secure trading
ONLINE PAYMENT EXPERTS

Payment Pages Setup Guide
Version 2

Published: 24 October 2019

Migrating from version 1?
Please read our quick start guide on page 118.

Table of Contents

1 The basics

Introduction

Payment Pages is a comprehensive, hosted e-commerce solution that is easy to integrate into your own website. This guide will provide you with all the information you need to start processing payments.

Features

- Process payments on our own dedicated HTTPS servers (that use the SSL protocol).
- Process payments without storing credit card details on your server.
- Customise the appearance to maintain the look and feel of your online store.
- Accept a large variety of currencies.
- Supports our full suite of fraud-prevention tools.
- Monitor all transactions using our online transaction management system, MyST.

Requirements

Before we get started, please ensure you have met the following requirements:

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:
https://docs.securetrading.com/document/toolbox/webservices-ips/

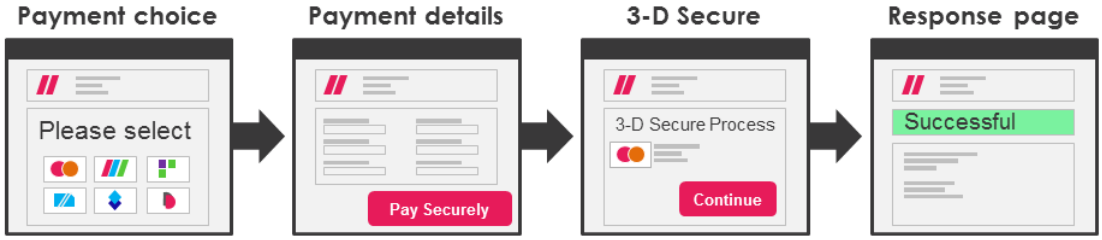
If you are unsure on any of the points above, please contact Secure Trading for assistance (see section 8.1).

1.1 Workflows

After the customer agrees to a purchase on your checkout, the customer is redirected to the Payment Pages, hosted by Secure Trading. This section describes the main workflows available to you:

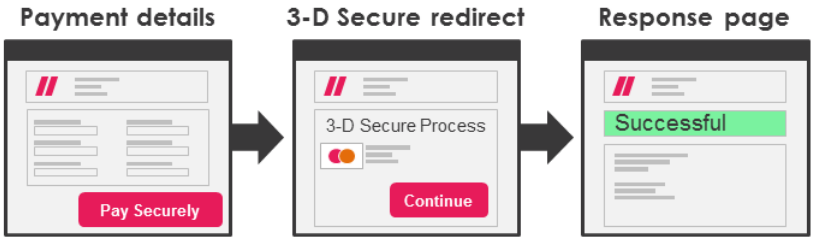
Workflow A

- The customer is redirected to our secure servers, where they presented with a choice between all payment methods enabled on your account.
- The customer selects their preferred payment method and is then prompted for their payment details.
- See section 1.1.1 to get started.



Workflow B

- The customer is redirected to our secure servers, where they enter their payment details (under default configuration, we prompt for card details).
- See section 1.1.2 to get started.

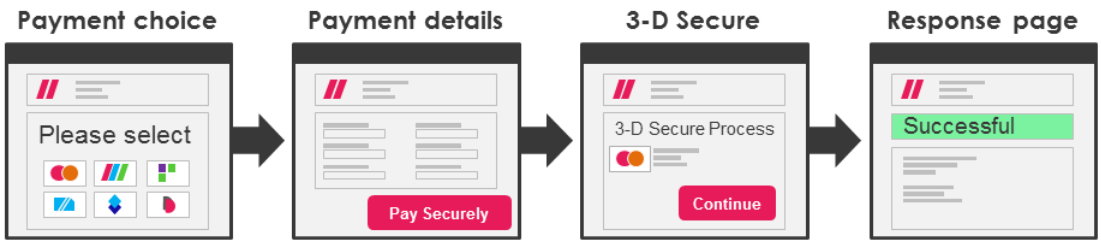


Workflow C (recommended for Alternative Payment Methods)

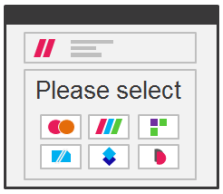
- The customer is redirected to our secure servers, where they are presented with a choice between all payment methods enabled on your account.
- The customer selects their preferred payment method and is then prompted for their payment details.
- If the customer has already entered the required payment details on your checkout, they are immediately redirected to the APM-hosted pages (otherwise, they go to the details page as described in Workflow A).
- See section 1.1.3 to get started.

1.1.1 Workflow A

1.1.1.1 Summary

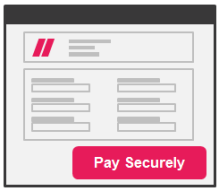


1.1.1.2 Checkout experience



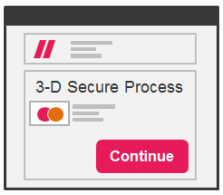
1. Payment choice

When posted to our servers, the customer is displayed all payment methods enabled on their account. Here they select their preferred payment method for the transaction.



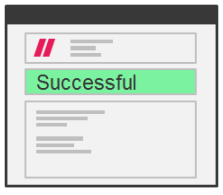
2. Payment details

The customer is displayed a form prompting for their payment details, billing address and delivery address. This form displays the appropriate fields for the payment method selected.



3. 3-D Secure v2

The customer will be displayed an overlay for authentication Access Control Server (ACS). For customers deemed high-risk of fraud, they may be prompted to verify their identity (e.g. enter a passcode). However, in most cases, the customer will briefly be shown a holding message before the payment is processed, without the need for additional authentication. See section 3.2 for further information on 3-D Secure v2.



4. Response

Finally, the customer is displayed confirmation that the payment was successful, along with the amount, currency and payment type used.

Alternatively, you can opt to have the customer redirected back to your website following successful payment. This is achieved by configuring a Payment Pages redirect (see section 1.3).

Please note that if a transaction is authorised, it is not guaranteed you will receive funds. Funds are not transferred to your account until settlement (see section 1.11).

1.1.1.3 Workflow A configuration

1. Here is an example of an HTML form you can use as a template for redirecting your customers to the Payment Pages. Start by copying and pasting the below to a text file and save as an HTML form.

```
<html>
<body>
<form method="POST" action="<DOMAIN>/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="submit" value="Pay">
</form>
</body>
</html>
```

See section 9.2 for a full list of supported domains for the <DOMAIN> placeholder.

2. Change the site reference (as highlighted in **bold** in the example above) to include the test site reference provided when you signed up. Update the other fields as needed, using the table below. For now, we're only covering the required fields, but you can submit more fields if needed. A full list can be found in section 9.1.

<table>
<tr><th>Required fields</th><th>Description</th></tr>
<tr><td>sitereference</td><td>The unique reference that you receive when you sign up.</td></tr>
<tr><td>currencyiso3a</td><td>The transaction currency (in ISO3A format).</td></tr>
<tr><td>mainamount</td><td>The amount of the transaction should be in main units.
Only include the amount value and the decimal place (no commas).

Currencies such as Japanese Yen which do not require a decimal place are submitted without. e.g. 1000 Yen would be 1000.

<u>Examples:</u>
<table>
<tr><th>Amount:</th><th>Correct mainamount</th><th>Invalid mainamount</th></tr>
<tr><td>£9,800</td><td>9800.00</td><td>£9,800</td></tr>
<tr><td>€123.99</td><td>123.99</td><td>123,99</td></tr>
<tr><td>$2.50</td><td>2.50</td><td>2.5</td></tr>
<tr><td>99¢</td><td>0.99</td><td>.99</td></tr>
<tr><td>(JPY)1250¥</td><td>1250</td><td>1250.00</td></tr>
</table></td></tr>
<tr><td>version</td><td>This value will be set to 2.</td></tr>
<tr><td>stprofile</td><td>Used to specify the styling used to render the Payment Pages. When using the default appearance, this is set to "default" (for further information on profiles, see section 2.1).</td></tr>
</table>

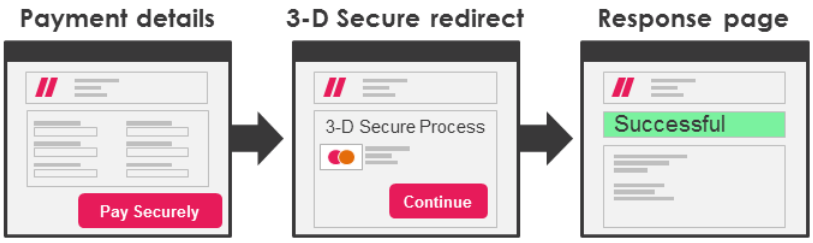
***Note:** We recommend that text submitted is encoded in UTF-8.*
Special characters must be URL-encoded (e.g. "&" should be submitted as "%26").

If card details are to be re-used in a future transaction (e.g. by a Subscription or by processing a re-authorisation), you must first obtain cardholder permission, and your request will need to include the additional field **credentialsonfile**. See section 1.3.

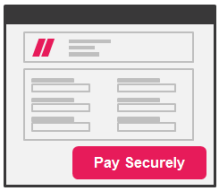
3. Save this as an HTML file. You can open this in your web browser, and a "**Pay**" button will displayed. Click this button, and you will be redirected to your test site, where you can process test payments.
4. When testing, attempt a payment with a Visa card using the PAN '4111 1111 1111 1111', or with Mastercard using the PAN '5100 0000 0000 0511'. These should provide a "Successful" response. Further information on testing can be found in section 1.8.

1.1.2 Workflow B

1.1.2.1 Summary

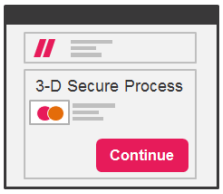


1.1.2.2 Checkout experience



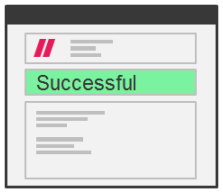
1. Payment details

When posted to our servers, the customer is displayed a form prompting for their payment details, billing address and delivery address. By default, the customer is prompted for card details, but this can be customised (see section 1.1.2.4 for further information).



2. 3-D Secure v2

The customer will be displayed an overlay for authentication Access Control Server (ACS). For customers deemed high-risk of fraud, they may be prompted to verify their identity (e.g. enter a passcode). However, in most cases, the customer will briefly be shown a holding message before the payment is processed, without the need for additional authentication. See section 3.2 for further information on 3-D Secure v2.



3. Response

Finally, the customer is displayed confirmation that the payment was successful, along with the amount, currency and payment type used.

Alternatively, you can opt to have the customer redirected back to your website following successful payment. This is achieved by configuring a Payment Pages redirect (see section 1.3).

Please note that if a transaction is authorised, it is not guaranteed you will receive funds. Funds are not transferred to your account until settlement (see section 1.11).

1.1.2.3 Workflow B configuration

1. Here is an example of an HTML form you can use as a template for redirecting your customers to the Payment Pages. Start by copying and pasting the below to a text file & save as an HTML form.

```
<html>
<body>
<form method="POST" action="<DOMAIN>/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="submit" value="Pay">
</form>
</body>
</html>
```

See section 9.2 for a full list of supported domains for the <DOMAIN> placeholder.

2. Change the site reference (as highlighted in **bold** in the example above) to include the test site reference provided when you signed up. Update the other fields as needed, using the table below. For now, we're only covering the required fields, but you can submit more fields if needed. A full list can be found in section 9.1.

Required fields	Description
sitereference	The unique reference that you receive when you sign up.
currencyiso3a	The transaction currency (in ISO3A format).
mainamount	The amount of the transaction should be in main units. Only include the amount value and the decimal place (no commas). Currencies such as Japanese Yen which do not require a decimal place are submitted without. e.g. 1000 Yen would be 1000. **Examples:**
version	This value will be set to 2.
stprofile	Used to specify the styling used to render the Payment Pages. When using the default appearance, this is set to "default" (for further information on profiles, see section 2.1).

Amount:	Correct **mainamount**	Invalid **mainamount**
£9,800	9800.00	£9,800
€123.99	123.99	123,99
$2.50	2.50	2.5
99¢	0.99	.99
(JPY)1250¥	1250	1250.00

Note: *We recommend that text submitted is encoded in UTF-8.*
Special characters must be URL-encoded (e.g. "&" should be submitted as "%26").

If card details are to be re-used in a future transaction (e.g. by a Subscription or by processing a re-authorisation), you must first obtain cardholder permission, and your request will need to include the additional field **credentialsonfile**. See section 1.3.

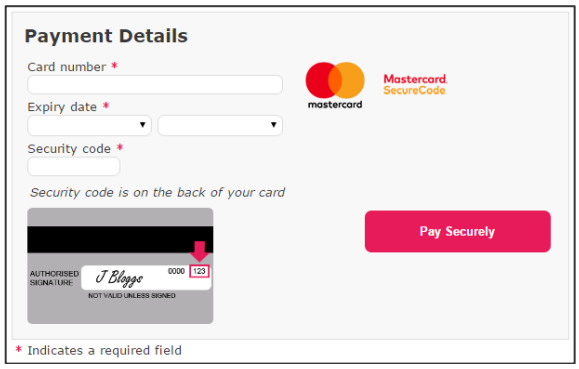
3. Save this as an HTML file. You can open this in your web browser, and a "**Pay**" button will displayed. Click this button, and you will be redirected to your test site, where you can process test payments.

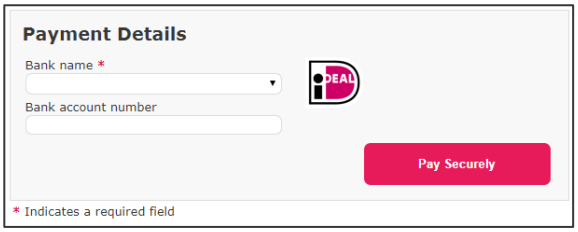
4. When testing, attempt a payment with a Visa card using the PAN '4111 1111 1111 1111', or with Mastercard using the PAN '5100 0000 0000 0511'. These should provide a "Successful" response. Further information on testing can be found in section 1.8.

1.1.2.4 Pre-selecting the payment method

Note: This is only supported for Workflow B.

By default, we ask for the customer's card details, but this can be configured to be restricted to a specific payment method by modifying the POST. The form we display to the customer will include the necessary fields for the specified payment method, and the relevant logo will be shown. The following examples show the payment details page for Mastercard (left) and iDEAL (right).





To specify a payment method in the POST, add the following to your HTML form (exchanging 'VISA' for your preferred payment method if required):

```
<input type="hidden" name="paymenttypedescription" value="VISA">
```

When specifying the payment method in the POST, it is still possible for the customer to change to a different payment method, in the two following ways:

- The customer can select a different payment method from a menu at the top of the page. This is always shown by default.
- If the customer submits the PAN of a different card type that is enabled on your account, we will detect the card type and process the payment in that type instead.

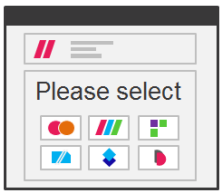
1.1.2.5 Verify card type

You can use verify card type to prevent the customer from changing to a different payment method from the one specified in the POST. See section 7.5 for further information.

1.1.3 Workflow C (recommended for Alternative Payment Methods)

1.1.3.1 Summary

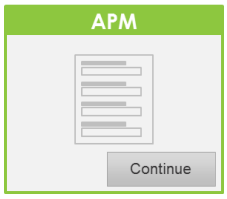
1.1.3.2 Checkout experience



1. Payment choice

When posted to our servers, the customer is displayed all payment methods enabled on your account. Here they select their preferred payment method for the transaction.

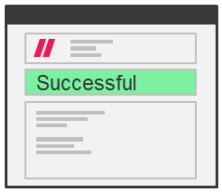
2. The customer selects an Alternative Payment Method (APM):
See section 4 for list of supported APMs



- If the customer has not already entered the required fields, they will be displayed the payment details page (a page hosted by Secure Trading) prior to being redirected to enter this information.
- If the customer has already entered the payment fields required by the APM and these have been submitted to Secure Trading along with the customer, the customer will be redirected to the APM-hosted pages (bypassing our hosted payment details page), where they follow on-screen prompts to complete the payment.

Workflow C and paying by card

Please note that the customer will always be shown our hosted payment details page when opting to pay by card (as described in Workflow A and B), as they will need to enter their card details.



3. Response

Finally, the customer is displayed confirmation that the payment was successful, along with the amount, currency and payment type used.

Alternatively, you can opt to have the customer redirected back to your website following successful payment. This is achieved by configuring a Payment Pages redirect (see section 1.3).

1.1.3.3 Workflow C configuration

- Here is an example of an HTML form you can use as a template for redirecting your customers to the Payment Pages. Start by copying and pasting the below to a text file and save as an HTML form.

```
<html>
<body>
<form method="POST" action="<DOMAIN>/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="ruleidentifier" value="STR-14">
<input type="hidden" name="version" value="2">
<input type="hidden" name="billingcountryiso2a" value="DE">
<input type="hidden" name="billingfirstname" value="Joe">
<input type="hidden" name="billinglastname" value="Bloggs">
<input type="submit" value="Pay">
</form>
</body>
</html>
```

See section 9.2 for a full list of supported domains for the <DOMAIN> placeholder.

- Change the site reference in the POST to include the test site reference provided when you signed up. Update the other fields as needed, using the table below. For now, we're only covering the required fields, but you can submit additional fields if needed. A full list can be found in section 9.1.

Required fields	Description
sitereference	The unique reference that you receive when you sign up.
currencyiso3a	The transaction currency (in ISO3A format).
ruleidentifier	The unique id (defined in the Rule manager) of the rule that will be triggered when processing the transaction. In this case, the field must be submitted with value "STR-14", which allows the customer to bypass our hosted payment details page when we already have all the fields required to redirect the customer to the APM.
mainamount	The amount of the transaction should be in main units. Only include the amount value and the decimal place (no commas). Currencies such as Japanese Yen which do not require a decimal place are submitted without. e.g. 1000 Yen would be 1000.
version	This value will be set to 2.
stprofile	Used to specify the styling used to render the Payment Pages. When using the default appearance, this is set to "default" (for further information on profiles, see section 2.1).
In order for the customer to bypass the Secure Trading-hosted payment details page and be immediately redirected to the APM's hosted pages, you will need to ensure that all required fields are submitted in the POST. *See section 4 for further info*	

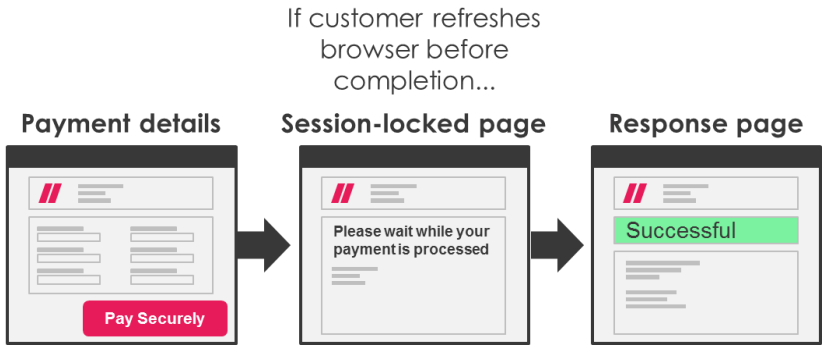
Note: *We recommend that text submitted is encoded in UTF-8.*
Special characters must be URL-encoded (e.g. "&" should be submitted as "%26").

If card details are to be re-used in a future transaction (e.g. by a Subscription or by processing a re-authorisation), you must first obtain cardholder permission, and your request will need to include the additional field **credentialsonfile**. See section 1.3.

- Save this as an HTML file. You can open this in your web browser, and a "**Pay**" button will be displayed. Click the button, and you will be redirected to your test site, where you can process test payments.

1.2 Session-locked page

If the customer refreshes their browser before their request has completed, they will be shown the session-locked page (default behaviour). This page will automatically refresh periodically until the initial request has been completed. Following this, the customer will be shown either a success or error message, depending on the final outcome of the request.



1.3 Configuring "request site security"

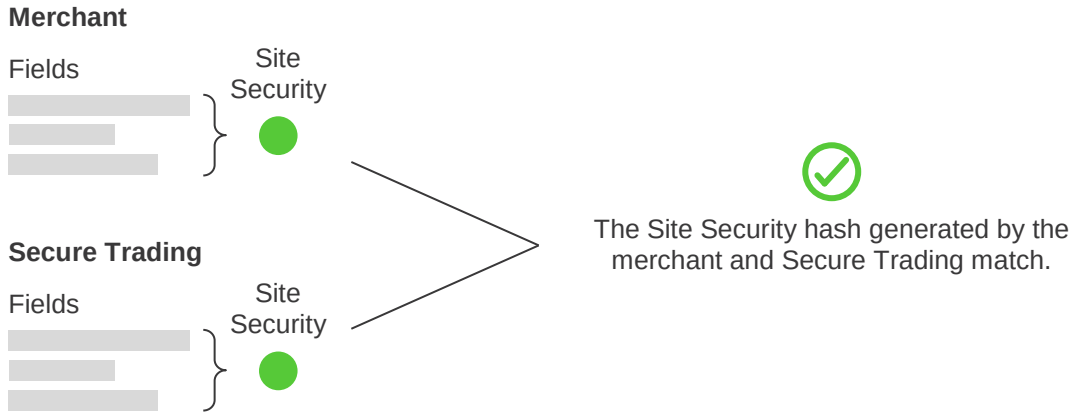
The site security process was updated in April 2019 to include a new field called '**sitesecuritytimestamp**', which is used to define a time restriction to be placed on requests. Although the previous implementation of site security remains supported, we recommend using the latest version.

The legacy process is documented on the following webpage:
https://docs.securetrading.com/document/toolbox/legacy-site-security/

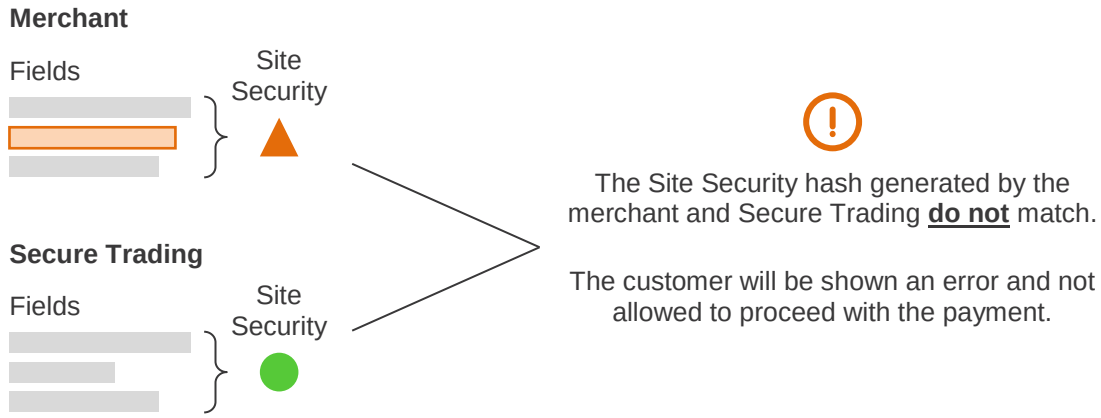
A field called **sitesecurity** must be included in the POST to ensure requests to the Payment Pages cannot be modified by a customer or third party. This field contains a hash that is generated from a selection of designated fields, including a password that has been established with the Support team.

