



Payment Pages Setup Guide
Version 2

Published: 31 December 2015



Migrating from version 1?

Please read our quick start guide on page 74.

Table of Contents

1	Introduction	4
2	Process Overview	5
2.1	Redirect to Merchant’s Website (optional)	6
2.2	AVS and Security Code checks	6
2.3	About MyST	6
2.4	URL Notifications	6
2.5	Settlement	7
2.6	Split Shipments	7
3	Posting Information	8
3.1	Configuring the HTTP POST	8
3.2	The result of the POST	9
3.3	Specifying required fields	11
3.4	Verify Card Type	12
3.5	Manually changing payment types on the billing details page	14
3.6	Response Page	15
3.7	“Cancel” and “Continue shopping” buttons	17
3.8	Testing	18
4	Allowed Fields	19
4.1	Required Fields	19
4.2	Address Verification System (AVS)	20
4.3	Billing Fields	21
4.4	Customer Fields	22
4.5	Locale	23
4.6	Settlement Deferral	23
4.7	Settlement Status	23
4.8	Order Reference	23
4.9	Pre-Authorisations and Final Authorisations	24
4.10	Charset	25
4.11	Custom Fields	25
4.12	Postcode validation	26
4.13	County validation	26
5	PayPal	27
5.1	Refunds	27
5.2	Order reference / Invoice ID	27
5.3	Delivery Address	28
6	Security	30
7	Additional Request Types	34
7.1	Risk Decision	34
7.2	Account Check	35
7.3	3-D Secure	39
7.4	Subscription	40
7.5	Currency Rate	40
7.6	How to configure Additional Request Types	48
8	Customisation	49
8.1	Custom logo	49
9	Rules	50
9.1	Rule types	50
9.2	Activating rules	51
9.3	Merchant Decline Rule (STR-1)	52


9.4	Payment Pages Advanced Redirects	53
9.5	URL Advanced Notifications	55
9.6	Response Site Security	57
9.7	Email notifications	60
10	Enhanced Post	63
10.1	Getting Started	63
10.2	Sending an Enhanced Post Request	64
10.3	PayPal and Enhanced Post	67
10.4	Subscriptions and Enhanced Post	68
11	iframe.....	70
11.1	Configuring your Website.....	70
11.2	Changing the appearance of the iframe.....	70
12	Google Analytics.....	71
12.1	Using Google Analytics Tracking Code	71
12.2	Google Analytics and Ecommerce Tracking	71
13	Going Live.....	72
13.1	Rules for Live Site Reference	72
13.2	Contact Secure Trading	72
13.3	Change your website	72
13.4	Live testing	72
14	Testing.....	73
14.1	Testing successful transactions	73
14.2	Testing unsuccessful transactions	73
15	Migrating from version 1	74
15.1	Customisation	74
16	Further Information and Support	75
16.1	Secure Trading Support	75
16.2	Secure Trading Sales.....	75
16.3	Useful Documents.....	75
16.4	Frequently Asked Questions	75
17	Appendix.....	76
17.1	Settle status	76
17.2	Charge description	77
17.3	Payment facilitator.....	77
17.4	Digital wallet	77

1 Introduction

Secure Trading Payment Pages are for merchants who need a simple and easily-implemented method of adding e-payment capability to their online commerce systems. Secure Trading Payment Pages works with custom-designed ecommerce systems as well as with many commercially available shopping cart applications.


Using Secure Trading Payment Pages you can:


- # Process payments on our own dedicated HTTPS servers (that use the SSL protocol) that allow you to process secure and reliable transactions.
- # Process payments without storing credit card details on your server.
- # Customise the Payment Pages with custom HTML/CSS to maintain the look and feel of your online store.
- # Accept a large variety of currencies.
- # Track all transactions using our online transaction management system, [MyST](#).


PAYMENTS SECURED BY

A UC GROUP COMPANY


Amount: £1.23 GBP
 Order reference: MyOrder123
 Merchant name: Test Merchant


Please select your payment method














Please make sure that you select the correct payment type.

Requirements

To process payments using Payment Pages you will need to check the following:

You have a **Secure Trading account** with either a test or live site reference. (e.g. "test_site12345" or "site12346" respectively)

You have a **MyST login** (provided in the welcome email) to perform certain maintenance tasks on your account.

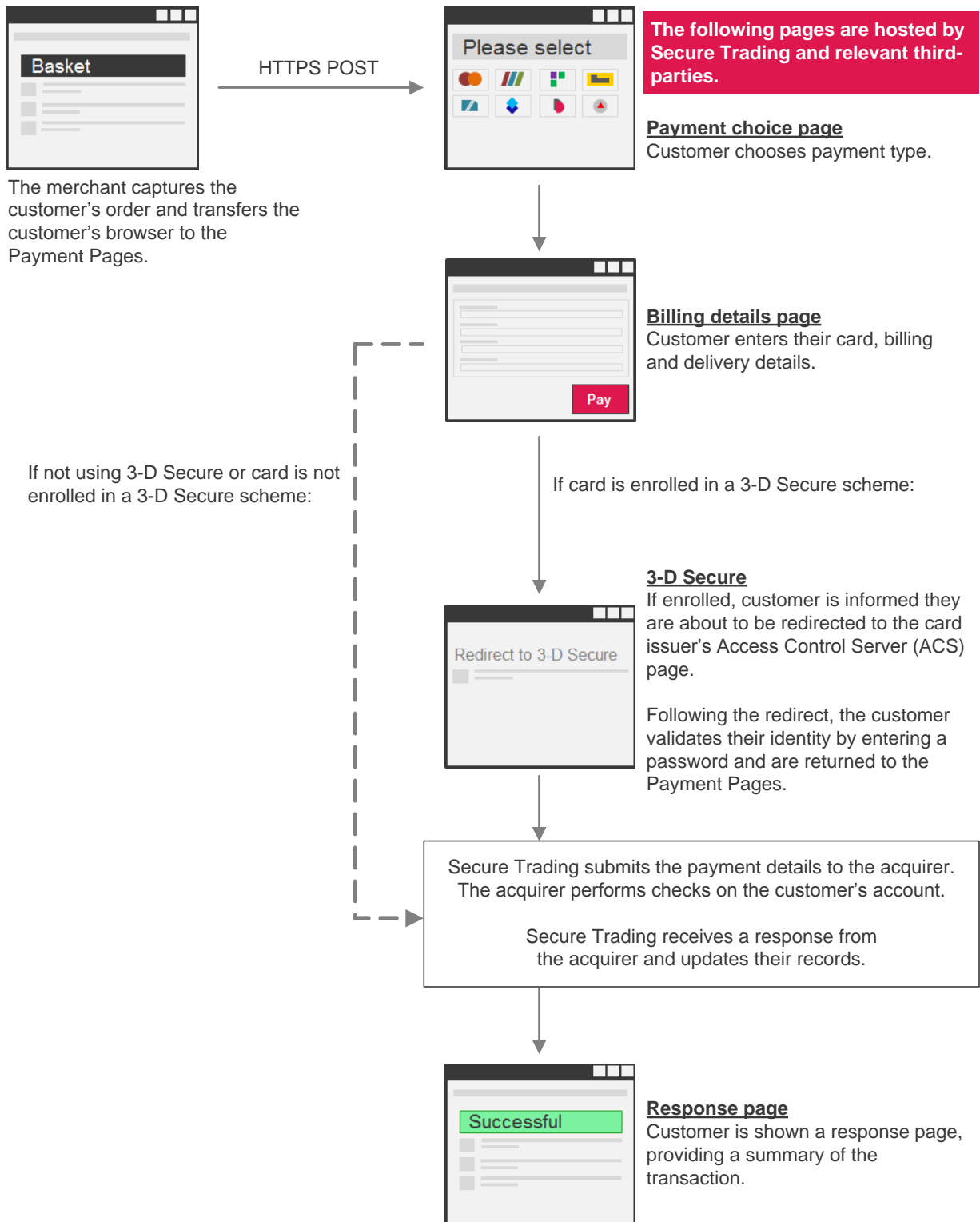
You have an **internet merchant account** for processing live transactions.


You are **PCI accredited**.
 For further information, please contact your acquiring bank.

Your firewall is configured to allow connections from Secure Trading's IP Ranges.
 Current IP Ranges can be viewed at <http://webapp.securetrading.net/ips.html>

If you are unsure on any of the points above, please contact Secure Trading for assistance (see section 16).

2 Process Overview



 **If a transaction is authorised, it is not guaranteed you will receive funds. Funds are not transferred to your account until settlement (see section 2.5).**

Payment Pages Setup Guide

2.1 Redirect to Merchant's Website (optional)

As an alternative to displaying the response page on Secure Trading's servers, you can configure a redirect (HTTP 302) back to your site upon the completion of a customer's order.

The customer's browser is redirected to a URL on your server, which can include fields supported by Secure Trading from the processed transaction.

In order to set up a redirect, please see section 9.4.

2.2 AVS and Security Code checks

The authorisation process is performed between the merchant's acquiring bank and the customer's card issuer. It is at this point that the AVS (Address Verification System) and CVV2 (security code) checks are performed.



Please note that the nature of checks performed will depend on the payment types, card issuers, card issuer region and acquirers involved in the transaction.

Please refer to the [STPP AVS & CVV2 document](#) for further information on address and security code checks.

2.3 About MyST

When you first sign up with Secure Trading you will be provided with a MyST username (email address) and password. MyST is a secure interface providing online real-time access to your payment history. The status of every transaction can be tracked, allowing your Secure Trading account to be managed more effectively. Secure Trading recommends regularly signing into MyST to ensure there are no issues with recent transactions processed on your account that require your attention.

You can sign in using the following URL: <https://myst.securetrading.net/login>
For further information on the MyST interface, please refer to the [MyST User Guide](#).

2.4 URL Notifications

In addition to using MyST, Secure Trading recommends that all merchants using Secure Trading's Payment Pages solution configure URL notifications to be kept informed of transactions processed on their accounts. For further information, please refer section 9.5.

2.5 Settlement



Please note that the procedure outlined in this section of the document applies to card-based payment methods. For further information on other payment types, please refer to additional Secure Trading documentation on [our website](#), or contact your acquiring bank / payment provider.

Once a transaction has been authorised the funds are then reserved against the customer's account for 7 days* while awaiting settlement. The instruction to transfer the funds is scheduled daily when Secure Trading submits a batch of all transactions that are pending settlement to your acquirer. This process is called settlement and is outlined below:

Step 1: Secure Trading submit settlement file to the acquirer

The initial phase of the settlement process occurs when Secure Trading submits a file to your acquirer. The file contains all transactions that are in status 'pending settlement', and this occurs daily.

Step 2: The funds are transferred to your bank account

When the acquirer has received the settlement file from Secure Trading, your acquirer commences the process of physically settling the money into your nominated bank account. The time frame of this payment differs between banks, and is beyond Secure Trading's control.



Please note that if reserved funds are not settled, they are released back onto the customer's card. We recommend that you regularly log in to MyST to check the status of your payments.

2.5.1 Deferred settlement

Settlement can be deferred for certain transactions. You can request this (see section 4.6), or transactions may be deferred by Secure Trading's internal fraud system (if enabled on your account). You should therefore sign in to MyST on a regular basis, to check the status of your transactions. Please refer to the [MyST User Guide](#) for further information.

2.6 Split Shipments

Split shipments provide you with more control over when reserved funds are settled. Instead of performing a single settlement within 7 days* as is the case with a standard authorisation, with split shipments you can perform multiple partial settlements.

STPP supports split shipments for certain acquirers. For further information, please refer to the [Split Shipment Guide](#).



***Please note** that certain acquiring banks have different procedures in regards to settlement with payments made with MasterCard. These differences are described in section 4.9.

3 Posting Information

In order to transfer your customers to Secure Trading's Payment Pages, you will need to perform an HTTP or HTTPS POST request. Based on the information posted, the system will then interpret this information and display the appropriate page to the customer.

3.1 Configuring the HTTP POST

Once you have a Secure Trading account set up and are ready to begin testing, you will need to establish a way of transferring a customer from your site to Secure Trading.



Please note that for the example outlined in this section, please submit your test site reference (e.g. **test_site12345**). When you go live, you will need to use your live site reference.

It is possible to set up a POST to the Payment Page. This can be achieved by creating a form on your webserver that will submit the information. If you copy the below to an HTML file, and open that page in your web browser, you will be displayed a button that will POST the information to Secure Trading's servers when clicked.

```
<html>
<head>
</head>
<body>
<!--YOUR HTML-->
<form method="POST"
action="https://payments.securetrading.net/process/payments/choice">
<input type="hidden" name="sitereference" value="test_site12345">
<input type="hidden" name="stprofile" value="default">
<input type="hidden" name="currencyiso3a" value="USD">
<input type="hidden" name="mainamount" value="100.00">
<input type="hidden" name="version" value="2">
<input type="hidden" name="orderreference" value="myorder12345">
<input type="submit" value="Pay">
</form>
</body>
</html>
```

The above example includes the required fields that need to be included in the POST (highlighted above in **bold**). The optional field **orderreference** has also been included. All optional fields can be submitted in this way. For more information on these fields or the additional fields that can be included, please refer to section 4.



Please note that the method above describes how to process an Authorisation Request through the Payment Pages. It is possible to perform additional request types, as described in section 7.



Ensure the contents of your HTTPS POST is smaller than 1kb. Failing to do so may result in a slower response time and impact your customer's experience.

Payment Pages Setup Guide

3.2 The result of the POST

3.2.1 Payment choice page

Once you have successfully completed the setup of the POST, then either the link or the button when pressed should return a page similar to **Figure 2**.

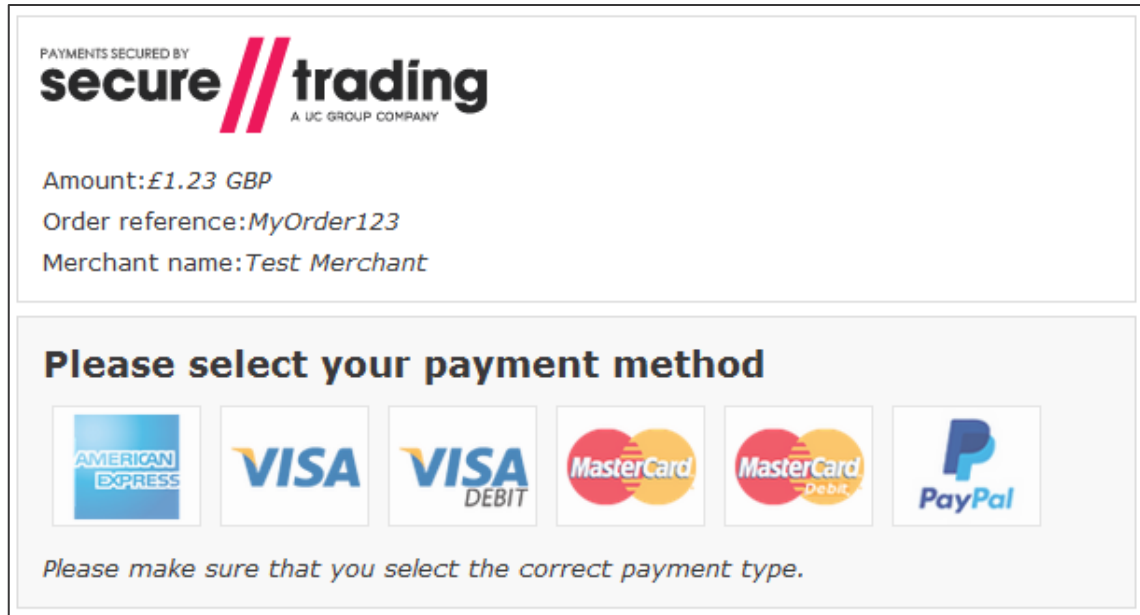


Figure 2 - Default payment choice page

Figure 2 is a screenshot of the default payment choice page with default styling. On this page, the customer will choose the payment type with which they would like to make the payment.

