



Paymentsite

Paymentsite Hosted Payments User's Guide

Last updated: June 7, 2018
Document version 2.2.5.0

INTRIX
Technology, Inc

Paymentsite Hosted Payments is created, owned, hosted, and managed by Intrix Technology, Inc

*The information contained within this document may not be reproduced without permission from an Intrix Technology officer.
All material is confidential and may only be used for the purpose for which it is disclosed.*

© 2018 Intrix Technology, Inc

Paymentsite Hosted Payments User’s Manual

Table of Contents

- 1 Introduction to Paymentsite Hosted Payments..... 2
 - 1.1 Ease of Use:..... 2
 - 1.2 Security: 2
 - 1.3 Other Features: 2
- 2 Payment Flow – Payment Page Redirect 4
- 3 Payment Flow – Payment Page In A Frame 5
- 4 Using Hosted Payments for Retail Transactions 5
- 5 Transaction Types 6
- 6 Formatting the HPP Page 6
 - 6.1 Style Sheet Control..... 7
 - 6.1.1 Using a Pre-Built Style Sheet 7
 - 6.1.2 Developing a Custom Style Sheet 7
 - 6.2 Mobile Device Optimization 9
- 7 Submitting Transactions for Processing..... 9
- 8 Sample Code 9
 - 8.1 Sample HTML 9
 - 8.2 Sample MD5 hash code 11
- 9 Setting up Hosted Payments..... 12
- 10 Input Field Definitions..... 16
- 11 Receipt Options..... 21
- 12 Response Fields..... 21
- 13 Integrating and Testing a Merchant Implementation 23
- 14 Fraud Protection: AVS and Card Code 24

Paymentsite Hosted Payments User's Manual

1 Introduction to Paymentsite Hosted Payments

Paymentsite Hosted Payments from Intrix Technology is a hosted payment processing solution that allows merchants to collect payments from a web page without concerns about Payment Card Industry (PCI) security standards for collecting and storing sensitive customer information. Because the payments are processed on pages hosted by the Intrix Technology Level 1 PCI- certified secure payment gateway, merchant PCI requirements are greatly simplified. The solution is easily added to any web site with a simple HTML form. Some of the benefits of this solution are:

1.1 Ease of Use:

- HTML form post provides the easiest method to integrate with the Gateway
- To accept credit card and/or checks on a web page, all the merchant needs to do is get a gateway account and put a few lines of HTML code on their web page
- Settled funds are deposited directly into the merchant's bank account
 - Funds from all transaction types are generally available the next business day

1.2 Security:

- Data transmission happens using secure sockets layer (SSL) protocols to ensure confidential communications
- The Gateway submits a response to the merchant's web site to avoid data tampering attacks.
- Merchants should further secure transactions by sending an MD5 hash to the gateway before sending the customer to the hosted payments page
 - The amount and other transaction data sent in the MD5 hash must match the data in the transaction (see MD5 section for details)
 - This protects the transaction from being intercepted and tampered with
- Merchants do not have to collect, transmit or store sensitive cardholder information to process transactions
 - There is no need for merchants to purchase and install a Secure Sockets Layer (SSL) digital certificate
 - This eliminates the complexity of securely handling and storing sensitive information, greatly simplifying compliance with the Payment Card Industry (PCI) Data Security Standard

1.3 Other Features:

- Full featured payment processing enables credit card authorizations, sales, and captures as well as electronic check payments
 - Since the Hosted Payments solution is intended for card-not-present transactions, returns, credits, and voids are not allowed through the posted interface, but are supported by logging into the Paymentsite merchant portal
- Fraud protection measures (AVS, Card security code) are included
- Payment forms and receipts are customizable to match the merchant's web site
- Transactions flow options are as follows:

