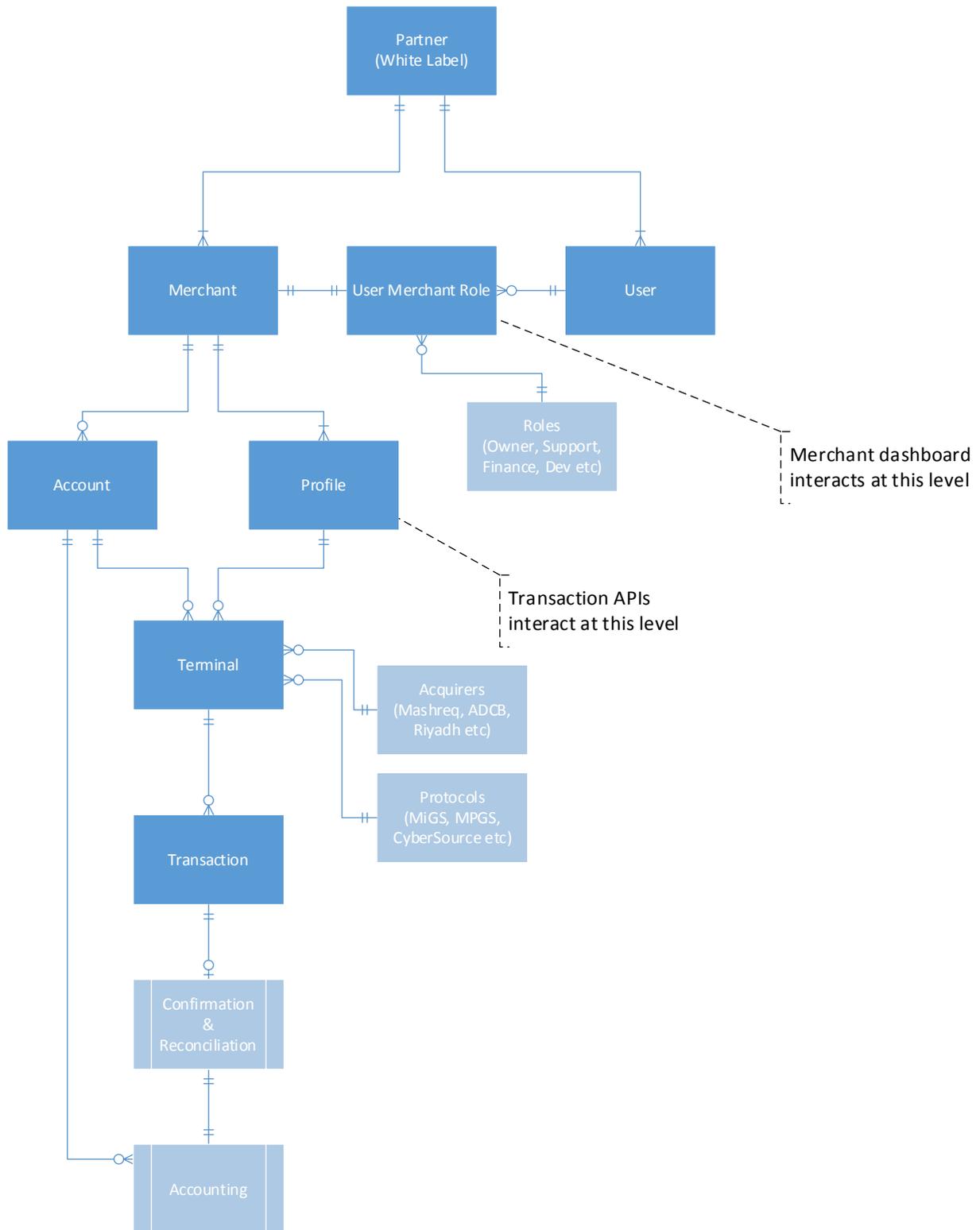
# 3. Sign Up and Verification

Creating an account with PayTabs is simple and easy. Get started by setting up an account using basic customer information and company details. An email verification to generate a new password is instantly sent upon registration.
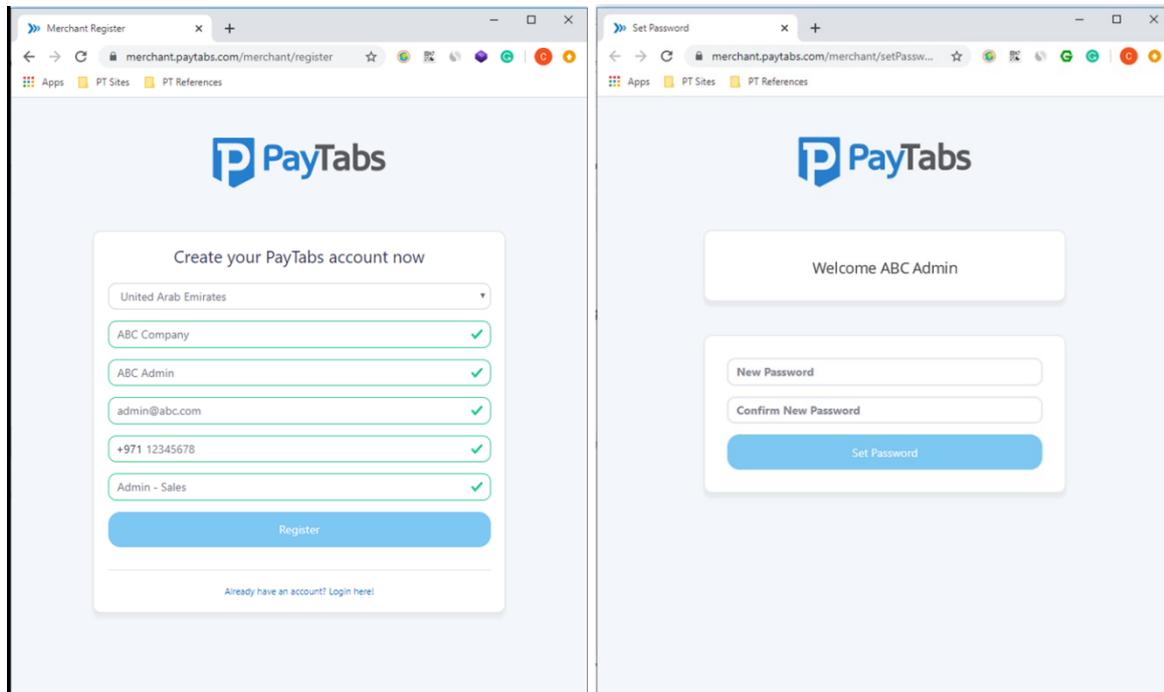
# 4. Account Activation

There are 5 Stages to complete the onboarding process; *Company Details, Trading Details, Bank Details, Ownership Details*, and *Document Collection*. Merchant is required to enter accurate information for all stages as compliance to standard Know-Your-Customer (KYC) and Know-Your-Business (KYB) procedure. Activation will be confirmed after successful review and approval from PayTabs team.

## Stage 1: Company Details

## Stage 2: Trading Details



## Stage 3: Banking Details

## Stage 4: Ownership Details



## Stage 5: Document Collection

# 5. User Creation and Role Assignment

Each merchant can have more than one user (login) associated with it. Each user associated with a merchant can be given a specific role and set of permissions, which controls what that user will be able to do when they login.

In the Team panel, users can add team members and assign roles to manage transaction monitoring, reporting and other processing functions.