3.2.1.1 Bypassing the payment choice page

It is possible to bypass the payment choice page and send the customer directly to the billing details page (section 3.2.2) where they enter their card details. This is achieved by posting to this URL:

<https://payments.securetrading.net/process/payments/details>

3.2.2 Billing details page


If the customer wishes to process a credit/debit card transaction, they will be redirected to a page similar in appearance to that shown in **Figure 3**.



Please note the appearance of the billing details page will vary depending on payment type chosen. The billing details page for most major cards will have the layout shown in **Figure 3**.

PAYMENTS SECURED BY
secure // trading
A UC GROUP COMPANY

Amount: £1.23 GBP
Order reference: MyOrder123
Merchant name: Test Merchant



Select a logo to choose a different payment method

Billing Details (Edit)

Title

First name

Last name

House name/no.

Street

Town

County

Country

Postcode

Email

Telephone

Telephone type

Delivery Details (Edit)

Use billing details

Title

First name

Last name

House name/no.

Street

Town

County

Country


Postcode

Email

Telephone

Telephone type


Payment Details

Card number * 

Expiry date *

Security code *

Security code is on the back of your card



Pay Securely

* Indicates a required field

Figure 3 - Billing details page for a card

3.3 Specifying required fields

As shown in **Figure 3**, fields required by Secure Trading to process a transaction are highlighted on the page with an asterisk. It is possible to specify additional fields to be required on the page using the methods below. If the customer fails to enter the information required, the payment will not be processed. A warning will be shown and the relevant fields are highlighted on the page. This allows the customer to make corrections and try again.

3.3.1 Customising the POST



Please note if you have PayPal enabled, you will need to instead refer to section 3.3.2.

You can modify your POST to Payment Pages to specify additional required fields. This is demonstrated in the following HTML example (the fields specified as required are highlighted in **bold**):

```
<html>
<body>
<!--YOUR HTML-->
<form method="POST"
action="https://payments.securetrading.net/process/payments/choice">
<!--Other fields-->
<input type="hidden" name="strequiredfields" value="billingpostcode">
<input type="hidden" name="strequiredfields" value="billingfirstname">
<input type="hidden" name="strequiredfields" value="billinglastname">
<input type="submit" value="Pay">
</form>
</body>
</html>
```



To prevent the customer from modifying the required fields specified in the POST, you **must** include these fields in your site security hash (see section 6).

3.3.2 Using the MyST Rule Manager

You can create custom rules in the MyST Rule Manager that specify fields as required under certain conditions. For example, you can specify fields to be only required when paying by card, as to not affect payment types that redirect the customer to third parties to enter their payment details (e.g. PayPal).

Sign in to [MyST](#) and create a rule with action type "Payment pages required fields". For information on how to get started with the Rule Manager, please refer to the [Rule Manager supplement](#).

Payment Pages Setup Guide

3.4 Verify Card Type

It is possible to configure the customer's ability to pay in different payment types, after they have chosen their preferred payment type on the payment choice page (**Figure 2**).

Secure Trading offers three configurations to handle customers who select a card type on the payment choice page (**Figure 2**), but enter the details of a different card type on the details page (**Figure 3**). These configurations are outlined in detail, below. To change the verify card type solution to be used on your site, please contact Secure Trading support (see section **16.1**).



Please note that by default, new sites are configured to use "Auto Correct" (configuration "0").



Although Secure Trading correctly identifies the majority of cards submitted to the Payment Pages, we may not always correctly assign the card type when our Bank Identification Number (BIN) records differ from the records maintained by our supported acquirers.

3.4.1 Auto Correct (Default) – Configuration "0"

The payment is processed in the correct payment type, but the customer is not informed beforehand if the card details they have entered did not match the card type they selected on the payment choice page.

The customer can change to a different payment type (after they have selected one from the payment choice page) by selecting a new payment type from the top of the billing details page (see section **3.4**).

3.4.2 Fail if PAN doesn't match – Configuration "1"

This configuration prevents a customer from changing the payment type they are paying with after they have reached the billing details page. This is designed for merchants who have implemented their own hosted payment choice page, allowing customers to select a payment type before inputting their payment details on Secure Trading's hosted billing details page (as shown in **Figure 3**).

If the customer enters card details that do not match the card type, and attempt to process a payment, the payment will not be processed and a red warning message is shown at the top of the page (**Figure 4**). They cannot proceed with the payment until they enter payment details for the pre-specified payment type.



There has been a problem with your payment:

Card number does not match card type (Ref:42-71-6)

Figure 4 - Payment details entered does not match pre-specified payment type (Error)

Payment Pages Setup Guide

3.4.2.1 Posting directly to the billing details page

You may wish to bypass the payment choice page by redirecting the user directly to the billing details page with a pre-defined payment type. This section outlines how to perform this operation.

To post directly to Secure Trading's hosted billing details page (as shown in **Figure 3**), follow the steps outlined in section **3.1**, substituting the URL with "https://payments.securetrading.net/process/payments/details". You can optionally include the additional field **paymenttypedescription**, which is the payment type the customer is using to make the payment.



Using verify card type configuration "1" ensures the customer will not be able to pay in any other payment type other than the one specified in the POST.

Example

Differences from the POST to Secure Trading's hosted payment choice page are highlighted in **bold**:

```
<html>
<head>
</head>
<body>
<!--YOUR HTML-->
<form method="POST"
action="https://payments.securetrading.net/process/payments/details">
<input type="hidden" name="sitereference" value="test_site12345">
<input type="hidden" name="stprofile" value="default">
<input type="hidden" name="currencyiso3a" value="USD">
<input type="hidden" name="mainamount" value="100.00">
<input type="hidden" name="version" value="2">
<input type="hidden" name="paymenttypedescription" value="VISA">
<input type="submit" value="Pay">
</form>
</body>
</html>
```

3.4.3 Payment Pages redisplay choice if PAN doesn't match – Configuration "2"

The customer is shown a yellow warning at the top of the page (**Figure 5**), if the card details they have entered did not match the card type they selected on the payment choice page.

The customer needs to click "Pay" again in order to make the payment with the card type associated with the previously submitted details. They can amend their address and billing details before paying, or opt to pay using a different payment type by choosing an alternative from the top of the page (see section **3.4**).



The card number you have entered does not match the payment method you selected. If you continue your transaction will be processed as American Express

Figure 5 - Payment details entered does not match pre-specified payment type (Warning)

3.5 Manually changing payment types on the billing details page

For sites configured to use verify card type configurations “0” and “2” (see sections 3.3.1 and 3.3.3, respectively), a list of payment types are displayed at the top of the billing details page (as shown in **Figure 6**). The customer can click a different payment type, and the billing details page will be redisplayed with fields and content relevant to the selected payment type.



Please note if your site is only configured to accept payments in one payment type, no other payment types will be shown.

PAYMENTS SECURED BY
secure // trading
A UC GROUP COMPANY

Amount: £123.99 GBP
Order reference: MyOrder123
Merchant name: Test Merchant

AMERICAN EXPRESS VISA VISA DFRIT MasterCard
MasterCard PayPal

Select a logo to choose a different payment method

Billing Details *(Edit)* **Delivery Details** *(Edit)*

Use billing details

Title [dropdown]
First name [text]
Last name [text]

Title [dropdown]
First name [text]
Last name [text]


Figure 6 – Payment options as seen on billing details page




Please note that sites using verify card type configuration “1” will **never** show payment types on the billing details page, even if the customer enters invalid payment details, or the payment is otherwise unsuccessful. This means that once the customer is viewing the billing details page, they cannot change the payment type they are paying in.

3.6 Response Page

Following a successful authorisation, the customer will be shown a response page (as shown in **Figure 8**). This page contains information about the processed authorisation that is useful for the customer to take note of for future reference.

PAYMENTS SECURED BY

A UC GROUP COMPANY

 **Successful**

Receipt

Transaction reference: 42-5-63 Auth code: 61 Card number: *****0511	Amount: £1.23 Currency: GBP Order reference: MyOrder123 Payment type: MasterCard Merchant name: Test Merchant
--	--

Billing Details

Mr Paying Customer

No 789
Test Street
Bangor
Gwynedd
United Kingdom
TE45 6ST

customer@email.com
Home 01234567890

*Please **print** this page for your records.*

Delivery Details

Mr Paying Customer

No 789
Test Street
Bangor
Gwynedd
United Kingdom
TE45 6ST

customer@email.com
Home 01234567890

Figure 8 - Response page for a card



Secure Trading recommends emailing these details to the customer following authorisation. Information on configuring email notifications for your account can be found in section 9.7.

3.6.1 Refresh warning

After a successful authorisation request, by default the customer is shown a response page with a unique reference number for the request.

If the customer navigates back to the billing details or payment choice pages using the navigation buttons in their browser and attempts to make another payment, they will be redirected to the same response page (with the same reference number as before).

A warning will be displayed at the top of the page (as shown in **Figure 9**) to remind the customer a payment has already been processed.

This is to assist in preventing duplicate authorisation requests from being processed accidentally.

PAYMENTS SECURED BY
secure // trading
A UC GROUP COMPANY

⚠ It appears you have pressed refresh or attempted to go back in your browser.

You have already performed a transaction, no new transaction has been performed.

If you want to alter your details please contact the website you processed the payment through.

✔ Successful

Receipt

Transaction reference:	Amount:
42-5-63	£1.23
Auth code:	Currency:
61	GBP
Card number:	Order reference:
*****0511	MyOrder123

Figure 9 - Refresh warning on response page

Payment Pages Setup Guide

3.7 “Cancel” and “Continue shopping” buttons

3.7.1 “Cancel” buttons

Secure Trading Payment Pages can be configured to show “Cancel” buttons on the payment choice page and/or the billing details page. When clicked, the customer is redirected to a URL of your choosing.

Please select your payment method

AMERICAN EXPRESS VISA VISA DEBIT MasterCard MasterCard Debit PayPal

Please make sure that you select the correct payment type.

Cancel

Figure 10 - Payment choice page configured to show “Cancel” button

Payment Details

Card number * VISA

Expiry date *

Security code *

Security code is on the back of your card

AUTHORISED SIGNATURE *J Bloggs* 0000 123
NOT VALID UNLESS SIGNED

Cancel **Pay Securely**

* Indicates a required field

Figure 11 - Billing details page configured to show “Cancel” button

3.7.2 "Continue shopping" button

Secure Trading Payment Pages can be configured to show a "Continue shopping" button on the response page, following a successful authorisation request. When clicked, the customer is redirected to a URL of your choosing.

Billing Details	Delivery Details
<i>Mrs Paying Customer</i>	<i>Mrs Paying Customer</i>
<i>No 789</i>	<i>No 789</i>
<i>Test Street</i>	<i>Test Street</i>
<i>Bangor</i>	<i>Bangor</i>
<i>Gwynedd</i>	<i>Gwynedd</i>
<i>United Kingdom</i>	<i>United Kingdom</i>
<i>TE45 6ST</i>	<i>TE45 6ST</i>
<i>customer@email.com</i>	<i>customer@email.com</i>
<i>Home 01234567890</i>	<i>Home 01234567890</i>
<i>Please print this page for your records.</i>	
<div style="background-color: #e91e63; color: white; padding: 10px; display: inline-block; border-radius: 5px;">Continue shopping</div>	

Figure 12 - Response page configured to show "Continue shopping" button

3.7.3 Configuration

To set up these buttons on Payment Pages, please contact Secure Trading support (refer to section 16.1). Please inform support of the required URL(s) and buttons required for your solution.

3.8 Testing

You can test the different payment configurations through your Payment Pages using the testing details found in section 14 of this document. Secure Trading recommends that you test your system thoroughly before processing real transactions through your live account.

3.8.1 Best practices

You will need to monitor payments on your account and ensure they were processed successfully. This can be performed by signing into MyST and manually checking processed transactions (refer to the [MyST User Guide](#)) or by configuring automated notifications (see section 9). We strongly recommend that you include the following in your checks:

- # Ensure the error code is "0", indicating a successful transaction. An error code of "70000" indicates that the customer's bank declined the payment and the customer was prompted to try again with different payment details. Other error codes will require manual investigation. For a full list of error codes, go to this URL: <http://webapp.securetrading.net/errorcodes.html>
- # If you are expecting a transaction to be scheduled for settlement, ensure the settle status is "0" or "1" (see section 17.1 for a full list of settle status values).
- # Check the amount and currency of the transaction is correct.
- # If you have configured redirects (9.4) or URL notifications (9.5), ensure the response site security hash is correct, by following the instructions in section 9.4.4.

4 Allowed Fields

The examples provided in previous sections of the document focus on the fields required by Secure Trading. Secure Trading recommends that you submit as much information as possible with your transactions, as this can help you gain more information about a customer that can be used to tackle fraud. This section of the document lists both the required and the additional field names that can be included within the POST submitted from your website to Secure Trading, and the benefits of including this information.



It is important that the field names you post match those within the following tables, as only these fields are recognised by Secure Trading's servers. The field names are case sensitive.



Please note that the system does not support multiple fields with the same name, unless explicitly stated.

4.1 Required Fields

The table below includes the required field names that need to be passed through to Secure Trading in order to display your payment page.

Field name	Details
sitereference	The unique Secure Trading site reference that you receive when you sign up.
stprofile	Used to specify the styling used to render the Payment Pages. When using the default appearance, this is set to "default". For information on customising the appearance of your Payment Pages, please refer to the customisation document .
currencyiso3a	The currency that the transaction will be processed in. There is a list of available currencies on our website: http://webapp.securetrading.net/currencycodes.html
mainamount	The amount of the transaction should be in main units, with no commas, so £1000 would be 1000.00 Currencies such as Japanese Yen which do not require a decimal place can be submitted without. So 1000 Yen would be 1000
version	This value will be set to 2.