Paymentsite Hosted Payments User's Manual

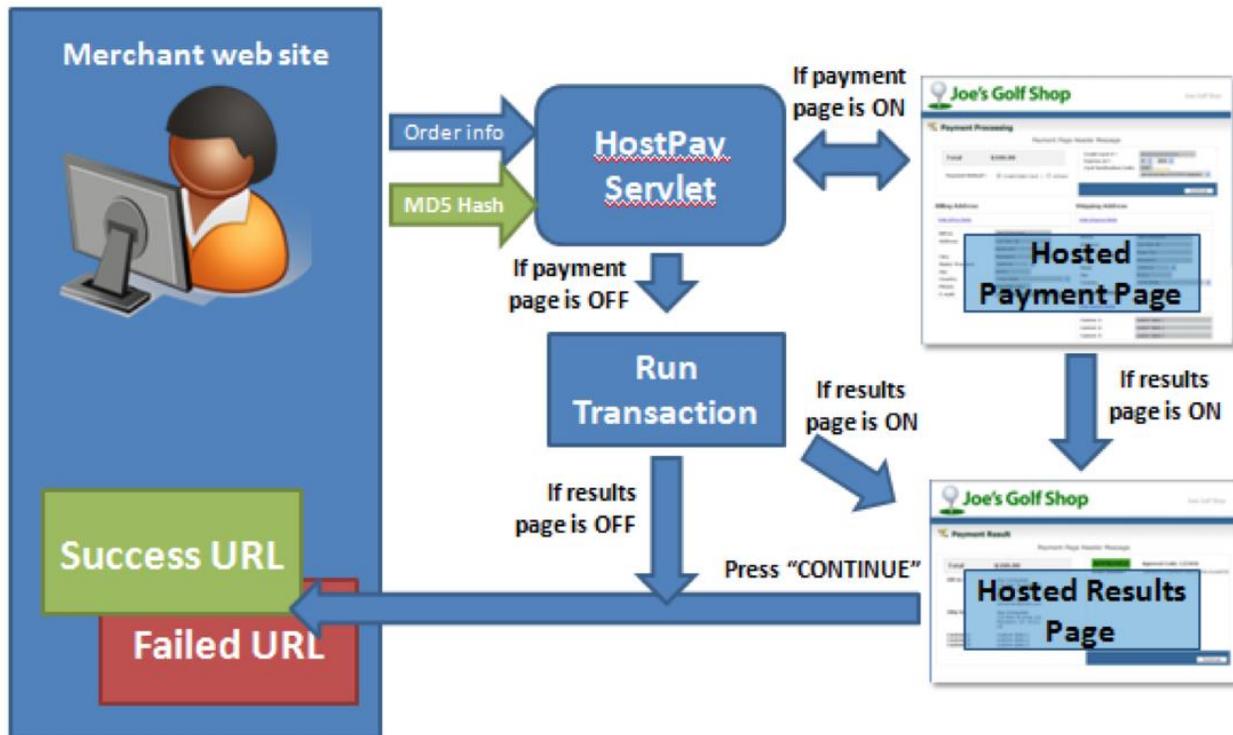
- Option 1 – HPP Redirect
 - From the Merchant's webpage
 - To a hosted payments page
 - To a hosted receipt page
 - Then back to the Merchant's website
- Option 2 – HPP in a frame
 - From the merchants website or application
 - Still at the merchants website or application, but with the HPP in a frame embedded on the page or in the screen
 - Still at the merchants website or application, but with the transaction results having been received from the HPP result
- Account on file allows the customer to save their card or checking account information so they don't need to re-enter each time they shop with a particular merchant
 - Repeat shoppers enjoy greater security since their sensitive information is not being transmitted each time they make a purchase
- The Paymentsite merchant portal, a full-featured, intuitive Virtual Terminal and Back Office portal is included:
 - The Virtual Terminal allows for processing in-person (and other) transactions, scheduling of recurring payments, and performing returns and credits
 - The Back office provides:
 - Customer information upload
 - Comprehensive, real-time downloadable transaction reports
 - Unlimited users with user access management
 - Full suite of real-time transaction reporting

Paymentsite Hosted Payments User's Manual

2 Payment Flow – Payment Page Redirect

With the payment page redirect, the consumer leaves your web site and arrives at the branded payment page at Paymentsite to provide their payment method details directly into the PCI compliant Paymentsite system.

There are several options the merchant may use with Hosted Payments. They can choose to turn the payments page on or off and the results page on or off. They should protect their orders from being intercepted by sending a MD5 Hash separately from the order.



If you turn the payments page off, you must post all the payment data with the transaction. It is important to note that if you choose this option, you are taking on additional PCI compliance burden since you will be collecting and storing payment data on your own web servers.

If you turn the payments page on, the customer's payment data will be collected directly on the gateway. Your PCI compliance responsibility in this case reduces greatly.

Merchants may also customize the hosted payments and results pages with their own logo.

Paymentsite Hosted Payments User's Manual

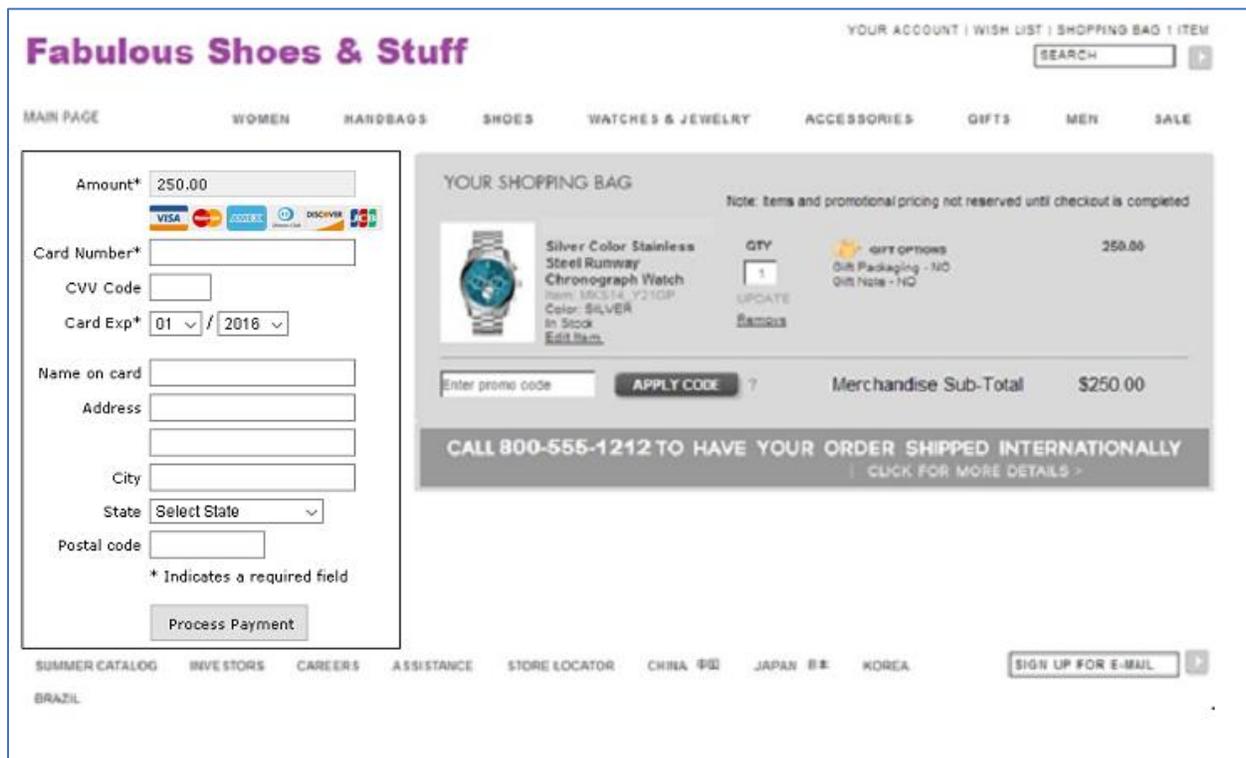
3 Payment Flow – Payment Page In A Frame

With the frame based payment page, the consumer stays on your web site or in your application, and inside a frame on your page, you display the frame based Paymentsite page in order for the consumer to provide their payment method details directly into the PCI compliant Paymentsite system. This approach also works for non-consumer facing environments where staff may be accepting payments.