1.3.1 Process overview

We will read the fields in your request prior to processing an authorisation and re-generate the hash on our servers. For valid requests, the request site security hash that we generate must match the value submitted in your POST. This indicates the request has not been modified by the customer or third party:



If someone tries to modify the value of one of your designated fields, the hash we calculate on our servers will not match the hash submitted in the POST. In this case, the payment will be halted and an error message is shown to the customer.



1.3.2 Start with your designated fields

When request site security is enabled, the default fields that will be used when generating the hash are as follows:

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

To add or remove fields from this list, please contact Support (see section 8.1). By including a field in your generated hash, this field cannot be modified by the customer or an unauthorised third party. We recommend including as many unique fields as possible. We support the inclusion of custom fields in your list of designated fields.

You must not include fields that the customer can change while using the Payment Pages, for instance, in most cases their name, billing and delivery details. This can prevent legitimate transactions from being processed.

The customer's IP address may change during the processing of a transaction, especially when browsing from mobile devices. For this reason, we recommend against opting to include this field as one of your designated fields.

Once the fields have been chosen, you will need to provide Support with an alphanumeric password to be included in the hashed information. If you would like to change the password or add/remove fields from the hash, you must notify Support (see section 8.1).

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.

1.3.3 Use your designated fields to generate the hash

Step 1

Append the **values** of the designated fields **in the order shown in section 1.3.2**. For example, consider a request with the following fields:

currencyiso3a = USD
mainamount = 100.00
sitereference = test_site12345
version = 2
stprofile = default
sitesecuritytimestamp = 2019-05-28 14:22:37
password = PASSWORD

Using this example, we would have the following string generated:

```
USD100.00test_site123452default2019-05-28 14:22:37PASSWORD
```

(Any blank fields are omitted from the hash)

Site security timestamp

As accurately as possible, this timestamp should reflect the time the customer's browser is to be redirected to the Payment Pages. (This timestamp value must **NOT** be in the future)

The value submitted in this field must be in the format YYYY-MM-DD hh:mm:ss. The timestamp must be in the UTC time zone. (e.g. "2019-05-28 14:22:37")

The customer has 3 hours from the time specified to complete the transaction, otherwise an error will displayed on screen (see section 1.3.5).

Order of the fields

When generating the hash, the fields must be in the same order as listed in section 1.3.2. If the fields are not in the correct order, the request will fail.

The order in which fields are hashed can be changed if required. Please contact the Support team for assistance.

The **sitesecuritytimestamp** and **password** fields **must** always be the last two fields in the string used to generate the hash. They cannot be repositioned among the other fields or removed entirely.

Fields with multiple values

If a field included in the hash has multiple values:

These values are concatenated in the order submitted in the POST.
Consider the following additional fields:
ruleidentifier=STR-7&ruleidentifier=STR-6

When included in the string generated above, it becomes:
USD100.00test_site123452default**STR-7STR-6**2019-05-28 14:22:37PASSWORD

Step 2

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.

Example string:

```
USD100.00test_site123452default2019-05-28 14:22:37PASSWORD
```

Hashing using SHA-256 will leave us with the following hash:
8a38a961bb00230745765f55cfd9ff386397d64f080b6d05f65cc5f85c4eff24

We have provided sample code to generate this hash in a number of different languages. (See section 9.4)

Step 3

Precede the hash with an "h":
h8a38a961bb00230745765f55cfd9ff386397d64f080b6d05f65cc5f85c4eff24

This is the final value that would need to be submitted for this transaction.

It is important that the generated hash is prefixed with the letter "h".
This is to ensure the latest version of the site security feature is used.
Failure to do so could invalidate the hash and stop legitimate transactions.

1.3.4 Update the POST to include additional fields

You will need to update your POST to include the following additional fields, as shown in the example below:

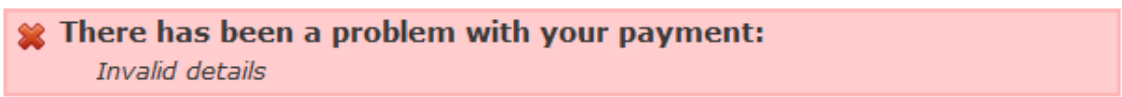
- **sitesecurity** – Includes the hash generated following the process described above.
- **sitesecuritytimestamp** - The timestamp of when the customer's browser is redirected to the Payment Pages (the same value as included in the hash).

```
<html>
<head>
</head>
<body>
<!--YOUR HTML-->
<form method="POST" action="<DOMAIN>/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="h8a38a961bb00230745765f55cfd9ff386397d64f080b6d05f65cc5f85c4eff24">
<input type="hidden" name="sitesecuritytimestamp" value="2019-05-28 14:22:37">
<input type="submit" value="Pay">
</form>
</body>
</html>
```

See section 9.2 for a full list of supported domains for the <DOMAIN> placeholder.

1.3.5 Troubleshooting

For any payment that is attempted with an incorrect hash, the customer will be presented with an error (such as shown below) and no payment will be processed:



1.4 Credentials on File (CoF)

Visa and Mastercard have mandated that you must obtain cardholder consent before storing card details for future use (e.g. by a Subscription or by processing a re-authorisation). Following this, you must appropriately identify credentials that are to be stored for later, by assigning a Credentials on File (CoF) flag in your POST to Payment Pages.

Please refer to the highlighted part of the following example:

```
<html>
<body>
<form method="POST" action="<DOMAIN>/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="credentialsonfile" value="1">
<input type="submit" value="Pay">
</form>
</body>
</html>
```

See section 9.2 for a full list of supported domains for the <DOMAIN> placeholder.

- If you plan to re-use the card details in a future transaction, submit:
  - **credentialsonfile** with value "1"
- If you do not plan to re-use the card details, you can omit the field from the request.

Important: The credentialsonfile value needs to be included in the string used to generate your request site security hash, as described in section 1.3. Failure to do so will result in the customer being shown an "Invalid details" error message.

1.4.1 Additional notes

Future payments that utilise previously-stored credentials will need to be processed using MyST or our API, and must include the following fields:

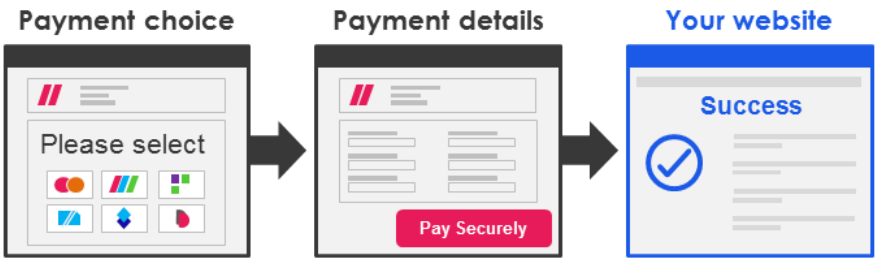
- **credentialsonfile**
- **initiationreason** (only if payment is a Merchant Initiated Transaction - MIT)

Refer to our **MyST documentation** or **Recurring payments XML Specification** for further information.

1.5 Redirects

1.5.1 For successful transactions (STR-6)

By default, when a transaction has been processed successfully, the customer will be displayed our response page. This has a message indicating the transaction was successful, along with details regarding the payment for the customer's records. Alternatively, you may prefer to host a response page on your own server:



This can be configured on your site by adding the following to your POST to Payment Pages:

```
<!--Enables rule that redirects the customer following a successful
transaction-->
<input type=hidden name="ruleidentifier" value="STR-6">

<!--Update the below with the URL for the redirect-->
<input type=hidden name="successfulurlredirect"
value="http://yourwebsite.com/successful">
```

The URL of your hosted response page must be externally facing. We 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.

Important: Both "STR-6" and the URL of the redirect need to be included in the string used to generate your request site security hash, as described in section 1.3. Failure to do so will result in the customer being shown an "Invalid details" error message.

1.5.2 For declined transactions (STR-7)

By default, if a customer's card declines, we will redisplay the payment form with an error, prompting them to try a different method of payment (recommended). Alternatively, you can instead opt to redirect customers to a different URL when their card declines.

This can be configured on your site by adding the following to your POST to Payment Pages:

```
<!--Enables rule that redirects the customer following a declined
transaction-->
<input type=hidden name="ruleidentifier" value="STR-7">

<!--Update the below with the URL for the redirect-->
<input type=hidden name="declinedurlredirect"
alue="http://yourwebsite.com/declined">
```

Important: Both "STR-7" and the URL of the redirect need to be included in the string used to generate your request site security hash, as described in section 1.3. Failure to do so will result in the customer being shown an "Invalid details" error message.

1.5.3 For all error cases (STR-13)

By default, if any errors are encountered that prevented the transaction from being processed successfully, we will redisplay the payment form with an error, prompting them to try a different method of payment (recommended). Alternatively, you can instead opt to redirect customers to a different URL when an error occurs.

This can be configured on your site by adding the following to your POST to Payment Pages:

```
<!--Enables rule that redirects the customer following an error-->
<input type=hidden name="ruleidentifier" value="STR-13">

<!--Update the below with the URL for the redirect-->
<input type=hidden name="errorurlredirect"
alue="http://yourwebsite.com/error">
```

Important: Both "STR-13" and the URL of the redirect need to be included in the string used to generate your request site security hash, as described in section 1.3. Failure to do so will result in the customer being shown an "Invalid details" error message.

If the only rule for redirects enabled on your site is STR-13, it will be triggered in all error cases (including declines).

If STR-13 **AND** STR-7 are enabled, all errors will cause STR-13 to be triggered **EXCEPT** in a declined final state, where STR-7 is triggered instead.

1.5.4 Fields returned

URL redirects using system rules (STR-13) will include the following fields of information, by default:

- transactionreference
- requestreference
- orderreference
- sitereference
- errorcode
- settlestatus
- paymenttypedescription

If request site security is enabled on your site, the redirect will also include the response site security hash (this is covered in further detail in section 1.5.5).

If you would like to include additional fields, you can update your POST to include stextraurlredirectfields. The following 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="<DOMAIN>/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>
```

See section 9.2 for a full list of supported domains for the <DOMAIN> placeholder.

You can configure custom rules that exclude the default fields listed above (see section 9.3).

Important: The names of all additional fields to be returned in the redirect need to be included in the string used to generate your request site security hash, as described in section 1.3. Failure to do so will result in the customer being shown an "Invalid details" error message.

1.5.5 Response site security

If request site security is enabled on your site, you will also receive a hashed responsesitesecurity value in any redirects sent to your system. We strongly recommend 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. Follow these steps to generate the hash:

Step 1

Append all **values** of the fields included in the redirect in **ASCII alphabetical order** (including any extra fields you have specified), with the password placed at the end (ignoring the responsesitesecurity field itself).

The password used when generating the hash is the same password previously agreed with the Support team when configuring your request site security (section 1.3).

For example, consider a redirect with the following fields:

- errorcode = 0
- orderreference = Order
- paymenttypedescription = VISA
- requestreference = RR555
- settlestatus = 0
- sitereference = test_site12345
- transactionreference = 2-44-66

Using the example above, we would have the following string generated, with your agreed password appended at the end of the string:

0OrderVISARR5550test_site123452-44-66PASSWORD

(Any blank fields are omitted from the hash)

Step 2

Hash the fields using SHA-256.

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

```
1a8b45c137c1d1df8ce6ff923421043f879a85a181e9c0d96a8904211af8b0b0
```

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

Check the hash matches

For valid redirects, the response site security hash that we generate must match the value you have generated using the steps above. This indicates that Secure Trading was the source of the redirect and that it has not been modified by the customer or a third party. If the hash you generate does not match that returned in the redirect, this potentially indicates that a field has been modified or that there is some other problem with the redirect. Please contact our Support team for assistance (see section 8.1).

1.5.6 Advanced

Using the MyST Rule Manager, you can configure redirects that happen in other scenarios. For further information, please refer to our online documents.

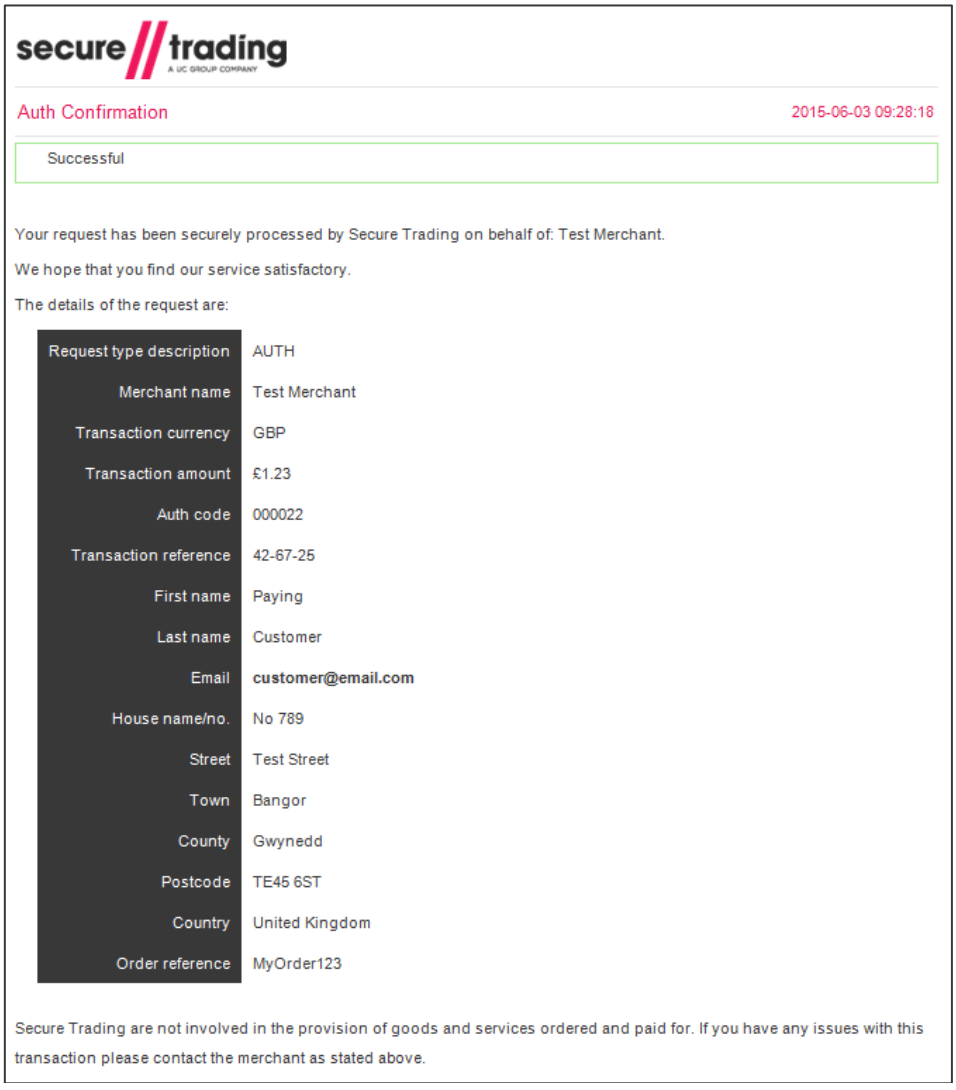
1.6 Email notifications

You can request 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

1.6.1 Customer emails

These are sent to the email address specified in the **billingemail** field. They are configured to be sent to customers following payment, summarising the transaction and acting as a receipt of payment for their records. By default, they look like this:



secure trading
A GC GROUP COMPANY

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.

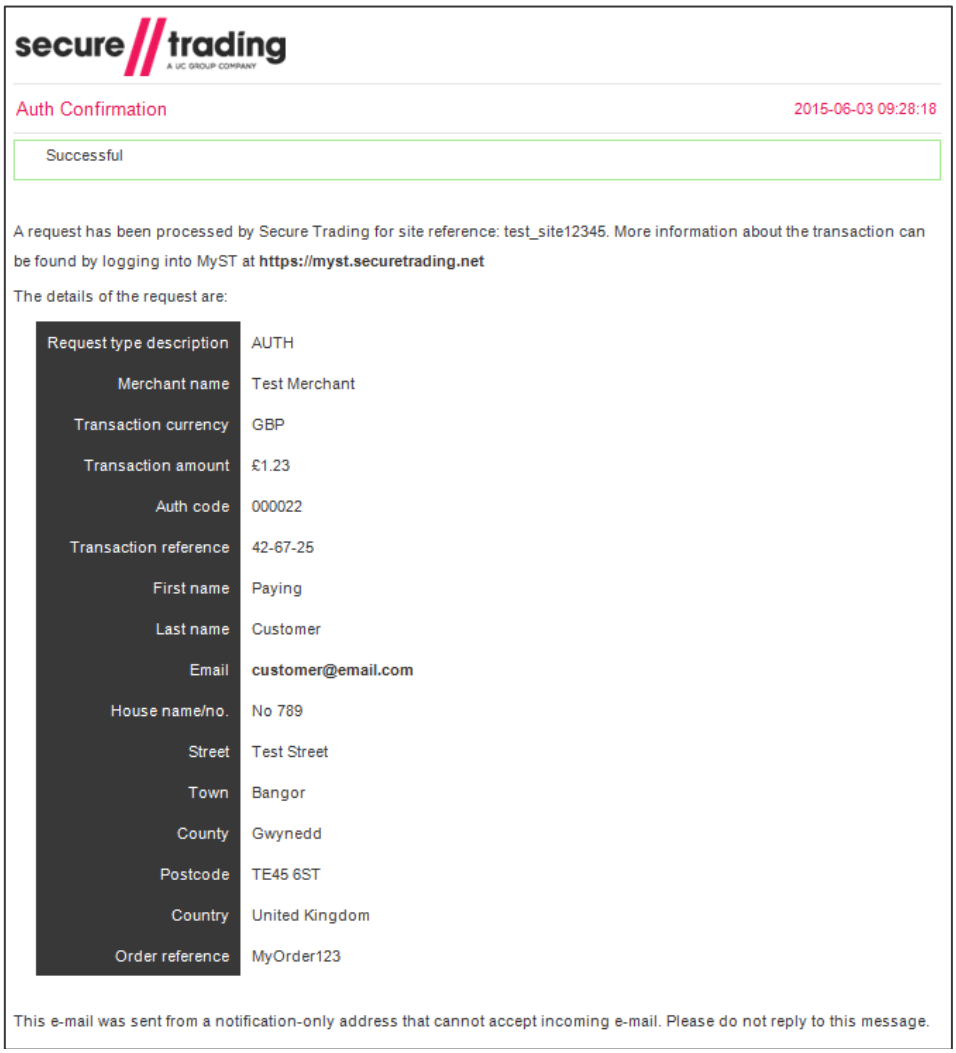
The details of the request are:

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.

1.6.2 Merchant emails

These are configured to be sent to members of your company or organisation, and are sent to an email address of your choosing. By default, they look like this:



secure trading
A GC GROUP COMPANY

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.

1.6.3 Enabling emails

It is simple 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">
```

Important: Any rule identifiers submitted (e.g. "STR-2") and the merchant email address (if submitted) need to be included in the string used to generate your request site security hash, as described in section 1.3. Failure to do so will result in the customer being shown an "Invalid details" error message.

1.6.3.1 Further information on the emails

- All emails are sent from no-reply@securetrading.com.
- You can specify multiple recipients provided addresses are comma-separated:
  e.g. "first@email.com,second@email.com"
- Email notifications for successful transactions have the subject: "Successful transaction processed".
- Email notifications for declined transactions have the subject: "Transaction declined".

1.6.4 Testing and troubleshooting

Once you have enabled the rules, you can test that this works on your test site reference. The emails are only sent when the following criteria have been met:

- The rule has been configured and activated on your site reference.
- For customer emails, the billingemail field must be submitted in the HTTPS POST, or entered by the customer on the Payment Pages.
- For merchant emails, the merchantemail field must be submitted in the HTTPS POST.

1.6.5 Advanced

You can use the MyST Rule Manager to perform more advanced customisation on email notifications, such as:

- Configure additional emails rules that have more specific conditions.
- Specify the reply to address and the subject.

(For further information, please refer to our online documents)

Additional features (see section 2.6 for further information):

- Customise the information displayed.
- Use HTML to completely redesign the layout of the email.

1.7 URL notifications

URL notification actions are requests that can be sent to a pre-defined URL. These notifications contain information about requests processed on your site.
Please note: We do not support localhost, loopback or multicast IP ranges in the URL.

1.7.1 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:

```
<!--This enables the successful URL notification rule-->
<input type=hidden name="ruleidentifier" value="STR-8">

<!--Update the below with the URL the notification will be sent to-->
<input type=hidden name="successfulurlnotification"
value="http://yourwebsite.com/successful">
```

Important: Both "STR-8" and the URL for the notification need to be included in the string used to generate your request site security hash, as described in section 1.3. Failure to do so will result in the customer being shown an "Invalid details" error message.

1.7.2 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:

```
<!--This enables the declined URL notification rule-->
<input type=hidden name="ruleidentifier" value="STR-9">

<!--Update the below with the URL the notification will be sent to-->
<input type=hidden name="declinedurlnotification"
value="http://yourwebsite.com/declined">
```

Important: Both "STR-9" and the URL for the notification need to be included in the string used to generate your request site security hash, as described in section 1.3. Failure to do so will result in the customer being shown an "Invalid details" error message.

1.7.3 Notifications for ALL requests

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

```
<!--This enables the all URL notification rule-->
<input type=hidden name="ruleidentifier" value="STR-10">

<!--Update the below with the URL the notification will be sent to-->
<input type=hidden name="allurlnotification"
value="http://yourwebsite.com/all">
```

Please note: When you include ruleidentifier STR-10 in the POST, you will receive notifications for ALL request types. For example, when processing a transaction with 3-D Secure enabled, you will receive two URL notifications; one for the **THREEDQUERY** request and another for the subsequent **AUTH** request.

Important: Both "STR-10" and the URL for the notification need to be included in the string used to generate your request site security hash, as described in section 1.3. Failure to do so will result in the customer being shown an "Invalid details" error message.

1.7.4 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 request, but if your system does not respond, Secure Trading will continue to resend notifications for up to 48 hours until confirmation is received.

If we do not receive confirmation within 48 hours, we will send an email with further details to the default email address associated with your site reference (contact the Support team to update this address; see section 8.1).

1.7.5 Fields returned

URL notifications using system rules (STR-x) will include the following fields of information, by default:

- transactionreference
- requestreference
- orderreference
- sitereference
- errorcode
- settlestatus
- paymenttypedescription

If request site security is enabled on your site, the notification will also include the response site security hash (this is covered in further detail in section 1.7.7).