Payment Pages Setup Guide

4.1.1 Visa Additional Authorisation Data Merchant Category Code (MCC) 6012

Visa has mandated that UK-based merchants with a Merchant Category Code (MCC) of 6012 are required to send the customer's date of birth, account / card number, last name and postcode, as outlined below:

Field name	Details
customerdob	The account holder's date of birth. Must be in the format YYYY-MM-DD.
customeraccountnumber type	Either "CARD" or "ACCOUNT".
customeraccountnumber	If account number type is "ACCOUNT", the account holder's account number. If account number type is "CARD", the account holder's card number.
customerlastname	The account holder's last name.
customerpostcode	The customer's postcode.
customercountryiso2a	The country for the account holder's billing address. This will need to be in ISO2A format. List of Country Codes: http://webapp.securetrading.net/countrycodes.html



Your Merchant Category Code (MCC) is a four-digit number assigned to you by your acquirer. It is used to classify the business by the type of products or services it provides. If you are unsure of the value of your merchant category code, please contact Secure Trading Support (section 16.1).

4.2 Address Verification System (AVS)

The Address Verification System provides a further level of security to a transaction as it allows you to carry out checks regarding the validity of the address information supplied by the customer in relation to the card used.

4.2.1 What is Address Verification?

A customer's billing address is checked against the address that the card issuer holds for that card. Your bank will indicate whether there is a match between the entered address and the card address on record.

When obtaining an authorisation for a transaction, Secure Trading will pass the customer's address (if provided) to the acquiring bank along with the details required for authorisation.

4.2.2 Availability

The availability of the Address Verification System is dependent on the acquiring bank and card issuer, although it should be noted that most cards support this functionality.

The ability to conduct address checks is dependent on the location of your acquiring bank in relation to the location of the issuing bank of the card being presented. Most acquirers do support the process but only on locally issued cards. All UK cards and a number of US cards are address checked by all UK acquirers. Please contact Secure Trading for further information on the supported acquirers and card types (see section 16.1). Please refer to the **STPP AVS & CVV2** document (see section 16.3) for further information on AVS.

Payment Pages Setup Guide

4.2.3 Address Field Names

In order to perform Address Verification on a card, you will need to include the address details within your POST.



Please note that in order for the AVS checks to be performed, it is the **billing** address details that need to be included.

The table below includes the various field names that you can pass to Secure Trading's system in order for the address details to be checked.

Field name	Details
billingpremise	The house number or first line of the customer's billing address.
billingstreet	The street entered for the customer's billing address
billingtown	The town entered for the customer's billing address.
billingcounty	The county entered for the customer's billing address. This is displayed as "State code (eg. NY)" on pages with US locale and "County" on other configurations. For US addresses, the state would be entered in this field. Valid formats: <ul style="list-style-type: none"> # Preferred: Two character state code, e.g. "NY". # Full state name (no abbreviations), e.g. "New York".
billingpostcode	The postcode entered for the customer's billing address.

4.3 Billing Fields

You may also submit the following billing fields through Secure Trading's systems.

Field name	Details
billingprefixname	This will be the customer's prefix. The options available are Mr, Mrs, Miss, Dr, Ms, Prof and Rev.
billingfirstname	The customer's first name.
billinglastname	The customer's last name.
billingcountryiso2a	The customer's country for their billing address. This will need to be in iso2a format. For a list of countries, please see: http://webapp.securetrading.net/countrycodes.html
billingemail	The customer's e-mail address. This can then be used for correspondence with the customer. Maximum length of 255 (maximum of 64 characters before the "@" symbol).
billingtelephone	The customer's telephone number. Requires <code>billingtelephonenumber</code> to be specified. Valid characters: <ul style="list-style-type: none"> # Numbers 0-9 # Spaces # Special characters: + - ()
billingtelephonenumber	The type of telephone number inputted. The options available are: <ul style="list-style-type: none"> # H = Home # M = Mobile # W = Work Required if <code>billingtelephone</code> is entered.

4.4 Customer Fields

You may also submit details with regards to an additional address for the customer. This usually relates to the delivery address. These fields are included below.

Field name	Details
customerpremise	The house number or first line of the customer's additional/delivery address.
customerstreet	The street entered for the customer's additional/delivery address
customertown	The town entered for the customer's additional/delivery address.
customercounty	The county entered for the customer's additional/delivery address. This is displayed as "State code (eg. NY)" on pages with US locale and "County" on other configurations. For US addresses, the state would be entered in this field. Preferred format: Two character state code, e.g. "NY".
customerpostcode	The postcode entered for the customer's additional/delivery address.
customertelephone	The customer's telephone number associated with their additional/delivery address. Requires <code>customertelephontype</code> if entered. Valid characters: // Numbers 0-9 // Spaces // Special characters: + - ()
customertelephontype	The type of telephone number entered. The options available are: // H = Home // M = Mobile // W = Work Only required if <code>customertelephone</code> is entered.
customercountryiso2a	The country for the customer's additional/delivery address. This will need to be in ISO2A format. For a list of country codes, please see: http://webapp.securetrading.net/countrycodes.html
customeremail	The customer's e-mail address associated with their additional/delivery details. This can then be used for correspondence with the Customer. Maximum length of 255.

Payment Pages Setup Guide

4.5 Locale

For customers from the United States, Secure Trading provides an option to use US English for names of fields displayed on the Payment Pages (this does not affect the name of fields processed by STPP):

Field name	Details
locale	<p>By default, Payment Pages will use UK English, unless otherwise specified, using the values below:</p> <ul style="list-style-type: none"> // en_US = US English for field names. (e.g. postcode becomes zipcode and county becomes state). // en_GB = UK English for field names (as default).

4.6 Settlement Deferral

It is possible to defer settlement on transactions by submitting `settleduedate` through the Payment Pages system. This field is detailed below (for more information on settlement, please see section 2.3):

Field name	Details
settleduedate	The date the merchant wishes for the transaction to settle. This needs to be in the format YYYY-MM-DD.



Please note that the due date can be up to a maximum of 7 days after the authorisation date.

4.7 Settlement Status

You can set the status of a transaction by submitting the `settleststatus` field to Secure Trading's system:

Field name	Details
settleststatus	<p>This value relates to the status of the transaction. The possible vales are:</p> <ul style="list-style-type: none"> 0 – Pending Settlement. 1 – Pending Settlement, manually overridden. 2 – Suspended. 100 – Settled (This is only currently available for certain acquirers. For more information, contact Secure Trading Support; please see section 16.1). The default value is 0.

(See section 17.1 for a full list of settle status values)

4.8 Order Reference

You can pass your own reference for a transaction, to be stored in the database.

Field name	Details
orderreference	Your own reference for the transaction. This can be useful when matching transactions to orders within your system.

4.9 Pre-Authorisations and Final Authorisations

MasterCard Europe have mandated that **MasterCard** and **Maestro** transactions processed with certain European acquiring banks must be flagged as either pre-authorisation or final authorisation. Such transactions are subject to acquirer-specific conditions.

We recommend that you contact your acquirer for information on whether this mandate applies to your configuration and to clarify whether to process your transactions as pre-authorisations or final authorisations.

By default, Secure Trading will process MasterCard and Maestro authorisations as final authorisations. You can change this default behaviour to submit pre-authorisations, by contacting Secure Trading Support (see section 16.1).

Alternatively, see section 4.9.2 for information on overriding the default behaviour on a transaction-by-transaction basis.

4.9.1 About Pre-Authorisations and Final Authorisations

Pre-authorisation and final authorisation can be summarised as follows:

Pre-Authorisation:

- # Settlement can be deferred by up to **7 days** following authorisation.
- # Funds are reserved on the customer's account for up to **30 days**.
- # During this time, the amount to be settled can be updated to a value that is lower than the amount authorised.
- # Pre-authorisations are more flexible than final authorisations, but may be subject to higher processing fees by your acquiring bank.

Final authorisation:

- # Settlement can **only** be deferred by up to **4 days** following authorisation ⁽¹⁾⁽²⁾.
- # Funds are reserved on the customer's account for up to **7 days**.
- # Following authorisation, the amount value should not be changed ⁽¹⁾.
- # Final authorisations are less flexible than pre-authorisations, but may be subject to lower processing fees by your acquiring bank.

⁽¹⁾ Failure to adhere to these conditions may incur a fine from MasterCard.



⁽²⁾ Secure Trading will allow final authorisations to be settled up to 7 days after authorisation, but you should aim to settle within 4 days to avoid incurring a fine.

For full terms and conditions, please contact your acquiring bank.



Split shipments require the initial authorisation to be sent through as a pre-authorisation. Please refer to the [Split Shipment Guide](#) for further information.

4.9.2 Override

You can include the `authmethod` field in the HTTP POST to indicate whether the payment is a pre-authorisation or a final authorisation. This overrides the default behaviour when submitted. The values that can be submitted are:

- # "PRE" - Requests a "pre-authorisation".
- # "FINAL" - Requests a "final authorisation" (default).

Payment Pages Setup Guide

4.10 Charset

In order for data to be transmitted, the customer's browser encodes it using a character encoding. Secure Trading's servers need to know this encoding (or charset) in order to correctly decode the data. Many browsers do not provide this information, in which case Secure Trading will assume the character encoding is ISO-8859-1. This is compatible with all browsers but can result in some characters (in particular non-western characters) being interpreted incorrectly.

You can tell the browser to specify the correct charset by including a hidden field “_charset_” within your HTML form. Browsers will automatically fill the value of this field with the charset they are using, so there is no need to specify a value for this field, for example:

```
<INPUT TYPE=hidden NAME="_charset_" />
```



Please note that you can find more information on charset, by referring to http://en.wikipedia.org/wiki/Character_encoding

4.11 Custom Fields

Secure Trading allows you to pass custom fields through their system.

The field names do not need to be a specific case and will not be saved in the database.

You can include these custom fields within the HTTP POST to Secure Trading's Payment Pages. No customisation is required of the Payment Pages system.



The maximum allowed length of custom fields submitted to STPP is 100 characters. Any custom fields exceeding this limit will be truncated or cause an error.



Please note that the field names should **not** be the same as the Secure Trading field names outlined above, or end with “_html”.



Please note that if you would like to receive any custom fields back in a POST from Secure Trading's servers, please refer to the [MyST Rule Manager supplement](#) for information on configuring rules.

Payment Pages Setup Guide

4.12 Postcode validation

If included within the request, validation is performed on the `postcode`.



Please note that postcode validation is dependent on the `country` supplied. If no `country` is supplied, then no additional validation is performed.

The following table outlines the format the postcode needs to be in when it is submitted to Secure Trading.

T represents Text (A-Z or a-z) and N represents Number (0-9):

Country	Validation
United States (US)	Needs to be a 5 or 9 digit zip code. // NNNNN // NNNNNNNNN
Great Britain (GB)	Needs to be between 6 and 8 characters long, including spaces. Can be one of the following formats: // TN NTT // TNT NTT // TNN NTT // TTN NTT // TTNN NTT // TTNT NTT
Canada (CA)	Needs to be 6 or 7 characters long, including spaces. Can be one of the following formats: // TNT NTN // TNTNTN
Other	The format of postcodes for other countries is not validated by Secure Trading.

4.13 County validation

If the `country` is entered and is United States (US), the `county` field needs to be a valid two-digit state code (e.g. "NY" for New York). For a list of US state codes, see: <http://webapp.securetrading.net/usstatecodes.html>

5 PayPal



[PayPal](#) is an international e-commerce business allowing payments and money transfers to be made online. To enable PayPal, please follow the steps outlined in the [Enabling PayPal](#) guide.



Please note that PayPal do not support iframe integration.

Once you have completed the steps outlined in the Enabling PayPal guide, the PayPal logo will be shown alongside existing payment methods.

Please select your payment method



Please make sure that you select the correct payment type.

When a customer chooses to pay with PayPal, they will be redirected to PayPal's website to verify their identity. Upon successful verification, Secure Trading will automatically contact PayPal to retrieve the delivery details.



If using Enhanced Post with PayPal, you may need to modify your request to the Payment Pages. Please refer to section [10.3](#) for additional information.

5.1 Refunds

To ensure our records remain in sync with PayPal, we strongly recommend that you only perform refunds through MyST. Do not perform refunds directly using your PayPal admin portal.

5.2 Order reference / Invoice ID

If submitting the order reference field, the value of this field is sent to PayPal as the invoice ID. PayPal performs checks for duplicate invoice IDs, therefore please ensure any order reference submitted in the HTTPS POST is unique to each transaction.

(A list of all fields you can submit in the POST can be found in section 4)



Please note that you can configure your PayPal account to disable the check on duplicate invoice IDs. Contact PayPal Support for further information.

Payment Pages Setup Guide

5.3 Delivery Address

By default, the customer selects their delivery address from their PayPal account. Alternatively, the customer can use the address entered on your website. This behaviour is controlled by sending the `paypaladdressoverride` field in the initial request to the Payment Pages:

<code>paypaladdressoverride</code>	Result
0	Customer will be offered a choice between the delivery address entered on your website and addresses on their PayPal account.
1	Customer will use the delivery address entered on your website.
2	Customer will not be prompted to choose a delivery address on PayPal's website (best suited to online services and downloads).

5.3.1 PayPal address fields

(Only applicable when `paypaladdressoverride` is 0 or 1)

All customer delivery fields (see section 4.4) can be submitted to PayPal, however the following fields are required:

```

// customerprefixname *
// customerfirstname *
// customermiddlename *
// customerlastname *
// customersuffixname *
// customerpremise
// customertown
// customercountryiso2a
// customerpostcode
    
```

*You must submit at least one of the customer name fields.



To ensure the customer cannot modify the delivery address submitted to the Payment Pages, the fields must be included in your Site Security. This is detailed in section 6.

5.3.1.1 Example of POST using address override

Fields required for address override are highlighted in **bold**:

```
<html>
<head>
</head>
<body>
<!--YOUR HTML-->
<form method="POST"
action="https://payments.securetrading.net/process/payments/choice">
<input type="hidden" name="sitereference" value="test_site12345">
<input type="hidden" name="stprofile" value="default">
<input type="hidden" name="currencyiso3a" value="USD">
<input type="hidden" name="mainamount" value="100.00">
<input type="hidden" name="version" value="2">
<input type="hidden" name="paypaladdressoverride" value="1">
<input type="hidden" name="customerprefixname" value="Mr">
<input type="hidden" name="customerfirstname" value="James">
<input type="hidden" name="customerlastname" value="Thompson">
<input type="hidden" name="customerpremise" value="789">
<input type="hidden" name="customertown" value="Bangor">
<input type="hidden" name="customercountryiso2a" value="GB">
<input type="hidden" name="customerpostcode" value="TE45 6ST">
<input type="submit" value="Pay">
</form>
</body>
</html>
```

6 Security

To ensure the request to Secure Trading has not been modified by a malicious user, a field called **sitesecurity** can be included in the POST to the Payment Pages. This field contains a cryptographic hash of a predefined set of field values.