With this model, transaction results are fed back to a location defined by the merchant, and the entire customer interaction is controlled, the customer never leaves your site.

The flow of data is essentially the same as with the redirect, but the customer experience is very different.

The style and format of the payment page and its frame are controlled through a style sheet (css). The format can be made to match your website exactly. For more information, see “hp_css”.



4 Using Hosted Payments for Retail Transactions

Paymentsite Hosted Payments is also configurable to work for retail transactions. Merchants/developers who wish to create a retail system can perform retail swiped transactions using Hosted Payments using one of two methods:

Paymentsite Hosted Payments User's Manual

1. The merchant can pass the track data from the card reader to the Paymentsite Gateway in the hp_trackdata field.
2. The hosted payment form on the Paymentsite Gateway can be configured to accept credit card track data. This is the simpler method, and reduces PCI compliance burden on the merchant, since the credit card data is collected on the gateway, not the merchant's system.

5 Transaction Types

The Paymentsite hosted Payments Solution allows for the following transaction types:

Authorization: If the merchant needs to make a credit or debit card sale, but won't be able to ship merchandise for several days; the merchant should use an authorization. An authorization transaction ensures the availability of fund and places a hold on those funds with the customer's bank, but does not transfer funds until a post-authorization or capture transaction is sent from the merchant. Once the goods are shipped, the merchant can capture the transaction to obtain the funds. This type of transaction is not sent for settlement until you submit a credit card post- authorization, or if the merchant marks the funds as shipped in the Back Office reports.

Post-authorization: (a.k.a., post-auth or Capture) A post-authorization transaction sets a previous authorization transaction to capture the funds once the goods are shipped to the customer. The funds are then sent for settlement with the next batch. Merchants can perform a post-authorization transaction through the Hosted Payments interface—or they can use the Back Office to perform this function.

Sale: a credit or debit card Sale transaction is automatically submitted to the processor for both authorization and capture. If approved, the transaction will settle with the next batch settlement and funds will automatically be deposited in the merchant's bank account usually the next business day.

An electronic check sale transaction submits the information to the automated clearing house (ACH) network for funding.

Other transaction types such as returns, credits, and voids are supported but the merchant must log into the merchant back office and virtual terminal in order to perform these functions.

6 Formatting the HPP Page

There are several aspects of the hosted payment page's format that can be customized and controlled within the http post. These include:

- Page style/theme
- Mobile device optimization

Paymentsite Hosted Payments User's Manual

6.1 Style Sheet Control

The appearance of the HPP is controlled, to some extent, by the Cascading Style Sheet used. Intrix hosts several style sheets that can be referenced, or the solution can use a CSS file that is available on your website (it must be hosted at a URL that is publicly accessible). That URL is then passed in in the HPP request, and the Paymentsite HPP will use your style sheet when displaying the form.

6.1.1 Using a Pre-Built Style Sheet

To use one of the existing style sheets, simply include URL of that style sheet in the HPP request, using the tag `hp_css`.

The URLs for Integration (while you are developing your solution) are below. Once your code is promoted to Production, references should be changed to the Paymentsite Production URLs instead.

<https://apiint.paymentsite.com/hostpay/docs/css/HostedStyle0.css>

Default CSS, a simple black and white style. If nothing is passed in for the CSS, then this style sheet will be used. If a custom style sheet is passed in the request but is missing some data elements, the values in HostedStyle0 will be used.

<https://apiint.paymentsite.com/hostpay/docs/css/HostedStyle1.css>

CSS with gray background, may be suited to use in an application (as opposed to a website).

<https://apiint.paymentsite.com/hostpay/docs/css/HostedStyle2.css>

CSS with a green theme

<https://apiint.paymentsite.com/hostpay/docs/css/HostedStyle3.css>

CSS with a blue theme

<https://apiint.paymentsite.com/hostpay/docs/css/HostedStyle4.css>

CSS with a maroon theme

6.1.2 Developing a Custom Style Sheet

Elements of the style sheet can be customized in a variety of ways. The following elements can be defined and customized in your instance of a css:

Name	Can Be Customized	Purpose	Items To Change
body	yes	defines the body of text, including the page background	font-size font-family color background <i>Note: several of these can dramatically change the format/size of the HPP</i>
.bold	No	Used to bold an element	
.submitButton	Yes	submit button style	text-align

Paymentsite Hosted Payments User's Manual

			font-size font-family color border-radius background-color
input.textEntryName	Yes	style for text entry fields	font-size font-family color
select.textEntryName	Yes	style for drop-down fields (excluding expiration dates)	font-size font-family color
select.textEntryCardExp	Yes	Style for drop-down fields for expiration dates	font-size font-family color
.label	Yes	Field label style	font-size font-family color
.required_field	Yes	style for fields that are required to be completed	background-color
select.error	Yes	style for an error with a drop-down field	border font-family font-style font-weight <i>usually the same as textarea.error & input.error</i>
textarea.error	Yes	Style for an error in a text entry field	border font-family font-style font-weight <i>usually the same as select.error & input.error</i>
input.error	Yes	Style for an error with input data	border font-family font-style font-weight <i>usually the same as select.error & textarea.error</i>