If you would like to include additional fields, you can update your HTTPS POST to include stextraurlnotifyfields. The following 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="<DOMAIN>/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>
```

See section 9.2 for a full list of supported domains for the <DOMAIN> placeholder.

Important: The names of all additional fields to be returned in the notification need to be included in the string used to generate your request site security hash, as described in section 1.3. Failure to do so will result in the customer being shown an "Invalid details" error message.

1.7.6 Advanced

Using the MyST Rule Manager, you can configure URL notifications that are sent in other scenarios. For further information, please refer to our online documents.

1.7.7 Response site security

If request site security is enabled on your site, you will also receive a hashed responsesitesecurity value in any URL notifications sent to your system. We strongly recommend 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. Follow these steps to generate the hash:

Step 1

Append all **values** of the fields included in the URL notification in **ASCII alphabetical order** (including any extra fields you have specified), with the password placed at the end (ignoring the responsesitesecurity field itself).

The password used when generating the hash is the same password previously agreed with the Support team when configuring your request site security (section 1.3).

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

- errorcode = 0
- orderreference = Order
- paymenttypedescription = VISA
- requestreference = RR555
- settlestatus = 0
- sitereference = test_site12345
- transactionreference = 2-44-66

Using the example above, we would have the following string generated, with your agreed password appended at the end of the string:

0OrderVISARR5550test_site123452-44-66PASSWORD

(Any blank fields are omitted from the hash)

Step 2

Hash the fields using SHA-256.

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

```
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

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

Check the hash matches

For valid URL notifications, the response site security hash that we generate must match the value you have generated using the steps above. This indicates that Secure Trading was the source of the notification and that it has not been modified by the customer or a third party. If the hash you generate does not match that returned in the notification, this potentially indicates that a field has been modified or that there is some other problem with the notification. Please contact our Support team for assistance (see section 8.1).

1.8 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.

1.8.1 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 security code checks (see section 3.1 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.

1.8.2 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	Simulates a transaction decline.
600.10	Simulates an error processing the payment.

To simulate “Not matched” responses for AVS and security code 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 & security code checks. Please ensure your system is able to handle these scenarios.

1.8.3 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 (see section 1.9) or by configuring automated notifications (see section 1.7). 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: https://docs.securetrading.com/document/toolbox/error-codes/
- If you are expecting a transaction to be scheduled for settlement, ensure the settle status is “0” or “1”.
- Check the amount and currency of the transaction is correct.
- If you have configured redirects (1.3) or URL notifications (1.7) with request site security enabled, calculate the response site security hash and ensure it matches the value that we return.

1.9 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 monitored, 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 URLs:

- https://myst.securetrading.net/login (European Gateway)
- https://myst.securetrading.us/login (US Gateway)

For further information on the MyST interface, please refer to our **MyST documentation**.

1.10 Going live

After you have finished configuring your site and have tested thoroughly, follow the final steps below to begin processing live payments.

1.10.1 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.

1.10.2 Apply styling to live site reference

If you have modified the appearance of the Payment Pages using custom HTML, CSS and/or JavaScript (section 2.1), these changes will also need to be applied to your live site reference.

1.10.3 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 live site reference and request to go live. You will receive a response when your live site is ready to begin processing payments.

1.10.4 Make changes to your website

The POST described in section 1.1 will need to be updated to use your live site reference. This is achieved by modifying the site reference field submitted to Secure Trading. When your live site reference is referenced, transactions will be processed by your acquiring bank.

1.10.5 Live testing

Once you have switched to your live site reference, we recommend performing 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 (see section 1.9). Therefore you can cancel transactions processed on live cards.

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

You're all set!

Remember to sign in to MyST and to check your transactions regularly to ensure payments are being processed successfully (section 1.9).

If you need assistance, please contact the Support team.
See section 8.1 for contact details.

1.11 Settlement

The following procedure 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 we submit a batch of all transactions that are pending settlement to your acquirer. This process is called settlement and is outlined below:

Step 1: Settlement file submitted to acquirer

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

Step 2: Funds transferred to your bank account

When the acquirer has received the settlement file, 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 not determined by Secure Trading.

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

*Certain acquiring banks have different procedures in regards to settlement with payments made with Mastercard. See section 7.3 for further information.

1.11.1 Deferred settlement

Settlement can be deferred for certain transactions. You can request this by modifying the POST (using settlestatus or settleduedate fields; section 9.1.4), or transactions may be deferred by our internal fraud system (if enabled on your account; section 3.3). You should therefore sign in to MyST on a regular basis, to check the status of your transactions (see section 1.9).

1.11.2 Split shipment

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.

We support split shipments for certain acquirers. For further information, please refer to the Split Shipment Guide.

*Certain acquiring banks have different procedures in regards to settlement with payments made with Mastercard. See section 7.3 for further information.

1.11.3 Settle status

Settle status	Caption	Description

0	Pending settlement	Transaction that has been authorised by card issuer for payment.
		// 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 section 3).

1	Manual settlement	Transaction that has been authorised by card issuer for payment.
		// Settles automatically.
		// Does not require further action from merchant.
		// Bypasses fraud and duplicate checks, if enabled (see section 3).
		// Can be updated or cancelled.

10	Settling	Details of this transaction have been sent to the acquiring bank for settlement.
		// 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. // 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.
		// 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 section 3).
		// If left in a suspended state Secure Trading will automatically cancel the transaction 7 days after the authorisation date.
		(This limit is extended to 31 days for pre-authorisations – see section 7.3)

3	Cancelled	Transaction has been cancelled and will not settle.
		// 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.

2 Customise

You can customise the appearance and layout of your Payment Pages by using the following features:

Appearance and layout

This section outlines how to change the appearance and layout of your Payment Pages to better reflect your brand identity. **See section 2.1.**

Custom logo

You can easily update your Payment Pages to display your own logo, without needing to write any custom mark-up. **See section 2.2.**

Locale

By updating your POST to Payment Pages, you can change the language and formatting of text displayed in the browser, in order to better suit the needs of your international customers. **See section 2.3.**

iframes

You can use iframes to display the Payment Pages within the layout of your website. **See section 2.4.**

Required fields

You can specify fields to be required on your Payment Pages. If the customer fails to provide information in all the required fields or enters invalid information, the payment will not continue and the field in question will be highlighted on-screen. This allows the customer to make corrections and try again. **See section 2.5.**

Email customisation

This section explains how to customise the appearance of automated emails sent following transactions. **See section 2.6.**

2.1 Appearance and layout

This section outlines how to change the appearance and layout of your Payment Pages to better reflect your brand identity.

You can customise the appearance of your Payment Pages by submitting the field **stprofile**. By specifying different **stprofile** values in each POST to Payment Pages, you can apply different styling to each session.

There are two types of **stprofile**:

- Default **stprofile**
  Fastest way to get up-and-running

  We provide a number of standard profiles that are ready to use.
  Default profiles are responsive and suit most use-cases without modification.

  See section 2.1.1.

- Custom **stprofile**
  Provides you with advanced customisation options

  Apply your own HTML and CSS mark-up.
  Further customise the pages using Javascript.
  Upload your mark-up to our system using MyST, and reference when needed.

  See section 2.1.2.

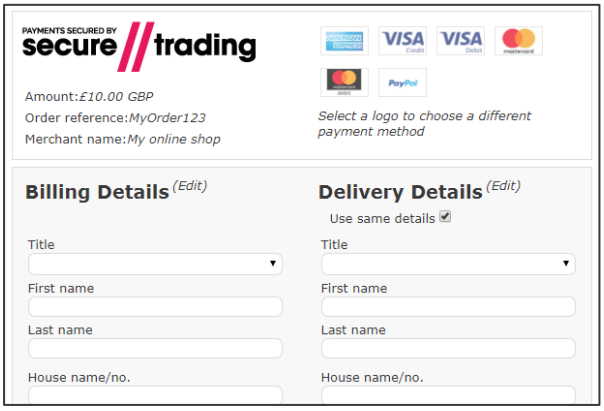
2.1.1 Default stprofile

We provide a number of standard profiles that are ready to use.
Default profiles are responsive and suit most use-cases without modification.

There are two different options for specifying default **stprofiles**:

1. Update your POST to Payment Pages to include an extra field that specifies the desired profile to be applied (as described below).
2. Contact our Support team to assign a specific default **stprofile** that will be applied to all of your Payment Pages sessions (see section 8.1).

2.1.1.1 Standard layout



The standard layout for a default **stprofile** is to first display the billing and delivery address fields.

This is followed by fields for the customer to enter their payment credentials. These fields are dependent on the payment method selected by the customer, so a card payment such as Visa Debit would require the customer to enter their card number, but a bank transfer method may instead prompt the customer for their bank account number.

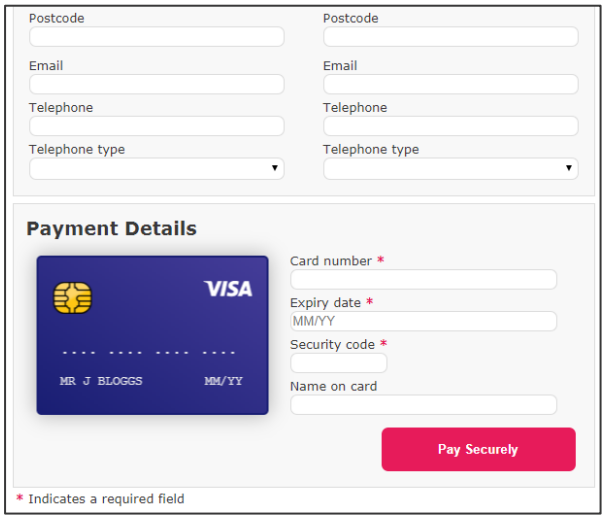
Ensure the following is included in your POST to Payment Pages:

```
<input type="hidden"
name="stprofile" value="default">
```

You can submit a customer's billing details in the post to Payment Pages (see section 9.1.2) and apply one of our default **stprofile** options to hide unnecessary address and contact fields from the form on the Payment Pages.

We strongly recommend that you ensure all of your transactions have a billing address, as these details are used in AVS checks to help prevent attempts at fraud (see section 3.1).

2.1.1.2 Dynamic card preview – Show the address fields



If you would like to display a live preview of the customer's card, beneath the form where the customer enters their address details, include the following in your POST to Payment Pages:

```
<input type="hidden"
name="stprofile" value="default">

<input type="hidden"
name="stdefaultprofile"
value="st_paymentcard">
```

Important: If including the above in your POST, "st_paymentcard" needs to be included in the string used to generate your request site security hash, as described in section 1.3. Failure to do so will result in the customer being shown an "Invalid details" error message.

2.1.1.3 Dynamic card preview – Hide the address fields

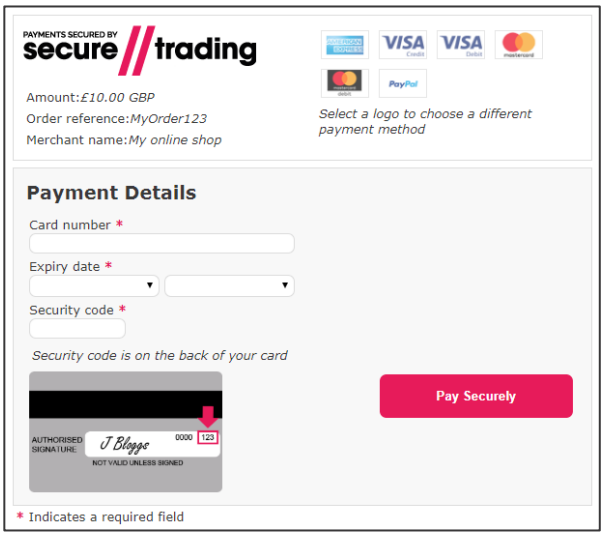
If you would like to hide the address fields and display a live preview of the customer's card, include the following in your POST to Payment Pages:

```
<input type="hidden"
name="stprofile" value="default">

<input type="hidden"
name="stdefaultprofile"
value="st_paymentcardonly">
```

Important: If including the above in your POST, "st_paymentcardonly" needs to be included in the string used to generate your request site security hash, as described in section 1.3. Failure to do so will result in the customer being shown an "Invalid details" error message.

2.1.1.4 Static card image – Hide the address fields



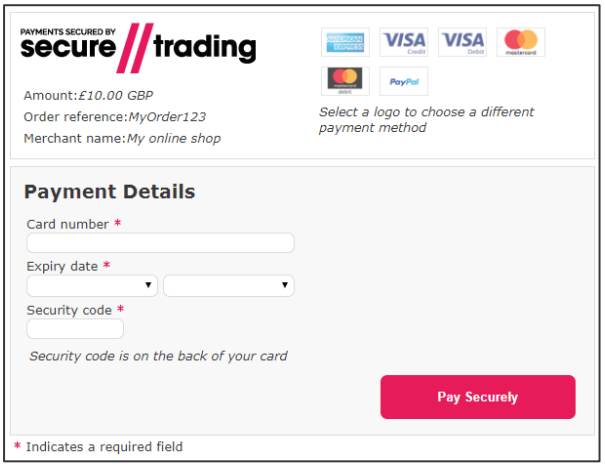
If you would like to hide the address fields and only prompt for the payment details, include the following in your POST to Payment Pages:

```
<input type="hidden"
name="stprofile" value="default">

<input type="hidden"
name="stdefaultprofile"
value="st_cardonly">
```

Important: If including the above in your POST, "st_cardonly" needs to be included in the string used to generate your request site security hash, as described in section 1.3. Failure to do so will result in the customer being shown an "Invalid details" error message.

2.1.1.5 No card image – Hide the address fields



If you would like to hide the address fields and image of the card, and only prompt for the payment details, include the following in your POST to Payment Pages:

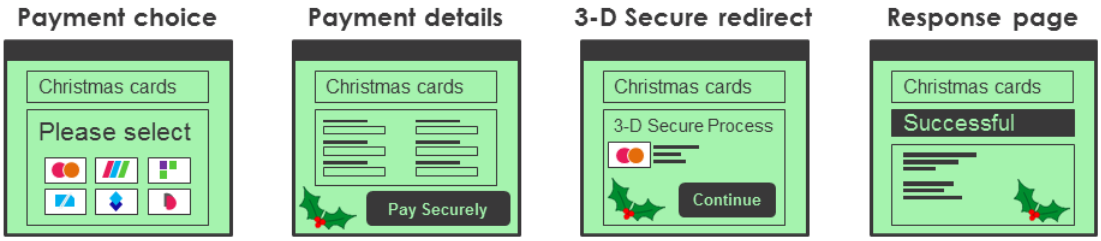
```
<input type="hidden"
name="stprofile" value="default">

<input type="hidden"
name="stdefaultprofile"
value="st_iframe_cardonly">
```

Important: If including the above in your POST, "st_iframe_cardonly" needs to be included in the string used to generate your request site security hash, as described in section 1.3. Failure to do so will result in the customer being shown an "Invalid details" error message.

2.1.2 Custom stprofile

You can develop your own **stprofile**s. For example, if you were hosting an online shop for purchasing greeting cards, you could develop **stprofile**=christmas for customers purchasing Christmas cards. This uses HTML, CSS and Javascript files uploaded to your account to provide a customised appearance and layout.



For basic changes to the styling (hiding certain elements, changing fonts and colours, etc.), you can opt to upload a single CSS file that will apply changes to all four pages for a single stprofile. The file is called <stprofile>.css (e.g. 'christmas.css').

Likewise, you can upload your own JavaScript file for an stprofile, using the filename <stprofile>.js (e.g. 'christmas.js').

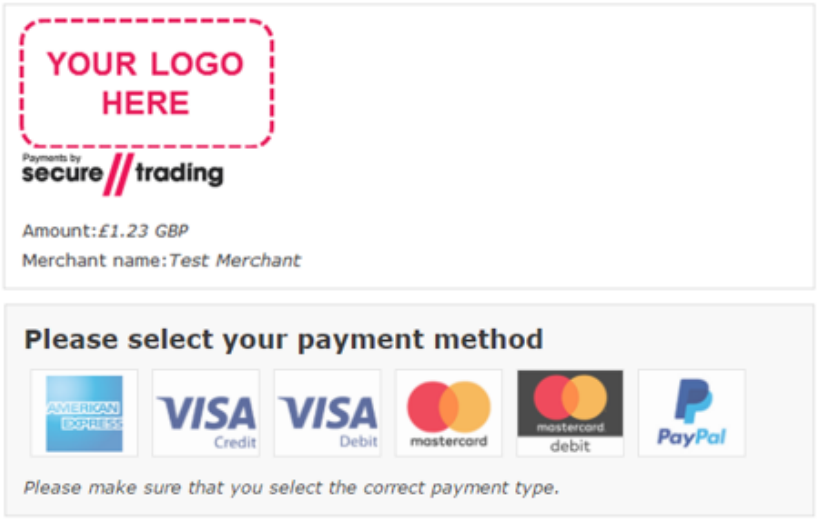
You can perform deeper customisation by modifying the HTML on each page.

If you opt to hide any default fields from the page (e.g. customer delivery address), in favour of submitting these details in the HTTPS POST, please ensure these fields are validated against our specification. If the data submitted is invalid and the fields are not visible on the page, the customer will be unable to correct the field error and continue with their payment.

For instructions on how to apply custom HTML mark-up to your Payment Pages, please refer to our online guide:
http://www.securetrading.com/paymentpages/customisation.html

2.2 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.

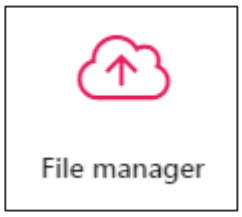


To configure, follow these steps:

1. Sign in to MyST (see section 1.9).

2. Click "**Sites**" from the side-bar and then click on your site reference (or alternatively search for your site reference using the universal search functionality).
   Your customisations will only be performed on this site reference.
   *The image will be displayed on all **stprofiles** (section 2.1) for this site reference.*

3. Click the "**File manager**" icon.
   You must have the role 'Site admin', 'Developer', 'Developer 2' or 'File Manager' to access the File Manager.



4. Upload an image called "merchantlogo" (e.g. "merchantlogo.png").
   We support the following image extensions: bmp, gif, jpeg, jpg, png, svg, tif, tiff.
   Maximum file size is 1024kb.
   We recommend against using an image with dimensions exceeding 256x256px.

Please note that it can take up to 10 minutes for uploaded files to be listed in the MyST File Manager and for your changes to be reflected on your Payment Pages.

For information on the MyST File Manager, see our **MyST documentation**.

2.3 Locale

By updating your POST to Payment Pages, you can change the language and formatting of text displayed in the browser, in order to better suit the needs of your international customers. Read on to learn how.

2.3.1 Modify the POST

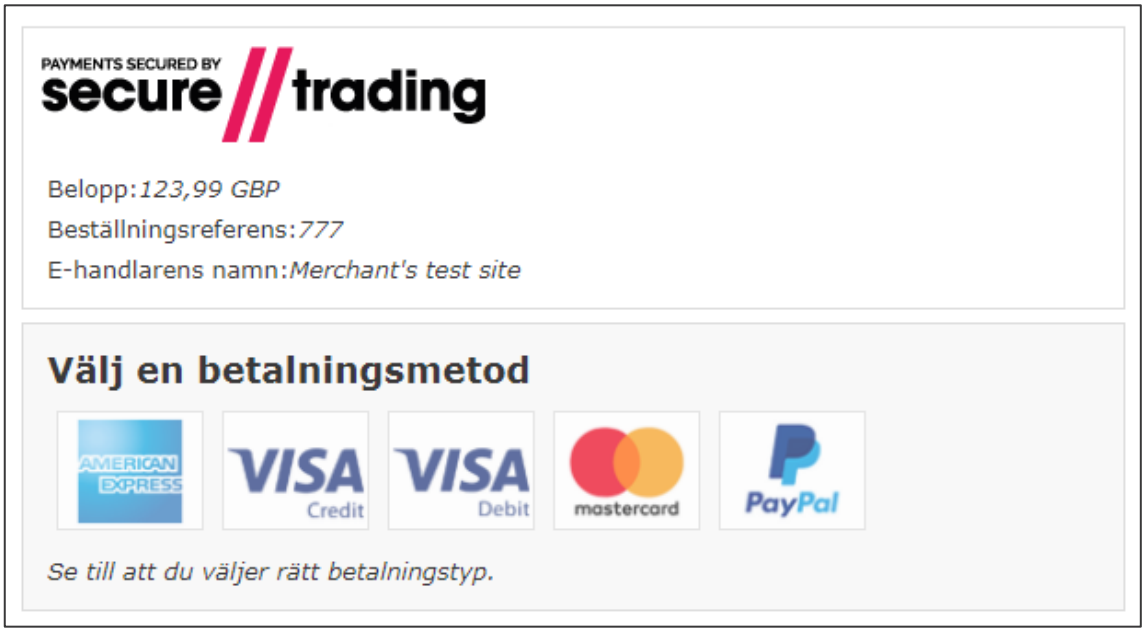
Please refer to the following HTML example. Your system will need to submit the additional field **locale**, highlighted below in **bold**. We will use the value of this field when rendering the page, to ensure the correct language is displayed to the customer.

Please note that only pages hosted by Secure Trading are translated. If the customer is being redirected to a page hosted by a third-party (e.g. when using an APM), the language displayed is controlled by the aforementioned third party.

The following example sets the language of the Payment Pages to Swedish:

```
<html>
<body>
<!--YOUR HTML-->
<form method="POST" action="<DOMAIN>/process/payments/choice">
<!--Other fields-->
<input type="hidden" name="locale" value="sv_SE">
<input type="submit" value="Pay">
</form>
</body>
</html>
```

See section 9.2 for a full list of supported domains for the <DOMAIN> placeholder.



For a full list of supported territories, refer to section 9.1.6.

2.4 Iframes

You can use iframes to display the Payment Pages 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.

Iframes may not be rendered correctly in certain web browsers. (e.g. certain mobile web browsers)

We provide additional HTML/CSS mark-up for cases where iframes are displayed within iOS browsers. Refer to section 9.5.

PayPal and Apple Pay do not support iframe integrations.