Any field that you do not want the customer to modify must be included in your site security hash. For example:

If you are submitting address details in the request to Payment Pages, you must include the fields in the site security hash in order to prevent the customer changing their address.

Follow the steps below to use this security feature:

Step 1: Field Selection

You will need to notify Secure Trading Support (see section **16.1**) of the fields to include in the hash. The default fields for new accounts are:

```
// currencyiso3a
// mainamount
// sitereference
// settlestatus
// settleduedate
// authmethod
// paypaladdressoverride
// strequiredfields
// version
// stprofile
// ruleidentifier
// stdefaultprofile
// successfulurlredirect
// declinedurlredirect
// successfulurlnotification
// declinedurlnotification
// merchantemail
// allurlnotification
// stextraurlnotifyfields
// stextraurlredirectfields
// password
```

Secure Trading recommends including as many unique fields when creating the hash as possible. Including only the **merchant** and **currency** fields will end up creating the same hash even though the amount field may have been compromised. To prevent anyone from changing the amount, we recommend including the **mainamount** field.



Please note that although the fields **authmethod**, **settlestatus** and **settleduedate** are optional, they can affect settlement. Even if these fields are not submitted to Secure Trading, we recommend including them when you set up the fields with support. The way the hash is generated will not change, but it will mean that a malicious user will not be able to affect the settlement of a transaction through your account.

Once the fields have been chosen, you will need to provide Secure Trading with a password that is appended to the end of the hash. If you would like to change the password or add/remove fields from the hash you must notify Secure Trading support.



Secure Trading will never ask for your Site Security password after first-time configuration. Never share your Site Security password with third parties. Do not store hard copies of this password.

Payment Pages Setup Guide

Step 2: Hash Generation

You will need to set up your system to generate the hash using the SHA-256 algorithm. When generating the hash, only the field **values** are used.



Please note that although we continue to support MD5 & SHA-1 hashing algorithms for existing merchants, we strongly recommend all merchants move to using SHA-256, which is more secure.



Please note that the order of the fields within the hash must be correct. If the correct details are not supplied, the transaction will be stopped.

For example, consider a request with the following fields:

Field Name	Field Value	Position
currencyiso3a	USD	1 st
mainamount	100.00	2 nd
sitereference	test_site12345	3 rd
settlestatus		4 th
settleduedate		5 th
authmethod		6 th
paypaladdressoverride		7 th
strequiredfields		8 th
version	2	9 th
stprofile	default	10 th
ruleidentifier		11 th
successfulurlredirect		12 th
declinedurlredirect		13 th
successfulurlnotification		14 th
declinedurlnotification		15 th
merchantemail		16 th
allurlnotification		17 th
stextraurlnotifyfields		18 th
stextraurlredirectfields		19 th
password	PASSWORD	20 th

Using the example above, we would have the following string generated:
USD100.00testsite_123452defaultPASSWORD

(Any blank fields are omitted from the hash)



If the fields are not in the correct order, the request will fail.
The password must **always** be at the end of the string.

If a field included in the hash has multiple values:

These values are concatenated in the order submitted in the POST to Secure Trading. Consider the following additional fields:

(e.g. `fieldname=bravo&fieldname=alpha`),

When included in the string generated above, it becomes:

USD100.00testsite_123452default**bravoalpha**PASSWORD

Example

Python Example

```
#!/usr/bin/python

import hashlib
stringToHash= "USD100.00test_site123452defaultPASSWORD"
print hashlib.sha256(stringToHash).hexdigest()
```

PHP Example

```
<?php
echo hash("sha256", "USD100.00test_site123452defaultPASSWORD");
?>
```

Java Example

```
import java.math.BigInteger;
import java.security.MessageDigest;
public class mysha256 {
    public static void main(String args[]) throws Exception {
        String stringToHash = "USD100.00test_site123452defaultPASSWORD";
        MessageDigest digestObj = MessageDigest.getInstance("SHA-256");
        digestObj.update(stringToHash.getBytes());
        String merchantHash = String.format("%064x", new
        BigInteger(1, digestObj.digest()));
        System.out.println(merchantHash);
    }
}
```

Perl Example

```
#!/usr/bin/perl

use Digest::SHA qw(sha256_hex);
$stringToHash = "USD100.00test_site123452defaultPASSWORD";
$merchantHash = sha256_hex($stringToHash);
print $merchantHash;
```

Step 3: Submitting the Hash

The field **sitesecurity** must be included in the post to the Payment Pages. The value of **sitesecurity** needs to be the hash generated. To ensure the latest version of the site security feature is used, the hash must be prefixed with a “g” before submitting to Secure Trading. For more information, see 3.1.



Please note that it is important that the generated hash is prefixed with a “g”. Failure to do so could invalidate the hash and stop legitimate transactions.

For any payment that is attempted with an incorrect hash, the customer will be presented with an error (such as shown in **Figure 13**) and no payment will be processed.



There has been a problem with your payment:

Invalid details

Figure 13 - Security Hash mismatch error

Example of URL with Security Hash

Using the same values from the steps, above, here is an example of a request to Payment Pages with the `sitesecurity` field appended (using the `sha256` algorithm type):

```
<html>
<head>
</head>
<body>
<!--YOUR HTML-->
<form method="POST"
action="https://payments.securetrading.net/process/payments/choice">
<input type="hidden" name="sitereference" value="test_site12345">
<input type="hidden" name="stprofile" value="default">
<input type="hidden" name="currencyiso3a" value="USD">
<input type="hidden" name="mainamount" value="100.00">
<input type="hidden" name="version" value="2">
<input type="hidden" name="orderreference" value="myorder12345">
<input type="hidden" name="sitesecurity"
value="ge3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b8
55 ">
<input type="submit" value="Pay">
</form>
</body>
</html>
```

This ensures that if the customer modifies any of the fields used to create the hash that are passed in the request, Secure Trading will not process the payment (as when the hash is re-generated on Secure Trading's systems, the values will differ).

7 Additional Request Types

This section describes the additional request types that can be processed along with a payment processed through Payment Pages. To enable these request types on your site please contact Secure Trading support. For more information, see section 7.6.

7.1 Risk Decision

The purpose of Risk Decision requests is to minimise fraud by analysing customer details and highlighting possible fraudulent activity by using Secure Trading's Fraud Control system. This is to assist you in making a decision of whether or not to process a customer's transaction, based on the perceived level of risk.

This is achieved by checking the industry's largest negative database and also searching for suspicious patterns in user activity. The system uses neural-based fraud assessments that can be configured specifically for your account and is constantly updating the fraud checks used to combat new risks.

Based on the decision returned by the Fraud Control system a customer that is deemed as suspicious can be prevented from processing a payment.

To enable Fraud Control on your account, please contact Secure Trading Support (see section 16.1).

7.1.1 Process

Once the customer submits their details to the Payment Pages a Risk Decision assessment is processed by the Fraud Control system, where the billing, delivery and payment details are analysed by a rule-based system and includes:

- // The industry's largest negative database.
- // Neural-based fraud assessments.
- // Tumbling or swapping, where there is an unusual usage pattern in the card number, expiration date or customer details associated with a transaction.



Please note dependent on your Fraud Control profile, the rules can be configured specifically for your account. For more information, contact Secure Trading Support (see section 16.1).

The Fraud Control system will analyse these details and respond with one of the following results:

- // **ACCEPT** - The details are not deemed suspicious.
- // **DENY** - The details are suspicious and a transaction should not be performed.
- // **CHALLENGE** - Further investigation is recommended.

7.1.2 Performing Authorisations automatically based on Risk Decision responses

Based on the result of the Risk Decision, you can decide whether to automatically proceed with the Authorisation or not. By default, the Payment Pages have the following process flow:

1. If the Risk Decision returns an Accept, then continue with the authorisation.
2. If the Risk Decision returns a Challenge or Deny, then process the authorisation, but suspend the transaction allowing for further investigation.



Please note the default process flow can be customised. For example, you could choose not to process the authorisation if the Risk Decision returns a Deny. For more information, contact Secure Trading Support (see section 16.1).

Payment Pages Setup Guide



Please note the test details to use with the Secure Trading test Fraud Control system can be found in section **14.3**.

7.1.3 Additional fields

The following optional fields can be posted to the payment pages to improve the Fraud Control risk decision process:

Field Name	Details
billingdob	The Customer's Date of Birth. Must be in the format YYYY-MM-DD.
customershippingmethod	The shipping method. Can be one of the following values: <ul style="list-style-type: none"> // C = Low Cost // D = Designated by Customer // I = International // M = Military // N = Next Day/Overnight // O = Other // P = Store Pickup // T = 2 day Service // W = 3 day Service



Secure Trading recommends submitting as much data as possible to assist the Fraud Control risk decision process.

7.2 Account Check

An Account Check is an optional request to help minimise fraud. It allows payment details to be validated, and checks that the details entered by the customer matches those on the card issuer's records. No funds will be reserved or transferred by the Account Check request.



Please note that Account Checks are only available for certain Acquiring Banks. Please contact the Secure Trading support team for more information (see section **16.1**).

Payment Pages Setup Guide

The checks performed by an Account Check Request consist of the following:

- # Use of the Address Verification System (AVS) to check if the provided first line of the billing address for the customer matches that on the card issuer's records.
- # Checks to see if the billing postcode provided by the customer matches that on record for their card.
- # Checks to see if the security code (CVV2) provided by the customer matches that on record for their card.



Please note that the checks performed on an Account Check Request are the same as those carried out on a regular e-commerce Authorisation (AUTH) Request.

Please refer to the **STPP AVS & CVV2** document (see section 16.3) for further information on address and security code checks.

No funds will be reserved as part of an Account Check.

The results of these checks are returned in the security response of the Account Check. The security response consists of three different fields, each containing the result of an individual check. The names of the fields are listed, below:

Field name	Comment
<code>securityresponseaddress</code>	The results of the checks performed by the AVS on the first line of the billing address.
<code>securityresponsepostcode</code>	The results of the checks on the billing postcode.
<code>securityresponsesecuritycode</code>	The results of the security code checks.

An Account Check Request will analyse the details provided by the customer and respond with the following results for each check performed:

Security response value	Description	Comment
0	"Not Given"	Your bank was not provided with the information required to perform this check.
1	"Not Checked"	Your bank was unable to perform checks on the information provided.
2	"Matched"	The information provided by the customer matches that on the card issuer's records.
4	"Not Matched"	The information provided by the customer does NOT match that on the card issuer's records.

For example, if the `securityresponseaddress` and `securityresponsepostcode` have a value of 2, but the `securityresponsesecuritycode` has a value of 4, this indicates that the first line of the address and the postcode match those on the card issuer's records, but the security code (CVV2) entered by the customer does not match the code found on the back of their card.

Payment Pages Setup Guide

Alternatively, you can view security responses in the Single Transaction View for the Account Check transaction in MyST (see **Figure 14**). Please refer to the MyST User Guide (see section **16.3**) for more information.

Security Response			
Security code	Matched	House no.	Matched
Postcode	Matched		

Figure 14 - Security Response in MyST



If an amount is submitted in an Account Check Request, it is only stored for the purpose of inheritance by future requests (such as performing a later Authorisation request), which refers to this parent Account Check transaction. The amount sent in an Account Request is not reserved, as Account Checks never reserve funds.



Please note that the `settlestatus` submitted with an Account Check will be inherited by any subsequent requests that refer to it as a parent.

Account Check requests can be processed for all payment types, which are supported by your acquirer that can process Account Checks through Secure Trading.

To enable Account Check on your account, please contact Secure Trading Support (see section **16.1**).

7.2.1 Account Check Rules (opt-in)

Optional rules can be enabled on your account by the Secure Trading Support team, which will use the results of the Account Check to decide whether or not to process an associated Authorisation transaction. The recommended process flow is as follows:

1. If the Account Check returns a **'Matched'** Response, then process the Authorisation.
2. If the Account Check returns a **'Not Checked'** Response, then process the Authorisation, but suspend the transaction allowing for manual investigation to take place.
3. If the Account Check returns a **'Not Matched'** Response, then do **NOT** process an Authorisation.



The process flow above can be customised. For example, you could choose to process the Authorisation if the Account Check returns **'Not Matched'**.

To configure rules for Account Checks, please contact Secure Trading Support (see section **16.1**).

7.2.2 ACH Account Checks

You can also perform Account Checks with payments processed using the Automated Clearing House (ACH) payment method, but please be aware that there are differences in the nature of checks performed, as described below:

7.2.2.1 Account Verification Check

Your bank will perform checks to verify that the customer's account is valid and in good standing. The response returned following these checks indicates the level of risk associated with processing transactions using the account details provided by the customer. Transactions that do not receive a definitive response may be checked against the negative database (see section 7.2.2.2).



Please note that the availability of the Negative Database check will depend on the configuration of your account by your acquirer. Please contact your acquirer for further information.

7.2.2.2 Negative Database Check

Your bank may also search a large National database for negative reports against the payment details submitted in your request. This database contains information on over 150 million accounts. This information can be used to determine if the account details are low risk or high risk (these are the only responses possible during this check).

7.2.2.3 Security Response for ACH Account Checks

After performing an ACH Account Check, you are returned a security response from the acquiring bank, in the form of a number, which indicates the result of the checks performed on the customer's bank account details. The `securityresponsesecuritycode` field within the security response provides the result of the checks performed by your acquiring bank on the customer's payment details.

The table below lists all of the possible security responses that can be returned in the `securityresponsesecuritycode` field:

Security response	Comment	MyST description
1	Undetermined risk: The acquiring bank was unable to complete checks on the information you provided in the request.	"Not Checked"
2	Low risk: The information you provided in the request is deemed low or medium risk by the acquiring bank and is therefore considered acceptable for further transactions.	"Matched"
4	High risk: The information you provided in the request is deemed high risk by the acquiring bank and is therefore considered inappropriate for further transactions.	"Not Matched"



Secure Trading recommends against proceeding with further transactions using payment details that return a high risk (4 – "Not Matched") response.



When performing combined ACH Account Check and Authorisation Requests, it is recommended that you set up rules, which use the results of the Account Check carried out by the acquiring bank to either allow or prevent future authorisations. See section 7.2.2.4.

Payment Pages Setup Guide

7.2.2.4 ACH Account Check Rules

Rules can be assigned on your account by the Secure Trading support team, which will use the results of the Account Check to decide whether or not to process an associated Authorisation transaction. The recommended process flow is as follows:

- // If the Account Check returns a low risk (2 – “**Matched**”) or undetermined risk (1 – “**Not Checked**”) response, then process the Authorisation.
- // If the Account Check returns a high risk (4 – “**Not Matched**”) response, then do **NOT** process an Authorisation.



Please note the default process flow can be customised. For more information, contact Secure Trading Support (see section **16.1**).

7.3 3-D Secure

3-D Secure is a protocol designed to reduce fraud and Chargebacks during e-commerce Internet transactions. Cardholders are asked to identify themselves at the point of sale before the purchase can be completed. This usually means entering a PIN or other password after entering their credit card details.