Paymentsite Hosted Payments User's Manual

6.2 Mobile Device Optimization

The HPP can be optimized to work better on mobile devices. If you have detected you are displaying your website on a mobile device, include the mobile attribute in the post:

```
<input type="hidden" name="hp_mobile" value="1"/>
```

Instead of the default

```
<input type="hidden" name="hp_mobile" value="0"/>
```

7 Submitting Transactions for Processing

To submit a transaction to the Paymentsite Hosted Payments solution for processing, the merchant embeds HTML code into a web form and submits it to the Gateway. The customer filling out the form is then automatically transferred to the secure payment form on the Paymentsite payment gateway. An additional step of sending an MD5 Hash with the transaction amount and item ID number to the gateway is recommended to ensure transactions are not intercepted or spoofed in transit. If the MD5 hash is sent, the gateway will check the information in the hash against the information sent from the customer order page to ensure the information matches. Using the MD5 Hash method protects the merchant from potential interception and mis-posting of an order with an artificially lowered price.

8 Sample Code

8.1 Sample HTML

Below is some sample HTML form code that shows the fields that might be submitted for a credit card sale. The merchant can choose which fields they wish to collect themselves and which they want the Paymentsite Hosted Payments page to collect. If the merchant wishes to avoid the hassles associated with PCI standards, they should NOT collect any card or bank account information on their own servers.

Platform	Posting URL
PaymentSite	https://api.paymentsite.com/hostpay/HostPay

```
<html>
<head>
<title>Merchant Webform</title>
</head>
<body>
<h1>Merchant XYZ</h1>
<p>Customer Checkout</p>
<form method="post" action="https://<Hosted Payments Url>">
<input name="hp_merchant_id" type="hidden" value="123456" />
<input name="hp_txntype" type="hidden" value="sale" />
<input name="hp_amount" type="hidden" value="100.00" />
<input name="hp_method" type="hidden" value="ccard" />
<input name="hp_cardnum" type="hidden" value="4111111111111111" />
<input name="hp_expmonth" type="hidden" value="12" />
```

Paymentsite Hosted Payments User's Manual

```
<input name="hp_expyear" type="hidden" value="2011" />
<input name="hp_bname" type="hidden" value="Joe Consumer" />
<input name="hp_baddr" type="hidden" value="123 Main St." />
<input name="hp_bcity" type="hidden" value="Moorpark" />
<input name="hp_bstate" type="hidden" value="CA" />
<input name="hp_bcountry" type="hidden" value="US" />
<input name="submit" type="submit" />
</form>
</body>
</html>
```

Sample HTML code for Hosted Payments Page in a frame:

Below is sample code for the frame based version of the HPP:

```
<html>
<head>
<title>Merchant Frame Version</title>
</head>
<body>
<h1>Merchant XYZ</h1>
<p>Customer Checkout</p>
<form action="https://<Hosted Payments Url>" method="post" target="hp_iframe"
name="form_iframe">
<input type="hidden" name="hp_merchant_id" value="12345"/>
<input type="hidden" name="hp_amount" value="12.00"/>

<input type="hidden" name="hp_cmd" value="process"/> <!-- process or savepayment -->
<input type="hidden" name="hp_method" value="ccard"/> <!-- ccard or echeck -->
<input type="hidden" name="hp_txnatype" value="sale"/> <!-- sale or auth or postauth -->
<input type="hidden" name="hp_layout" value="frame"/> <!-- frame -->
<input type="hidden" name="hp_frameborder" value="1"/> <!-- 1 or 0 -->

<!-- save payment flags when hp_cmd is process -->
<input type="hidden" name="hp_save_payment" value="0"/> <!-- 1:save or 0:not save, if it is 1
hp_save_customer or hp_customer_token is required-->
<input type="hidden" name="hp_save_customer" value="0"/> <!-- 1:save or 0:not save -->

<!-- save payment with existing customer -->
<input type="hidden" name="hp_customer_token" value=""/>

</form>
```

Paymentsite Hosted Payments User's Manual

```
<iframe name="hp_iframe" id="hp_iframe" width="300px" height="470px" scrolling="auto"
frameborder="0" allowTransparency="true"></iframe>
<script type="text/javascript">
document.form_iframe.submit();
</script></form>
</body>
</html>
```

8.2 Sample MD5 hash code

When the merchant signs up for the Hosted Payments service, they will be giving a unique key. The merchant should save the key in a secure location, inaccessible to hackers. The merchant can then use this key to create MD5 hash signatures that they submit with each transaction. Since both the merchant and Paymentsite Hosted Payments are using the same key to create MD5 hash signatures, it is easy to verify that the signature does indeed belong to the intended merchant. This prevents others from tampering with the transaction.

NOTE: During the integration coding phase, it is easier to complete the process without using the MD5 encryption. Once the basic coding is done, MD5 encryption should be turned on. Production traffic should not be processed without using the encryption, due to the security risks of transmitting data that can be intercepted and modified.

An MD5 hash can be generated on a web server using any common web programming language. The sample below is written in JSP, but PERL, PHP, or other web languages can also be used to generate the Hash. Once the hash is generated, it should be posted to the gateway separately from the order. The MD5 Hash should contain the order amount, item ID number, and timestamp.