2.4.1 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="<DOMAIN>/process/payments/choice?sitereference=test_site12345&mai
namount=10.00&currencyiso3a=GBP&version=2&stprofile=default"
width="100%" height="600" scrolling="auto"
style="border:0px;"></iframe>
```

See section 9.2 for a full list of supported domains for the <DOMAIN> placeholder.

The example above includes the minimum required fields needed in the URL (highlighted in **bold**). For further information on these fields, or additional fields that can be included, see section 9.4.

2.4.2 Iframe-optimised layout

You can easily update your POST to Payment Pages to hide the address fields from the page. We provide an alternative default layout that is more compact and easier to fit within an iframe.

This configuration presumes that you are prompting the customer for the necessary billing and delivery address details on your own website and including these in the POST to Payment Pages, or that these address details are not required (e.g. purchase made by a returning customer).

See section 2.1.1.5 for instructions.

2.4.2.1 Advanced

You can perform further customisation to the appearance and layout of the Payment Pages within an iframe by modifying the HTML/CSS mark-up. See section 2.1.2 for further information.

2.5 Required fields

You can specify fields to be required on your Payment Pages. If the customer fails to provide information in all the required fields or enters invalid information, the payment will not continue and the field in question will be highlighted on-screen. This allows the customer to make corrections and try again.

By default, the customer is required to enter their payment details (card number, expiry date, security code) on the Payment Pages. This section of the document explains how to specify additional fields to be required.

If you are integrating with PayPal, you must use the MyST Rule Manager to specify required fields, as explained in section 2.5.2.

2.5.1 Customising the POST (for card payments only)

You can modify your POST to Payment Pages to specify required fields for the customer. This is demonstrated in the following HTML example. The fields specified as required are highlighted in **bold**; the customer will be required to enter these fields on your Payment Pages in addition to their payment details:

```
<html>
<body>
<!--YOUR HTML-->
<form method="POST" action="<DOMAIN>/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>
```

See section 9.2 for a full list of supported domains for the <DOMAIN> placeholder.

The fields that you specify as required in the POST need to be included in the string used to generate your request site security hash, as described in section 1.3. Failure to do so will result in the customer being shown an "Invalid details" error message.

2.5.2 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 PayPal to enter their payment details.

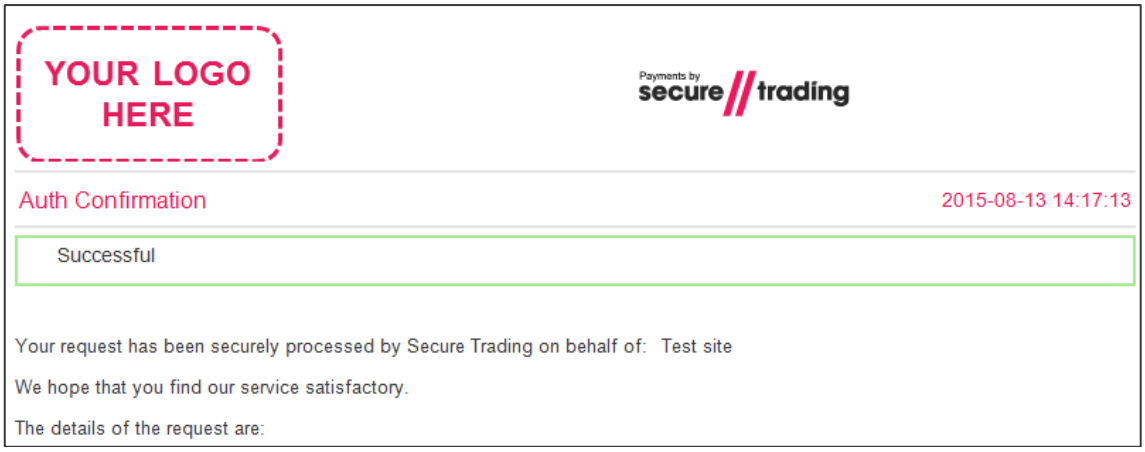
Sign in to MyST and create a rule with action type 'Payment pages required fields'. For information on how to get started with the Rule Manager, please refer to our online documents.

2.6 Email customisation

This section explains how to customise the appearance of automated emails sent following transactions (see section 1.6 to enable emails).

2.6.1 Include your logo

You can include your logo at the top of automated emails without needing to write any custom mark-up. This is shown alongside a small "Payments by Secure Trading" icon.



To configure, follow these steps:

- Sign in to MyST (see section 1.9).
- Click "**File manager**" from the options on the left.
  You must have the role 'Site admin', 'Developer', 'Developer 2' or 'File Manager' to access the File Manager.
- Choose your site reference from the upper-left and click "**Change site**".
  Your customisations will only be performed on this site reference.
  *The image will be displayed on all **stprofiles** (section 2.1) for this site reference.*
- Upload an image called "emaillogo" (e.g. "emaillogo.png").
  We support the following image extensions: bmp, gif, jpeg, jpg, png, svg, tif, tiff.
  Maximum file size is 1024kb.
  We recommend against using an image with dimensions exceeding 256x256px.

Please note that it can take up to 10 minutes for uploaded files to be listed in the MyST File Manager and for your changes to be reflected in emails that we send.

For information on the MyST File Manager, please refer to our **MyST documentation**.

2.6.2 Using mark-up

You can upload custom HTML to customise the appearance of the emails sent to customers or members of your organisation. Each file will need to contain HTML mark-up that makes use of st.fields (see example in section 2.6.2.1). Using the MyST File Manager, you will need to upload the following files:

- defaultsuccessfulcustomer.email - Defines appearance of email sent to customer following a successful transaction.
- defaultdeclinedcustomer.email - Defines appearance of email sent to customer following a declined transaction.

The files described above will only modify the appearance of emails when stprofile is set to “default” in the POST.

If you are using custom mark-up to customise the appearance of the Payment Pages (section 2.1), you can replace “default” with your stprofile name:

e.g. For stprofile "christmas", the file containing HTML for a success customer email would be named: christmassuccessfulcustomer.email

2.6.2.1 Customer email example HTML

The following is an example of HTML mark-up for a simple email to be sent to the customer following a successful payment.

- You can include fields listed in section 9.1, by including {{st.<fieldname>.value}}.
  - **Note:** You can also reference custom fields you have included in the POST.
- You can opt to reference custom images by including {{st.resource.<imagename>}}.
  - **Note:** Image names are case-sensitive.
- You must always include at least one of the following, that displays Secure Trading’s logo in the email:
  - {{stresource.securetradingprocessed.png}} *(Small logo)*
  - {{stresource.securetradinglogo.png}} *(Full-sized logo)*
  - {{stresource.securetradinglogo-inverted.png}} *(Logo for dark backgrounds)*

```
<html>
  <body>
    <img src="cid:{{stresource.yourimage.jpg}}"/>
    <img src="cid:{{stresource.securetradingprocessed.png}}"/>
    <p>Thank you for your order received today</p>
    <ul>
      <li>Amount: {{st.mainamount.value}}</li>
      <li>AuthCode: {{st.authcode.value}}</li>
      <li>Reference: {{st.transactionreference.value}}</li>
    </ul>
  </body>
</html>
```

2.6.2.2 Testing and troubleshooting

Now you have uploaded the required files, you can test that this works on your test site reference. Email mark-up is only applied when the following criteria have been met:

- The required files are uploaded to the same site reference the requests are being processed on.
- The stprofile submitted in the POST matches the stprofile in the name of the .email file uploaded.

3 Protect

We provide the following features and services to minimise the risk of fraud on your account:

AVS and security code checks

The Address Verification System and security code checks provide you with a further level of security to a transaction, allowing additional checks regarding the validity of the address and security code information supplied by the customer. **See section 3.1.**

3-D Secure v2

3-D Secure v2 is a protocol designed to reduce fraud and chargebacks during e-commerce transactions. It allows card issuers to provide an extra level of protection, by authenticating customers at point of sale (e.g. with a secret PIN or password). **See section 3.2.**

Fraud checks

When enabled on your account, the fraud check service analyses authorised transactions for attributes that may be considered suspicious, prior to settlement being performed. **See section 3.3.**

Duplicate checks

This is to automatically prevent assumed duplicate transactions (e.g. If the customer refreshes their browser and inadvertently sends two requests). **See section 3.4.**

Protect Plus

Provides an additional layer of protection. It makes use of the industry's largest negative database to perform a comprehensive suite of fraud assessments, including identity checks against the UK electoral roll and BT databases. **See section 3.5.**

Viewing the results of checks

This section explains how to use MyST to view the results of checks performed on transactions processed on your account.
See section 3.6.

3.1 AVS and security code checks

The Address Verification System and security code checks provide you with a further level of security to a transaction, allowing additional checks regarding the validity of the address and security code information supplied by the customer.

3.1.1 Introduction to AVS

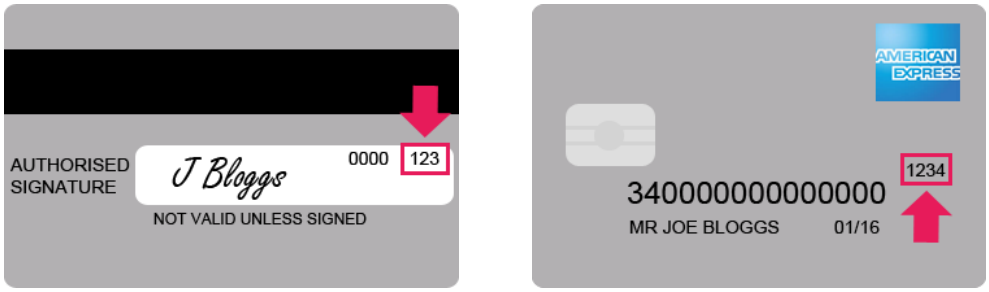
A customer's address is checked against the address that the card issuer holds for that card. The issuing bank will indicate to the acquiring bank whether there is a match between the entered address and the registered card address. The checks performed are focused on the house number and postcode provided by the customer.

3.1.2 Introduction to security code checks

The security code is a three or four digit number printed on credit and debit cards. It is not stored by Secure Trading, and also must never be stored by merchants.

It is imperative that you never store the customer's security code. Please ensure that no log files or databases contain the security code information on your system.

The number is often printed on the back of the card, on the signature strip, as pictured below-left. Alternatively, on American Express cards the security code can be found on the front of the card, on the right–hand side, above the embossed card number, as pictured below-right:



The security code that the customer has entered is checked against the security code that the card issuer holds for their card. The issuing bank will indicate to the acquiring bank whether there is a match between the entered security code and the correct security code associated with the card.

3.1.3 Process overview

Here is how the AVS and security code checks fit into the standard payment process:

1. The customer opts to perform a payment and their details are passed on to Secure Trading.
2. Secure Trading submits this information to the acquiring bank.
3. The acquiring bank contacts the customer's bank. The customer's bank checks the premise, postcode and security code entered by the customer against what is on their records.
4. The acquiring bank returns the results of these checks to Secure Trading.
5. Secure Trading assigns response codes and make this information available to you.
6. Depending on your account configuration, Secure Trading may perform certain actions on the transaction if the results of the AVS and security code checks do not meet a required standard. This behaviour is configured as part of your **security policy** (explained in section 3.1.6).

Some acquirers will use the results of the AVS or security code checks to decline the transaction, if either the address or security code entered by the customer is incorrect. Others will authorise the transaction and allow you to decide whether or not to continue with the transaction.

3.1.4 Requirements

3.1.4.1 Supported cards and banks

The availability of the AVS and security code check facility 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.

Security code checks are performed on all Visa, Mastercard and American Express branded cards worldwide and the results are checked internationally by all acquirers.

Please contact our Support team (see section 8.1) for further information on supported acquirers and card types.

3.1.4.2 Required fields

For checks to be successfully performed on the customer's details, the customer will need to input their billing address and card details (including the security code) on the Payment Pages.

If the customer fails to submit the required information, the checks will return a "Not given" response. We cover the AVS / security code responses in section 3.1.5.

3.1.5 Response codes

There are four different possible responses following AVS and security code checks. Each response is assigned a distinct code, as shown in the following table:

Code	Description	Comment
0	"Not given"	Your acquirer was not provided with the information required to perform this check.
1	"Not checked"	Your acquirer 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.

A "Not checked" response may be that the card issuer does not support address or security code checking for the card supplied or that the information was not provided. Most foreign cards issued will not be address checked.

Together, the AVS and security code checks consist of three total checks, and we assign a response code for each:

- Billing premise
- Billing postcode
- Card security code

For information on the viewing the results of AVS and security code checks, see section 3.6.

3.1.6 Security policy

Your account's security policy consists of preferences on how we respond to instances where the address (premise & postcode) and security code entered by the customer does not directly match those found on the card issuer's records. We can automatically suspend transactions that return certain response codes listed in section 3.1.5.

By default, we suspend all transactions where the security code check returns a "Not matched" response.

This behaviour can be completely disabled if preferred. Alternatively, the criteria can be expanded to suspend in more situations.

To discuss or make changes to your security policy, please contact Support (see section 8.1).

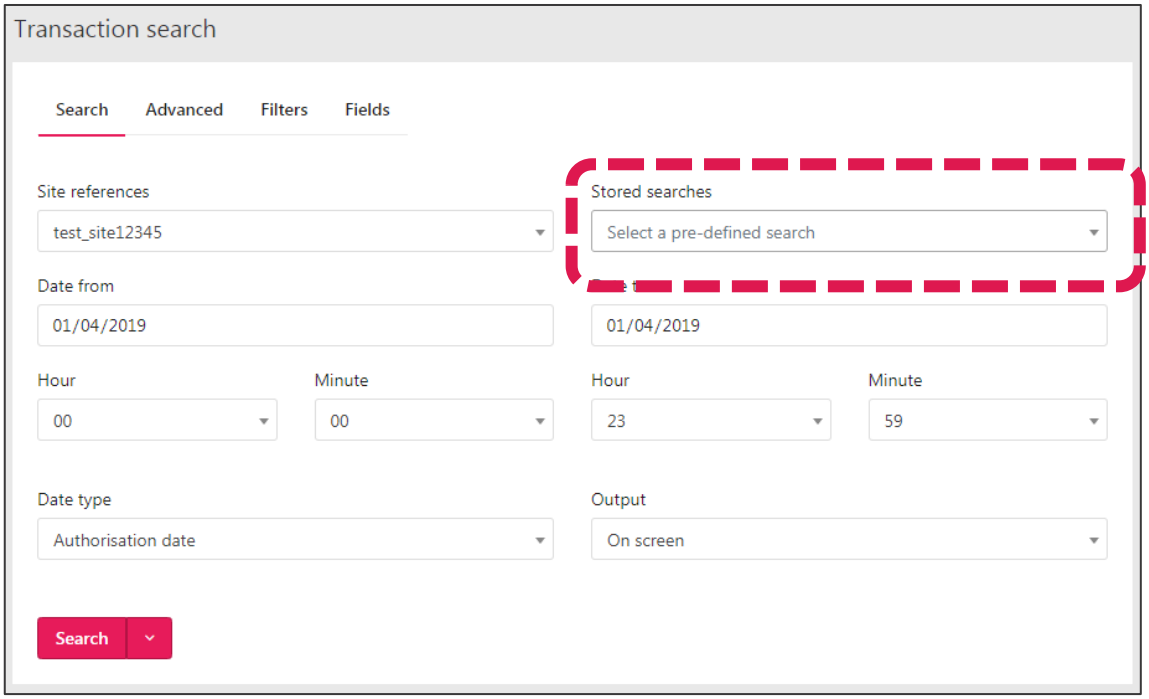
3.1.7 Account checks (opt-in)

Account checks are only available for certain acquirers.
Contact the Support team for further information (see section 8.1).

An account check is a type of request that performs the AVS and security code checks without reserving funds on the customer's account. When enabled, account checks are performed immediately prior to each standard authorisation on your account.

To enable account checks, you will need to contact the Support team to opt-in (see section 8.1). We strongly recommend enabling rules on your account that automatically prevent authorisations from being processed, when the account checks indicate that the security code the customer entered didn't match the value printed on the back of their card. Such rules can only be configured by Support.

Each account check has a unique transaction reference and you can use this to view details of the request in MyST. They are displayed in MyST as request type "ACCOUNTCHECK". Default transaction searches only display standard "AUTH" requests, but you can opt to have all requests processed on a site reference displayed by changing the "Stored searches" drop-down to the blank option, as shown below, before clicking "**Search**":



For information on viewing the results of AVS and security code checks, see section 3.6.

3.2 3-D Secure v2

3-D Secure v2 is a protocol designed to reduce fraud and chargebacks during e-commerce transactions. It allows card issuers to provide an extra level of protection, by authenticating cardholders at the point of sale (e.g. with a secret password or biometrics) if the payment is deemed high risk.

3.2.1 Process overview

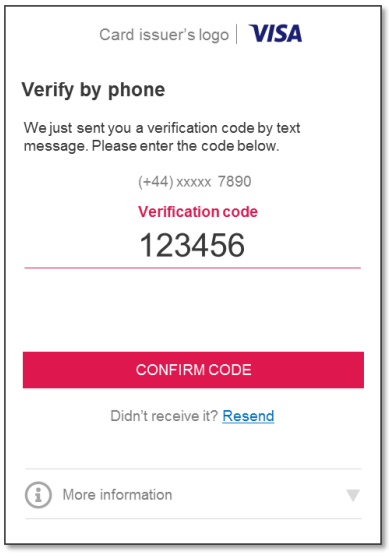
***Note: You will still benefit from the merchant liability shift, even when payment authentication is bypassed.**

3.2.2 What are the advantages?

- Reduces the likelihood of fraudulent transactions from being completed.
- In the event of a dispute with the transaction at a later date, the card issuer will take financial responsibility for the chargeback in most instances.

Note: *The liability issues associated with 3-D Secure transactions lie outside the scope of this guide. For further info, please refer to our question on the liability shift in our FAQs.*

3.2.3 What the customer sees



After the customer has entered their card details, checks are performed behind-the-scenes using metadata made available by their browser. In most cases, the transaction is deemed low-risk, and the customer will briefly be shown a holding message before the payment is processed (without needing to enter further information).

Alternatively, in cases where the customer is deemed sufficiently high-risk, they will be displayed an overlay for authentication, hosted by the Access Control Server (ACS), where they will be prompted to verify their identity (e.g. through biometrics, such as a finger-print reader, or by entering a PIN).

If authentication is successful, the transaction will be processed.

3.2.4 Configuration

Most merchants will already have 3-D Secure v1 enabled on their site reference(s).

To upgrade your existing 3-D Secure v1 implementation on your test site reference to v2, please contact our Support team.

To check if your live site can be upgraded to enable 3-D Secure version 2, please contact our Support Team (see section 8.1).

3.2.5 Benefits

3.2.5.1 Enhanced data checks

The 3-D Secure 2.0 protocol introduces support for the seamless transmission and checking of a richer set of metadata and session data during the transaction, allowing the majority of payments - which are deemed low risk – to be processed without interrupting customers to perform authentication. Authentication is instead only performed on the minority of payments that are deemed high risk. This reduces the time that the average consumer takes to complete a transaction.

3.2.5.2 Easier authentication

Rather than purely relying on PIN or passwords that the customer may struggle to remember, authentication can now be performed by biometrics (fingerprint / facial recognition) or sending a code to a customer's mobile device. This makes it easier for your customers to complete payments and ultimately reduces shopping cart abandonment.

3.2.5.3 Native mobile support

3-D Secure has been updated to provide comprehensive support for modern mobile devices, simplifying the authentication process for all customers, regardless of the type of device used to process the payment.

3.2.5.4 Liability-shift

In addition to reducing the likelihood of fraudulent transactions, in the event of a dispute with the transaction at a later date, the card issuer will take financial responsibility for the chargeback in most instances.

Note: *The liability issues associated with 3-D Secure transactions lie outside the scope of this guide. For further info, please refer to our question on the liability shift in our FAQs.*

3.3 Fraud checks (opt-in)

When enabled on your account, the fraud check service analyses authorised transactions for attributes that may be considered suspicious, prior to settlement being performed. This allows you to manually inspect and manage suspicious transactions processed on your account. These checks are performed at pre-defined times throughout the day.

Secure Trading cannot guarantee to identify all fraudulent transactions.

Fraud checks are disabled by default on all new site references. To enable fraud checks on your account, please contact the Support team (see section 8.1).

3.3.1 Fraud rating

The fraud check analyses all transactions processed on your account and assigns a numerical **fraud rating**, which indicates the level of risk based on a number of pre-defined criteria.

- Before the fraud checks have been processed, the fraud rating will be -1.
- Following the processing of the fraud checks, a fraud rating of 0 indicates that no suspicious characteristics were detected.
- Every suspicious attribute found by the fraud checks will increment the fraud rating. A higher fraud rating indicates a higher likelihood of fraud.
- All transactions with a fraud rating of 2 or higher are collated into a daily email notification sent to the email address associated with your account.
- By default, we will suspend all transactions with a fraud rating of 5 of higher.

You can configure the thresholds that trigger these actions (e.g. in order to reduce the occurrences of false-positives) by contacting the Support team (see section 8.1).

For information on how to view the fraud rating, see section 3.6.

For further information on Fraud Checks, including the criteria we use to calculate the fraud rating, please refer to the fraud checks document:
http://www.securetrading.com/wp-content/uploads/2014/12/Fraud-Checks.pdf

3.4 Duplicate checks (opt-in)

When enabled on your account, duplicate checks suspend transactions that appear identical to previous transactions processed within the last 15 minutes. This is to automatically prevent assumed duplicate transactions (e.g. If the customer refreshes their browser and inadvertently sends two requests).

To enable duplicate checks on your account, please contact our Support team (see section 8.1).

3.5 Protect Plus (opt-in)

Provides an additional layer of protection. It makes use of the industry's largest negative database to perform a comprehensive suite of fraud assessments, including identity checks against the UK electoral roll and BT databases.

3.5.1 How it works

3.5.1.1 What checks are performed?

We analyse the customer's billing, delivery and payment details using a rule-based system to detect suspicious patterns in user activity. Our system will assist in making a decision on whether to process a customer's transaction based on the perceived level of risk.
Checks performed include:

- 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.

Protect Plus does not guarantee against fraud. You should consider all data regarding a transaction before accepting the payment.

3.5.1.2 What happens after the checks are performed?

The Protect Plus system will analyse transaction details and one of the following statuses:

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

By default, we automatically suspend authorised transactions where the results are "CHALLENGE" or "DENY". This will allow you to investigate further and make a more informed choice on whether or not to authorise a suspicious transaction. This behaviour can be changed. Please contact the Support team for further information (see section 8.1).

3.5.2 Configuration

To enable Protect Plus on your Secure Trading account, please contact the Sales team (see section 8.2). Once Protect Plus has been enabled, it will automatically be processed with every payment made through your payment page, without any additional configuration on your system. It is recommended that your system submits as much data as possible as this will improve the accuracy of the checks. See section 9.1 for a list of fields that can be included in your POST to Payment Pages.

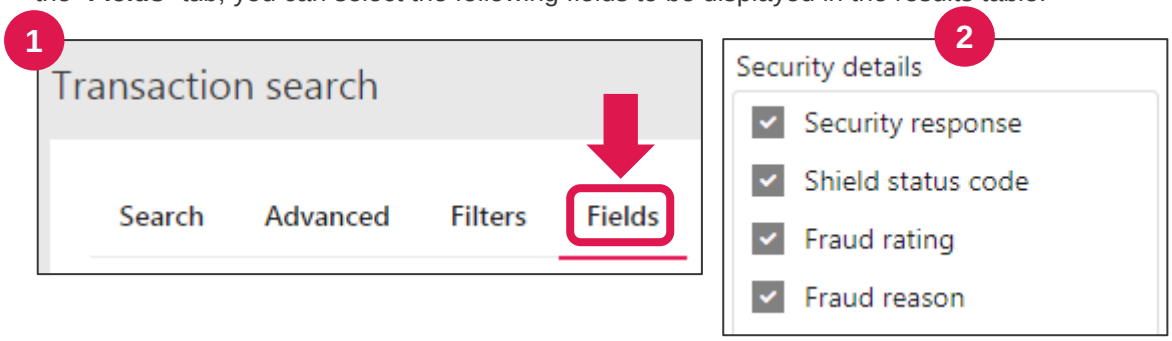
For further information on Protect Plus, please refer to the Protect Plus Guide: http://www.securetrading.com/wp-content/uploads/2014/12/Protect-Plus-Guide.pdf

3.6 Viewing the results of checks

MyST is a password-protected online management area which allows all Secure Trading merchants to monitor their transactions and manage their account. If you're new to MyST, we recommend reading our **MyST documentation** and familiarise yourself with the transaction search page and understand how to view transactions.

3.6.1 The transaction search page

The results of Protect checks can be viewed in MyST. On the "**Transaction search**" page, under the "**Fields**" tab, you can select the following fields to be displayed in the results table:



Field name	Description
Security response	Shows the results of AVS and security code checks (see section 3.6.2).
Shield status code	Shows the results of Protect Plus checks.
Fraud rating	Shows the fraud rating.
Fraud reason	Shows how the fraud rating was calculated (refer to the **Fraud Checks document** for info on how to interpret this field).

You can select additional fields of interest for inclusion in the search output, and then click "**Search**" to search your site reference(s) when ready. The results will look like this:

Reference	Status	Curr	Settle amount	Sec resp	Fraud rating	Fraud reason
72-5-126	Pending	GBP	£100.00	222	0	
72-5-125	Pending	GBP	£200.00	220	0	
72-5-124	Suspended	GBP	£300.00	400	3	PS

You can click on a transaction reference to view further details for the transaction.

3.6.2 Further information on security response

On the search page, the security response has been condensed to three digits:

- The 1st digit represents the results of checks on the security code.
- The 2nd digit represents the results of checks on the billing postcode.
- The 3rd digit represents the results of checks on the first line of the billing address.

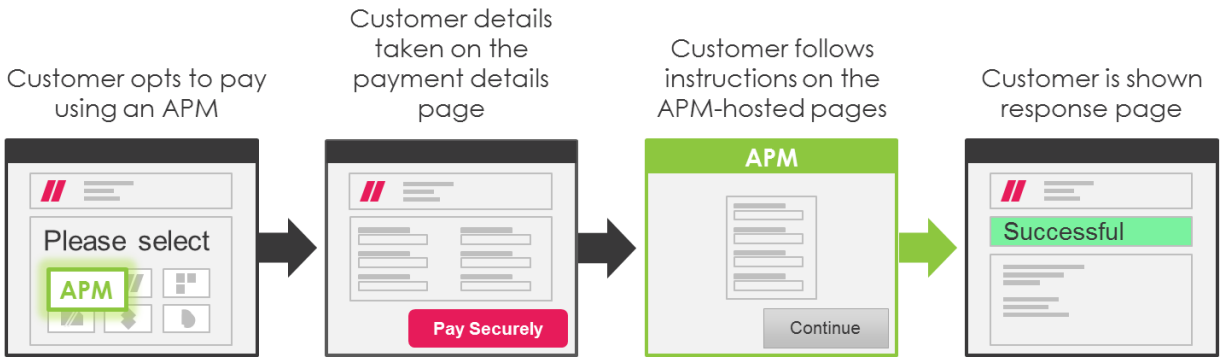
(The response codes '0', '1', '2' and '4' are explained in section 3.1.5)

4 Alternative Payment Methods (APM)

We support a range of Alternative Payment Methods (APM) that can be offered to your customers during the payment process.

4.1 What the customer sees

Your enabled APMs are shown as additional methods of payment on your existing checkout, alongside credit/debit cards. The steps performed by the customer while on the APM-hosted pages will vary depending on the selected payment method*. Here is an overview of the process from the customer's perspective:



*If the customer chooses to pay using PayPal, they will be immediately redirected to the PayPal-hosted checkout page, bypassing our hosted payment details page altogether. Further information on the payment process for PayPal can be found in section 4.14.

By following **Workflow C** (see section 1.1.3), the customer can bypass the payment details page if all of the additional payment fields required by the APM have already been submitted in the POST. Any additional required fields for specific APMs are documented later in this section.

4.2 Configuration

4.2.1 Enabling APMs on your account

To enable new APMs on your account, please get in touch with your account manager. Once enabled, the new APMs should be displayed on your Payment Pages, providing the payment is for a currency your account supports for the APM.

4.2.2 URL notifications

Before you begin testing, we recommend that you contact our Support team and request that rules are enabled on your account, which submit URL notifications to your system in the following scenarios:

- When a payment is authorised (see section 4.2.2.1).
- When funds have been settled (see section 4.2.2.2).

4.2.2.1 Configuring the authorisation notification

We recommend including at least the following fields in your authorisation notification:

- Acquirer Response Message (acquirerresponsemessage)
- Base Amount (baseamount) (e.g. £10.50 is “1050”)*
- Main Amount (mainamount) (e.g. £10.50 is “10.50”)*
- Billing Country (billingcountryiso2a)
- Currency (currencyiso3a)
- Error Code (errorcode)
- Live Status (livestatus)
- Order Reference (orderreference)
- Payment Type (paymenttypedescription)
- Request Type (requesttypedescription)
- Settle Status (settlestatus)
- Site Reference (sitereference)
- Transaction Reference (transactionreference)
- Transaction Started Timestamp (transactionstartedtimestamp)

*Please choose your preferred format.

The following APMs utilise additional fields that are useful to be returned in notifications, in addition to the list above. Refer to these sections for further information:

- Cash to Code (see section 4.8.2)
- paysafecard (see section 4.15.3)
- SEPA Direct Debit (see section 4.22.1)

4.2.2.2 Configuring the settlement notification

We recommend including the following fields in your settlement notification:

- Settle Status (settlestatus)
- Site Reference (sitereference)
- Transaction Reference (transactionreference)

4.2.2.3 Check the notification

You will need to check the contents of each notification received and respond accordingly by following the processes outlined in our online documents. In particular, you will need to look at the **settlestatus** value:

- **On authorisation:** If the **settlestatus** is "0", "1" or "10", the payment has been authorised and you are not required to take further action at this time. However, values of "2" or "3" indicate funds are **not** scheduled for settlement (*suspended* and *cancelled*, respectively).
- **On settlement:** If the **settlestatus** has been updated to "100", this indicates that the funds have been settled into your account. Alternatively, if this has been updated to "3", this indicates there has been a problem and the payment was subsequently cancelled.

4.2.3 Modify your POST

For most APMs, there is no need to modify the POST submitted to Secure Trading. However, if you are implementing **Workflow C** (see section 1.1.3) to bypass our hosted payment details page, you will need to modify your POST to include the billing country and billing name, for example:

```
<html>
<body>
<form method="POST" action="<DOMAIN>/process/payments/choice">
<input type="hidden" name="sitereference" value="test_site12345">
<input type="hidden" name="stprofile" value="default">
<input type="hidden" name="currencyiso3a" value="EUR">
<input type="hidden" name="mainamount" value="95.00">
<input type="hidden" name="version" value="2">
<input type="hidden" name="billingcountryiso2a" value="DE">
<input type="hidden" name="billingfirstname" value="Joe">
<input type="hidden" name="billinglastname " value="Bloggs">
<input type="submit" value="Pay">
</form>
</body>
</html>
```

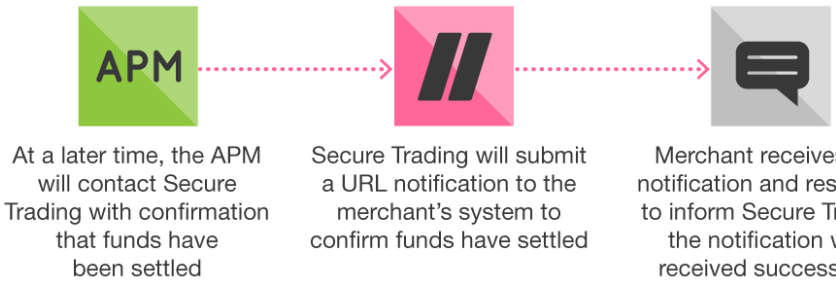
See section 9.2 for a full list of supported domains for the <DOMAIN> placeholder.

In addition to the above, each APM is subject to specific requirements
This can include restrictions on the customer's billing country, payment currency and required fields. Additionally, you may need to submit extra fields in the POST.

4.3 Settlement

The settlement process for APMs differs from the standard process followed with card-based payment methods.

4.3.1 Process overview



4.3.2 Settlement

Once a payment has been processed with an APM, funds will not be transferred into your account until the settlement process has been completed. When we receive confirmation that the funds have been settled, we will submit a URL notification to your system (see section 4.2.2).

The notification can be sent within minutes of processing the payment, or it could potentially take several days, depending on the APM involved in the transaction.

Certain APMs settle funds immediately. When implementing an APM on your account, please refer to the relevant documentation we provide on the APM for information on any deviations from standard APM processes.

4.3.3 Checking the notification

You will need to check the contents of the notification and respond accordingly by following the processes outlined in our online documents. In the notification received, you will need to look at the updated **settlestatus** value:

- If this has been updated to "100", this indicates that the funds have been settled into your account.
- Alternatively, if this has been updated to "3", this indicates there has been a problem and the payment was subsequently cancelled.

4.4 Refunds

APM refunds are subject to the following requirements:

- You cannot refund a payment until settlement has been completed. A refund can only be processed if the **settlestatus** is "100", which indicates the funds have been successfully transferred onto your bank account.
- You cannot refund a greater amount than was originally settled.
- Support for refunds vary between different APMs. We recommend reading on for further information on features supported by each APM.
- A refund request will only be successful if the payment details are still valid.

4.5 Chargebacks

Chargebacks can occur when processing transactions through certain APMs. Click here to learn more about chargebacks. If APM payments can be subject to chargebacks, this will be documented for the APMs involved.

4.6 Alipay

Alipay is a Chinese e-wallet that belongs to AntFinancial, an affiliate of the Alibaba group, the largest e-commerce company in the world. When selecting Alipay, customers will be redirected to their hosted pages, enter their personal details and agree to the payment, before being redirected back to the Payment Pages. Once completed, you will receive confirmation via a URL notification.

	**Supported billing address countries** No restrictions on billing countries.
	**Supported currencies** AUD, CAD, CHF, DKK, EUR, GBP, HKD, JPY, KRW, NOK, NZD, SEK, SGD, THB, USD
	**Refunds** Full and partial refunds supported.
	**Chargebacks** Chargebacks not supported.

4.6.1 Field specification

Field name	Description
orderreference	**(Required in POST)** Your own reference for the transaction. *(Note: This cannot be entered by the customer on the payment details page and must be submitted in the POST)*

4.7 Bancontact

Bancontact is a Belgian debit card solution with no chargeback risk, which is a unique feature for debit cards. When selecting Bancontact, customers must enter their card details on the Payment Pages. After that, they will be redirected to their bank's hosted pages, where they sign in, review the pre-filled payment details and agree to the payment, before being redirected back to the Payment Pages. Once completed, you will receive confirmation via a URL notification.

	**Supported billing address countries** Belgium (BE)
	**Supported currencies** EUR
	**Refunds** Full and partial refunds supported (permitted for up to 365 days).
	**Chargebacks** Chargebacks not supported.

4.8 Cash to Code

Cash to Code allows customers to complete online payments using cash at one of the thousands of retail locations across Europe. Customers select a deposit amount within the app and a barcode is generated that can be presented at their chosen point-of-sale, allowing them to pay in cash and instantly have their gaming account credited.

	**Supported billing address countries** No restrictions on billing countries.
	**Supported currencies** EUR
	**Refunds** Refunds not supported.
	**Chargebacks** Chargebacks not supported.

4.8.1 Process overview

1. On the payment choice page, the customer opts to pay with Cash to Code.
2. The customer enters their details on the payment details page and is redirected to Cash to Code.
3. The customer is prompted to select their preferred retail location. The customer's browser now displays a code.
4. The customer provides their unique code to the retailer they selected earlier, and completes the payment by paying with cash.

4.8.2 Field specification

Field name	Description
billingalias *	**(Required in POST)** An alias provided by you, to identify the customer. This field is alphanumeric. Max length 100. *(Note: This cannot be entered by the customer on the payment details page and must be submitted in the POST)*
billingid *	**(Required in POST)** A unique identifier for the customer. Each customer must have their own unique id. This id must be re-used by returning customers. This field is alphanumeric. Max length 100. *(Note: This cannot be entered by the customer on the payment details page and must be submitted in the POST)*
*** We recommend including these fields in your authorisation notifications (see section 4.2.2.1).**	

4.9 eps-Überweisung

eps (e-payment standard) is an Austrian real-time bank transfer system. When selecting eps, customers will be prompted to select their bank and then to sign in to their online banking account. After reviewing the pre-filled payment details, they can agree to the payment, before being redirected back to the Payment Pages. Once completed, you will receive confirmation via a URL notification.

	Supported billing address countries Austria (AT)
	Supported currencies EUR
	Refunds Full and partial refunds supported (permitted for up to 365 days).
	Chargebacks Chargebacks not supported.

4.10 giropay

Giropay is a German online payment method that is supported by over 1,500 German banks. When selecting Giropay, customers will be prompted to select their bank and then to sign in to their online banking account. After reviewing the pre-filled payment details, they can agree to the payment, before being redirected back to your website. Once completed, you will receive confirmation via a URL notification.

	Supported billing address countries Germany (DE)
	Supported currencies EUR
	Refunds Full and partial refunds supported (permitted for up to 365 days).
	Chargebacks Chargebacks not supported.

4.10.1 Field specification

Field name	Description
bic	**(Optional)** Valid BIC (Bank Identifier Code) of customer's bank. This field value must have a length of either 8 or 11.

4.11 iDEAL

iDEAL is a Dutch real-time bank transfer method. When selecting iDEAL, customers will be prompted to select their bank and then to sign in to their online banking account. After reviewing the pre-filled payment details, they can agree to the payment, before being redirected back to the Payment Pages. Once completed, you will receive confirmation via a URL notification.

	Supported billing address countries Netherlands (NL)
	Supported currencies EUR
	Refunds Full and partial refunds supported (permitted for up to 365 days).
	Chargebacks Chargebacks not supported.

4.12 Multibanco

Multibanco is a Portuguese online banking payment method. When selecting Multibanco, customers will be presented with two options. The first allows the customer to pay via online banking, by signing in to their Multibanco account. After reviewing the pre-filled payment details, they can agree to the payment, before being redirected back to your website. The second option allows the customer to pay the amount in cash at a bank or ATM. Once completed, you will receive confirmation via a URL notification.

	Supported billing address countries Portugal (PT)
	Supported currencies EUR
	Refunds Refunds not supported.
	Chargebacks Chargebacks not supported.

4.13 MyBank

MyBank is a real-time bank transfer system that operates in Italy, Belgium, France and Luxembourg. When selecting MyBank, customers will be prompted to select their bank and then to sign in to their online banking account. After reviewing the pre-filled payment details, they can agree to the payment, before being redirected back to your website. Once completed, you will receive confirmation via a URL notification.

	Supported billing address countries Italy (IT)
	Supported currencies EUR
	Refunds Full refunds supported (permitted for up to 365 days).
	Chargebacks Chargebacks not supported.

4.14 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**.

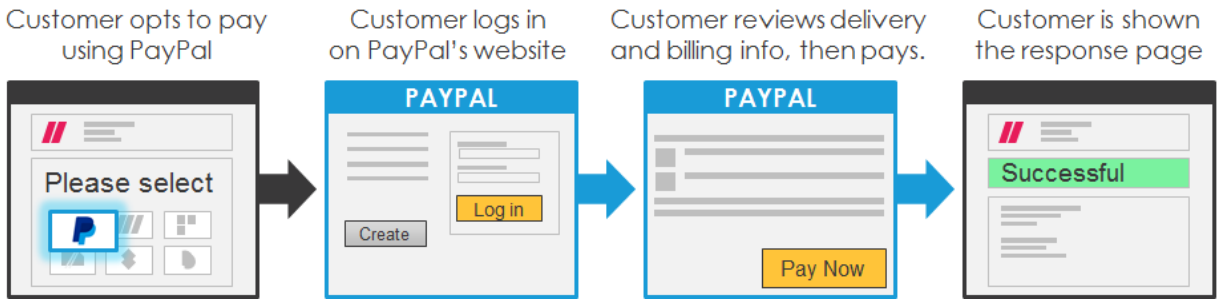
	Supported billing address countries No restrictions on billing countries.
	Supported currencies AUD, CAD, EUR, GBP, JPY, USD
	Refunds Full and partial refunds supported.
	Chargebacks Chargebacks not supported.

Unlike most other APMs, the **billingcountryiso2a**, **billingfirstname** and **billinglastname** fields are not required in the POST.

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

Please note: PayPal do not support the iframe integration described in section 2.4.

4.14.1 Process overview



4.14.2 Field specification

4.14.2.1 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, so please ensure any order reference submitted in the POST is unique to each transaction.

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

4.14.2.2 PayPal address override

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 POST to the Payment Pages:

paypaladdressoverride	Outcome
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).

4.14.2.3 PayPal address fields

(Only applicable when paypaladdressoverride is 0 or 1)

All customer delivery fields 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 above must be added to your designated fields for your request site security (see section 1.3).

4.14.2.4 Locale

You can include the PayPal locale field (paypallocaleiso2a) in the POST to localise the content displayed on the PayPal checkout. For a full list of supported values that can be submitted in this field (e.g. paypallocaleiso2a=GB for the UK), please refer to PayPal's documentation: https://developer.paypal.com/docs/classic/api/locale_codes/

4.14.3 Refunds

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

Important: The value for the address override ("0", "1" or "2") needs to be included in the string used to generate your request site security hash, as described in section 1.3. Failure to do so will result in the customer being shown an "Invalid details" error message.

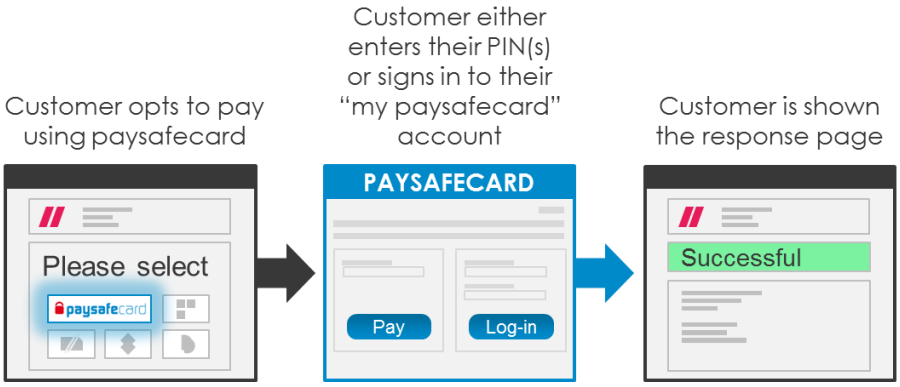
4.15 paysafecard

paysafecard is a simple and safe prepaid payment method that allows customers to make payments online without the use of a bank account or credit card information.

	Supported billing address countries No restrictions on billing countries.
	Supported currencies ARS, AUD, BGN, CAD, CHF, CZK, DKK, EUR, GBP, HRK, HUF, MXN, NOK, NZD, PEN, PLN, RON, SEK, TRY, USD, UYU
	Refunds Refunds not supported.
	Chargebacks Chargebacks not supported.

4.15.1 Process overview

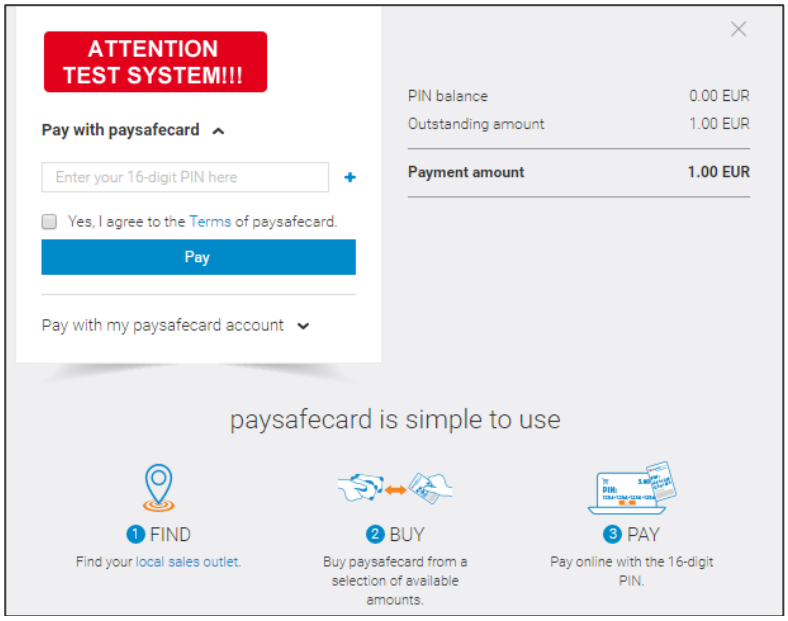
Once you have enabled paysafecard and configured your site, the paysafecard logo will be shown alongside existing payment methods.



Please note: Funds are settled immediately after the customer has completed the payment. It is not possible for paysafecard transactions to be left in a suspended state (settle status "2").

4.15.2 Test environment

When testing, you will be redirected to paysafecard's sandbox page, which simulates the page that will be displayed to your customers (screenshot below).



4.15.3 Field specification

You can submit the following additional fields in the POST to impose restrictions on payments processed with paysafecard.

Field name	Description
billingid *	**(Required in POST)** A unique identifier for the customer. Each customer must have their own unique id. This id must be re-used by returning customers. This field is alphanumeric. Max length 100. *(Note: This cannot be entered by the customer on the payment details page and must be submitted in the POST)*
paysafeminage	**(Optional)** Specifies the minimum age of the "my paysafecard" account holder. e.g. To restrict the minimum age to be 18, submit "18" in this field.
paysafekyclevel	**(Optional)** Specifies the required KYC level for the "my paysafecard" account holder. There are two levels: "*SIMPLE*" - The customer has successfully completed the initial registration process and confirmed their mobile number and email address. "*FULL*" - In addition to the above, the customer has also provided proof of identification (e.g. passport, driving license) and proof of address (e.g. utility bill).
paysafecountryrestriction	**(Optional)** Restricts the payment to be processed exclusively from the country specified (in iso2a format). e.g. "GB" for United Kingdom.
*** We recommend including these fields in your authorisation notifications (see section 4.2.2.1).**	

Please note that if you submit any of the aforementioned fields, the customer may be forced to sign in to their "my paysafecard" account to verify their details (e.g. to check their age).

4.15.4 Iframes

The paysafecard-hosted page can be hosted in an iframe.
Always allow vertical scrolling or dynamic sizing. Maximum height of 840px.

paysafecard's payment page is optimised automatically for mobile devices.
If a customer is using a device with a resolution with width smaller than 600px, a payment panel optimised for mobile devices will be automatically shown. This is also the case if the embedded iframe has a smaller width than 600px.

4.16 PayU

PayU is a real-time bank transfer system. When selecting PayU, customers will be prompted to select their bank and then to sign in to their online banking account. After reviewing the pre-filled payment details, they can agree to the payment, before being redirected back to your website. Once completed, you will receive confirmation via a URL notification.

	Supported billing address countries Czech Republic (CZ) and Poland (PL).
	Supported currencies CZK, PLN
	Refunds Full and partial refunds supported (permitted for up to 365 days).
	Chargebacks Chargebacks not supported.

4.17 PostFinance

PostFinance is a Swiss real-time bank transfer system. When selecting PostFinance, customers will be prompted to select their bank and then to sign in to their online banking account. After reviewing the pre-filled payment details, they can agree to the payment, before being redirected back to your website. Once completed, you will receive confirmation via a URL notification.

	Supported billing address countries Switzerland (CH)
	Supported currencies CHF, EUR
	Refunds Full and partial refunds supported (permitted for up to 365 days).
	Chargebacks Chargebacks not supported.

4.17.1 Field specification

Field name	Description
mobileview	**(Optional)** Submit "1" for the mobile-enabled variant of PostFinance, otherwise leave blank.

4.18 Przelewy24

Przelewy24 is a Polish real-time bank transfer method. When selecting Przelewy24, customers will be prompted to select their bank and then to sign in to their online banking account. After reviewing the pre-filled payment details, they authorise the payment, before being redirected back to the Payment Pages. Once completed, you will receive confirmation via a URL notification.

	Supported billing address countries Poland (PL)
	Supported currencies EUR, PLN
	Refunds Full and partial refunds supported. Permitted for up to 90 days – after this the customer must seek refund directly with Przelewy24.
	Chargebacks Chargebacks not supported.

4.18.1 Field specification

Field name	Description
billingemail	**(Required from customer)** The billing email address. This can then be used for correspondence with the customer. Maximum length of 255 (maximum of 64 characters before the"@" symbol).

4.19 QIWI

QIWI is an e-wallet that operates in Russia, Kazakhstan and Ukraine. Customers will be prompted for their QIWI wallet credentials (phone number and password), after which they can complete the order using their preferred payment method. Once completed, you will receive confirmation via a URL notification.

	Supported billing address countries Kazakhstan (KZ), Russia (RU) and Ukraine (UA)
	Supported currencies EUR, KZT, RUB, USD
	Refunds Refunds not supported.
	Chargebacks Chargebacks not supported.

4.19.1 Field specification

Field name	Description
billingtelephonetype	**(Required from customer)** The customer must indicate their phone number is a mobile phone number. If you are submitting this value in the POST, submit `billingtelephonetype=M`

billingtelephone	**(Required from customer)** The customer's telephone number. Valid characters:
	// Numbers 0-9
	// Spaces
	// Special characters: + - ( )

4.20 redpagos

redpagos is a Uruguayan cash payment method. When redpagos is selected, the payment details are displayed and can be printed. The amount required for the purchase can then be paid at local kiosks. Once completed, you will receive confirmation via a URL notification.

	Supported billing address countries Uruguay (UY)
	Supported currencies USD
	Refunds Refunds not supported.
	Chargebacks Chargebacks not supported.

4.20.1 Field specification

Field name	Description
billingdob	**(Required from customer)** The account holder's date of birth (format: YYYY-MM-DD).
billingemail	**(Required from customer)** The customer's billing email address. Maximum length of 255 (maximum of 64 characters before the "@" symbol).
nationalid	**(Required from customer)** Customer's national id.

4.21 SafetyPay

SafetyPay is a real-time bank transfer / cash payment method. When selecting SafetyPay, customers will be presented with two options. The first allows the customer to pay via online banking, by signing in to their online banking account. After reviewing the pre-filled payment details, they can agree to the payment, before being redirected back to your website. The second option allows the customer to pay the amount in cash at a bank. Once completed, you will receive confirmation via a URL notification.

	Supported billing address countries Austria (AT), Belgium (BE), Chile (CL), Colombia (CO), Costa Rica (CR), Ecuador (EC), Germany (DE), Mexico (MX), Netherlands (NL), Peru (PE), Puerto Rico (PR) and Spain (ES).
	Supported currencies EUR, USD
	Refunds Full and partial refunds supported (permitted for up to 90 days).
	Chargebacks Chargebacks not supported.

4.22 SEPA Direct Debit

SEPA Direct Debit is a direct debit payment method that operates in the eurozone. After selecting goods or services, customers reach the merchant's checkout. When selecting SEPA Direct Debit, customers enter their IBAN/BIC information, after which the amount will be automatically debited from the user's bank account. Once the payment has been submitted, the merchant receives a URL notification and the purchase can be delivered.

	Supported billing address countries Austria (AT), Belgium (BE), Cyprus (CY), Estonia (EE), Finland (FI), France (FR), Germany (DE), Greece (GR), Ireland (IE), Italy (IT), Latvia (LV), Lithuania (LT), Luxembourg (LU), Malta (MT), Monaco (MC), Netherlands (NL), Portugal (PT), Slovakia (SK), Slovenia (SI) and Spain (ES)
	Supported currencies EUR
	Refunds Only CFT Refunds supported (permitted for up to 365 days).
	Chargebacks Payments may be subject to chargebacks.

Our integration of SEPA Direct Debits only supports one-off payments.

4.22.1 Field specification

Field name	Description
billingemail	**(Required from customer)** The billing email address. This can then be used for correspondence with the customer. Maximum length of 255 (maximum of 64 characters before the "@" symbol).
iban	**(Required from customer)** The customer's IBAN. *(Note: This cannot be submitted in the POST and must be entered by the customer on the payment details page)*

We recommend including the **mandatereference** field in your authorisation notifications (see section 4.2.2.1).
This field contains a unique identifier for the direct debit.

4.23 Sofort

Sofort is a real-time bank transfer method that operates in Germany, Austria, The Netherlands and Belgium. When selecting Sofort, customers will be prompted to select their bank and then to sign in to their online banking account. After reviewing the pre-filled payment details, they can agree to the payment, before being redirected back to the Payment Pages. Once completed, you will receive confirmation via a URL notification.

	Supported billing address countries Austria (AT), Belgium (BE), Germany (DE), Italy (IT), Netherlands (NL), Poland (PL), Spain (ES) and Switzerland (CH).
	Supported currencies EUR
	Refunds Full and partial refunds supported (permitted for up to 365 days).
	Chargebacks Chargebacks not supported.

4.23.1 Field specification

Field name	Description
bankid	**(Optional)** The customer's Bank Identification Code (BIC).

4.24 Trustly

Trustly is a real-time bank transfer system. When selecting Trustly, customers will be prompted to select their bank and then to sign in to their online banking account. After reviewing the pre-filled payment details, they can agree to the payment, before being redirected back to your website. Once completed, you will receive confirmation via a URL notification.

	Supported billing address countries Denmark (DK), Estonia (EE), Finland (FI), Italy (IT), Norway (NO), Poland (PL), Spain (ES) and Sweden (SE).
	Supported currencies DKK, EUR, NOK, PLN and SEK
	Refunds Full and partial refunds supported (permitted for up to 365 days).
	Chargebacks Chargebacks not supported.

4.24.1 Field specification

Field name	Description
nationalid	**(Optional)** The customer's social security number.

4.25 Verkkopankki

Verkkopankki is a real-time bank transfer system that operates in Finland. When selecting Verkkopankki, customers will be prompted to select their bank and then to sign in to their online banking account. After reviewing the pre-filled payment details, they can agree to the payment, before being redirected back to your website. Once completed, you will receive confirmation via a URL notification.

	Supported billing address countries Finland (FI)
	Supported currencies EUR
	Refunds Refunds not supported.
	Chargebacks Chargebacks not supported.

4.26 WeChat Pay

With over a billion users, **WeChat** is the most popular instant messaging app in China. Users who have provided bank account information may use the app to pay bills, order goods and services, transfer money to other users, and pay in participating stores. When the customer selects WeChat Pay to process a payment on your checkout, the WeChat app will open on the customer's device. The customer checks the recipient of the funds and the amount displayed, then selects to pay either with a bank card, or using their WeChat balance. The customer enters their password to complete the payment. A confirmation is displayed following a successful transaction, before the customer's device is redirected back to your website. Once completed, you will receive confirmation via a URL notification.

	Supported billing address countries China (CN)
	Supported currencies EUR and USD
	Refunds Full and partial refunds supported (permitted for up to 90 days).
	Chargebacks Chargebacks not supported.

4.27 Zimpler

Zimpler is a mobile wallet / invoicing method that operates in Finland and Sweden. When choosing Zimpler, customers must enter their mobile phone number. They will then receive a code via SMS, which must be entered into the hosted checkout page to initiate the payment. Once the transaction has been submitted, an invoice will be sent by SMS to the customers for payment. Once the transaction has been completed, you will receive confirmation via a URL notification, and you can deliver the goods / services to the customer.

	Supported billing address countries Finland (FI) and Sweden (SE)
	Supported currencies EUR, SEK **Note:** • EUR payments can only be processed with **billingcountryiso2a** set to “FI”. • SEK payments can only be processed with **billingcountryiso2a** set to “SE”.
	Refunds Full refunds supported.
	Chargebacks Chargebacks not supported.

4.27.1 Field specification

Field name	Description
billingemail	**(Required from customer)** The customer’s billing email address. Maximum length of 255 (maximum of 64 characters before the ”@” symbol).
billingtelephonetype	**(Optional)** At time of writing, only a mobile phone number can be submitted to Zimpler. To indicate the **billingtelephone** submitted is a mobile phone number, the **billingtelephonetype** must be submitted as "M".

billingtelephone	**(Optional)** The customer’s telephone number. Valid characters:
	// Numbers 0-9
	// Spaces
	// Special characters: + - ( )

5 Digital wallets

This section explains how to accept digital wallet transactions on your Payment Pages checkout.

5.1 About digital wallets

Digital wallets streamline the checkout experience for your customers, by allowing them to store their payment card details securely within an encrypted virtual wallet. When making a purchase online, customers can quickly authenticate their session (e.g. by entering a PIN, using a fingerprint reader or through facial recognition technology) and agree to a payment, all without having to re-enter any of the billing information required.

5.2 Requirements

5.2.1 Enabling digital wallets

To enable digital wallets on your test site reference, please contact our Support team (see section 8.1). Once enabled, the digital wallets will be displayed on the payment choice and payment details pages (providing the browser supports the service) and you can test your solution.

The digital wallets we support are listed below (section 5.3).

5.2.2 Modify your POST to Secure Trading

You will need to modify your POST submitted to Secure Trading to include the following two fields. These changes will ensure that the billing and delivery information are retrieved from the customer's wallet. This expedites the payment process, providing a more seamless checkout experience for the customer.

Field name	Description
billingcontact detailsoverride	"1" – Uses billing details from the customer's wallet.
customercontact detailsoverride	"1" – Uses delivery details from the customer's wallet.

Example

The following is an example of how the POST should be updated (the additional fields are shown in **bold**).