For example, a user may be given a customer support type role where they can lookup transactions but would not have any access to the accounting system, the developer or integration sections. A finance role would be able to see transactions and the accounting system. There are several different roles with different abilities, and additional roles can be created if required.
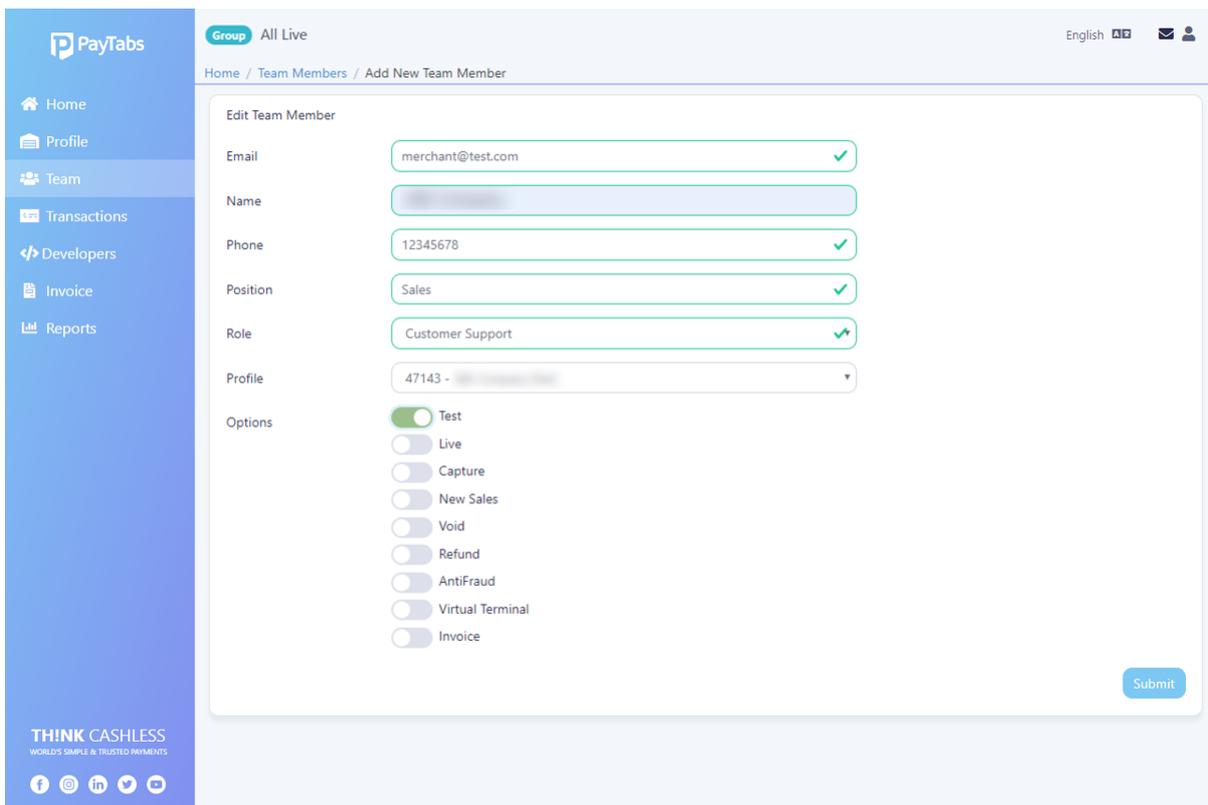
# 6. Profile Management

The initial setup is a testing profile, which is automatically created when they first register. This allows for things such as integration work and getting familiar with the operation of the system to happen in parallel with their application being processed. Once a merchant has been approved, a *Live* profile is created. The merchant can now switch between the test and live profiles at any time, both at the merchant dashboard level and within the integration to the system.

The *Test* profile will always remain active, allowing the merchant to do any additional integration work or testing they may want at any time without affecting their live processing. All transactions are segregated at the profile level.
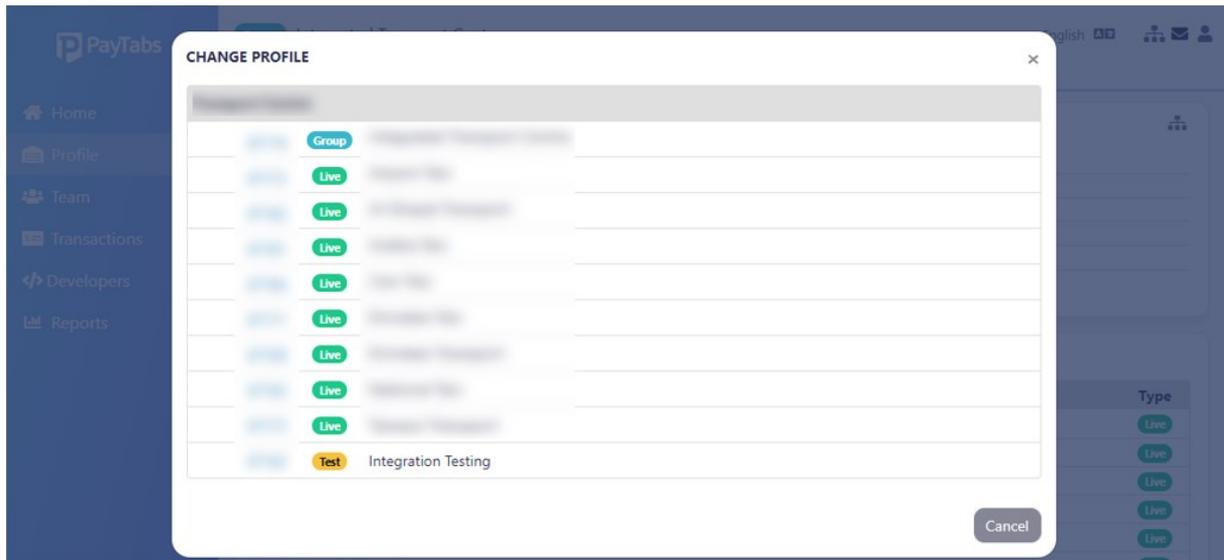


## 6.1 Accounts

Each merchant, once accepted, will have at least one *account* which manages the payments to the merchant. An account operates under a single trading currency. This trading currency does not need to match the transaction currency, any transaction processed in a different currency will be converted to the account currency when pushed to the system. This does not affect the currency the transaction itself is processed in.
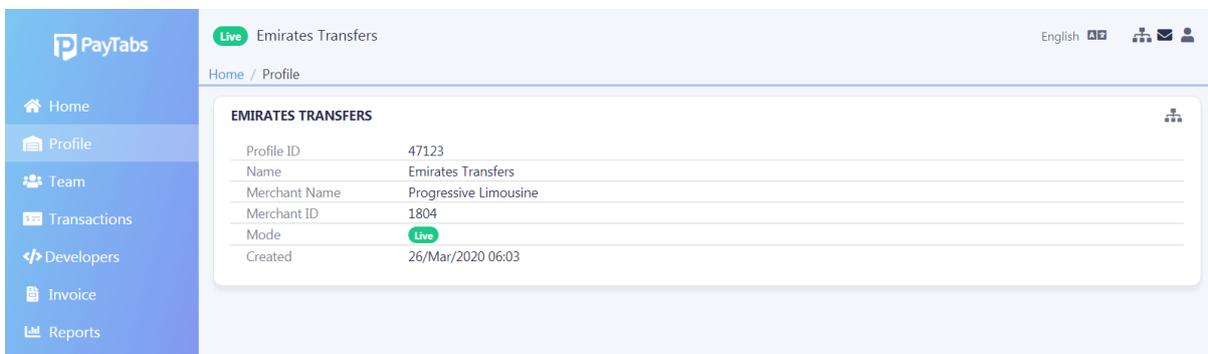
# 7. Transaction Reporting

## 7.1 PayTabs Dashboard – Home Panel

The Home dashboard displays transactions ordered by latest transaction date. 'Transactions Today', 'Sales Today' and 'Sales This Month' are shortcuts to Transaction Panel.



## 7.2 Transactions Panel

The 'Sales This Month' shortcut from the Home Panel displays on the Transaction Panel the list of **A**uthorised transactions for the current month. Option to save in Excel or CSV format is available, as well as applying additional filters.

The Transaction table displays the following fields

| Field | Description | Values |
|---|---|---|
| Ref | Transaction reference number | - |
| Customer Name | Customer name | - |
| Type | Transaction type | Sale<br>Void – To reverse full authorised amount<br>Authorization<br>Capture – To capture a previously authorised amount<br>Release – To release an amount previously authorised<br>Refund<br>Register – Authorization that cannot be captured |
| Payment Method | Payment method | MasterCard<br>Visa<br>Electron<br>Maestro<br>AMEX<br>JCB<br>[this list is not exhaustive] |
| Currency | Authorization Currency | AED<br>[this list is not exhaustive] |
| Amount | Transaction amount | - |
| Date | Transaction execution date | - |
| Time | Transaction execution time | - |
| Status | Transaction status | A: Authorised<br>H: Hold – Authorised but on hold<br>P: Pending<br>V: Voided<br>E: Error<br>D: Declined<br>[This list is not exhaustive.] |

Several filters are available to search for transactions - Cart ID, Email, Transaction Status and Date range, where Transaction Status can be Authorised, Error, Declined, Any status, Any status except Authorised.

## 7.3 Transaction Details

Transaction details are shown below. It has three sub-tabs: Payment Method, Customer Details and Notes.

