PHP Payment Gateway Integration Guide

Overview

This Integration pack will allow you to integrate with the Payzone Payment gateway, using the test or live merchant details available from Payzone (visit www.takepayments.com for more details).

Getting Started Checklist

Before you start your integration, please run through this checklist to ensure you have everything that you need. Please refer to the FAQ's at the end of this document for more information on where to locate this information.

1. Access to the Merchant Management System: **https://mms.payzoneonlinepayments.com/Default.aspx**
2. Test merchant ID / gateway account ID
3. Merchant password
4. Pre-shared key
5. Hash method

Choosing an Integration Method

There are three integration key methods that can be used to integrate into the payment system. The one that is most appropriate will depend on a number of factors. Our system doesn't make the merchant select which integration method can be used, and allows different integrations against the same Gateway Account to be in place simultaneously – there are certain situations which this will actually be necessary. Once you have reviewed the information below and decided on the most appropriate integration method for your needs, please refer to the integration specific documentation for the technical details on its implementation.

Module / Plugin

We have a library of plugins & modules for inclusion in the leading e-commerce / shopping cart platforms. These modules include the integration methods below.

Platforms supported include: WooCommerce, Magento, OpenCart, ZenCart - for a full up to date list please visit **http://www.takepayments.com/developer-support/shopping-carts**.

Difficulty: Very easy - This integration method is the easiest to implement, as the plugin / module just needs installing and setting up with your details.

Hosted Payment Form

We can provide a secure payment form which the customer is redirected to during the checkout process. They will complete the order on our system and then be redirected back to the merchant's system with the results of the transaction. Our system allows this payment form to be completely re-skinned so that it closely matches the merchant's own branding.

This method is generally used by merchants who are using a shopping cart that does not support the Direct/API integration method, merchants who cannot host secure (HTTPS) pages or merchants who would like to completely outsource the payment process of their website – usually for PCI compliance reasons. Please review the Result Delivery Methods section below for information on the different result delivery methods.

Difficulty: Easy - This integration uses the users browser as a data relay, for the payment request. There are some additional steps required to securely transmit the data to/from the payment gateway, as well as handling the response.

Direct/API Integration

Direct/API processing allows merchants to keep their customers on their site throughout the entire checkout process. This provides a much smoother checkout experience, and keeps the details of the underlying payment processor completely hidden from the customers. The API for this method exposes the full functionality of the payment system. This method requires the merchant's system to be able to serve out HTTPS pages, which will require them to have an SSL certificate.

Difficulty: Intermediate - This integration method is the simple to implement, as well as giving you the most control of the transaction process, however this method requires that port 4430 be open outbound on your server (hosting providers will be able to support)

Transparent Redirect

The Transparent Redirect method allows the merchant's system to appear to keep the customer on their own system during the checkout process, but the card details don't actually touch the merchant's system – they get posted directly across to the payment system. This approximates the appearance and experience of the Direct/API method, but it has the same compliancy requirements as the Hosted Payment Form method.

This method requires the merchant's system to be able to serve out HTTPS pages, which will require them to have an SSL certificate.

Difficulty: Hard - This integration uses the users browser as a data relay, there are some additional steps required to securely transmit the data to/from the payment gateway, as well as handling the response. These additional steps add complexity to the integration.

All of the above methods demonstrate how to post the transactional data across to the payment page in a secure manner. The transaction data MUST be protected as it is being delivered to the payment form via the customer's browser. The data is protected by the use of Hashing. Hashing is used to produce a unique "signature" for the data being passed (it is generated using not only the data being transmitted, but also secret data that is not transmitted, so the fraudster cannot recreate the hash digest with the data that is passed via their browser). The hash signature is then re-calculated on receipt of the transmitted data, and if it does not match the hash signature that was transmitted with the data, then the data has been tampered with, and the transaction will stop with an error message. The same process (in reverse) should be carried out by this site on receipt of the transaction results.

The worst kinds of customer tampering could be lowering the transaction price (say from £100.00 down to £1.00) or making a failed transaction look like an authorised one. This is called a "man-in-the- middle" attack.

Result Delivery Methods - Hosted Payment Form

For the Hosted Payment Form method, Merchant's systems need to know the result for each completed transaction. The Server Result Methods determine how the transaction results are delivered back to the merchants system. They all have their own reasons to choose/not choose them. This is a decision that the merchant must make. Below is some information to help decide which method is most suited. Once decided, there is a section in this document for each of the methods to explain the implementation and its requirements in more detail.

POST

Choosing the POST method will deliver the full results via the customer's browser as a form post back to the CallbackURL. This is usually the least difficult method to implement. The downside is, if the CallbackURL does not begin with HTTPS (notice the significance of the S), then the connection is not secure. If that is the case, most modern browsers throw a security warning to the customer explaining that sensitive information is being passed over to an insecure connection. We do not send sensitive information back, but the browsers are trying to safeguard the customer. As a result, we show the customer a dialog informing them of the reason why they are about to see a security warning and how to handle it.