In the event of a dispute with the transaction at a later date, the card issuer will usually take responsibility of the Chargeback instead of the merchant. The liability issues involved with 3-D Secure transactions are out of the scope of this document. For a detailed indication of the liabilities involved, contact your bank.

3-D Secure transactions may be processed to reduce the likelihood of fraudulent transactions on your account. It may take several weeks to enable 3-D Secure depending on your acquirer. Please contact Secure Trading support for more information (see section **16.1**).



Please note that only certain payment types support 3-D Secure.

7.3.1 Process

A THREEDQUERY request is used to determine whether the customer’s card is enrolled in the 3-D Secure scheme. The THREEDQUERY request submits information to a directory server hosted by a card issuer (e.g. Visa). If the card is in the 3-D Secure scheme, then after the customer has entered their payment details, they will be redirected to a log-in screen that enables them to validate their identity through an Access Control Server (ACS), hosted by their card issuer.



Please note that the size of the ACS page displayed in the customer’s browser is controlled by the ACS provider (cannot be modified by merchants or Secure Trading).

As a guideline, Visa US states that the Verified by Visa authentication window should be 390x400 pixels in size.

Payment Pages Setup Guide

7.4 Subscription

Subscription payments allow transactions to be automatically re-processed without the need for the customer to re-enter their payment details e.g. payments can be scheduled to be processed on the first of each month for £10.00.

7.4.1 Process

Processing a Subscription payment is the same as processing a standard Authorisation using the Payment Pages, with additional fields included to schedule the subscription. The additional fields define how many Subscription payments are to be processed and the gap between these payments.

Once the initial transaction is processed, the subsequent Subscription payments are scheduled to be processed by the Secure Trading Subscription Engine.

For more information, refer to the **STPP Subscriptions and Payment Pages** (see section 16.3).

7.5 Currency Rate

Currency Rate Requests are used when performing Dynamic Currency Conversion (DCC) transactions. The CURRENCYRATE Request contains the currency information required for the currency conversion provider to return a conversion rate based on the current rates. By enabling CURRENCYRATE Requests on your Payment Pages, the customer is able to choose an alternative currency in which to perform the payment, provided their card supports the currency conversion.



Please note that in order to perform DCC, you will need to have a merchant number that allows this functionality. For more information, please contact your acquiring bank.

In addition, an account with a currency rate provider is required. To set up a currency rate provider on your Secure Trading account, please contact Secure Trading Sales (see section 16.2).

7.5.1 Process

The steps to process a payment with a CURRENCYRATE request are the same as processing a standard authorisation using the Payment Pages (see section 3), with additional DCC fields included in the request. A DCC payment consists of two parts:

1. A CURRENCYRATE Request – Requests an up-to-date conversion rate from a DCC provider.
2. An AUTH Request – Requests the acquiring bank to authorise the payment in the customer's preferred currency.



Please note that in certain configurations, these additional fields are not required. Please see section 7.5.4, for more information.

The customer is initially shown a choice page, where they can select the payment type that they wish to use. This is the same as the normal payment type choice page, except the amount is initially hidden (Figure 15). This is because the currencies and respective amounts to be offered to the customer have yet to be established.

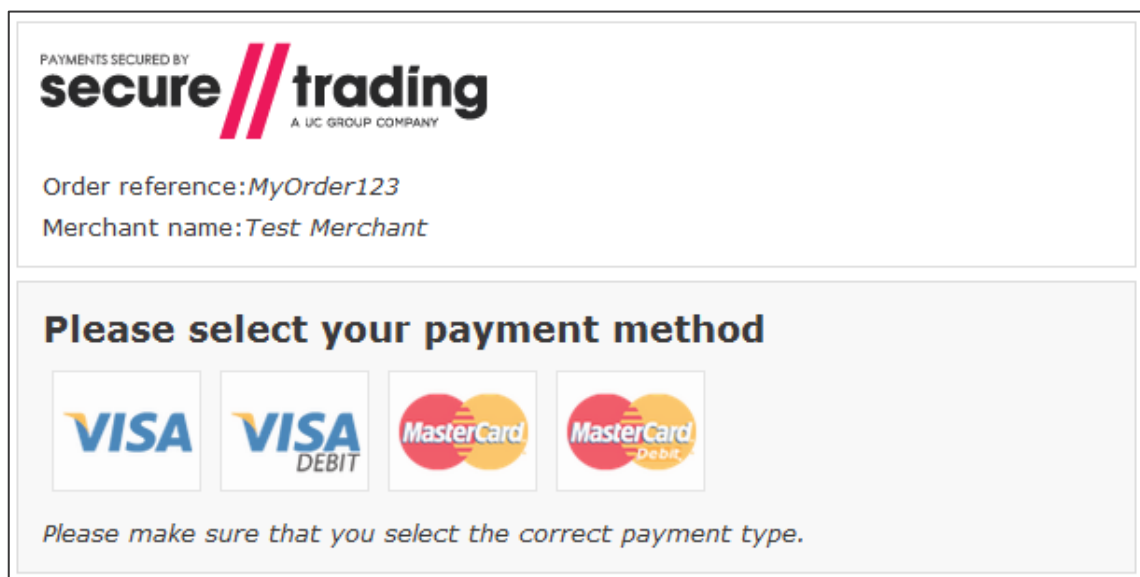


Figure 15 - DCC Payment Pages: Payment type choice page

Payment Pages Setup Guide

If the customer chooses a payment type that supports DCC, they are informed that they are able to pay in an alternative currency to the merchant currency submitted, as shown in **Figure 16**. Here they will be able to see the amount in the merchant currency.



Secure Trading's implementation of DCC is currently only supported by MasterCard and Visa branded cards.


Payment Details

Card number *

Expiry date *

Security code *

Security code is on the back of your card



Currency Details

Your card will be validated and then verified that it can perform international transactions.

You will be given the choice to pay in your currency at a specific exchange rate or pay in (GBP) **£123.99**

[Next](#)

* Indicates a required field

Figure 16 - DCC Payment Pages: DCC first page

Secure Trading will use the card number (PAN) entered by the customer to establish their local currency, by submitting the information in a CURRENCYRATE Request. The conversion rate partner will supply a conversion rate that is used to convert the amount in the merchant currency to an amount in the customer's local currency.



Please note that if the cardholder's local currency is the same as the currency you submitted, the customer will not be shown a conversion rate and instead will make the payment in your account's currency.




Please note that amounts paid in the customer's currency have a small fee added to them to cover the cost of the conversion by the third-party conversion rate provider. This fee is determined by calculating a percentage of the amount in the customer's currency and adding this to the total amount. For more information, please contact your conversion rate provider.

Payment Pages Setup Guide

The amounts in both currencies are displayed on the payment page. The customer will be able to choose between paying in either currency (**Figure 17**).

Payment Details

If you change your card number you will be offered another opportunity to select the transaction currency.

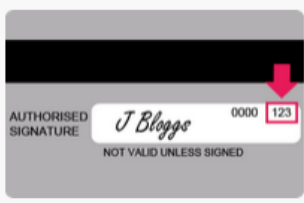


Card number *
4111111111111111

Expiry date *
02 2017

Security code *
123

Security code is on the back of your card



Currency Details

Pay in your currency (USD) **\$193.74**

The exchange rate of 1.5626 is based on *name of bank* rate plus a 2.50% international conversion margin as returned on 2015-05-28. This is not an additional fee, and replaces currency conversion charges normally applied. The currency conversion service is provided by *conversion rate provider*.

Pay in the merchant currency (GBP) **£123.99**


If GBP is not the currency of the card, the exchange rate will be determined by your card issuer at a later date without further consultation.

Cardholder choice is final.

Pay Securely

* Indicates a required field

Figure 17 - DCC Payment Pages: "DCC" currency choice page for Visa




If the customer changes their card number (PAN) at this stage, before clicking "Pay", Secure Trading will need to perform a new CURRENCYRATE Request to re-establish the customer's local currency using the new card. The customer will be redisplayed the billing details page (**Figure 16**) along with the following warning that the new amounts calculated may differ from the amounts previously shown:

⚠ You have changed your payment details. The amount in your local currency will be recalculated and may differ from the amount previously shown.

Once the payment currency has been selected, a subsequent AUTH Request is performed by Secure Trading to your acquiring bank. This uses the currency and respective amount chosen by the customer on the Payment Pages.

7.5.2 Response Page

Following a successful DCC payment, the customer is shown a response page with details of the transaction processed (Figure 18). This includes information on the currency conversion performed on the transaction.

PAYMENTS SECURED BY

A UC GROUP COMPANY

✔ **Successful**

Receipt

Transaction reference: <i>42-67-1</i>	Order reference: <i>MyOrder123</i>
Auth code: <i>000001</i>	Payment type: <i>Visa</i>
Card number: <i>#####1111</i>	Merchant name: <i>Test Merchant</i>

Conversion Details

Transaction amount:
\$193.74

Transaction currency:
USD

Exchange rate:
1.5626

Margin:
2.50%

Bank:
name of bank

The exchange rate of 1.5626 is based on **name of bank** plus a 2.50% international conversion margin as returned on 2015-05-28. This is not an additional fee, and replaces currency conversion charges normally applied.

I recognise that I was given a choice of payment currencies and that I could have paid in GBP £123.99 . I accept the Exchange Rate used to perform the currency conversion and that my decision to pay in USD is final.

The currency conversion service is provided by **conversion rate provider**.

Billing Details

Ms Paying Customer

No 789
Test Street
Bangor
Gwynedd
United Kingdom
TE45 6ST

customer@email.com
Home 01234567890

Retain this copy for statement verification.
*Please **print** this page for your records.*

Delivery Details

Ms Paying Customer

No 789
Test Street
Bangor
Gwynedd
United Kingdom
TE45 6ST

customer@email.com
Home 01234567890

Figure 18 - Response page following a DCC transaction

7.5.3 Required DCC Disclaimer Text

Secure Trading actively ensures that the text shown in the default Payment Pages for DCC payments complies with rules specified by the relevant card schemes and third parties. For this reason, we strongly recommend against modifying any of the text shown relating to the currency conversion performed and the exchange rates provided, both on the billing details and receipt pages.



If you customise your site's Payment Pages, it is your responsibility to ensure your solution is still compliant with all rules specified by relevant card schemes and third parties.

7.5.4 Configuration

To set up DCC on your Secure Trading account, please contact the support team (see section 16.1). There are two ways that DCC can be enabled on your account.

1. The support team can configure your live site in such a way that all requests, where the customer's payment type supports DCC, are processed as DCC. The request you make to the payment pages remains unchanged from a standard Authorisation.
2. Appending "`dcctype=DCC`" to your POST (see section 3.1) will result in DCC being performed on a request, if the customer's payment type supports it. Not including these fields in your POST will result in normal Authorisation Requests without the customer being able to choose an alternative currency.



Ensure you only submit currencies supported by your account.

7.5.5 DCC Fields

Following CURRENCYRATE Requests, Secure Trading returns additional DCC fields for future reference, as listed in the table, below.

These fields are displayed in the “**Single Transaction View**” for the CURRENCYRATE and AUTH Requests in MyST (please refer to the **MyST User Guide** in section 16.3, for more information).



Please note that a CURRENCYRATE Request is only shown as a parent (in the Related Transactions tab) to the child DCC AUTH Request when the customer has opted to pay in an alternative currency (when **offered** is ‘1’).

It is possible to view CURRENCYRATE Requests associated with any DCC AUTH Request in MyST submitting the **orderreference** on the transaction search page. The **orderreference** for the CURRENCYRATE is the same as the AUTH.

The fields can be returned in a URL POST or email on completion of a transaction. For further information, please refer to section 9. When adding a destination, please select the fields shown below in order to include DCC information:

Field name	Comment
dccbaseamount	The base amount the customer has paid in the submitted currency (£10.50 is 1050).
dcccurrencyiso3a	The currency you submitted in the POST to Payment Pages.
dccenabled	Whether or not DCC is enabled on your account. 1 - Your Secure Trading account is enabled for DCC. 0 - Your Secure Trading account is not enabled for DCC.
dccconversionrate	The conversion rate used to convert the amount in the submitted currency to the amount in the customer’s currency.
dccconversionratesource	The source of the conversion rate provided by the DCC provider.
dccmainamount	The main amount the customer has paid in the submitted currency (£10.50 is 10.50).
dccmarginratepercentage	The percentage used to calculate the currency conversion fee, applied to the amount in the customer’s currency.
dccoffered	This value represents whether the customer has chosen to pay in the submitted currency or their local currency. 1 - Customer has chosen to pay in their local currency. 2 - An error has occurred, which has prevented the customer from paying in their local currency, so they are paying in the submitted currency, instead. 3 - The customer has chosen to pay in the submitted currency.
dccprovider	The institution that provides the conversion rate.
dcctype	“DCC”

Payment Pages Setup Guide

7.5.6 Updating DCC Authorisations

It is possible to perform transaction updates to DCC Authorisations, by using MyST (please refer to the **MyST User Guide** in section 16.3, for more information). It is **NOT** possible to change the currency of the payment after it has been authorised by the acquiring bank. When updating the settle amount, it is in the amount in the currency chosen by the customer to make the payment that will be changed.



Deferred settlement is **NOT** supported for DCC transactions.

7.5.7 Refunding settled DCC transactions

STPP supports the refunding of DCC transactions. Please consider the two options available:

7.5.7.1 Option 1 – Perform a refund using MyST

A new CURRENCYRATE transaction is performed when performing a refund through the MyST, in order to refund the customer in their chosen currency using an up-to-date conversion rate.



Instructions on how to perform refunds using MyST can be found in the **MyST User Guide**. All Secure Trading documents can be found on [our website](#).

7.5.7.2 Option 2 – Submit an XML Refund Request using STAPI / Web Services

You can choose to use the same currency conversion rate as the original transaction or perform a new CURRENCYRATE transaction in order to obtain an up-to-date currency conversion rate.



For information on performing refunds for DCC transactions using STAPI / Web Services, please consult the following documentation:

- **[XML Specification document](#)**
- **[Web Services User Guide](#)**
- **[DCC XML Specification](#)**

All Secure Trading documents can be found on [our website](#).

7.5.8 Subscriptions with DCC Payments

Secure Trading does not support the use of DCC payments with Subscriptions.

7.6 How to configure Additional Request Types

Once enabled, Additional Request Types are automatically processed with every payment made through your payment page, without any additional configuration on your system. To enable any of the request types outlined in this section on your Secure Trading Payment Pages account, please contact Secure Trading support (see section 16.1).



Please note that Subscriptions require additional fields to be submitted in order to be scheduled in the Secure Trading Subscription Engine. For further information, please refer to the [STPP Subscriptions and Payment Pages](#) document.



Please note that Currency Rate Requests may require additional fields to be submitted in order to process currency conversions. Please see section 7.5.4, for further information.