**Payment Method** shows Channel used, Card details, Issuer details and RRN.
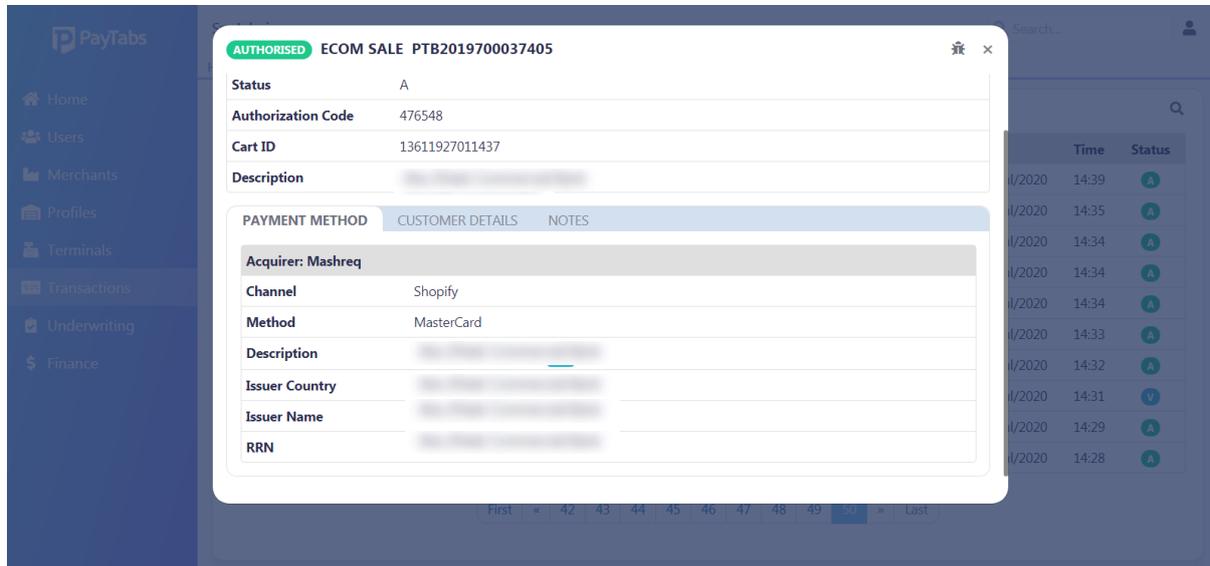


**Customer Details**
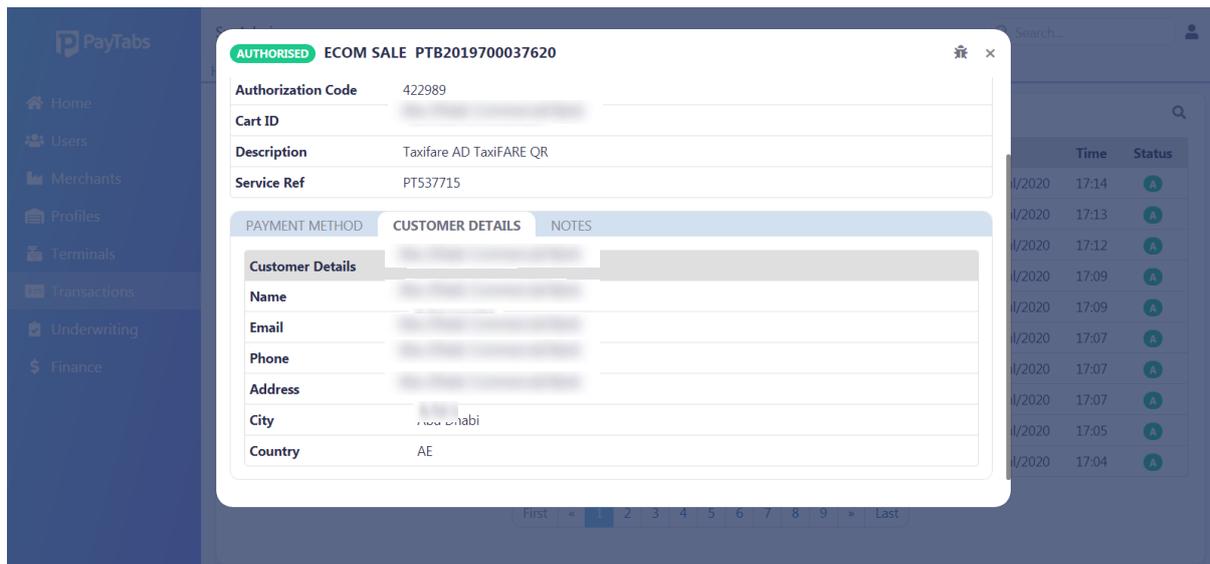
## 7.4 Refunding an Authorised Sale Transaction

Indicate the amount to be refunded to execute a refund request on an authorised transaction.
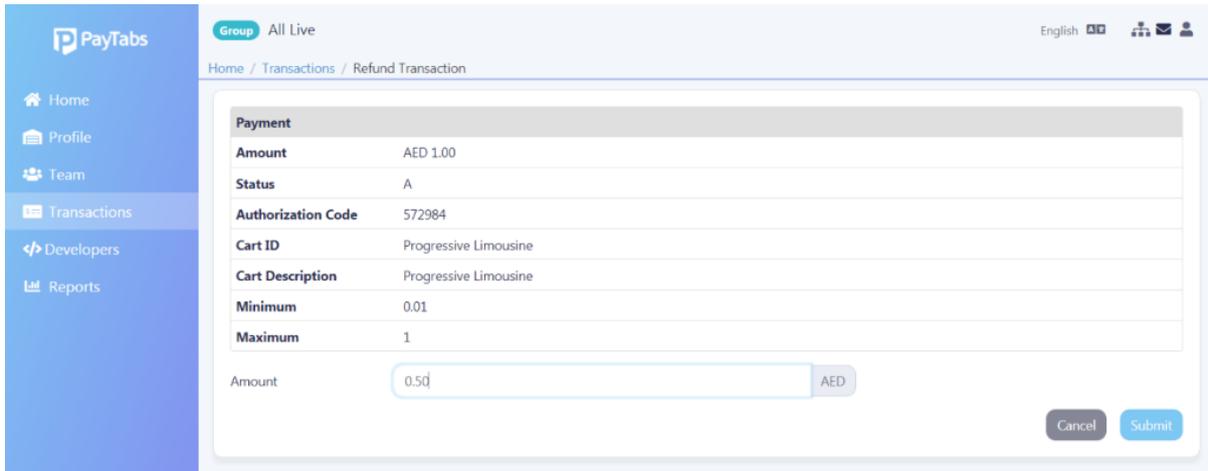


## 7.5 Void Functionality

Users can only refund a transaction with an Authorised status. If there is a need to cancel a transaction that has an Authorised status, you may be able to issue a partial release or void instead.
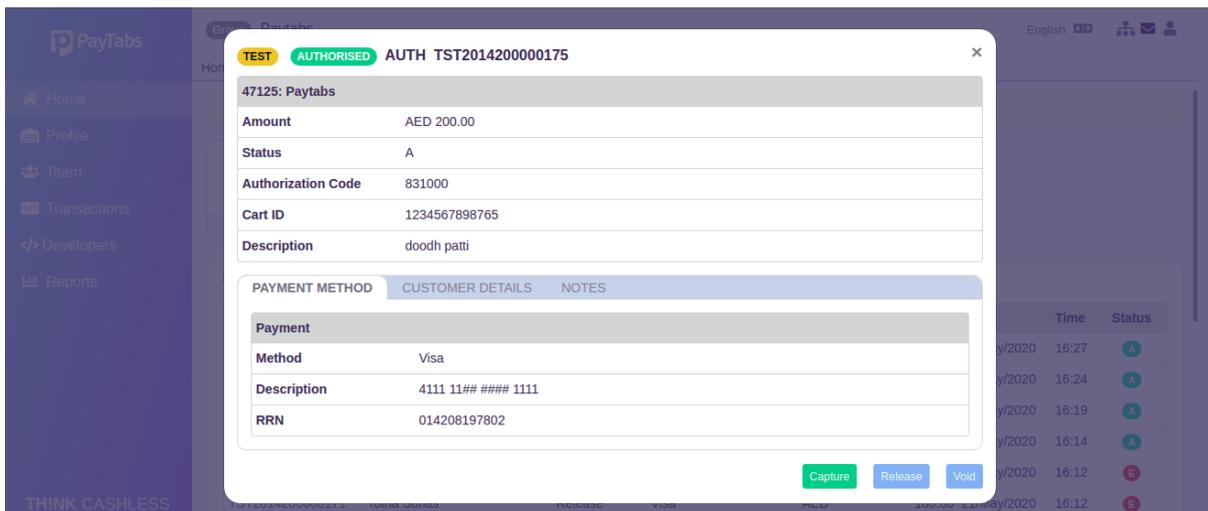
# 8. Other Available Features