The next two Server Result Methods exchange the transaction results directing with the merchants system and the payment page (removing the customer's browser from the process).

SERVER

When chosen, the results are PUSHED TO the ServerResultURL on the merchant's website BEFORE the customer is redirected back to the merchant's site. This has the advantage of getting around the modern security warning if the merchant is not using HTTPS (Secure Connection). The downside is, this is probably the hardest of the methods to implement.

SERVER_PULL

When chosen, the results are PULLED FROM the payment form by the merchant's system AFTER the customer has been redirected back to the website. This has the advantage of getting around the modern security warning if you're not using HTTPS (Secure Connection). Its downside, it is not necessarily the easiest of the methods to implement.

Frequently Asked Questions

Where do I find my Merchant ID?

Log into the MMS, under Account Admin -> Gateway Account Admin. The Merchant ID's are available in the Gateway Account: dropdown - in the format PAYZON-1234567.

Which merchant ID / gateway account should I use?

Please ensure you use the [Test Account] initially in all scenarios, once you have successfully tested the transactions you can use the [ECOM] account for your online payments.

Where do I find my merchant password?

You can reset your Merchant Password by logging into the MMS and going to Account Admin -> Gateway Account Admin. Select the relevant account in the Gateway Account: dropdown and ensure you tick 'Immediately Expire Old Password'. Click change password and your password will be updated.

Please note: Each gateway account has a separate password and will need to be reset individually.

Where do I find my pre-shared key?

Your pre-shared key is available from Account Admin ->Account Settings. You can also reset the Pre-shared key using this screen.

Where do I find the hash method?

Your hash method is available from Account Admin ->Account Settings. You can also change the hash method using this screen.

How do I enable transaction email?

Account Admin -> Account Settings, tick the 'Transaction Email Enabled' and select the email audience in the "Transaction Email Recipient" dropdown.

Please note: These emails will be delivered in addition to any emails generated by your shopping cart / e-commerce site.

I am getting a Hash Digest error?

The Hash Digest error means that the information that was received by the payment gateway, is not the expected information. Please check the below information have been entered correctly and match the information it the payment gateway in the first instance. If the below are correctly please check server / site logs for information on the error and reach out to **online@payzone.co.uk** and advise the error you are receiving and any relevant logs.

- Merchant ID
- Merchant password
- Pre-shared key
- Hash method

I am getting a variable input error?

The variables error means that the information that was received by the payment gateway, is not the expected information. Please check the below information have been entered correctly and match the information it the payment gateway in the first instance. If the below are correctly please check server / site logs for information on the error and reach out to **online@payzone.co.uk** and advise the error you are receiving and any relevant logs.

- Merchant ID
- Merchant password
- Pre-shared key
- Hash method

What do the response status codes mean?

The Payzone gateway sends a numeric status code back for all transactions, each number defines a different outcome for the transactions

- 0 - Payment successful
- 3 - 3D secure authentication requested
- 4 - Payment referred
- 5 - Payment rejected
- 20 - Duplicate Transaction identified
- 30 - Unknown error occurred

Why is the page is timing out? / Why am I getting a Could not communicate with payment gateway error?

If you are using Direct API method then please check the below information is correct, if you are using Direct or Transparent please reach out to **online@payzone.co.uk** and advise the error you are receiving and any relevant logs.

- Outbound port 4430 is open for communication
- Merchant ID
- Merchant password
- Pre-shared key
- Hash method
- Ensure no special characters are being passed unescaped in the form

I am getting a TransactionDateTime expired error?

This usually occurs when the payment has been started but left idle for a long time, if this is happening for all orders then check the server time has the correct time zone offset configured.

After completing the payment, I get a yellow warning message?

This message is just to advise users that they are going from a secure site (Payzone) to an insecure site (no SSL etc), to remove this error please install and enable HTTPS.

When sending the payment, I get a “merchant doesn't exist” error?

Check the Merchant ID has been entered correctly.

When sending the payment, I get a “form was not skinned” error?

Check the Merchant ID has been entered correctly.

When sending the payment, I get a “invalid merchant details” error?

Check the below information has been entered correctly.

- Merchant ID
- Merchant password
- Pre-shared key
- Hash method

When sending the payment, I get a “required variable: ##### is missing” error?

This error will display if some of the expected information is not received, please double check the form that submits to the payment gateway for the variable that is mentioned in the error.

In the MMS, a transaction is showing as “issuer authentication expired”?

This message appears 2 hours after the transaction was started, if the transaction has not been completed. Such as when the customer closes the 3D secure authentication page.

I have a question that isn’t in these FAQs?

Please reach out to **online@payzone.co.uk**, detailing the question and attaching any supporting information.