Following is a PHP method for generating an MD5 hash:

```
<?php echo hash_hmac('md5', 'value of the time stamp*random 4
digits*amount*item id', 'the secret key'); ?>
```

And a Java method:

```
<%@ page import="sun.misc.*" %>[SEP]<%@ page import="java.util.*" %>[SEP]<%@
page import="java.security.*" %>[SEP]<%@ page import="javax.crypto.*"
%>[SEP]<%@ page import="javax.crypto.spec.SecretKeySpec" %> <%@ page
import="java.text.SimpleDateFormat" %>

<%

private String md5Hash(String sKey, long ts, String sRand, String
sAmount, String sItemid) throws Exception

{[SEP]SecretKey secretKey = new SecretKeySpec(sKey.getBytes(), "HmacMD5");
```

Paymentsite Hosted Payments User's Manual

```
Mac mac = Mac.getInstance("HmacMD5"); mac.init(secretKey); String
concat = ts + "*" + sRand + "*" + sAmount + "*" + sItemid; byte[]
result = mac.doFinal(concat.getBytes());

StringBuffer buf = new StringBuffer(result.length * 2); for(int i=0;
i< result.length; i++)

if(((int) result[i] & 0xff) < 0x10)

buf.append("0"); buf.append(Long.toString(((int) result[i] & 0xff,
16));

return buf.toString();
```

9 Setting up Hosted Payments

When the merchant signs up for a Hosted Payments account, they will receive a secure login for the Paymentsite merchant center, which contains a virtual terminal they can use for processing payments and their transaction reports.

To set up their hosted payments account, merchants must contact support who will provide them a form they fill out to configure the fields and settings for their hosted payment pages.

Merchants can opt to show or hide fields on their payment and receipt pages, so they have complete control over which information they collect themselves and which they wish the hosted pages to collect.

Additionally, merchants can configure the following settings by contacting support. These settings must be provided before the merchant can begin using Paymentsite Hosted Payments.

Setting	Function
Success URL	Customers will be redirected to this URL if the transaction is approved and if the 3-way redirect method is in use. The results of the transaction will be posted to this URL unless it is an html page. If the frame method is in use, the you control what the user sees when the transaction is complete.
Fail URL	Your customers will be redirected to this URL if the transaction fails to process successfully and if the 3-way redirect method is in use. The results of the transaction will also be posted to this URL unless it is an html page. If the frame method is in use, the you control what the user sees when the transaction is complete.
Submitted From	The domain where the request originated. This information is used to validate if the request came from the correct merchant's web site.

Paymentsite Hosted Payments User's Manual

Setting	Function
Success URL is Post	Indicates if the success URL can accept posted fields or not
Fail URL is Post	Indicates if the failure URL can accept posted fields or not
Show Billing Fields	Indicates whether billing fields will be displayed on the Paymentsite hosted page
Show Shipping Fields	Indicates whether shipping fields should be displayed on the Paymentsite hosted page
Show Card Number Fields	Indicates whether to show the card number and expiration date fields on the Paymentsite-hosted payments page
Show Check Fields	Indicates whether to show the card number and expiration date fields on the Paymentsite-hosted payments page
Show Result Page	Indicates whether the Paymentsite-hosted transaction results page will be displayed to the customer
Top Logo URL	The top logo that appears on the hosted payment page
Top Bar Color	The color of the bar at the top of the hosted payment page
Continue Bar Color	The color of the 'continue' bar on the hosted payment page
Header Message	The text that appears at the top of the hosted payment page
Signature Life (Minutes)	How long a signature remains active. This value controls the life in minutes of the signature if it is posted ahead of the transaction. A transaction must be processed within this threshold.
Custom field labels & visibility settings	You can have up to 5 custom fields that you can post to the hosted payments server and use as you please. Specify the labels for each custom field and whether or not you want them to appear.
MD5 Hash Key	Intrix provided key unique for each merchant which is used to create hash values in the request and response
Use Signature Flag	If set, the system will use an MD5 hash to authenticate the transaction. The signature must be posted using the <i>hp_signature</i> tag along with the <i>hp_cmd=process</i> command, or ahead of time using the <i>hp_cmd=signature</i> command. Even if this flag is not set, the merchant can always post the signature with the transaction using the

Paymentsite Hosted Payments User's Manual

Setting	Function
	<i>hp_signature</i> tag, and the system will authenticate the transaction against the posted value.

A sample hosted payment page showing the location of the Top logo URL, the Header Message, the Top Bar color and the 'Continue' Bar color is included below.