```
<form method="POST" action="<DOMAIN>/process/payments/choice">
...
<input type="hidden" name="billingcontactdetailsoverride" value="1">
<input type="hidden" name="customercontactdetailsoverride" value="1">
...
<input type="submit" value="Pay">
</form>
```

See section 9.2 for a full list of supported domains for the <DOMAIN> placeholder.

5.2.3 Additional considerations

Before you start accepting live payments using these wallets, you will need to read the documentation we provide for each wallet you enable (section 5.3), to ensure you are meeting any additional requirements and have sufficiently tested your solution. Once satisfied, contact our Support team and request for the wallets to be enabled on your live site reference.

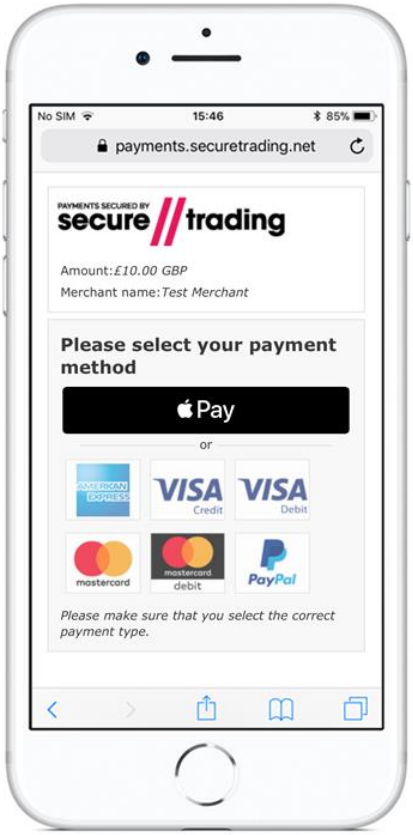
5.3 Supported digital wallets

Apple Pay
See section 5.4

Visa Checkout
See section 5.5

5.4 Apple Pay

Apple Pay is a wallet-based mobile payment service by Apple Inc. that lets users process payments using an iPhone, iPad or Mac (**full list of supported devices**). Customers benefit from a familiar and streamlined checkout experience, where their billing information can be pre-filled, ready for purchase. Customers are authenticated quickly by placing their finger on the built-in reader or through facial-recognition. Apple Pay uses tokens to ensure no sensitive payment information is stored with Apple, on the customer's device or on your own servers.



	Supported billing address countries AE, AU, CA, CH, CN, DK, ES, FI, FR, GB, GG, HK, IE, IM, IT, JE, JP, NZ, RU, SE, SG, SM, TW, US, VA Full list of supported countries: https://support.apple.com/en-gb/ht207957
	Supported currencies Dependent on your acquiring bank.
	Payment types Dependent on the customer's card issuer.
	Refunds Full and partial refunds supported.
	Chargebacks Payments may be subject to chargebacks.

If you have any queries on features supported by Apple Pay, please contact our Support team (see section 8.1).

5.4.1 Requirements

- Apple Pay is only available to eligible customers. Please refer to Apple's documentation for the full list of requirements.
- Your acquiring bank must support Apple Pay with Secure Trading. Contact our Support team for further information (see section 8.1).

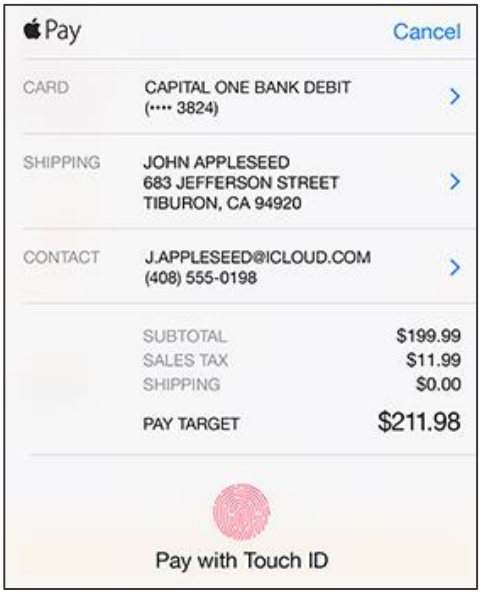
In order to test your solution, we recommend that you have access to a device that supports Apple's sandbox testing for Apple Pay.

Apple Pay does not support the iframe integration described in section 2.4.

5.4.2 Process overview

1. The customer's browser is sent to the Payment Pages. We will check if the device supports Apple Pay.
2. If supported, Apple Pay will be displayed first among the other available payment methods. The customer presses the Apple Pay logo to proceed.
3. A panel slides into view (Apple Pay payment sheet) with a summary of the order. The customer can review the order and update their payment details, if needed.
4. The customer's identity is verified, either by placing their finger on the Touch ID sensor or through facial recognition, depending on their device.
5. If successful, on-screen confirmation will be displayed and the customer will be redirected to our hosted response page.

5.4.3 Payment sheet



Payment sheet with addresses displayed

5.4.3.1 Card

The customer will be able to select from the cards saved in their Apple Wallet.
Information on the Apple Wallet: https://support.apple.com/en-gb/HT204003
The cards supported for payment are dependent on payment methods enabled on your Secure Trading account.

When selecting their preferred card for the transaction, only cards supported by your site configuration are displayed to the customer on the payment sheet.

5.4.3.2 Address

The addresses in the payment sheet will be populated by information stored on the customer's Apple Pay account. If the customer has multiple addresses stored, they will be able to choose between them.

5.4.3.3 Label and amount

The **mainamount** value is displayed on the payment sheet, alongside the label, which shows the name of your company / business provided to our Support team when you first signed up with us.

5.4.3.4 Authentication

The method of authentication will differ based on the device being used to complete the payment. The customer may be prompted to place their finger on the Touch ID sensor, or look at the Face ID sensor.
Information on Apple Pay authentication: https://support.apple.com/en-gb/HT201239

5.4.4 Testing

Your test site reference will connect to the Apple Pay testing sandbox. Therefore, in order to process payments on your test site reference, you will need to add test card details to the Apple Wallet on your supported device(s).

You will be required to use the test card details provided by Apple. Please refer to this URL:
https://developer.apple.com/support/apple-pay-sandbox/

Please be aware that the test card details we provide in our testing documentation cannot be used when processing Apple Pay test transactions.

5.4.5 Additional notes

5.4.5.1 Account checks

You can process account checks (see section 3.1.7) with Apple Pay transactions, providing your acquiring bank supports this functionality. Contact our Support team (see section 8.1) to enable account checks on your account. Account checks will be processed automatically prior to every payment, with no changes required to your checkout.

5.4.5.2 AVS and security code checks

AVS (Address Verification Service) checks will be processed if supported by your bank, but security code checks are not possible with Apple Pay. This is because the security code cannot be stored on the customer's phone or with Apple, and therefore cannot be sent on to the bank during the authorisation process for checks to be performed. As such, the response for the security code checks will always be "0", indicating the security code was not sent.

For further info on the AVS process, please refer to our AVS and security code checks document.

The security code setting on your security policy is not applicable for Apple Pay transactions, and therefore, they cannot be suspended based on the security code. However, AVS checks are still performed, and transactions can still be suspended due to your security policy configuration.

5.4.5.3 Fraud and duplicate checks

If enabled on your account, fraud and duplicate checks will be run for all Apple Pay transactions.

For further information on fraud and duplicate checks, please refer to our Fraud checks document.

5.4.5.4 Subscriptions

If your merchant number permits recurring payments with Apple Pay and your account has been configured by our Support team, you will be able to process subscriptions by following our Subscriptions document.

5.4.5.5 Protect Plus

Protect Plus analyses the customer's billing, delivery and token details using a rule-based system to detect suspicious patterns in user activity. The system will assist you in deciding whether to process a customer's transaction based on the perceived level of risk.

For further information on Protect Plus, please refer to our Protect Plus Guide.

5.4.5.6 Refunds

You can refund previously-settled Apple Pay transactions by using MyST (click here to learn more). Full and partial refunds are supported.

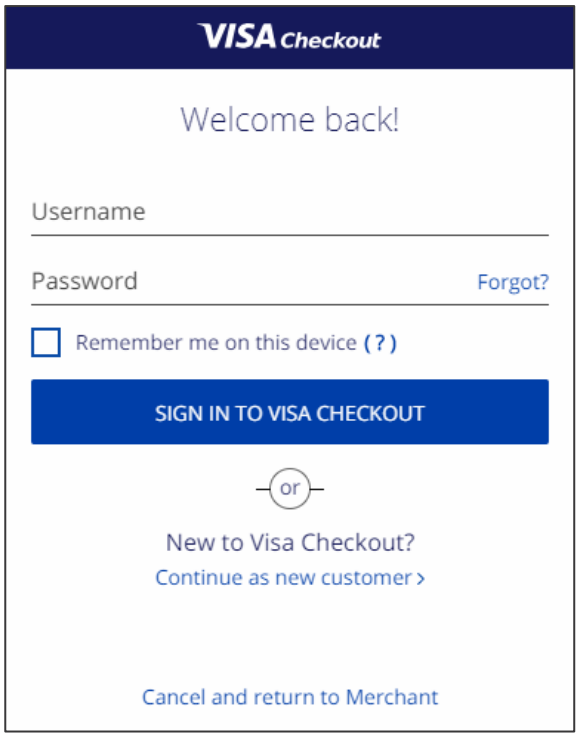
5.4.5.7 Chargebacks

Apple Pay transactions may be subject to chargebacks. This is dependent on your acquiring bank.

Please refer to our Chargebacks document for further information.

5.5 Visa Checkout

Visa Checkout is a digital wallet provided by Visa Inc. that allows customers to process payments in a fast and secure manner. Customers are authenticated by entering their username and password or alternatively they can use the fingerprint reader built into their device. This means that after initial setup, enrolled customers do not have to fill out their credit card number or invoicing address to complete a payment.

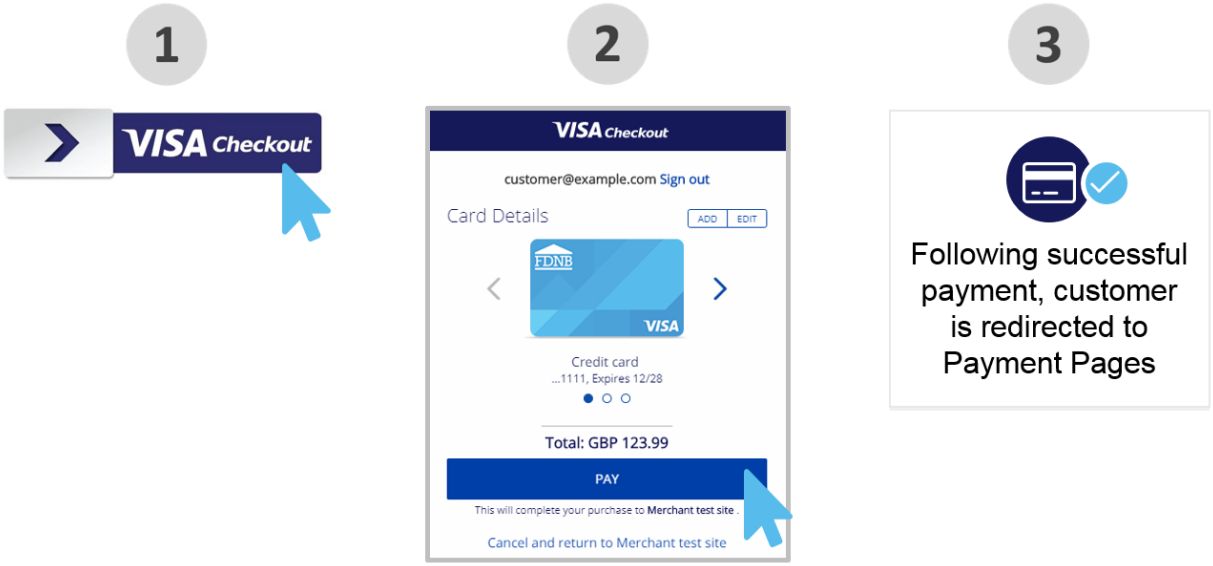


	Supported billing address countries AE, AR, AU, BR, CA, CL, CN, CO, FR, GB, HK, IE, IN, MX, MY, NZ, PE, PL, SG, US, ZA Full list of supported countries: https://developer.visa.com/capabilities/visa_checkout/docs
	Supported currencies Dependent on your acquiring bank.
	Payment types Supported by all Mastercard and Visa-branded cards.
	Refunds Full and partial refunds supported.
	Chargebacks Payments may be subject to chargebacks.

If you have any queries on features supported by Visa Checkout, please contact our Support team (see section 8.1).

5.5.1 Process overview

The customer's browser is sent to the Payment Pages, where Visa Checkout is displayed amongst other payment types and wallets enabled on your account.



1. The customer taps the Visa Checkout button, and an overlay is displayed, prompting them for their username and password.

2. Following authentication, the customer can review the order and update their address and payment details, if needed. When they are ready to proceed, the customer presses the "PAY" button.

3. If successful, the customer will be redirected to our hosted response page.

5.5.2 Payment Widget

When the customer presses the Visa Checkout button, the Visa Checkout Payment Widget is displayed. This is a secure interface hosted by Visa Checkout that allows existing customers to sign in, choose their preferred payment card and delivery address (if applicable), and agree to the transaction. Alternatively, users who have not yet signed up to use Visa Checkout can register without leaving the Payment Pages and complete the payment once they are ready. Once the payment has been completed, the customer is redirected back to the response page to allow for a success message to be displayed.

Further information can be found in Visa's own documentation.

5.5.3 Testing

Your test site reference will connect to the Visa Checkout testing sandbox. Therefore, you will need to add our test card details to a Visa Checkout wallet in order to process payments on your test site reference.

5.5.4 Additional notes

5.5.4.1 Account checks

You can process account checks (see section 3.1.7) with Visa Checkout transactions, providing your acquiring bank supports this functionality. Contact our Support team (see section 8.1) to enable account checks on your account. Account checks will be processed automatically prior to every payment, with no changes required to your checkout.

5.5.4.2 AVS and security code checks

AVS (Address Verification Service) checks will be processed if supported by your bank, but security code checks are not possible with Visa Checkout. This is because the security code is not stored in the customer's wallet, and therefore cannot be sent on to the bank during the authorisation process for checks to be performed. As such, the response for the security code checks will always be "0", indicating the security code was not sent.

For further info on the AVS process, please refer to our AVS and security code checks document.

The security code setting on your security policy is not applicable for Visa Checkout transactions, and therefore, they cannot be suspended based on the security code. However, AVS checks are still performed, and transactions can still be suspended due to your security policy configuration.

5.5.4.3 Fraud and duplicate checks

If enabled on your account, fraud and duplicate checks will be run for all Visa Checkout transactions.

For further information on fraud and duplicate checks, please refer to our Fraud checks document.

5.5.4.4 Subscriptions

If your merchant number permits recurring payments with Visa Checkout and your account has been configured by our Support team, you will be able to process subscriptions by following our Subscriptions document.

5.5.4.5 Protect Plus

Protect Plus analyses the customer's billing, delivery and card details using a rule-based system to detect suspicious patterns in user activity. The system will assist you in deciding whether to process a customer's transaction based on the perceived level of risk.

For further information on Protect Plus, please refer to our Protect Plus Guide.

5.5.4.6 Refunds

You can refund previously-settled Visa Checkout transactions, by using MyST (click here to learn more). Full and partial refunds are supported.

5.5.4.7 Chargebacks

Visa Checkout transactions may be subject to chargebacks. This is dependent on your acquiring bank.

Please refer to our Chargebacks document for further information.

5.6 Identifying Digital Wallet transactions

As with regular card payments, digital wallet transactions are identified on our system by their card brand (i.e. “Visa” or “Mastercard Debit”). To distinguish card payments processed with digital wallets from those that were not, you will need to review the **walletsource** field.

- For Apple Pay transactions, the **walletsource** will be set to “APPLEPAY”.
- For Visa Checkout transactions, the **walletsource** will be set to “VISACHECKOUT”.

5.6.1 URL notifications

If you have URL notifications enabled on your site reference, we recommend updating your notifications to allow you to identify digital wallet transactions. To do this, you will need to submit an additional field in your POST to Payment Pages, in order to return the **walletsource** field (in addition to the default fields that are always returned).

Refer to section 1.7 for information on how to configure URL notifications.

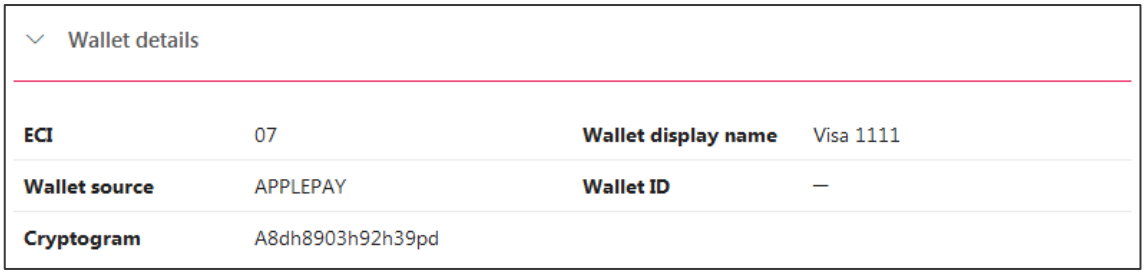
```
<form method="POST" action="<DOMAIN>/process/payments/choice">
...
<input type="hidden" name="ruleidentifier" value="STR-10">
<input type="hidden" name="allurlnotification"
value="http://www.yourwebsite.com/all">
<input type="hidden" name="stextraurlnotifyfields"
value="walletsource">
...
<input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