For advanced functionality, Secure Trading offer an Enhanced Post feature, which allows you to specify which request types are processed for individual transactions through the Payment Pages. For further information, see section 10.

8 Customisation

Secure Trading allows merchants to customise their Payment Pages solution by uploading files to their account using MyST and modifying the HTTPS POST to reference these files.



Merchant's Payment Pages are called.



Custom files are called to restyle the Payment Pages.



Customised Payment Pages are displayed to the customer.



The steps required to customise the Payment Pages can be found in the [Payment Pages Customisation](#) document.

This supplement can be viewed using the following URL:
<http://www.securetrading.com/paymentpages/customisation.html>

8.1 Custom logo

You can easily update your Payment Pages to display your own logo, without needing to write any custom mark-up. This is shown alongside a small "Payments by Secure Trading" icon.

**YOUR LOGO
HERE**

Payments by
secure // trading

Amount: £1.23 GBP
Merchant name: Test Merchant

Please select your payment method

AMERICAN EXPRESS

VISA

MasterCard

PayPal

Please make sure that you select the correct payment type.

To configure, sign in to MyST, click "File manager" from the options on the left, and upload an image called "merchantlogo". We support the following image extensions: bmp, gif, jpeg, jpg, png, svg, tif, tiff.

9 Rules

When enabled, Secure Trading will perform certain actions on requests processed on your site reference using rules configured on your account.



The following information will explain how to use rules in conjunction with your Payment Pages implementation. It is recommended that you read this in conjunction with the [MyST Rule Manager supplement](#), which provides information on managing your rules.

9.1 Rule types

9.1.1 Secure Trading Rules

Rules with a Rule ID of “STR-x” (where x is a number) are Secure Trading Rules. e.g. STR-1



Rules and site security

If you are enabling Secure Trading Rules (starting with “STR-“), you must ensure you are using the latest version of site security, otherwise this could affect your service and the ability to process payments.

How to check if you are using the latest version:

- If the site security hash starts with the letter “g” you are using the new version.
- If the site security hash does not start with the letter “g” you are using the old version.

For information on the latest version of site security, refer to section 6. If you are unsure, contact Support for further assistance (section 16.1).

Secure Trading provides a number of pre-defined rules that can be activated on any of your site references (inactive by default). These rules are displayed within the rule manager interface in MyST and can be activated or deactivated by following the instructions outlined in the [MyST Rule Manager supplement](#). Secure Trading Rules are always performed before User-Defined Rules.

9.1.2 User-Defined Rules

Rules with a Rule ID of “UDR-x” (where x is a number) are User-Defined Rules. e.g. UDR-19 Using MyST, you can create, modify and activate your own custom rules on any of your site references.

For example, rules can be used to redirect the customer from the Payment Pages and back to your website, following a transaction. Please see section 9.4 for a walkthrough guide.

Further information on User-Defined Rules can be found in the [MyST Rule Manager supplement](#).

Payment Pages Setup Guide

9.2 Activating rules

9.2.1 Using MyST

Rules can be activated/deactivated on any of your site references by using the MyST Rule Manager. This can be used to easily activate rules on **ALL** of your processed requests, without having to modify your code. You must have a MyST account with role site admin, developer or developer 2 to use the Rule Manager.

Clicking on the “**Rule manager**” link on the left-hand side of the MyST screen will display the rules currently configured (if any) on the selected site. Tick the “Active” checkboxes next to the rules you would like to activate, and then click “**Save**”.

To deactivate rules, remove the ticks from the checkboxes and click “**Save**”.

Rule manager

Site reference
site12346

Type of action
ALL

Change

Information

Description
A rule is an action that is automatically run by Secure Trading based on conditions you have chosen. You may choose from a selection of pre-defined Secure Trading rules (STR) or, alternatively, you can create your own user defined rule (UDR).

Getting started
On the left hand side, select a site reference, choose the action type and click the “Change” button.

Please note:
It is advised that all new rules are tested via your test site before being applied to your live site.

Existing rules for site12346
Manage conditions
Manage actions

ID	Condition	Action	Active	Delete
STR-1	If a response matches Auth security code not matched	then Update a response to Merchant decline	<input type="checkbox"/>	<input type="checkbox"/>

Save

9.2.2 In the POST to Secure Trading

Rules can be activated for individual requests by submitting the unique rule identifier in the **ruleidentifier** field. Rules specified in the request will cause Secure Trading to perform certain actions if pre-defined criteria are met (regardless of whether or not said rules are active on your site references). The following code snippet is from an HTML form where two rules **STR-1** and **STR-2** are specified:

```
<form method="POST"
action="https://payments.securetrading.net/process/payments/choice">
...
<input type="hidden" name="ruleidentifier" value="STR-1">
<input type="hidden" name="ruleidentifier" value="STR-2">
...
<input type="submit" value="Pay">
</form>
```

9.3 Merchant Decline Rule (STR-1)



Please note that this rule is only supported by acquirers and payment methods that support security code checks.

When active, the STR-1 rule will automatically cancel transactions (update the settle status to 3) when the security code entered by the customer does not match the value held on the bank's records.

A "Merchant Declined" message will be displayed to your customers on the Payment Pages when they enter an incorrect security code.



If you intend to implement the merchant decline rule on a site reference where redirect and/or notification rules are already active, you should review section 9.3.1 and update your rules as required. Contact Support (see section 16.1) if you require further assistance.



Please note that if activated, the rule will also be enabled on payments processed using the Virtual Terminal, where a message of "Transaction Failed" will be displayed.

9.3.1 For merchants with existing rules

When a transaction is cancelled by an update transaction response rule (e.g. Merchant Decline), the error code may remain in status "0" (Ok). This would indicate that the payment was authorised by the acquiring bank, but later cancelled by Secure Trading. Therefore, you may need to update any active rules to take this possible outcome into account. To prevent a rule from being triggered on a merchant decline, remove the settle status "3" (Cancelled) from existing conditions on the affected site reference(s).



When creating new conditions using the MyST Rule Manager, we will automatically deselect settle status "3" when you select errorcode of "0", by default.

9.4 Payment Pages Advanced Redirects

For each transaction processed on the Payment Pages, you can specify a URL for the customer to be redirected to at the end of the payment. This allows you to host your own response page, in place of the page hosted by Secure Trading.



Please note that the URL of your hosted response page must be externally facing. Secure Trading cannot redirect to internal, intranet or loopback addresses.



We recommend only redirecting to secure HTTPS pages. When using iframes, some web browsers will refuse to redirect to non-secure pages as a security measure.

9.4.1 For successful transactions

Add the following highlighted fields to your HTTPS POST in order to redirect customers following a successful Payment Pages transaction:

- # **ruleidentifier** of "STR-6" - This enables the successful redirect rule.
- # **successfulurlredirect** - This specifies the URL for the redirect.

```
<form method="POST"
action="https://payments.securetrading.net/process/payments/choice">
...
<input type="hidden" name="ruleidentifier" value="STR-6">
<input type="hidden" name="successfulurlredirect"
value="http://www.yourwebsite.com/successful">
...
<input type="submit" value="Pay">
</form>
```

9.4.2 For declined transactions

By default, Secure Trading will automatically handle declined payments, by redisplaying the details page and providing the customer with another opportunity to perform a payment.

However, if you would prefer to handle this scenario by redirecting the customer to a page hosted on your system, add the following fields to your HTTPS POST:

- # **ruleidentifier** of "STR-7" - This enables the declined redirect rule.
- # **declinedurlredirect** - This specifies the URL for the redirect.

```
<form method="POST"
action="https://payments.securetrading.net/process/payments/choice">
...
<input type="hidden" name="ruleidentifier" value="STR-7">
<input type="hidden" name="declinedurlredirect"
value="http://www.yourwebsite.com/declined">
...
<input type="submit" value="Pay">
</form>
```

9.4.3 Fields returned

The redirect will include the following fields of information:

```
// transactionreference
// requestreference
// orderreference
// sitereference
// errorcode
// settlestatus
// paymenttypedescription
```

If site security is enabled on your site, the redirect will also include the response site security hash, as documented in section 9.6.

If you would like to include additional fields, you can update your HTTPS POST to include **stextraurlredirectfields**. The following HTTPS POST example will include the billing first name, last name and email address in a redirect, in addition to the default fields listed above:

```
<form method="POST"
action="https://payments.securetrading.net/process/payments/choice">
...
<input type="hidden" name="ruleidentifier" value="STR-6">
<input type="hidden" name="successfulurlredirect"
value="http://www.yourwebsite.com/successful">
<input type="hidden" name="stextraurlredirectfields"
value="billingfirstname">
<input type="hidden" name="stextraurlredirectfields"
value="billinglastname">
<input type="hidden" name="stextraurlredirectfields"
value="billingemail">
...
<input type="submit" value="Pay">
</form>
```

9.4.4 Response site security

If site security is enabled on your site, all of the default fields **AND** any additional fields specified in the HTTPS POST are included in the response site security hash. Your system will need to re-calculate this hash and ensure it matches the hash returned from Secure Trading. This is explained in section 9.6.

Payment Pages Setup Guide

9.5 URL Advanced Notifications

URL advanced notification actions are requests sent from Secure Trading to a pre-defined URL. These notifications contain information about transactions processed on your Secure Trading account.



Please note that we do not support localhost, loopback or multicast IP ranges in the URL.

9.5.1 Notifications for all transactions

For URL notifications to be performed following any Payment Pages transaction, add the following fields to your HTTPS POST:

- # **ruleidentifier** of "STR-10" - This enables the all URL notification rule.
- # **allurlnotification** - This specifies the URL for the notification.

```
<form method="POST"
action="https://payments.securetrading.net/process/payments/choice">
...
<input type="hidden" name="ruleidentifier" value="STR-10">
<input type="hidden" name="allurlnotification"
value="http://www.yourwebsite.com/all">
...
<input type="submit" value="Pay">
</form>
```

9.5.2 Notifications for successful transactions only

For URL notifications to be performed following a successful Payment Pages transaction, add the following fields to your HTTPS POST:

- # **ruleidentifier** of "STR-8" - This enables the successful URL notification rule.
- # **successfulurlnotification** - This specifies the URL for the notification.

```
<form method="POST"
action="https://payments.securetrading.net/process/payments/choice">
...
<input type="hidden" name="ruleidentifier" value="STR-8">
<input type="hidden" name="successfulurlnotification"
value="http://www.yourwebsite.com/successful">
...
<input type="submit" value="Pay">
</form>
```

9.5.3 Notifications for declined transactions only

For URL notifications to be performed following a declined Payment Pages transaction, add the following fields to your HTTPS POST:

- # **ruleidentifier** of "STR-9" - This enables the declined URL notification rule.
- # **declinedurlnotification** - This specifies the URL for the notification.

```
<form method="POST"
action="https://payments.securetrading.net/process/payments/choice">
...
<input type="hidden" name="ruleidentifier" value="STR-9">
<input type="hidden" name="declinedurlnotification"
value="http://www.yourwebsite.com/declined">
...
<input type="submit" value="Pay">
</form>
```

9.5.4 Fields returned

URL notifications will include the following fields of information:

```
// transactionreference
// requestreference
// orderreference
// sitereference
// errorcode
// settlestatus
// paymenttypedescription
```

If site security is enabled on your site, the notification will also include the response site security hash, as documented in section 9.6.

If you would like to include additional fields, you can update your HTTPS POST to include **stextraurlnotifyfields**. The following HTTPS POST example will include the billing first name, last name and email address in a URL notification, in addition to the default fields listed above:

```
<form method="POST"
action="https://payments.securetrading.net/process/payments/choice">
...
<input type="hidden" name="ruleidentifier" value="STR-10">
<input type="hidden" name="allurlnotification"
value="http://www.yourwebsite.com/all">
<input type="hidden" name="stextraurlnotifyfields"
value="billingfirstname">
<input type="hidden" name="stextraurlnotifyfields"
value="billinglastname">
<input type="hidden" name="stextraurlnotifyfields"
value="billingemail">
...
<input type="submit" value="Pay">
</form>
```

9.5.5 Response site security

If site security is enabled on your site, all of the default fields **AND** any additional fields specified in the HTTPS POST are included in the response site security hash. Your system will need to re-calculate this hash and ensure it matches the hash returned from Secure Trading. This is explained in section 9.6.

9.5.6 Receiving the notification

You must configure your system to accept the incoming URL notifications on port 443. If the response site security hash is correct, your system must respond with an HTTP 200 OK response (e.g. "HTTP/1.0 200 OK") within 8 seconds of receiving a notification.

One notification is sent per transaction, but if your system does not respond, Secure Trading will continue to resend notifications for up to 48 hours until confirmation is received.

9.6 Response Site Security



This section is only relevant to merchants that have implemented site security on their Payment Pages solution. For more information on configuring site security for the first time, please see section 6.

If site security has been enabled on your Payment Pages solution, you will also receive a hashed `responsesitesecurity` value in any redirects and URL notifications sent to your system, following transactions processed using Payment Pages.

Secure Trading strongly recommends that you recalculate the `responsesitesecurity` hash returned, to ensure it has not been modified by a customer or third party and that the fields were sent by Secure Trading. This is generated using a similar method for the request site security, as previously described section 6. Please read on for further information.



If you are using custom (“UDR”) rules for URL notifications, you will need to opt-in to response site security when creating the action, but the method used to generate the hash remains the same.

Payment Pages Setup Guide

9.6.1 Hash generation

The hash is generated in the same way as when including site security in your HTTPS POST, except the order the fields are appended before they are hashed is different (as described in step 1 below).

Step 1

Append all **values** of the fields included in the redirect or URL notification in **ASCII alphabetical order**, with the password placed at the end (ignoring the **responsesitesecurity** field itself).



For information on ASCII alphabetical order, please refer to this Wikipedia page: <http://en.wikipedia.org/wiki/ASCII>



Please note that the password used when generating the hash is the same password previously agreed with Secure Trading Support when configuring site security for the HTTPS POST.

If you are using custom (“UDR”) rules for URL notifications, you can specify a different password when creating the action, if needed.

For example, consider a redirect or URL notification with the following fields:

Field Name	Field Value	Position
errorcode	0	1 st
orderreference	Order	2 nd
paymenttypedescription	VISA	3 rd
requestreference	RR555	4 th
settlestatus	0	5 th
sitereference	test_site12345	6 th
transactionreference	2-44-66	7 th
password	PASSWORD	8 th

Using the example above, we would have the following string generated:
0OrderVISARR5550test_site123452-44-66PASSWORD

(Any blank fields are omitted from the hash)



If the fields are not in ASCII alphabetical order, the hash you generate will be incorrect. The password must always be at the end of the string.

Payment Pages Setup Guide

Step 2

Hash the fields using the same algorithm used in the HTTPS POST (by default this is sha256).

This generates the value that should be returned in redirects and URL notifications with the field values specified in step 1:

e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855

Note: The response site security isn't prefixed with a "g" as in the request site security.