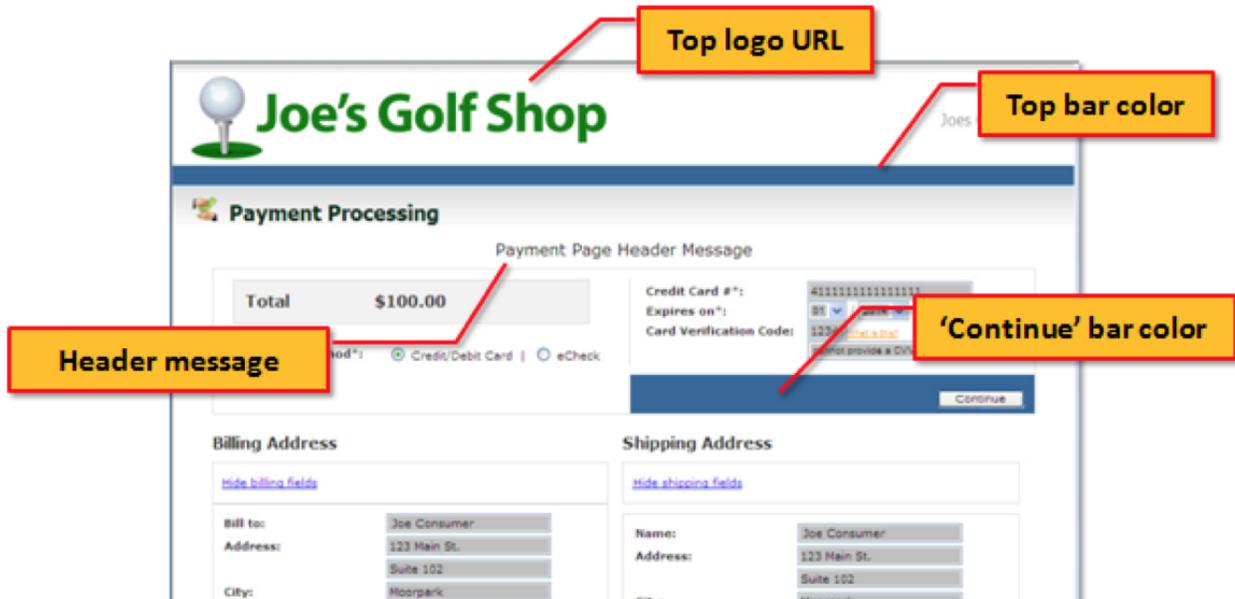


Figure 1 HPP Redirect web page

Paymentsite Hosted Payments User's Manual

Samples of the frame-based payment pages are located below.

INTRIX

Host Payment Demo page.

[Back](#)

Amount* 12.00

Card Number*

CVV Code

Card Exp* 01 / 2016

Name on card

Address

City

State

Postal code

* Indicates a required field

Figure 2 HPP Frame Accept Payment with visible border

INTRIX

Host Payment Demo page.

[Back](#)

Card Number*

CVV Code

Card Exp* 01 / 2016

Name on card*

Address*

City*

State*

Postal code*

* Indicates a required field

Figure 3 HPP Frame Save Card On File with no border

Paymentsite Hosted Payments User's Manual

10 Input Field Definitions

The fields the merchant may pass to the Paymentsite Hosted Payments Solution are shown in the table below.

Field name	Possible Values / Description	Required?
hp_cmd	Set to "process" to process a transaction, or "signature" if you are sending a signature, or to "savepayment" to create a card on file. The default value is "process".	Optional
hp_merchant_id	merchant account id	Required
hp_layout	Indicates if the page will be presented with a redirect of the consumer or if the payment page will be displayed embedded in a frame on a page. Leave empty to use Redirect or set to "frame" for a frame based presentation.	Optional
hp_frameborder	When hp_layout is set to "frame", this value determines if a border is drawn around the frame. Setting to "1" results in a border around the payment page, set to "0" or leave empty to set no border.	Conditionally required
hp_css	To control the style payment page, reference the URL where your CSS resides or use one of the pre-built CSSs. If this field is not included, default frame would be displayed.	Optional
hp_mobile	0 or 1. If set to 1, fields will be formatted for better display on a mobile device. If set to 0 or not provided, formatting will be set to default web browser format.	Optional

Paymentsite Hosted Payments User's Manual

Field name	Possible Values / Description	Required?
hp_signature	MD5 hash signature for a transaction request, can be posted with the process request, or before the process request with hp_cmd=signature. A secret key is used to create an MD5 hash for the following fields concatenated together and asterisk separated, hp_sig_timestamp, hp_sig_id, hp_amount, hp_sig_itemid. 1231231234*1234*100.00*sku-hat-111	Optional
hp_sig_timestamp	timestamp in GMT, seconds from Jan 1, 1970, required if merchant is configured to use signature authentication	Conditionally Required
hp_sig_id	a 4 digit random number, required if merchant is configured to use signature authentication	Conditionally Required
hp_sig_itemid	the item id for the item being purchased by the customer, required if merchant is configured to use signature authentication	Conditionally Required
hp_txntype	sale, auth, postauth	Configurable*
hp_amount	amount of transaction, sum of all elements of transaction including tax, shipping and fees if applicable	Required
hp_convenience_fee	convenience fee charged to consumer, included in Amount, if passed in, will display on page	Optional
hp_shipping_amount	Shipping charged to consumer, included in Amount, will display on page	Optional
hp_tax_amount	Tax amount charged to consumer, included in Amount, will display on page	Optional
hp_method	ccard or echeck	Configurable*
hp_eciind	ECI Indicator or transaction origin. retail, moto, eci	Configurable*
hp_trackdata	a field for passing credit card track data if Hosted Payments is being used for retail swipe. This field can be used to pass track1, track2 or both	Configurable*

Paymentsite Hosted Payments User's Manual

Field name	Possible Values / Description	Required?
hp_cardnum	credit or debit card number	Configurable*
hp_expmont	2 digit card expiration month	Configurable*
hp_expyear	4 digit card expiration year	Configurable*
hp_cvv	3 or 4 digit card code printed on the card which is used for security measures to verify whether the customer has the card in their possession	Configurable*
hp_cvvind	If a CVV code is not able to be provided for a transaction, this field is available to identify why it is not provided. Possible values are: illegible, no_imprint, not_provided	Configurable*
hp_routingnumber	routing number, req for hp_method=echeck	Configurable*
hp_accountnumber	account number, req for hp_method=echeck	Configurable*
Hp_bname	cardholder billing name	Configurable*
hp_baddr	billing address	Configurable*
hp_baddr2	billing address 2	Configurable*
hp_bcity	billing city	Configurable*
hp_bstate	billing state, 2 characters	Configurable*
hp_bzip	billing zip	Configurable*
hp_bcountry	billing country	Configurable*
hp_phone	billing phone number	Configurable*
hp_email	billing email address	Configurable*
hp_sname	shipping name	Configurable*
hp_saddr	shipping address	Configurable*
hp_saddr2	shipping address 2	Configurable*