## 8.1 Developers Panel

With a single dashboard, access several integration documentation and guides for seamless integration that will suit your platforms.
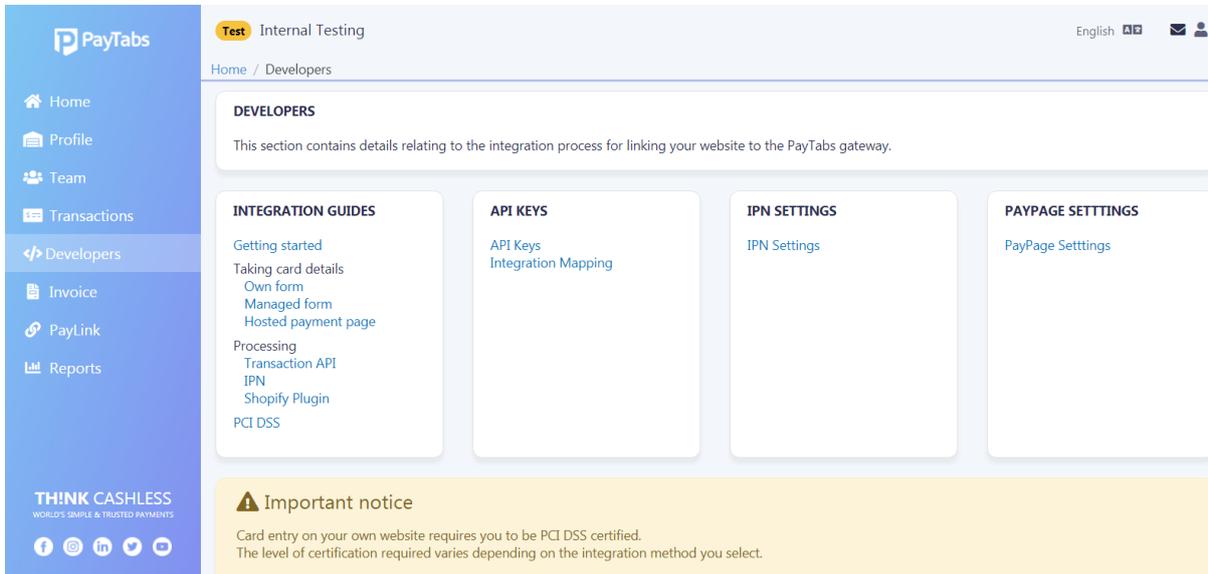


## 8.2 Instant Payment Notification (IPN) Service

As soon as a transaction is created or altered, IPN will instantly send a notification to the merchant's specified IPN Listener URL, which can have any code that will assist in updating ERP or dependent systems. Alternatively, the merchant may wish to save this information in his local database.

Access IPN Service

## Add an IPN configuration

## To view IPN configurations
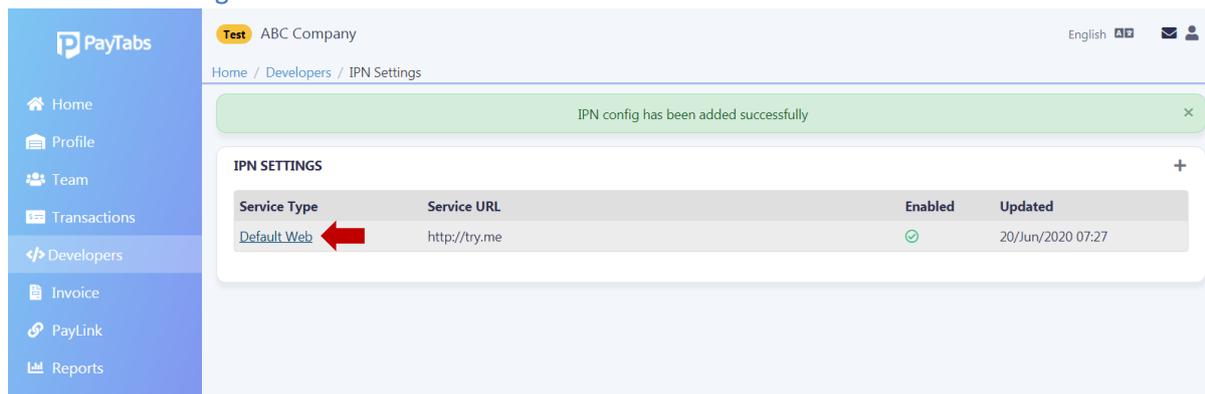




## Using IPN service

To use IPN service

a.  Include a callback URL in the transaction request, and that will be used as the first IPN for that transaction and/or

b.  Add manual IPN configs in the dashboard, and those will also be run for each transaction for all transaction events.

The IPN will be triggered as soon as the transaction is completed and expects to get a '200 OK' response from their site. If it does not, it goes into a queue to try again. It will be retried up to 5 times, with an increase delay between each attempt. Until it either gets a 200 OK response or the retry count is exceeded. If the IPN does not get the '200 OK' response, an entry is added to the transaction notes showing this, so we have a record that it was attempted to failed to get the correct response.

## 8.3 PayPage Settings

To configure the look and feel of PayPage

## 8.4 Reports Panel

Report manager is a three-step process: (a) Create report layout (b) Configure report generation, and (c) View/receive generated reports.

### Create/Edit report layout

## Report configuration

Reports can be configured in terms of time (daily, weekly or monthly), report layout, report format (xlsx or csv) and email of the report recipient.

Report can also be protected with a password, if required.
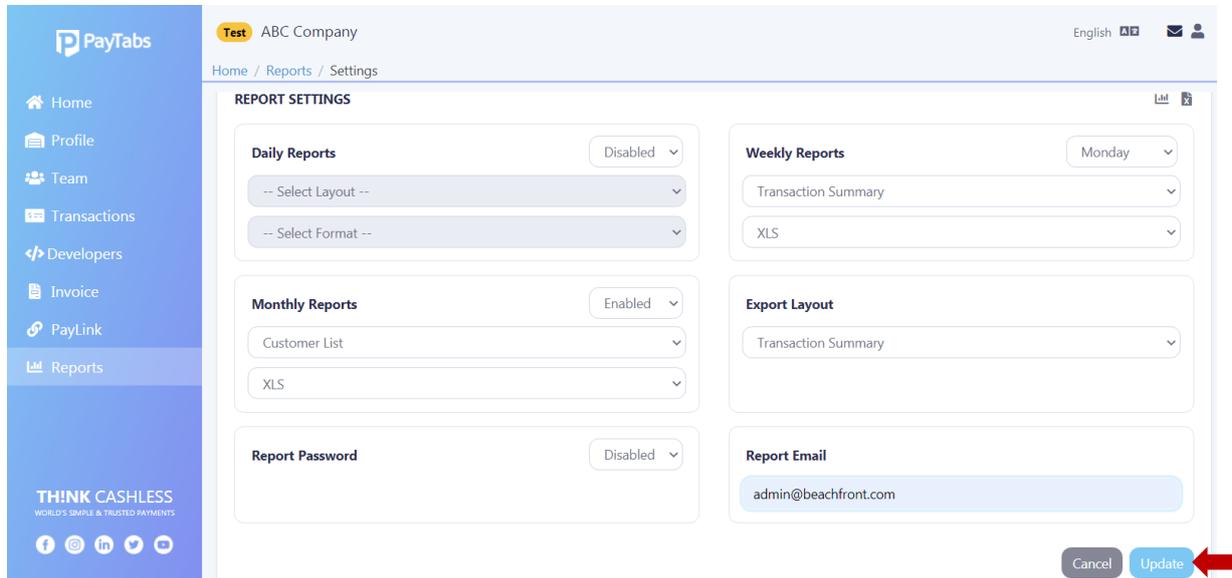