9.6.2 Check the hash matches

For valid redirects and URL notifications, the site security hash generated by Secure Trading must match the value you have generated using the steps in section 9.3.2.1. This indicates the redirect or URL notification has not been modified by the customer or third party and that it was sent by Secure Trading.

Merchant

Fields



Site Security



Secure Trading

Fields



Site Security



The Site Security hash generated by the merchant and Secure Trading match.

If the value of one of your designated fields (represented below by ●) has been altered, this will alter the hash from that calculated by Secure Trading. When you recalculate the hash on your servers, it will not match the hash submitted in the redirect or URL notification. In this case, you should contact Secure Trading Support for assistance (see section 16.1).

Merchant

Fields



Site Security



Secure Trading

Fields



Site Security



The Site Security hash generated by the merchant and Secure Trading **do not** match.

Do not accept the request and contact Secure Trading Support.

Payment Pages Setup Guide


9.7 Email notifications

You can request an email notifications be sent following transactions on the Payment Pages. The types of emails we can send on your behalf fall under two categories:

- # Customer emails
- # Merchant emails

9.7.1 Customer emails

These are sent to the email address specified in the `billingemail` field. They are designed to be sent to customers following payment, summarising the transaction and acting as a receipt of payment for their records. By default, they appear as follows:



Auth Confirmation 2015-06-03 09:28:18

Successful

Your request has been securely processed by Secure Trading on behalf of: Test Merchant.

We hope that you find our service satisfactory.

The details of the request are:


Request type description	AUTH
Merchant name	Test Merchant
Transaction currency	GBP
Transaction amount	£1.23
Auth code	000022
Transaction reference	42-67-25
First name	Paying
Last name	Customer
Email	customer@email.com
House name/no.	No 789
Street	Test Street
Town	Bangor
County	Gwynedd
Postcode	TE45 6ST
Country	United Kingdom
Order reference	MyOrder123

Secure Trading are not involved in the provision of goods and services ordered and paid for. If you have any issues with this transaction please contact the merchant as stated above.

Payment Pages Setup Guide

9.7.1 Merchant emails

These are designed to be sent to members of your company or organisation, and are sent to an email address of your choosing. By default, they appear as follows:



Auth Confirmation 2015-06-03 09:28:18

Successful

A request has been processed by Secure Trading for site reference: test_site12345. More information about the transaction can be found by logging into MyST at <https://myst.securetrading.net>

The details of the request are:

Request type description	AUTH
Merchant name	Test Merchant
Transaction currency	GBP
Transaction amount	£1.23
Auth code	000022
Transaction reference	42-67-25
First name	Paying
Last name	Customer
Email	customer@email.com
House name/no.	No 789
Street	Test Street
Town	Bangor
County	Gwynedd
Postcode	TE45 6ST
Country	United Kingdom
Order reference	MyOrder123

This e-mail was sent from a notification-only address that cannot accept incoming e-mail. Please do not reply to this message.

Payment Pages Setup Guide

9.7.1 Enabling emails

To enable email notifications on a transaction-by-transaction basis. For requests where you would like to receive email notifications, you will need to add the following fields to your POST to the Payment Pages:

```
<!--Sends email confirmation to the customer, following successful
transaction:-->
<input type=hidden name="ruleidentifier" value="STR-2">

<!--Sends email confirmation to the customer, following declined
transaction:-->
<input type=hidden name="ruleidentifier" value="STR-3">

<!--Sends email confirmation to the merchant, following successful
transaction:-->
<input type=hidden name="ruleidentifier" value="STR-4">

<!--Sends email confirmation to the merchant, following declined
transaction:-->
<input type=hidden name="ruleidentifier" value="STR-5">
```

```
<!--IMPORTANT: You also need to include the merchant's email address
for merchant emails to work-->
<input type=hidden name="merchantemail" value="merchant@email.com">
```

9.7.1.1 Further information on emails

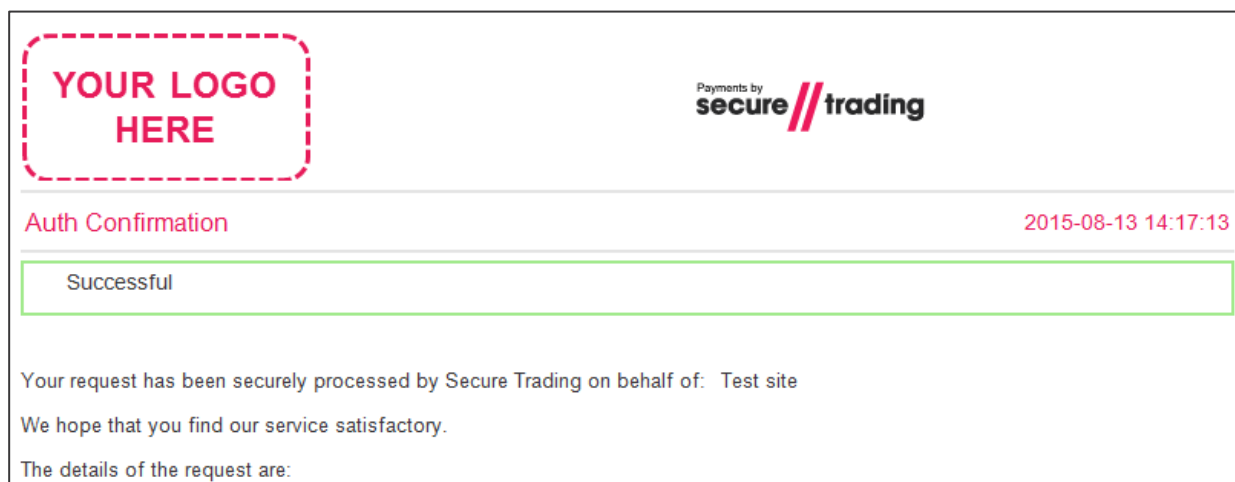
All emails are sent from no-reply@securetrading.com

Email notifications for successful transactions have the subject: "Successful transaction processed"

Email notifications for declined transactions have the subject: "Transaction declined"

9.7.2 Include your logo

You can include your logo at the top-left of the email. This is shown alongside a small "Payments by Secure Trading" icon.



To configure, sign in to MyST, click "File manager" from the options on the left, and upload an image called "emaillogo". We support the following image extensions: bmp, gif, jpeg, jpg, png, svg, tif, tiff.

10 Enhanced Post

Secure Trading allows for customisation of processed request types that are posted through the Payment Pages. A standard Payment Pages transaction consists of an Authorisation (AUTH) Request, which can be accompanied by any of the additional request types described in section 7. However, with Enhanced Post enabled on your account, you are able to choose to process combinations of specific request types by specifying the fields passed through in each HTTP Post.



Please note that to ONLY process a RISKDEC or ACCOUNTCHECK Request through the Payment Pages, without an associated AUTH, you must use the Enhanced Post feature.

10.1 Getting Started



Secure Trading recommends that you read section 3, before reading this section as it contains additional information which is relevant to this section.

To perform an Enhanced Post, you must first contact Secure Trading support (see section 16.1) to enable this functionality, and to specify all the request types you would like your site to be able to process. You can choose from the following:

Request Type	Description
AUTH	An Authorisation Request for a payment from a customer.
RISKDEC	A Risk Decision Request, to check for suspicious activity relating to the customer's account (see section 7.1 Risk Decision).
ACCOUNTCHECK	An Account Check Request, to check the status of the customer's account (see section 7.2 Account Check). Only available for certain acquiring banks; contact Support for further information (section 16.1).
THREEDQUERY ¹	A 3-D Query Request, to perform 3-D Secure on the customer's account, if they are enrolled (see section 7.3 3-D Secure).
SUBSCRIPTION ²	A Subscription Request, where payments will be processed automatically at pre-specified intervals (see section 7.4 Subscription).
CURRENCYRATE ¹	A Currency Rate Request, to perform currency conversion between two different currencies (see section 7.5 Currency Rate).
ORDER ¹	An Order Request, used to initiate a payment using PayPal. Required when offering PayPal as a payment option
ORDERDETAILS ¹	An Order Details Request, used to retrieve updated information about the transaction from PayPal after the customer has logged in and confirmed the payment (optional). See section 10.3 for more information.

¹ Must be submitted with an accompanying AUTH Request.

² Must be submitted with either an AUTH and/or ACCOUNTCHECK Request(s).

10.2 Sending an Enhanced Post Request

Once Secure Trading has enabled Enhanced Post and any combination of the aforementioned request types on your site, you can use Enhanced Post on a payment page by passing a standard HTTP POST to the Payment Pages, with the required fields (included in the examples that follow and detailed in section 4.1), and the Enhanced Post field(s), called "requesttypedescriptions".



Please note that the Enhanced Post fields are not mandatory, but when they are not submitted, an AUTH Request will **always** occur, amongst all other request types enabled for your site, as the default behaviour.

To set up a POST to the Payment Pages, create a form on your webserver that will submit the required fields, along with fields called "requesttypedescriptions" and the values of the request types you would like to be processed for the customer. The following HTML examples will render a webpage with a button that will direct the customer to your site's payment page. The **requesttypedescriptions** field is highlighted in **bold**.

10.2.1.1 Example of sending an AUTH with Enhanced Post

This request will process an AUTH request using the payment details entered.

```
<html>
<head>
</head>
<body>
<form method="POST"
action="https://payments.securetrading.net/process/payments/choice">
<input type="hidden" name="sitereference" value="test_site12345">
<input type="hidden" name="stprofile" value="default">
<input type="hidden" name="currencyiso3a" value="USD">
<input type="hidden" name="mainamount" value="100.00">
<input type="hidden" name="version" value="2">
<input type="hidden" name="requesttypedescriptions" value="AUTH">
<input type="submit" value="Pay">
</form>
</body>
</html>
```

10.2.1.2 Example of sending an ACCOUNTCHECK with Enhanced Post

This request will ONLY process an ACCOUNTCHECK request using the payment details entered.

```
<html>
<head>
</head>
<body>
<form method="POST"
action="https://payments.securetrading.net/process/payments/choice">
<input type="hidden" name="sitereference" value="test_site12345">
<input type="hidden" name="stprofile" value="default">
<input type="hidden" name="currencyiso3a" value="USD">
<input type="hidden" name="mainamount" value="100.00">
<input type="hidden" name="version" value="2">
<input type="hidden" name="requesttypedescriptions"
value="ACCOUNTCHECK">
<input type="submit" value="Pay">
</form>
</body>
</html>
```


Payment Pages Setup Guide

10.2.1.3 Example of sending an AUTH and ACCOUNTCHECK with Enhanced Post

This request will process an ACCOUNTCHECK **and** an AUTH request with the payment details entered.

```
<html>
<head>
</head>
<body>
<form method="POST"
action="https://payments.securetrading.net/process/payments/choice">
<input type="hidden" name="sitereference" value="test_site12345">
<input type="hidden" name="stprofile" value="default">
<input type="hidden" name="currencyiso3a" value="USD">
<input type="hidden" name="mainamount" value="100.00">
<input type="hidden" name="version" value="2">
<input type="hidden" name="requesttypedescriptions" value="AUTH">
<input type="hidden" name="requesttypedescriptions"
value="ACCOUNTCHECK">
<input type="submit" value="Pay">
</form>
</body>
</html>
```

10.2.2 The result of the POST

The page displayed to customers following an HTTP Post for an Enhanced Post is the same as for a regular Payment Pages transaction. Please refer to section 3.2 for more information.

10.2.3 Request Sequence

If multiple request types are sent in a single Enhanced Post request, they are always processed in a specific order defined by Secure Trading; regardless of the order the request types are submitted. This order is as follows:

Order (starting from 1)	Request Type
1	CURRENCYRATE
2	RISKDEC
3	ACCOUNTCHECK
4	ORDER
5	THREEDQUERY
6	ORDERDETAILS
7	AUTH
8	SUBSCRIPTION



10.2.4 Request Priority

With the enhanced POST feature, there are priorities that are assigned to certain request types.

Request types are classed as High-Priority if they are required in order to transfer funds and Low-Priority if they are **NOT** able to directly transfer funds, as shown in the table, below:

Request Type(s)	Priority
AUTH SUBSCRIPTIONS	HIGH
ACCOUNTCHECK CURRENCYRATE ORDER ORDERDETAILS RISKDEC THREEDQUERY	LOW

If a SINGLE (e.g. AUTH) High-Priority request type is sent, then the payment methods shown are ones that are able to process the high priority request.

If MULTIPLE (e.g. AUTH and SUBSCRIPTION) High-Priority request types are sent in a single request, then the payment methods shown will be those that can perform both request types (e.g. Maestro which cannot perform SUBSCRIPTIONS will not be shown)

If a High-Priority (e.g. AUTH) request type is sent along with a Low-Priority (e.g. ACCOUNTCHECK) request type in a single request, then the High-Priority request takes precedence over the Low-Priority. Only the payment types that are able to process the High-Priority request will be shown to the customer(s) (even though they may not be able to process the Low-Priority request).

If a SINGLE Low-Priority (e.g. ACCOUNTCHECK) request type is sent on its own, this behaves the same as a High-Priority request, and displays all payment types that are able to process that request type.

If MULTIPLE Low-Priority (e.g. ACCOUNTCHECK and RISKDEC) request types are sent in a single request, then the payment methods shown will be those that can perform both request types.

10.3 PayPal and Enhanced Post

When offering PayPal as a choice on your Payment Pages solution, you are required to include **requesttypedescriptions** for both **ORDER** and **AUTH** in the HTTP POST.

Your system can optionally include **requesttypedescriptions** for ORDERDETAILS, as highlighted in the example, below.

The inclusion of the ORDERDETAILS field affects the transaction performed as following:

Including ORDERDETAILS	Not including ORDERDETAILS
Secure Trading will contact PayPal after the customer has returned to the Payment Pages, and retrieve billing details the customer opted to use while on PayPal's checkout pages for the authorisation request.	Secure Trading will not contact PayPal after the customer has returned to the Payment Pages, and will instead only record billing details passed to Secure Trading in the HTTP POST. The customer may alter these details while on PayPal's checkout pages, but these changes will not be reflected in the authorisation request.

```
<html>
<head>
</head>
<body>
<form method="POST"
action="https://payments.securetrading.net/process/payments/choice">
<input type="hidden" name="sitereference" value="test_site12345">
<input type="hidden" name="stprofile" value="default">
<input type="hidden" name="currencyiso3a" value="USD">
<input type="hidden" name="mainamount" value="100.00">
<input type="hidden" name="version" value="2">
<input type="hidden" name="requesttypedescriptions" value="ORDER">
<input type="hidden" name="requesttypedescriptions"
value="ORDERDETAILS">
<input type="hidden" name="requesttypedescriptions" value="AUTH">
<input type="submit" value="Pay">
</form>
</body>
</html>
```

10.4 Subscriptions and Enhanced Post

To process Subscriptions through the Payment Pages, you must always provide the Subscription-specific fields outlined in the **STPP Subscriptions and Payment Pages document** (see section 16.3). When using Subscriptions with Enhanced Post you must also include the required **requesttypedescriptions** in the POST.