Paymentsite Hosted Payments User's Manual

Field name	Possible Values / Description	Required?
hp_scity	shipping city	Configurable*
hp_sstate	shipping state, 2 characters	Configurable*
hp_szip	shipping zip	Configurable*
hp_scountry	shipping country code, 2 characters	Configurable*
hp_refnum	merchant defined transaction identifier used to reverse a transaction if no response is received	Configurable*
hp_orderid	order id associated with this transaction, optional but the system will create a value if not passed by the merchant	Configurable*
hp_c_firstname	customer first name	Optional
hp_c_middlename	customer middle name	Optional
hp_c_customerid	ID assigned to customer by merchant	Conditionally Required
hp_c_lastname	customer last name	Optional
hp_c_addr1	Customer address, line 1	Optional
hp_c_addr2	Customer address, line 2	Optional
hp_c_city	customer city	Optional
hp_c_state	customer state	Optional
hp_c_zip	Customer zip code	Optional
hp_c_country	Customer country	Optional
hp_c_phone	Customer phone number	Optional
hp_c_email	Customer email	Optional

Paymentsite Hosted Payments User's Manual

Field name	Possible Values / Description	Required?
hp_savepayment or hp_save_payment	if set to 1, the payment information (hp_cardnum, hp_expmmonth, hp_expyear, and billing fields) will be saved, and a token (hp_payment_token) will be returned and can be used in follow up requests to identify payment information instead of passing the actual card number and expiration date.	Optional
hp_payment_token	a unique identifier for payment information that Hosted Payments returned from a previous request to save the payment information. This token can be passed with a request instead of the payment and billing fields.	Optional
hp_save_customer	if set to 1, a new customer will be saved to our system. A token hp_customer_token will be returned in the response and can be used in follow up requests to identify a customer. If this field is set to 1, then hp_c_customerid is mandatory. Can be used with hp_savepayment to save both the payment and customer information and associate the 2 with each other.	Optional
hp_customer_token	a unique identifier for a customer that Hosted Payments returns from a request to save the customer.	Optional
hp_cf_1	Custom field for the merchant's use—will be passed back to the merchant in the response	Configurable*
hp_cf_2	Custom field for the merchant's use—will be passed back to the merchant in the response	Configurable*
hp_cf_3	Custom field for the merchant's use—will be passed back to the merchant in the response	Configurable*
hp_cf_4	Custom field for the merchant's use—will be passed back to the merchant in the response	Configurable*

Paymentsite Hosted Payments User's Manual

Field name	Possible Values / Description	Required?
hp_cf_5	Custom field for the merchant's use—will be passed back to the merchant in the response	Configurable*

* Fields shown here as configurable are the fields that the merchant may decide to show or hide on the hosted pages. Some are required for a transaction to process, but are sensitive customer information protected by PCI standards, so if the merchant wishes to reduce PCI compliance hassles, we recommend the merchant chooses to show all sensitive required fields such as card number, account number, and CVV on the secure Paymentsite hosted pages versus collecting those fields on their own web server.

11 Receipt Options

Merchants may choose to use the Hosted Payment receipt pages or generate their own receipt pages using the response information passed back to the merchant web server after a transaction is processed.

To use the Paymentsite hosted payment receipt page, the merchant must set the Show Result Page setting to "Yes". If the merchant wishes to generate their own receipt page, they would set the Show Result Page to "No". These settings are updated by contacting support.

The merchant may host two separate results pages on their web server: one for approved transactions and one for failed (or declined) transactions. The merchant must identify both these URLs in the settings by contacting support. Whether or not the merchant chooses to use the Paymentsite hosted response pages, the merchant can still provide these two separate URLs for returning payees to their web site.

12 Response Fields

If the merchant indicates that their success and fail URLs can accept posted results, the Paymentsite hosted Payments solution will post back several fields to the merchant web server:

Field name	Description
hp_time	date and time of the transaction
hp_responsecode	response code, will be 0 if approved
hp_responsemsg	response message, APPROVED, DECLINED, or a relevant error message
hp_refnum	reference number passed in the request by the merchant

Paymentsite Hosted Payments User's Manual

Field name	Description
hp_transid	Hosted Payments system-defined transaction id
hp_avsresponse	avs response code
hp_cvvresponse	cvv response code
hp_authcode	process assigned authorization code
hp_orderid	either the system defined order id, or merchant assigned order id
hp_amount	transaction amount
hp_convenience_fee	convenience fee charged to consumer, included in Amount, if passed in, will display on page Optional
hp_shipping_amount	Shipping charged to consumer, included in Amount, will display on page Optional
hp_tax_amount	Tax amount charged to consumer, included in Amount, will display on page Optional
hp_save_payment_responsemsg	save payment response message, will be set to SAVED or other relevant error message
hp_signature_response	md5 hash response signature consisting of the concatenation of these fields: <code>hp_refnum*hp_amount*APPROVED or DECLINED</code> . The merchant can use this hash value to ensure that the fields posted back have not been altered in transit. refnum-123456*100.00*APPROVED
hp_payment_cc_firstlast	Provides the first and last 4 digits of the card provided by the consumer. This can be stored by the merchant without any PCI risk or exposure because it is not considered "sensitive data".
hp_cf_1	Custom field for the merchant's use
hp_cf_2	Custom field for the merchant's use
hp_cf_3	Custom field for the merchant's use
hp_cf_4	Custom field for the merchant's use

Paymentsite Hosted Payments User's Manual

Field name	Description
hp_cf_5	Custom field for the merchant's use

13 Integrating and Testing a Merchant Implementation

To ensure successful payment processing, merchants should test their payment gateway integration carefully before attempting to process any real payment transactions.