## View generated reports
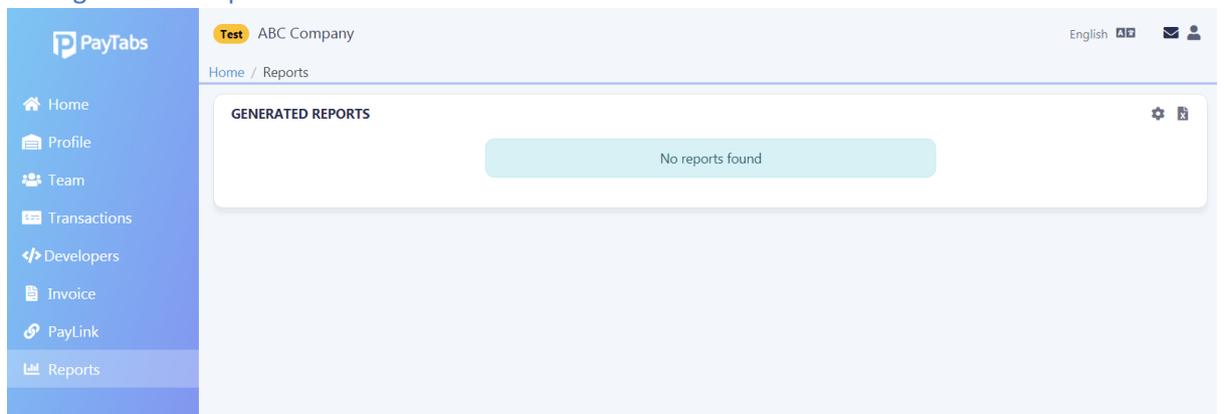
## 8.5 Invoice

Without any integration required, merchants can issue invoices from the dashboard by simply filling out the standard form which includes the Customer details and the Product/Service information.

### List invoices



### 8.5.1.  Create an invoice

It can be a standard (one-time use) invoice or re-usable template invoice.
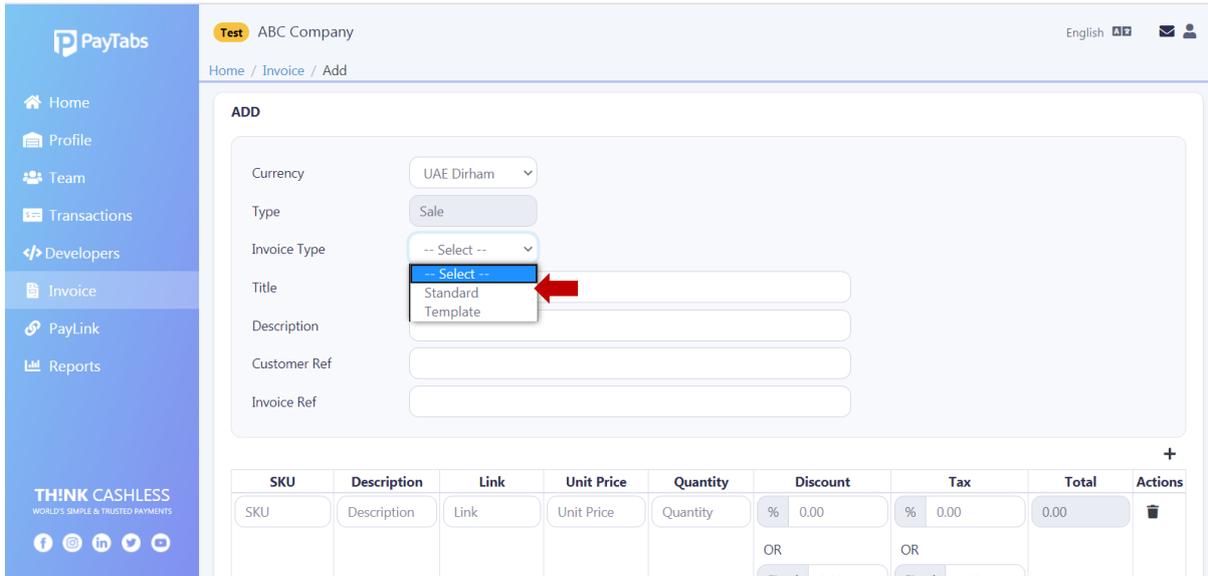


Configurable item pricing with discount and tax options, and option to include additional charges.
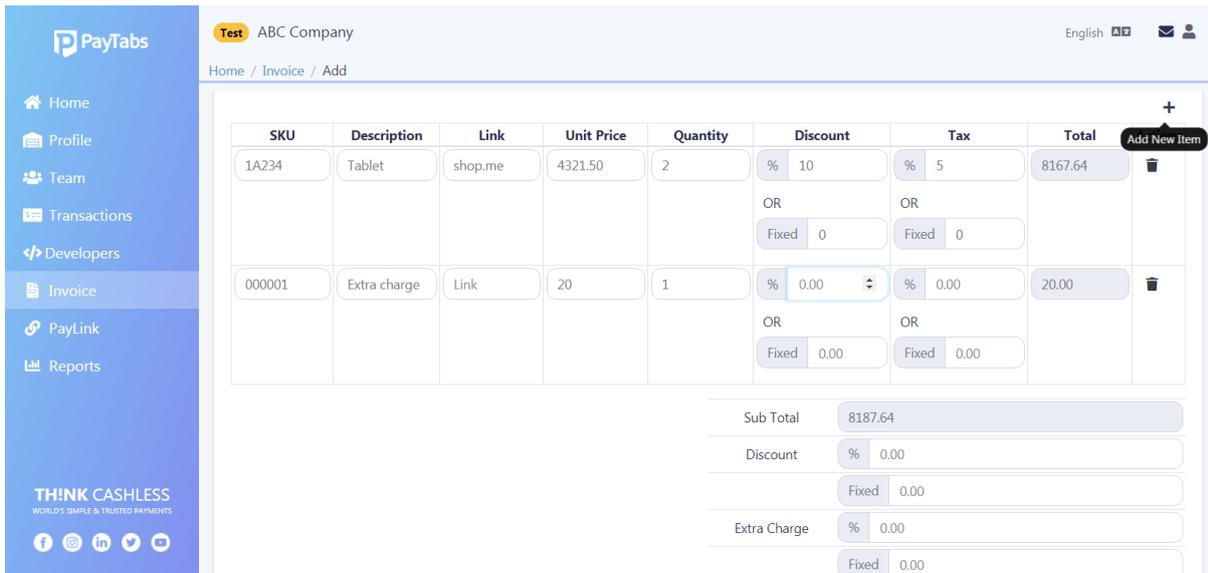


Customer Details and Shipping Details can be pre-filled.
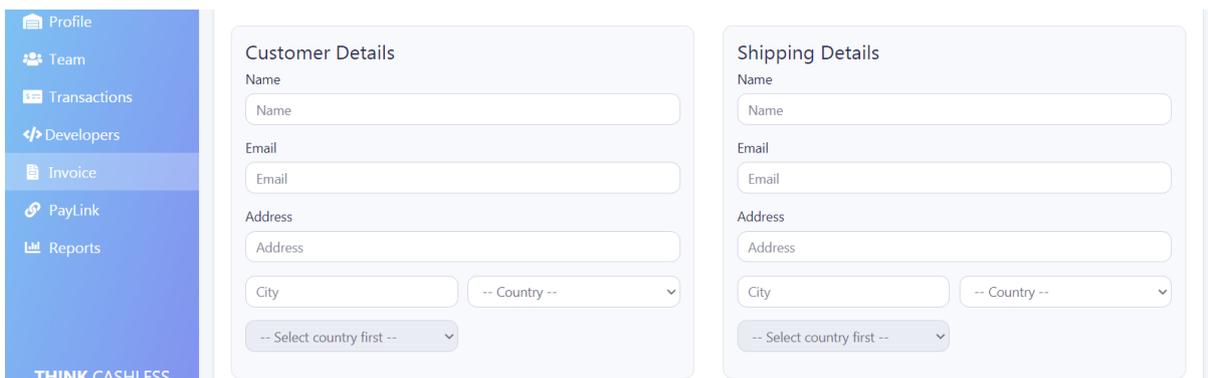
Option to Save or Save and Send by email are provided.
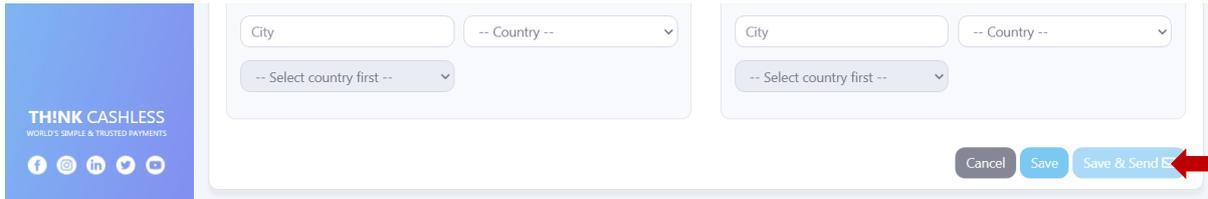


Note: The merchant can edit the invoice only when the status is 'Pending'.