See section 9.2 for a full list of supported domains for the <DOMAIN> placeholder.

Important: The names of all additional fields to be returned in the notification need to be included in the string used to generate your request site security hash, as described in section 1.3. Failure to do so will result in the customer being shown an “Invalid details” error message.

5.6.2 MyST

When viewing transaction details in MyST, you will be able to view the wallet source under the “Wallet details” heading:



6 DCC

6.1 Introduction

Dynamic Currency Conversion (DCC) is a feature that allows you to provide eligible customers with a choice of currencies for payment. The amounts are calculated using a third-party conversion rate provider with up-to-date conversion rates.

6.1.1 Requirements

Before you get started, please be aware of the following restrictions:

- Secure Trading's implementation of DCC is currently only supported by Mastercard and Visa-branded cards. Furthermore, DCC transactions can only be performed when supported by the customer's card issuer.
- You will need to have a merchant number that allows for DCC. For further information, please contact your acquiring bank.
- You will also need an account with a currency rate provider. To set up a currency rate provider on your Secure Trading account, please contact our sales team.
- Finally, you will need to contact support and enable DCC on your Secure Trading account.

6.2 Process overview

Typical DCC payments consist of two requests:

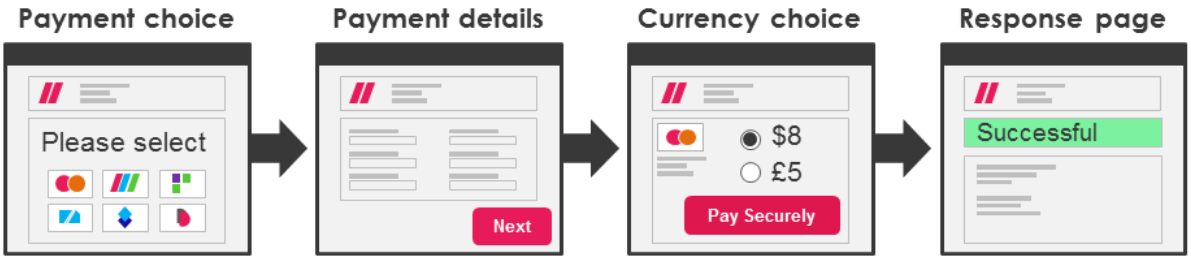
- A **CURRENCYRATE** request - This is used to retrieve an up-to-date conversion rate from a DCC provider. This is processed while the customer is on the Payment Pages, prior to confirming the purchase. We use this information to calculate the amount in the customer's local currency and display this as an option for payment.

The customer will be offered a choice to pay in either the currency you specify in the POST, or the local currency associated with their card. (If these two currencies are the same, the payment will be processed immediately in this currency)

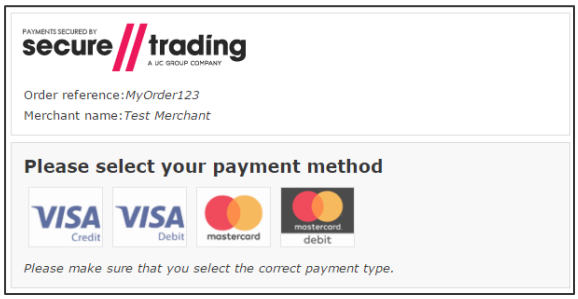
- An **AUTH** request - Once the customer has decided on the currency for the payment, an AUTH request is processed. This is to request the customer's bank to authorise the payment in the customer's preferred currency.

6.3 What the customer sees

6.3.1 Summary

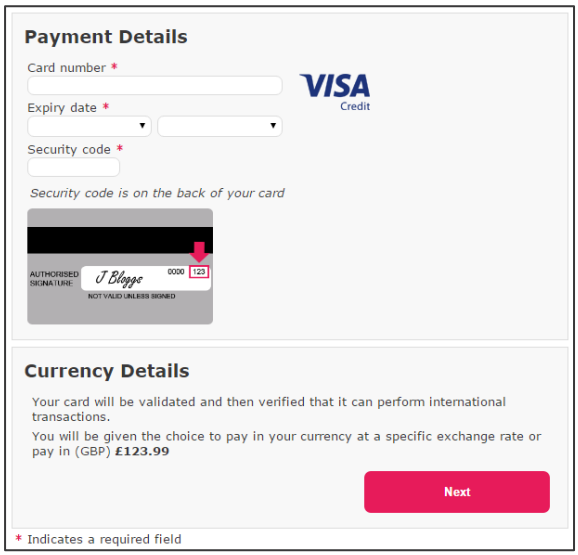


6.3.2 Payment choice



The customer is initially shown the payment choice page, where they can select the payment type that they wish to use. This differs from the normal choice page in that the amount is initially hidden. This is because the currencies and respective amounts to be offered to the customer have yet to be established. This comes after the customer enters their payment details on the next page.

6.3.3 Payment details



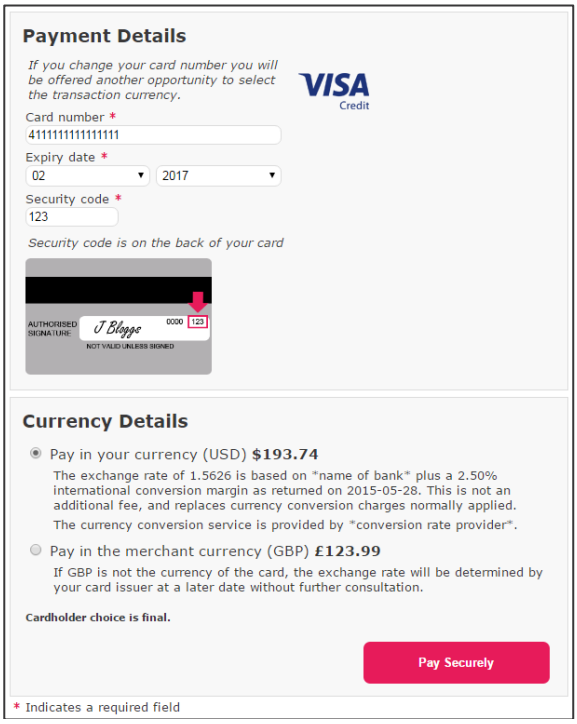
If the customer chooses a payment type that supports DCC, they are informed that they are able to pay in an alternative currency to the currency submitted in the POST. Here they will be able to see the amount in the currency you submitted in the request.

We 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 currency you submitted in the request to an amount in the customer's local currency.

If the cardholder's local currency is the same as the submitted currency, the customer will not be shown a conversion rate and instead will process the payment in this currency (skipping the currency choice page described in section 6.3.4).

The 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 further information, please contact your conversion rate provider.

6.3.4 Currency choice



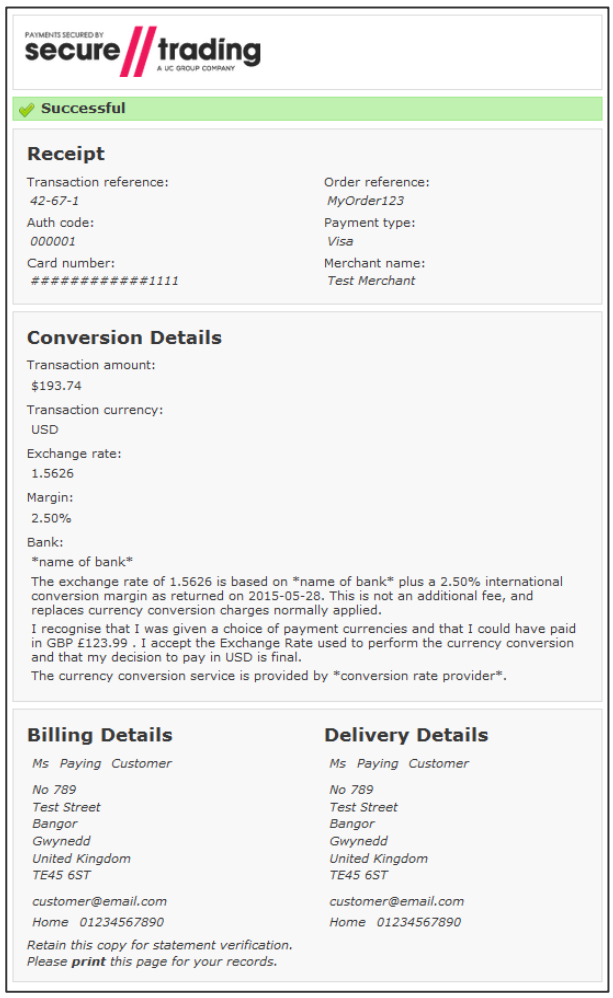
The amounts in both currencies are displayed on the currency choice page. The customer will be able to choose between paying in either currency.

If the customer changes their card number (PAN) at this stage, before clicking "**Pay Securely**", we will re-establish the customer's local currency using the new card and perform another CURRENCYRATE request to retrieve the new conversion rate. The customer will be redisplayed the payment details page, 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 will be processed by your acquiring bank. This uses the currency and respective amount chosen by the customer on the Payment Pages.

6.3.5 Response page



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

6.4 Configuration

To enable DCC on your account, please contact the Support team (see section 8.1). There are two methods that DCC can be enabled on your account:

1. Support 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 submit to the Payment Pages remains unchanged from a standard authorisation.

2. Including the field dcctype with the value "DCC" in your POST will result in DCC being performed on a request, if the customer's payment type supports it. Not including this field in your POST will result in a normal authorisation request being processed, without the customer being able to choose an alternative currency.

For DCC requests, it is imperative that you submit a currency that is supported by your account. This is to ensure the correct currencies are used when performing currency conversion.

6.4.1 DCC fields

Following CURRENCYRATE Requests, we will return additional DCC fields for your records, as listed in the table, below. These fields are displayed for the CURRENCYRATE and AUTH requests in MyST.

The fields can be returned in a URL notification (see section 1.7) on completion of a transaction. Include the fields shown below in order to include DCC information. They can also be included in an email notification (contact Support to enable this; section 8.1).

Field name	Description
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"

6.5 Testing

You should ensure you have thoroughly tested your system before processing live payments.

The card numbers listed in this test section are associated with specific local currencies. During your integration, you can use the following international test card details in order to test your system for successful and declined DCC transactions. When performing DCC, using a card with a currency that is different to the submitted currency should return the amount in both the customer's local currency and the submitted currency, which are displayed to the customer on the Payment Pages.

6.5.1 Successful authorisation

For a list of PANs in other currencies, please refer to the **Testing document**.

Country Code[1]	Currency Code[2]	Visa	Mastercard
DE	EUR	4500000000000007	5500000000000004
GB	GBP	4300000000002211	5311110000001511
JP	JPY	4900400000000005	5590410000000006
US	USD	4900460000000009	5590470000000018

6.5.2 Declined authorisation

Country Code[1]	Currency Code[2]	Visa	Mastercard
DE	EUR	4500000000002482	5500000000002422
GB	GBP	4300000000002492	5311110000002402
JP	JPY	4900400000002472	5590410000002432
US	USD	4900460000002492	5590470000002402

(You can also use an amount of **70000** in the currency chosen on the Payment Pages to generate a decline response)

[1] Country codes listed here are in ISO2A format. For further information, please see: https://docs.securetrading.com/document/toolbox/country-codes/

[2] Currency codes listed here are in ISO3A format. For further information, please see: https://docs.securetrading.com/document/toolbox/currency-codes/

6.6 Additional notes

6.6.1 Customisation

We actively ensure 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.

6.6.2 Updating DCC authorisations

It is possible to perform transaction updates to DCC Authorisations by using MyST. However, 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 process the payment that will be changed.

Deferred settlement is NOT supported for DCC transactions.

6.6.3 Refunding DCC authorisations

You can refund DCC authorisations using MyST. We will perform a new CURRENCYRATE transaction in order to refund the customer in their chosen currency using an up-to-date conversion rate.

6.6.4 Subscriptions

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

7 Additional features

7.1 Enhanced post

Enhanced post allows you to customise the request types processed in each POST to the Payment Pages.

7.1.1 Process overview

7.1.1.1 List of request types

First, you will need to consider the request types enabled on your account. By default, each POST sent to Secure Trading processes an authorisation request. You can achieve additional functionality by enabling any of the supported request types listed below: (You can enable/disable request types by contacting the Support team (see section 8.1).

Priority	Request Type	Description
1*	CURRENCYRATE	**For DCC (see section 5):** A Currency Rate Request, to perform currency conversion between two different currencies.
2	RISKDEC	**For Protect Plus (see section 3.5):** A Risk Decision Request, to check for suspicious activity relating to the transaction.
3	ACCOUNTCHECK	**For Account Check (see section 3.1.7):** An Account Check Request, to check the values of the security code and AVS responses submitted by the customer.
4	ORDER	**For PayPal (see section 4.14):** An Order Request, used to initiate a payment using PayPal. **Required when offering PayPal as a payment option.**
5	THREEDQUERY	**For 3-D Secure (see section 3.2):** A 3-D Query Request, to perform 3-D Secure on the transaction, if the customer's card is enrolled.
6	ORDERDETAILS	**For PayPal (see section 4.14):** An Order Details Request, used to retrieve updated information about the transaction from PayPal after the customer has logged in and confirmed the payment. **Required when offering PayPal as a payment option.**
7	AUTH	An Authorisation Request. **Required when processing an authorisation.**
8	SUBSCRIPTION	**For Subscriptions (refer to the Subscriptions and Payment Pages supplement):** A Subscription Request, where payments will be processed automatically at pre-specified intervals.

THREEDQUERY, SUBSCRIPTION, CURRENCYRATE, ORDER and ORDERDETAILS Requests must be submitted with an accompanying AUTH Request.

If you offer PayPal as a payment method, you MUST specify at least ORDER and AUTH request types to be enabled for enhanced post.

*If multiple request types are sent in a single Enhanced Post request, they are always processed in the order indicated by the numbers in the table above, regardless of the order the request types are submitted.

7.1.1.2 Standard POST behaviour

Each standard POST submitted to Payment Pages will utilise all request types enabled on your account.

e.g. if you have ACCOUNTCHECK, THREEDQUERY and AUTH enabled,
a standard POST will instruct us to process
ACCOUNTCHECK, THREEDQUERY and AUTH requests.

7.1.1.3 Over-riding with enhanced post

Enhanced post allows you to specify the request types utilised in each POST. This allows you to only call on certain request types when needed. Requests are processed in the order they are listed in the table in section 7.1.1.1.

e.g. if you have ACCOUNTCHECK, THREEDQUERY and AUTH enabled,
an enhanced POST can be used to instruct us to only process an ACCOUNTCHECK.

7.1.2 Implementing enhanced post

7.1.2.1 Enabling enhanced post

To enable enhanced post, you will first need to contact our Support team (see section 8.1) and decide on the request types that need to be enabled on your account (from the table found in section 7.1.1.1).

7.1.2.2 Submitting an enhanced post

You can use enhanced post by submitting a standard POST to the Payment Pages with the enhanced post field(s), called "requesttypedescriptions".

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 outlined in section 7.1.1.2.

The enhanced post is the equivalent of a blank slate. You must include each request type that you wish to process in each POST:

7.1.2.3 Example of sending an AUTH with enhanced post

This POST will **only** process an AUTH request:

```
<html>
<body>
<form method="POST" action="<DOMAIN>/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>
```

See section 9.2 for a full list of supported domains for the <DOMAIN> placeholder.

7.1.2.4 Example of sending an AUTH and ACCOUNTCHECK with enhanced post

This POST will process an ACCOUNTCHECK **and** an AUTH request:

```
<html>
<body>
<form method="POST" action="<DOMAIN>/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>
```

See section 9.2 for a full list of supported domains for the <DOMAIN> placeholder.

7.1.2.5 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 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 POST. The customer may alter these details while on PayPal's checkout pages, but these changes will not be reflected in the authorisation request.