To integrate and test an implementation:

1. Request a developer test account from Intrix. Intrix will provide the integration posting URL upon approval of your account, along with the URL and login credentials for the Back Office on the Integration Server. The test URL will use the domain <https://int.paymentsite.com>
2. Develop the web pages that will submit transactions to Paymentsite hosted Payments, containing the posting URL provided with your test account.
3. Contact support to set up your Hosted Payments configuration parameters.
4. Run a series of test transactions by submitting them through your web forms to the Paymentsite Integration Environment. The Integration Environment mimics the live Payment Gateway, but does not submit transactions to any financial institutions, so no actual money will be passed.
5. You may log into your Back Office in the Integration Environment to view and download transaction reports from your test transactions. Note that test transactions will not settle.
6. Once you are satisfied that your implementation is working correctly, change the posting URL in your test web pages from the integration URL to the live posting URL. Contact support to update your configuration settings in production—this information is not passed from Integration to the live system.
7. Confirm your production implementation by processing at least one live transaction from your web pages. Log into the Back Office system in Production and check your transaction reports to ensure the transaction is being passed to the live system rather than the Integration Server. Transactions run in production will transfer real money, so you may wish to test the live system using a small transaction amount (or void the transaction before it settles from your Back Office).

When passing transactions through a test account a simulated payment gateway will be used. To pass a successful transaction to the engine that approves pass an even dollar amount such as \$100.00. To simulate failed transactions and get a decline, pass an odd number such as \$100.01. To simulate a partial payment pass a value between \$300.00 to \$399.99. Don't forget odd numbers will decline.

Paymentsite Hosted Payments User's Manual

Amount	Description	Meaning
\$100.00	Even Cents	Will pass a successful authorized transaction which is approved
\$100.01	Odd cents	Will result in a transaction decline
\$300.00 to \$399.00	Range	Will cause a partial payment transaction, odd and even cents will affect approvals and declines as described above.

14 Fraud Protection: AVS and Card Code

The address verification system (AVS) and card code (CVV) are best practice fraud protection measures provided with the Paymentsite hosted Payments solution. If the merchant server accepts posted responses, whenever a transaction is processed by the Paymentsite hosted Payments system, the system will pass back response AVS and CVV codes to help merchants determine whether or not they wish to accept the transaction.

If desired, you can code your system to automatically reverse a transaction that comes back with an undesirable AVS or CVV response.

The AVS response is passed back to the merchant web server in the hp_avsresponse field. The values that are passed may be any of those shown in the table below.

Code	Alternates	Meaning
YYY	Y, YYA, YYD	Address: Match & 5 Digit Zip: Match
NYZ	Z	Address: No Match & 5 Digit Zip: Match
YNA	A, YNY	Address: Match & 5 Digit Zip: No Match
NNN	N, NN	Address: No Match & 5 Digit Zip: No Match
YYX	X	Address: Match & 9 Digit Zip: Match
NYW	W	Address: No Match & 9 Digit Zip: Match
XXW		Card Number Not On File
XXU		Address information not verified for domestic transaction
XXR	R, U, E	Retry / System Unavailable
XXS	S	Service Not Supported

Paymentsite Hosted Payments User's Manual

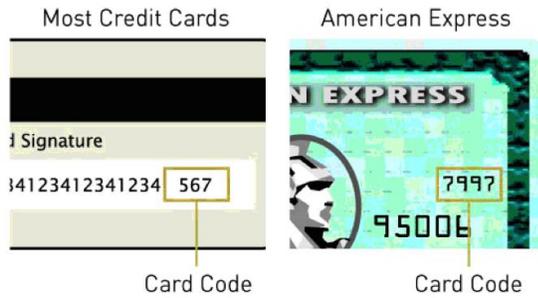
Code	Alternates	Meaning
XXE		Address Verification Not Allowed For Card Type
XXG	G, C, I	Global Non-AVS participant
YYG	B, M	International Address: Match & Zip: Not Compatible
GGG	D	International Address: Match & Zip: Match
YGG	P	International Address: Not Compatible & Zip: Match

Each of the digits in the AVS response have a meaning as well:

AVS CODE	DESCRIPTION
A	The street address matches, but the 5-digit ZIP code does not
B	Address information was not submitted in the transaction information, so AVS check could not be performed
E	The AVS data provided is invalid, or AVS is not allowed for the card type submitted
G	The credit card issuing bank is of non-U.S. origin and does not support AVS
N	Neither the street address nor the 5-digit ZIP code matches the address and ZIP code on file for the card
P	AVS is not applicable for this transaction
R	AVS was unavailable at the time the transaction was processed. Retry transaction
S	The U.S. card issuing bank does not support AVS
U	Address information is not available for the customer's credit card
W	The 9-digit ZIP code matches, but the street address does not match
Y	The street address and the first 5 digits of the ZIP code match perfectly

The Credit Card Verification Code, or Card Code, is a three- or four-digit security code that is printed on the back of credit cards (or on the front for American Express cards) as shown here:

Paymentsite Hosted Payments User's Manual



A card code that is passed with a transaction from the Paymentsite hosted Payments system goes to the credit card issuer for verification. The credit card issuer determines if the value matches the value on file for the customer's credit card and returns a code indicating whether the code matched or not.

The card code (CVV, CVC, or CID) response gets passed back to the merchant's server in the `hp_cvvresponse` field. Possible values for the card code response and their meanings are shown in the table below.

CARD CODE RESPONSE	DESCRIPTION
N	The Card Code does not match
P	The Card Code was not processed
S	The Card Code was not indicated
U	Card Code is not supported by the card issuer