## 8.5.2.  Send invoice via SMS or Email

Step 1 - Choose the invoice
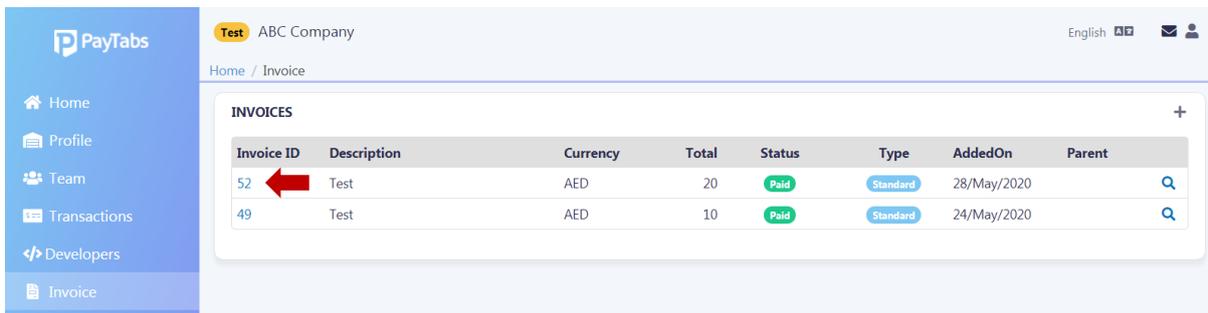


Step 2 – SMS: Enter customer phone number
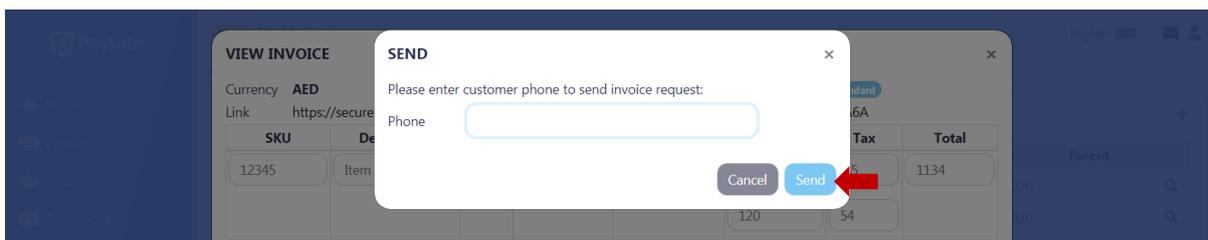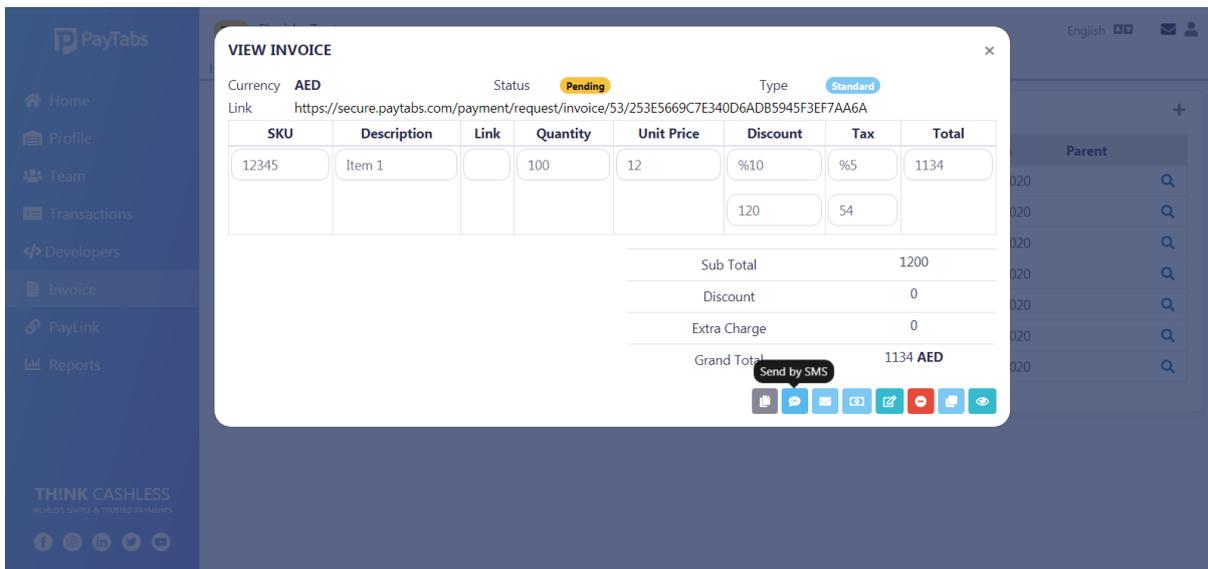
## Step 2 - Email: Enter customer name and email
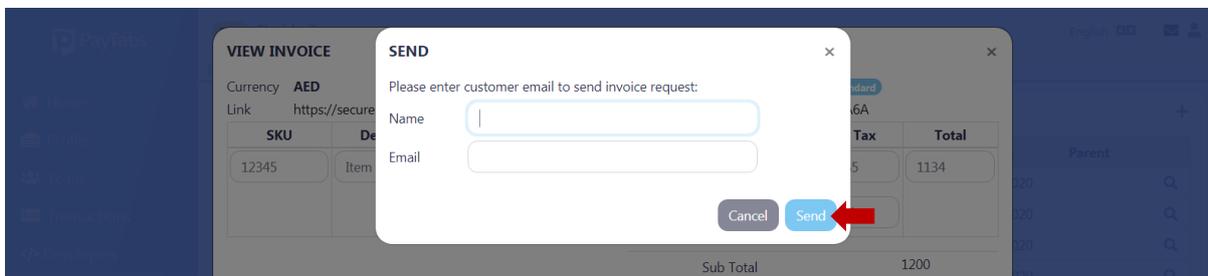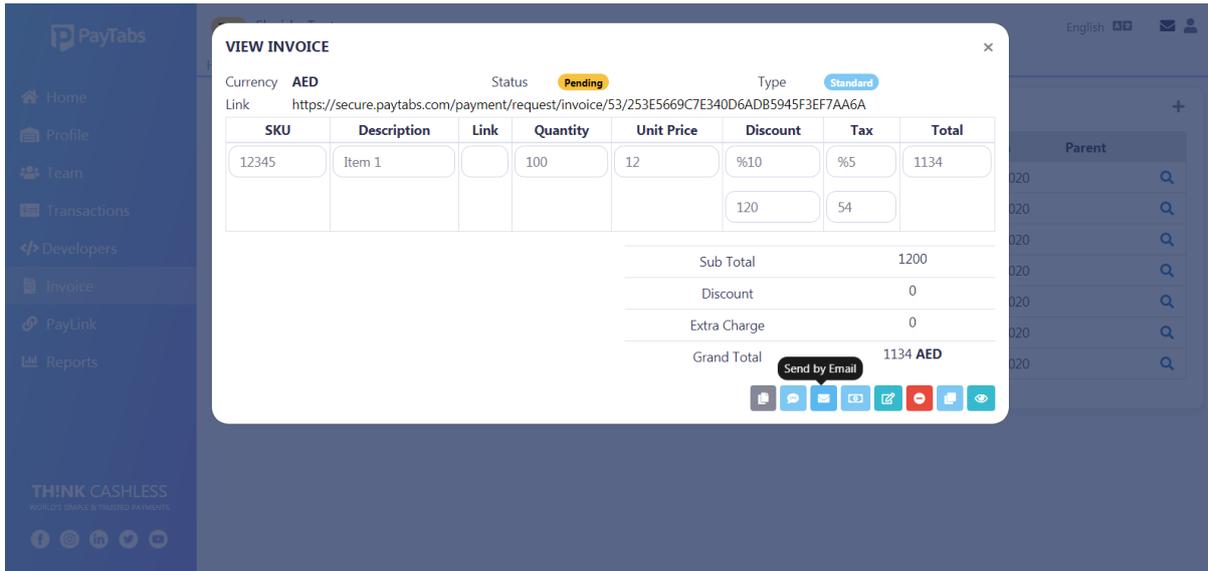
## 8.6 PayLink Creation

A basic payment interface for straightforward payment handling by providing the amount to be settled. The generated payment link is reusable - it shared or published to anyone. Can also be used as a way of directing customers to the payment page without needing any API interface.