Request type descriptions:

- # You must include either an AUTH and/or ACCOUNTCHECK Request(s).
(Section 10.4.1 explains the difference between these requests).
- # You must include a SUBSCRIPTION Request.



Account Checks are only available for certain acquiring banks. Please contact our Support team for further details (see section 16.1).

Example

```
<html>
<head>
</head>
<body>
<form method="POST"
action="https://payments.securetrading.net/process/payments/choice">
<input type="hidden" name="sitereference" value="test_site12345">
<input type="hidden" name="stprofile" value="default">
<input type="hidden" name="currencyiso3a" value="USD">
<input type="hidden" name="mainamount" value="100.00">
<input type="hidden" name="version" value="2">
<input type="hidden" name="requesttypedescriptions" value="AUTH">
<input type="hidden" name="subscriptionunit" value="DAY">
<input type="hidden" name="subscriptionfrequency" value="1">
<input type="hidden" name="subscriptionfinalnumber" value="5">
<input type="hidden" name="subscriptiontype" value="RECURRING">
<input type="hidden" name="subscriptionbegindate"
value="2013-04-30">
<input type="hidden" name="requesttypedescriptions"
value="SUBSCRIPTION">
<input type="submit" value="Pay">
</form>
</body>
</html>
```



Please note that Subscriptions require the additional Subscription fields (shown above) to be submitted in order to be scheduled in the Secure Trading Subscription Engine. For more information, please refer to the **STPP Subscriptions and Payment Pages** (see section 16.3).

10.4.1 Relationship between subscriptions and account checks

When specifying **ACCOUNTCHECK and SUBSCRIPTION request types** in an enhanced post, Secure Trading will perform checks on the customer's details before scheduling a subscription. You will need to contact Support to set up rules to automatically suspend transactions where the results of the ACCOUNTCHECK indicate details entered by the customer do not match those held on their bank's records. If the ACCOUNTCHECK is successful, subsequent payments will be automatically processed at regular intervals by the subscription engine. As ACCOUNTCHECKS do not reserve funds on the customer's account, no payment is processed for the first interval (e.g. for a monthly subscription, the first payment is only processed after the first month).

When specifying **AUTH and SUBSCRIPTION request types** in an enhanced post, Secure Trading will process the first payment immediately and schedule further payments in the subscription engine if the funds were settled successfully.

When specifying **ACCOUNTCHECK, AUTH and SUBSCRIPTION request types** in an enhanced post, Secure Trading will perform checks on the customer's details before processing the first payment. Please contact Support to configure rules to suspend transactions where the results of the ACCOUNTCHECK indicate details entered by the customer do not match those held on their bank's records. If the ACCOUNTCHECK is successful, the first payment will be processed immediately. Secure Trading will schedule further payments in the subscription engine if funds from the first transaction were settled successfully.

11 iframe

Secure Trading allows you to display your payment page within an iframe. This enables you to display the payment page within the layout of your website.



It is imperative that all web pages on your site are encrypted using Secure Socket Layer (SSL) to ensure correct functionality of iframes across all browsers.

PayPal cannot currently be integrated within an iframe.



Please note that iframes may not be rendered correctly in certain web browsers (e.g. certain mobile web browsers).

11.1 Configuring your Website

In order to include the iframe within your website, you need to include HTML code similar to the example below, within the HTML on your website:

```
<iframe src="https://payments.securetrading.net
/process/payments/choice?sitereference=
test_site12345&mainamount=10.00&currencyiso3a=GBP&version=2&stprofile=
default" width="100%" height="600" scrolling="auto"
style="border:0px;"></iframe>
```

The example above includes the minimum required fields needed in the URL (highlighted in **bold**). For more information on these fields, or additional fields that can be included, please refer to section 4.

11.2 Changing the appearance of the iframe

By following the instructions outlined in section 11.1, the standard payment page is included within your webpage. You can format the payment page to be displayed in a more iframe-friendly way, by modifying the HTML/CSS mark-up (see the [Payment Pages Customisation](#) document).

e.g. To make better use of the reduced space within the iframe, you could opt to hide certain optional fields/sections you consider unnecessary for the transaction.

12 Google Analytics

Google Analytics allow you to track users and monitor activity on your site.

12.1 Using Google Analytics Tracking Code

Google Analytics can be used with STPP Payment Pages by using custom JavaScript code. Follow the example below to use this feature.

Upload a file using the MyST File Manager called `default.js` containing the following code:

```
// Adding Google Analytics to SecureTrading Payment Pages.
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-XXXXX-X']);
_gaq.push(['_trackPageview']);

(function() {
  var ga = document.createElement('script'); ga.type =
'text/javascript'; ga.async = true;
  ga.src = ('https:' == document.location.protocol ? 'https://ssl' :
'http://www') + '.google-analytics.com/ga.js';
  var s = document.getElementsByTagName('script')[0];
s.parentNode.insertBefore(ga, s);
})();
```

Figure 25 JavaScript for Google Analytics

Replace the text marked in **bold**, “UA-XXXXX-X” to be your Google Analytics web property ID.



For merchants customising their Payment Pages using profiles, (see the [Payment Pages Customisation](#) document) upload this JavaScript file separately for each profile, with the filename [profile].js



Please note for more information on the MyST File Manager, please refer to the [MyST User Guide](#) for more information.



Please note that Google Analytics will set cookies on the customer’s browser. For more information on Google Analytics, visit <http://www.google.com/analytics/index.html>.

12.2 Google Analytics and Ecommerce Tracking

You can use Google Analytics and Ecommerce Tracking to link a specific referral source to payments made through your Payment Pages.

As the Ecommerce Tracking feature needs a completed transaction, the code should be added to your redirect pages, not the payment page itself.

For more information on Google Analytics and Ecommerce tracking, visit <https://developers.google.com/analytics/devguides/collection/gajs/gaTrackingEcommerce>

13 Going Live

13.1 Rules for Live Site Reference

When you are ready to switch your account live, you will need to consider any rules (emails, URL notifications, redirects, etc.) that may have been configured on your test site reference, as these will need to be re-configured on your live site reference to ensure they update your system as expected.

13.2 Contact Secure Trading

Once you have tested your system and you are ready to go live, please send an email to support@securetrading.com with your site reference and request to go live. You will receive a response when your live site is ready to begin processing payments.

13.3 Change your website

The POST will need to be updated to use your live site reference. This is done by modifying the **sitereference** field submitted to Secure Trading. For the example outlined in section 3.1, the change is outlined below (please note the data changed is marked in **bold**):

```
<html>
<head>
</head>
<body>
<form method="POST"
action="https://payments.securetrading.net/process/payments/choice">
<input type="hidden" name="sitereference" value="site12346">
<input type="hidden" name="stprofile" value="default">
<input type="hidden" name="currencyiso3a" value="GBP">
<input type="hidden" name="mainamount" value="100.00">
<input type="hidden" name="version" value="2">
<input type="submit" value="Pay">
</form>
</body>
</html>
```

The appearance of the button on the page or the page the customer is transferred to would be exactly the same as on your test site, but now that the live site reference has been used, the account will process transactions to your acquiring bank.

13.4 Live testing

Once you have switched to your live account, Secure Trading recommend that you perform a test transaction using a live card to ensure the transaction is processed as expected. You can sign in to MyST to manage your transactions. Therefore you can cancel transactions processed on live cards.



Please note that you should not use the same live card too many times, as the requests will still be authorised, and could cause the issuer to suspect fraud or the cardholder could exceed their limit.

14 Testing

During your integration, you will need to thoroughly test your system to ensure it is ready to process live payments. After Secure Trading has provided you with a test site reference, you can process transactions and check that your system handles the responses correctly. We recommend specifying the amount "10.50" when testing. Other amounts can be used but may return unexpected responses.

14.1 Testing successful transactions

You can process successful transactions by submitting the following PANs on the Payment Pages:

Payment type	Test PAN
Visa	4111111111111111
MasterCard	5100000000000511

To ensure these transactions pass AVS and CVV2 checks (see the [AVS & CVV2 document](#) for further details), you will also need to submit the following values:

Field name	Value
Billing premise	789
Billing postcode	TE45 6ST
Card security code	123



Please ensure you have tested your integration with all payment methods that will be made available to your customers. The [Testing document](#) contains a full list of payment credentials that can be used when testing.

14.2 Testing unsuccessful transactions

Your system will also need to be able to handle transactions that are not successful. You can process transactions with the following amounts to test for different responses returned by Secure Trading:

Main amount	Outcome
700.00	Transaction declined by bank response.
600.10	Bank system error response.

To simulate "Not matched" responses for AVS and CVV2 checks, you can submit the following values:

Field name	Value
Billing premise	123
Billing postcode	TE12 3ST
Card security code	214



The [Testing document](#) contains further test data for testing AVS & CVV2 checks. Please ensure your system is able to handle these scenarios.

15 Migrating from version 1

To migrate from Payment Pages version 1 to version 2, you will need to make the following changes to your existing HTTPS POST:

- # Change “**version**” from “1” to “2”.
- # Submit an additional field “**stprofile**” with a value of “default”



When getting started with version 2, perform these changes on your test site reference and ensure the appearance and behaviour is as expected before making changes to your live site reference.

The following is an example of an HTTPS POST to Payment Pages version 2, with the changes discussed above highlighted in **bold**:

```
<form method="POST"
action="https://payments.securetrading.net/process/payments/choice">
<input type="hidden" name="sitereference" value="test_site12345">
<input type="hidden" name="stprofile" value="default">
<input type="hidden" name="currencyiso3a" value="USD">
<input type="hidden" name="mainamount" value="100.00">
<input type="hidden" name="version" value="2">
<input type="hidden" name="orderreference" value="myorder12345">
<input type="submit" value="Pay">
</form>
```

When you have finished, the payment choice page will be displayed as follows:

PAYMENTS SECURED BY
secure // trading
A UC GROUP COMPANY

Amount: £1.23 GBP
Order reference: MyOrder123
Merchant name: Test Merchant

Please select your payment method

Please make sure that you select the correct payment type.

15.1 Customisation

In Payment Pages version 2, we have improved how you can customise the appearance and layout of your pages, allowing for greater flexibility.

New features supported:

- # Use custom HTML to perform advanced customisation on the payment pages.
- # The ability to implement different **stprofiles**, which allow you to switch between different layouts on your payment pages on a request-by-request basis.

If you have already implemented custom CSS on your Payment Pages, you will need to refer to our [customisation documentation](#) to make changes to your CSS to support version 2.

16 Further Information and Support

This section provides useful information with regards to documentation and support for the Merchant's Secure Trading solution.

16.1 Secure Trading Support

If you have any questions regarding integration or maintenance of the system, please contact our support team using one of the following methods.

Method	Details
Telephone	+44 (0) 1248 672 050
Fax	+44 (0) 1248 672 099
Email	support@securetrading.com
Website	http://www.securetrading.com/support/support.html

16.2 Secure Trading Sales

If you do not have an account with Secure Trading, please contact our Sales team and they will inform you of the benefits of a Secure Trading account.

Method	Details
Telephone	0800 028 9151
Telephone (Int'l)	+44 (0) 1248 672 070
Fax	+44 (0) 1248 672 079
Email	sales@securetrading.com
Website	http://www.securetrading.com

16.3 Useful Documents

The documents listed below should be read in conjunction with this document:

- # [STTP MyST User Guide](#) – This document outlines how to use MyST to monitor your transactions and manage your account.
- # [STTP XML Specification](#) – This defines the XML that is submitted in requests to Secure Trading via STAPI and Web Services, for AUTH, ACCOUNTCHECK and REFUND Requests.
- # [XML Reference 3-D Secure](#) – This document outlines how to process a 3-D Secure transaction.
- # [STTP Subscriptions and Payment Pages](#) – This document outlines how to process Subscriptions through the Payment Pages.
- # [STTP AVS & CVV2](#) – This document describes the checks performed on the address and security code submitted by the customer.
- # [MyST Rule Manager](#) – This document outlines how to configure rules that perform actions on your account under certain conditions.
- # [Payment Pages Customisation](#) – This document outlines how to customise your Payment Pages using HTML, CSS and JavaScript.

Any other document regarding the STPP system can be found on Secure Trading's website (<http://www.securetrading.com>). Alternatively, please contact our support team as outlined above.

16.4 Frequently Asked Questions

Please visit the FAQ section on our website (<http://www.securetrading.com/support/faq>).

17 Appendix

17.1 Settle status

Settle status	Caption	Description
0	Pending settlement	Transaction that has been authorised by card issuer for payment. <ul style="list-style-type: none"> # Settles automatically. # Can be updated or cancelled. # Does not currently require action from the merchant. # May be suspended by future fraud and duplicate checks, if enabled (see Fraud checks document).
1	Manual settlement	Transaction that has been authorised by card issuer for payment. <ul style="list-style-type: none"> # Settles automatically. # Can be updated or cancelled. # Does not require further action from merchant. # Bypasses fraud and duplicate checks, if enabled (see Fraud checks document).
10	Settling	The transaction is in the process of being settled. <ul style="list-style-type: none"> # Settles automatically. # Does not require further action from merchant. # Cannot be updated or cancelled.
100	Settled	Transaction has been settled into the merchant's account. <ul style="list-style-type: none"> # Does not require further action from merchant. # Cannot be updated or cancelled. # Can be refunded (unless all funds have already been refunded).
2	Suspended	Transaction is in a suspended state, awaiting further action from the merchant. <ul style="list-style-type: none"> # Will not be settled unless updated by the merchant to settle status '0' or '1'. # Alternatively, merchants can cancel this transaction by updating the settle status to '3'. # Transactions can be suspended by merchants to prevent settlement, allowing for manual investigation. # Transactions can be suspended by Secure Trading if fraud or duplicate checks (if enabled) raise an issue (see Fraud checks document). # If left in a suspended state, Secure Trading will automatically cancel the transaction 7 days after the authorisation date.
3	Cancelled	Transaction has been cancelled and will not settle. <ul style="list-style-type: none"> # This can be due to an error or due to the transaction being declined. # Merchants can also update the settle status to '3' to manually cancel transactions. # Cancelled transactions cannot be updated.

17.2 Charge description

This is a description of the payment that appears on the customer's bank statement. You can submit the charge description in requests to Secure Trading.

Please refer to this supplement for further information:

<http://www.securetrading.com/files/documentation/Charge-Description.pdf>

17.3 Payment facilitator

You can submit payment facilitator fields in requests to Secure Trading.

Please refer to this supplement for further information:

<http://www.securetrading.com/files/documentation/Payment-Facilitator.pdf>

17.4 Digital wallet

You can submit digital wallet credentials in requests to Secure Trading.

Please refer to this supplement for further information:

<http://www.securetrading.com/files/documentation/Digital-Wallet.pdf>