### Create PayLink
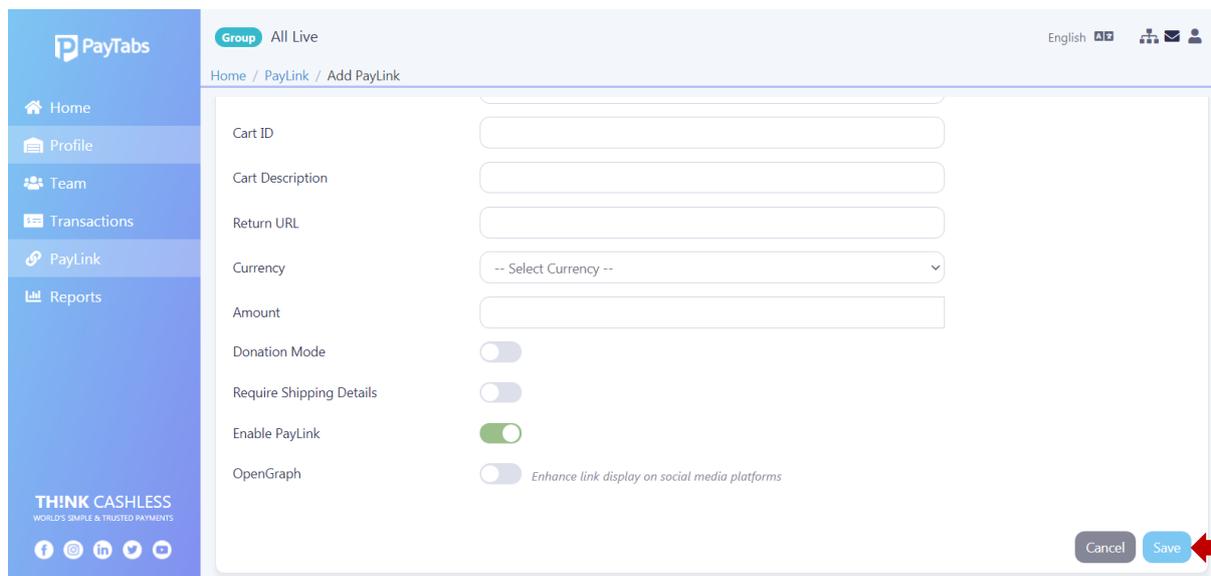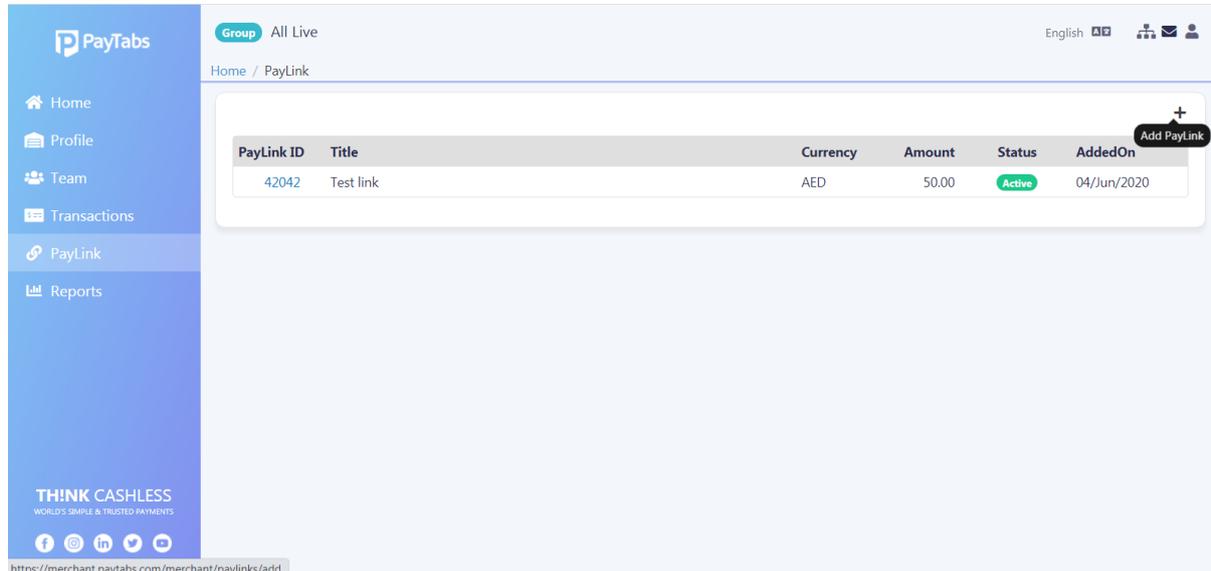


### Share PayLink - Clipboard

## Share PayLink - SMS
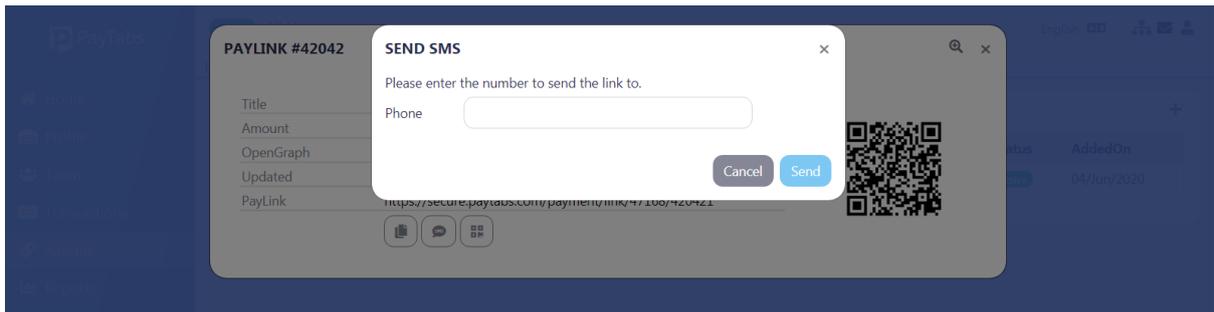


## Share PayLink – QR Code

## Donation Mode

Enter minimum and maximum amounts.

## OpenGraph Support

OpenGraph enhances how links look when shared on social media. It allows control over the title and description text used and allows a high-resolution image to be attached. Merchants can upload a specific custom image for each link. If enabled, then the link display on the dashboard includes buttons to share the link, currently this is tested and working with Facebook and Twitter. The link can still be directly shared as before, and if shared directly would still provide the enhanced view on Facebook/twitter if the link has OpenGraph enabled.
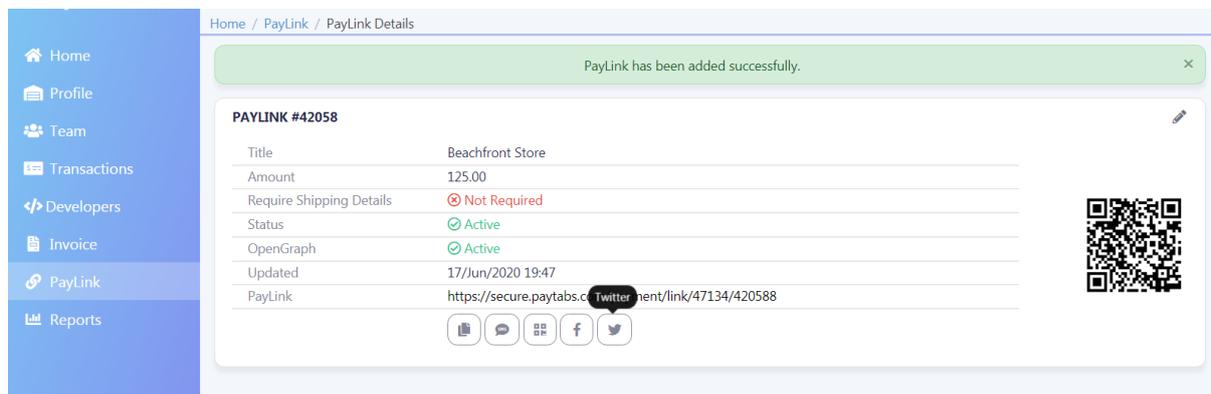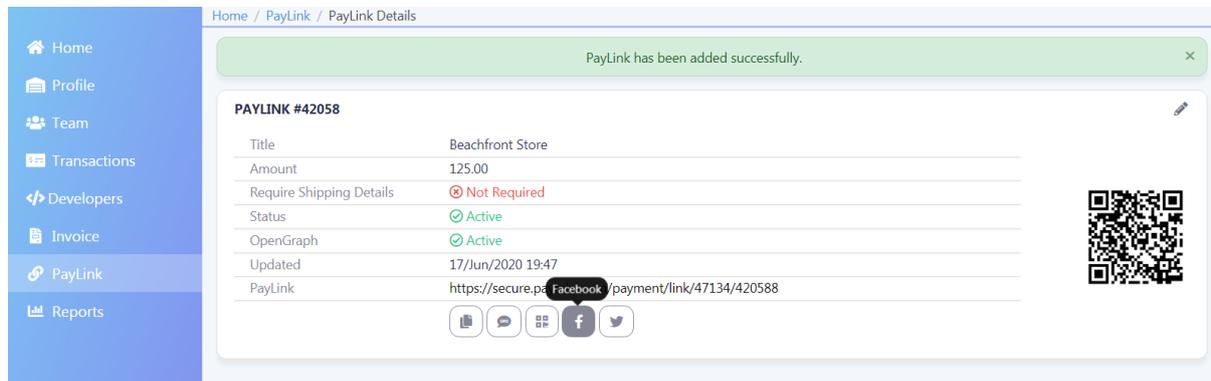




And the payment link will appear on Facebook and Twitter as follows:
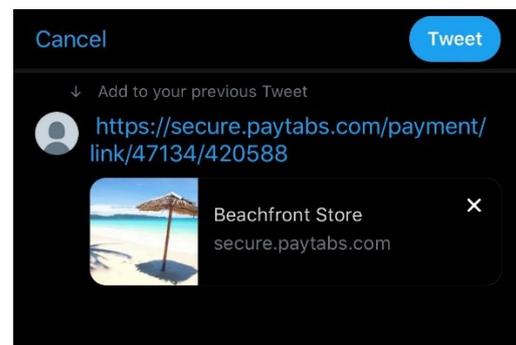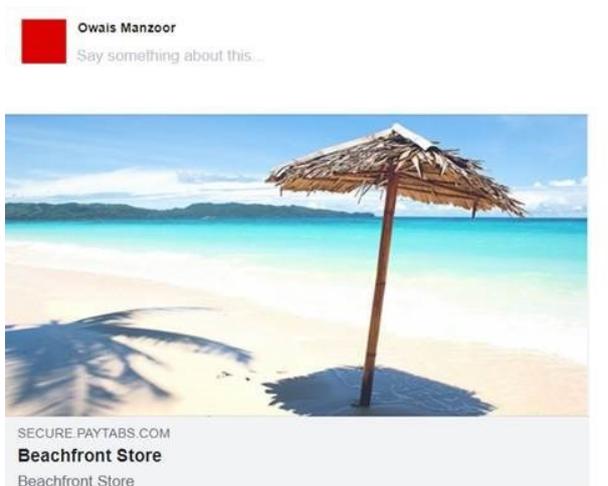
# 9. Two-Step Card Processing

**Scenario 1: Using Own Form for PCI SAQ D-merchant**

| Step 1 -<br>Take card details | 1. Merchant site displays card entry form.<br>2. Customer completes the card entry form.<br>3. Card details are sent to merchant's server. |
|---|---|
| Step 2 -<br>Make payment | 4. Using Transaction API, Server sends payment request including customer and card details to PayTabs gateway. All requests must be sent using HTTP POST to the Transaction API endpoint.<br>5. Gateway processes the request and responds with<br>    a. Final Transaction result or<br>    b. Redirection URL or<br>    c. Error message if gateway is unable to process request. |

**Scenario 2: Using Managed Form for PCI SAQ A- EP merchant**

| Step 1 -<br>Take card details | 1. Modify merchant's payment form to use PayTabs managed form for handling sensitive card data with payment token. Follow instructions.<br>2. Customer completes the card entry form.<br>3. Card details are sent to PayTabs gateway for storage and payment token creation.<br>4. PayTabs gateway creates and returns payment token.<br>5. Payment token is sent to merchant's server. |
|---|---|
| Step 2 -<br>Make payment | 6. Using Transaction API, Server sends payment request including customer details and payment token to PayTabs gateway. All requests must be sent using HTTP POST to the Transaction API endpoint.<br>7. Gateway processes the request and responds with<br>    a. Final Transaction result or<br>    b. Redirection URL or<br>    c. Error message if gateway is unable to process request. |

**Scenario 3: Using Hosted Payment Page if not PCI certified**

| Step 1 -<br>Take card details | 1. Hosted payment page provides payment form and handling of card details, including additional authentication, e.g. 3DS.<br>2. Customer completes the card entry form.<br>3. Card details are captured and processed by the hosted payment page. |
|---|---|
| Step 2 -<br>Make payment | 4. Using Transaction API, hosted payment page sends transaction request to PayTabs gateway. All requests must be sent using HTTP POST to the Transaction API endpoint.<br>5. The transaction API will return with a 'Redirection' response with URL.<br>6. Send URL to customer.<br>7. Customer completes transaction using the hosted payment page. |

# 10. Supplemental Information

## 10.1 Test Cards

**Visa Cards**

| Card number | Description |
| --- | --- |
| 4000000000000002 | 3D secure |
| 4111111111111111 | Without authentication |
| 4000000000000127 | Card enrolment option during purchase process |

**Mastercard Cards**

| Card number | Description |
| --- | --- |
| 5200000000000007 | 3D secure |
| 5200000000000114 | Without authentication |
| 5200000000000122 | Card enrolment option during purchase process |

## 10.2 Reason Code

code    status    message

0    A    Authorised

1    E    Authentication Failed

2    E    Invalid request

3    E    Invalid profile ID

4    E    Duplicate request

5    E    Request limit exceeded

100    E    Transaction cost or currency not valid

101    E    Cart ID not valid

102    E    Description not valid

103    E    Name not valid

104    E    Address not valid

105    E    Country not valid

106    E    Email not valid

107    E    Phone number not valid

108    E    IP address not valid

109    E    Invalid transaction mode

110    E    Invalid transaction type

111    E    Invalid transaction class

112    E    Method/Class/Currency combination not supported

113    E    Invalid transaction reference

114    E    Amount differs from original

115    E    Original transaction not authorised

116    E    Original transaction already voided

117    E    Original transaction mismatch

118    E    Amount greater than available balance

119    E    Original transaction can not be voided

120    E    Previous transaction is on hold

121    E    Transaction mode differs from original

122    D    Continuous authority not available on referenced transaction

200    E    Invalid card number

201    E    Invalid card expiry date

202    E    Invalid card security code (CVV)

203    E    Invalid account

204    E    Previous transaction in use

205    E    Invalid payment method

206    D    Currency mismatch

207    E    Invalid terminal

208    E    Invalid return url

209    E    Invalid merchant token

210    E    Invalid callback url

300    D    Not authorised

301    D    Card expiry date required

302    D    Card expired/Incorrect expiry date

303    D    Card is for ATM use only

304    D    Card security code (CVV) required

305   D   Card security code (CVV) mismatch
306   D   Address verification (AVS) mismatch
307   D   Card security code (CVV) and address (AVS) mismatch
308   D   Card is not enabled for e-commerce
309   D   3DSecure authentication not available for this card
310   D   3DSecure authentication rejected
311   D   Card cancelled
312   D   No/invalid account
313   D   Transaction not permitted by issuer
314   D   Not authorised
315   D   Not authorised
316   D   Insufficient funds
317   D   Blocked by acquirer
318   X   Authorisation expired
319   D   Unable to void
320   D   Unable to refund
321   C   Cancelled
322   D   Not supported by acquirer
323   D   Card limits exceeded
324   D   Terminal limits exceeded
325   D   Merchant limits exceeded
326   D   Account limits exceeded
327   D   OTP timeout
400   E   Internal system error
401   E   No response
402   E   Error connecting to service provider
500   D   Declined
501   D   Declined
502   D   Declined
503   D   Declined
600   P   Pending
601   H   On Hold