Example of sending an ORDER, AUTH and ORDERDETAILS request with enhanced post

This POST will process an ORDER, AUTH and ORDERDETAILS request:

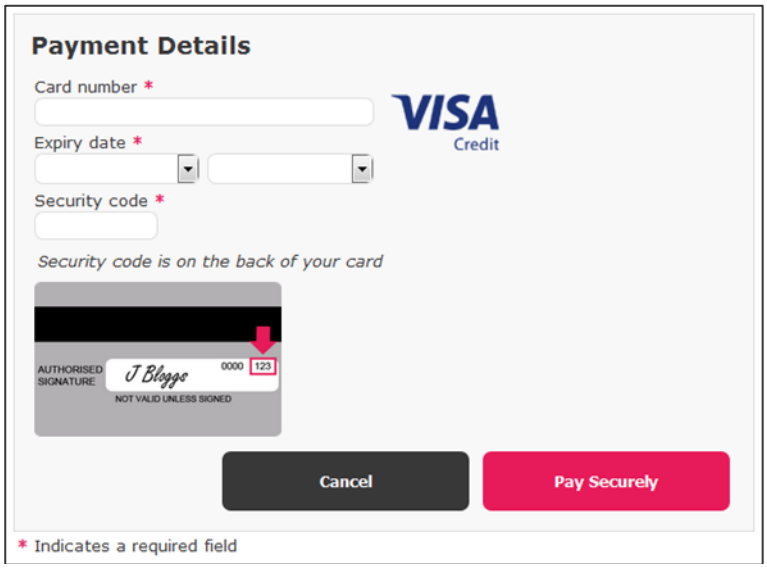
```
<html>
<body>
<form method="POST" action="<DOMAIN>/process/payments/choice">
<input type="hidden" name="sitereference" value="test_site12345">
<input type="hidden" name="stprofile" value="default">
<input type="hidden" name="currencyiso3a" value="USD">
<input type="hidden" name="mainamount" value="100.00">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

See section 9.2 for a full list of supported domains for the <DOMAIN> placeholder.

7.2 Action buttons

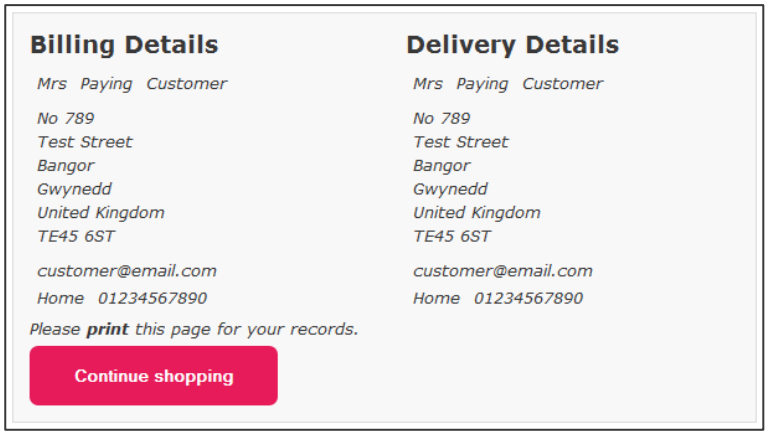
7.2.1 "Cancel" buttons

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



7.2.2 "Continue shopping" button

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.



7.2.3 Configuration

The action buttons described above can only be added to Payment Pages using the default **stprofile**.

To set up these buttons on Payment Pages, please contact the Support team (see section 8.1). Please inform support of the required URL(s) and buttons required for your solution.

7.3 Pre-Authorisations and Final Authorisations

You can use the **authmethod** field to designate an AUTH request as a pre-authorisation or a final authorisation. These are described as follows:

Pre-Authorisation:

- Settlement can be deferred by up to **31 days** following authorisation.
- During this time, the amount to be settled can be updated to a value that is lower than the amount authorised.
- The transaction can be cancelled by updating the **settlestatus** to "3".
- Funds are reserved on the customer's account for up to **31 days**.

Final authorisation (only supported by Mastercard):

- Settlement should **only** be deferred for up to **4 days** following authorisation.
- Following authorisation, the amount value must not be updated.
- Following authorisation, this transaction must not be cancelled.
- Secure Trading will automatically cancel all outstanding final authorisations after **7 days**, if they have not been settled (Funds are reserved on the customer's account for up to **7 days**).

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.

Failure to adhere to these conditions may incur a fine from Mastercard.
For full terms and conditions, please contact your acquiring bank.

We recommend that you contact your acquirer to ensure your system submits the correct **authmethod** value for your configuration.

By default, Secure Trading will process AUTH requests as follows:

- **Mastercard** payments are processed as final authorisations, if required by the participating acquirer.
- **Visa** payments will not include the **authmethod**, meaning they will be processed as standard authorisations.

You can change this default behaviour to submit pre-authorisations, by contacting Secure Trading Support (see section 8.1).
Alternatively, see section 7.3.1 for information on overriding the default behaviour on a transaction-by-transaction basis.

Please note that when performing **split shipments**, the **authmethod** field must always be set to "PRE".
For info on split shipments, please refer to the Split Shipment Guide.

7.3.1 Override

You can include the **authmethod** field in the 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).

Important: When submitted, auth methods "PRE" or "FINAL" must be included in the string used to generate your request site security hash, as described in section 1.3. Failure to do so will result in the customer being shown an "Invalid details" error message.

7.4 Google Analytics

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

7.4.1 Using Google Analytics tracking code

Google Analytics can be used with the 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 Secure Trading 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);
  })();
```

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

For merchants customising their Payment Pages using custom **stprofiles** (see section 2.1), upload this JavaScript file separately for each profile, with the filename [stprofile].js

Google Analytics will set cookies on the customer's browser. For further information on Google Analytics, refer to this URL: http://www.google.co.uk/analytics/index.html

7.5 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.

We offer three configurations to handle customers who select a card type on the payment choice page, but enter the details of a different card type on the details page. These configurations are outlined in detail in this section of the document. To change the verify card type solution to be used on your site, please contact the Support team (see section 8.1).

> 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.

7.5.1 Auto-correct (Default) - Configuration '0'

New sites are configured to use 'Auto Correct' (configuration '0') by default.

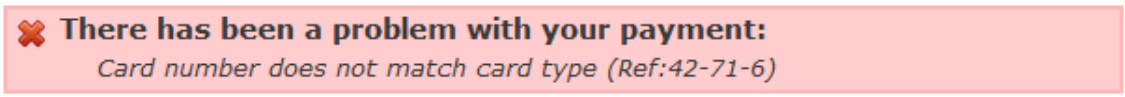
The payment is processed in the correct payment type, but the customer is not informed beforehand if the card details they have entered did not match the card type they selected on the payment choice page.

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 payment details page.

7.5.2 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 payment details page. This is designed for merchants who have implemented their own hosted payment choice page (e.g. using workflow B; section 1.1.2), allowing customers to select a payment type before inputting their payment details on our hosted payment details page.

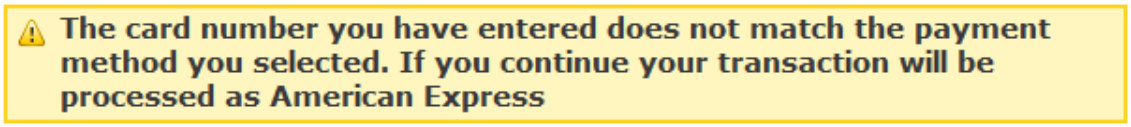
If the customer enters card details that do not match the card type, and attempt to process a payment, the payment will not be processed and a red warning message is shown at the top of the page.



They cannot proceed with the payment until they enter payment details for the pre-specified payment type.

7.5.3 Payment Pages redisplay choice if PAN doesn't match - Configuration '2'

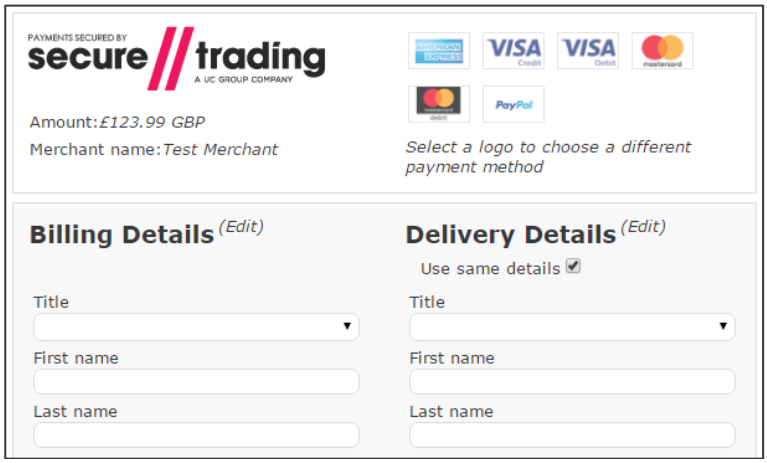
The customer is shown a yellow warning at the top of the page, if the card details they have entered did not match the card type they selected on the payment choice page.



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

7.5.4 Manually changing payment types on the payment details page

For sites configured to use verify card type configurations '0' and '2', a list of payment types are displayed at the top of the payment details page:



The customer can click a different payment type, and the payment details page will be redisplayed with fields and content relevant to the selected payment type.

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

Sites using verify card type configuration '1' will **never** show payment types on the payment 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 payment details page, they cannot change the payment type they are paying in.

7.6 Rules

When enabled, we 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 our online documents, which provides information on managing your rules.

7.6.1 Rule types

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

For information on the latest version of request site security, refer to section 1.3.
If you are unsure, contact Support for further assistance (section 8.1).

We provide 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 section 7.6.2. Secure Trading Rules are always performed before User-Defined Rules.

7.6.1.2 User-Defined Rules

Rules with a Rule ID of "UDR-x" (where x is a number) are User-Defined Rules. e.g. UDR-129
Using MyST, you can create, modify and activate your own custom rules on any of your site references.

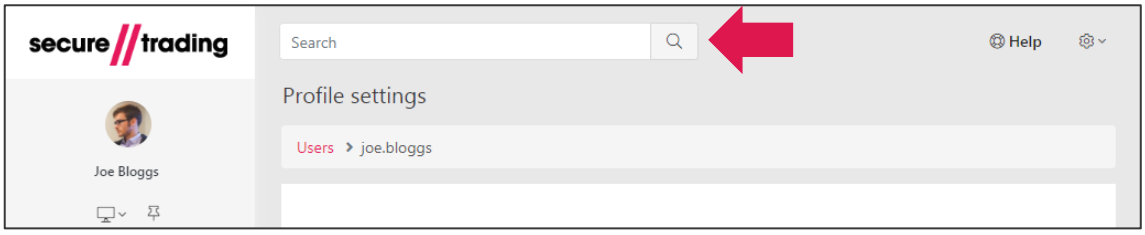
Further information on User-Defined Rules can be found in our online documents.

7.6.2 Activating rules

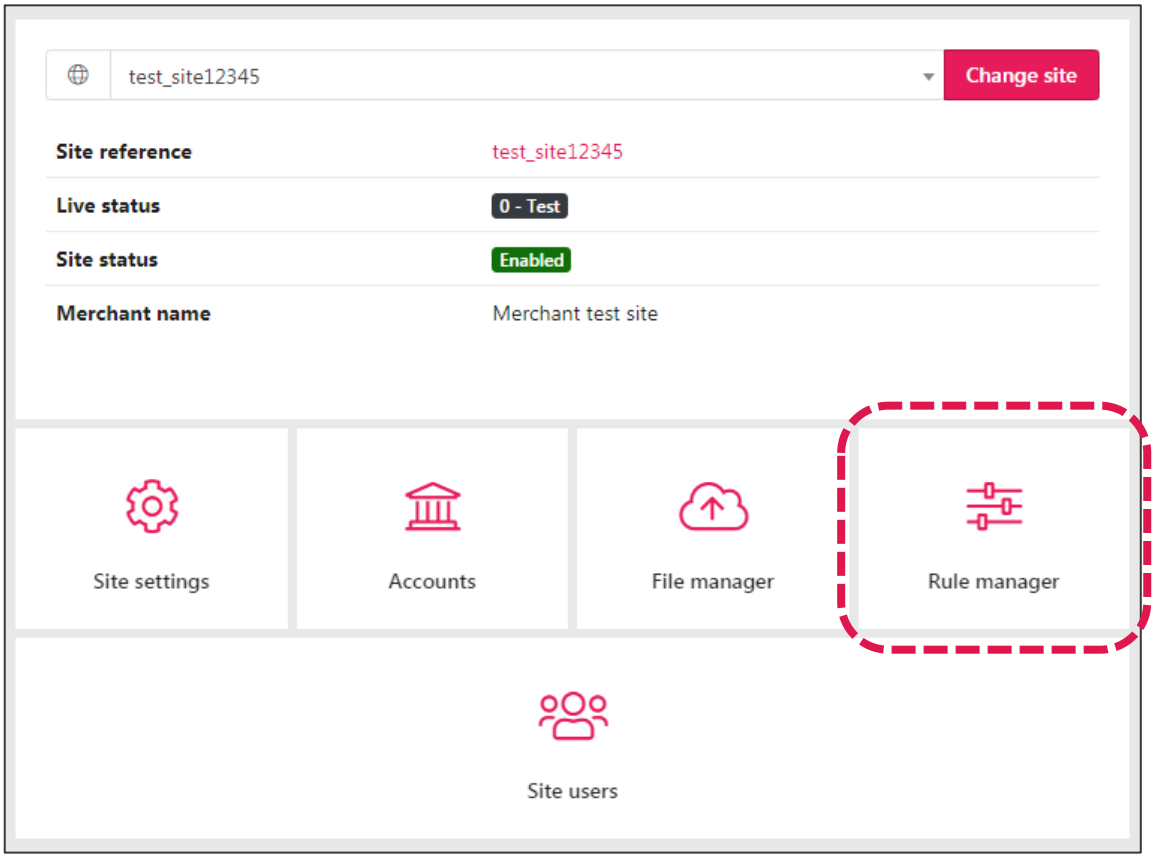
7.6.2.1 Using MyST

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.

Once signed in, type your site reference into the search box at the top of the page and submit.

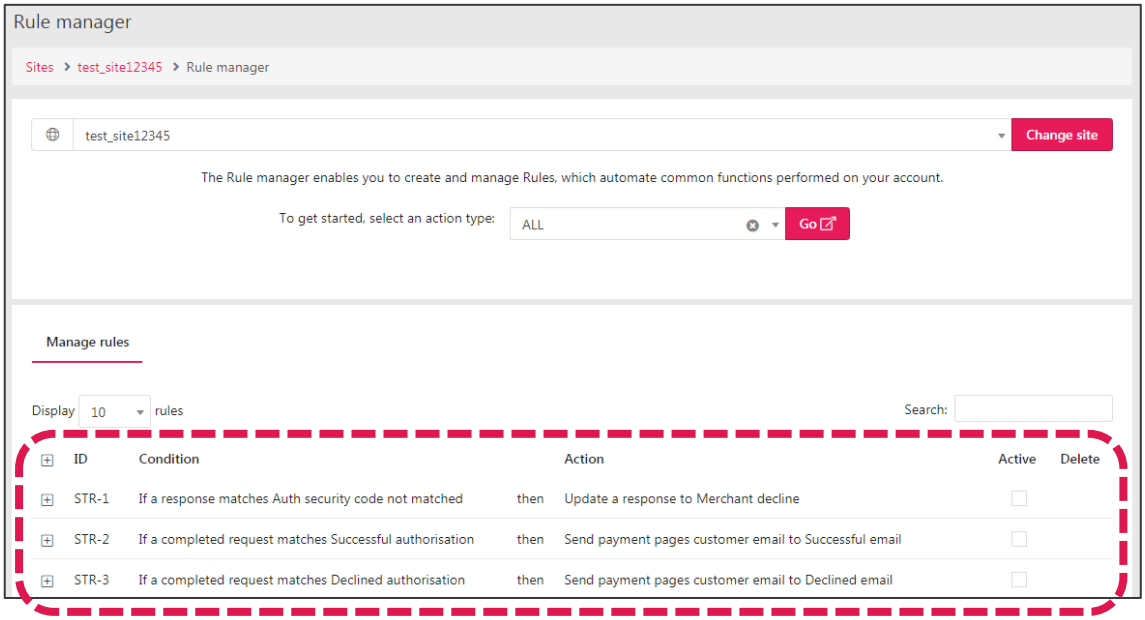


Then click "**Rule manager**".



From the Rule manager, you can view all rules available on your site reference. You can change the selected site reference and types of rules displayed on-screen by using the drop-down boxes at the top of the page.

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**".



7.6.2.2 In the POST to Payment Pages

Rules can be activated for individual requests by submitting the unique rule identifier in the **`ruleidentifier`** field. Rules specified in the request will lead certain actions to be performed if pre-defined criteria are met (regardless of whether or not said rules are active on your site references as described in section 7.6.2.1). The following code snippet is from an HTML form where two rules *STR-1* and *STR-2* are specified:

```
<form method="POST" action="<DOMAIN>/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>
```

See section 9.2 for a full list of supported domains for the <DOMAIN> placeholder.

Important: Any rule identifiers submitted (e.g. "STR-1") must be included in the string used to generate your request site security hash, as described in section 1.3. Failure to do so will result in the customer being shown an "Invalid details" error message.

7.6.3 Merchant decline

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 activated in the MyST Rule Manager, the rule will also be enabled for payments processed using the Virtual Terminal, where a message of "Transaction Failed" will be displayed.

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 7.6.3.1 and update your rules as required.
Contact our Support team (see section 8.1) if you require further assistance.

7.6.3.1 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).

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

7.7 Subscriptions

Subscriptions allow transactions to be automatically re-processed without needing to submit additional requests to Secure Trading. e.g. Payments can be scheduled to be processed on the first of each month for £10.00.

Please refer to this supplement for further information:
http://www.securetrading.com/files/documentation/STPP-Subscriptions-and-Payment-Pages.pdf

7.8 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

7.9 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

8 Further Information and Support

This section provides useful information with regards to documentation and support for your Secure Trading solution.

8.1 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

8.2 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

8.3 Useful Documents

You may find the following additional documents useful when configuring your Payment Pages:

- **AVS & Security Code checks**
- **Charge description**
- **Digital wallet**
- **Enabling PayPal**
- **Fraud Checks**
- **MyST documentation**
- **MyST Rule Manager**
- **Payment facilitator**
- **Payment Pages Customisation**
- **Protect Plus**
- **Split Shipments**
- **Subscriptions and Payment Pages**
- **Testing**

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.

8.4 Frequently Asked Questions

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

9 Appendix

9.1 POST fields

The following fields can be included within the POST submitted from your website to Payment Pages.

Requirements:

- All field names must be submitted in lowercase.
- Do not submit multiple fields with the same name in a single POST, unless documentation states this is permitted.
- We recommend that text submitted is encoded in UTF-8.
- Special characters must be URL-encoded (e.g. "&" should be submitted as "%26").

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

Quick reference:

- For additional fields recommended for submission when Protect Plus is enabled, see section 9.1.12.
- For additional fields required by Visa and Mastercard for UK-based merchants with MCC6012, see section 9.1.13. **Failing to submit these fields may result in the customer being displayed an invalid request error.**
- For additional fields required by Visa and Mastercard for merchants processing debt repayments, see section 9.1.14. **Failing to submit these fields may result in the customer being displayed an invalid request error.**

9.1.1 Required fields

The following fields are required in every POST to Payment Pages:

Field name	Description
sitereference	The unique Secure Trading site reference that you receive when you sign up.
currencyiso3a	The currency in which the transaction will be processed, using ISO3A format.
mainamount	The amount of the transaction should be in main units. e.g. £123.99 would be submitted like this: 123.99. Currencies such as Japanese Yen which do not require a decimal place can be submitted without. e.g. 1000 Yen would be 1000.
version	This value will be set to 2.
stprofile	Used to specify the styling used to render the Payment Pages. When using the default appearance, this is set to "default". See section 2.1.

9.1.2 Billing fields

You may also submit the following billing fields in the POST:

Field name	Description
billingprefixname	The billing name prefix, from the following list: Mr, Mrs, Miss, Dr, Ms, Prof, Rev, Sir, Lord, Lady, Dame & Mx.
billingfirstname	The billing first name.
billingmiddlename	The billing middle name.
billinglastname	The billing last name.
billingpremise	The house number or first line of the billing address.
billingstreet	The street entered for the billing address.
billingtown	The town entered for the billing address.
billingcounty	The county entered for the 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: // **Preferred:** Two character state code, e.g. “NY”. // Full state name (no abbreviations), e.g. “New York”.

billingpostcode	The postcode entered for the billing address.
	
	We perform the following validation for addresses in United States, Great Britain and Canada (where 'T' represents text A-Z or a-z and 'N' represents numbers 0-9):
	
	Great Britain:
	// TN NTT
	// TNT NTT
	// TNN NTT
	// TTN NTT
	// TTNN NTT
	// TTNT NTT
	
	United States:
	// NNNNN
	// NNNNNNNNN
	
	Canada:
	// TNT NTN
	// TNTNTN
	
	British Forces Post Office (BFPO)
	// “BFPO” N
	// “BFPO” NN
	// “BFPO” NNN
	// “BFPO” NNNN
	
	We also accept 3-4 digit ZIP codes for US addresses. These will be automatically preceded with zeroes, e.g. “123” will be changed to “00123”.
	
	If the country provided is not United States, Great Britain or Canada, or if no country is provided, the postcode field is not validated.

billingcountryiso2a	The country entered for the billing address, using ISO2A format.
billingemail	The billing email address. This can then be used for correspondence with the customer. Maximum length of 255 (maximum of 64 characters before the”@” symbol).

billingtelephone	The billing telephone number. Valid characters:
	// Numbers 0-9
	// Spaces
	// Special characters: + - ( )

billingtelephonetype	The type of telephone number entered.
	The options available are:
	// H = Home
	// M = Mobile
	// W = Work

9.1.3 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	Description
customerprefixname	The customer name prefix, from the following list: Mr, Mrs, Miss, Dr, Ms, Prof, Rev, Sir, Lord, Lady, Dame and Mx.
customerfirstname	The customer first name.
customermiddlename	The customer's middle name.
customerlastname	The customer last name.
customerpremise	The house number or first line of the customer's address.
customerstreet	The street entered for the customer's address
customertown	The town entered for the customer's address.
customercounty	The county entered for the customer's 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: // **Preferred:** Two character state code, e.g. "NY". // Full state name (no abbreviations), e.g. "New York".

customerpostcode	The postcode entered for the customer's address.
	We perform the following validation for addresses in United States, Great Britain and Canada (where 'T' represents text A-Z or a-z and 'N' represents numbers 0-9):
	Great Britain:
	// TN NTT
	// TNT NTT
	// TNN NTT
	// TTN NTT
	// TTNN NTT
	// TTNT NTT
	United States:
	// NNNNN
	// NNNNNNNNN
	Canada:
	// TNT NTN
	// TNTNTN
	British Forces Post Office (BFPO)
	// "BFPO" N
	// "BFPO" NN
	// "BFPO" N
	// "BFPO" NN
	We also accept 3-4 digit ZIP codes for US addresses. These will be automatically preceded with zeroes, e.g. "123" will be changed to "00123",
	If the country provided is not United States, Great Britain or Canada, or if no country is provided, the postcode field is not validated.

customercountryiso2a	The country entered for the customer's address, using ISO2A format.
customeremail	The customer's email address. This can then be used for correspondence with the customer. Maximum length of 255 (maximum of 64 characters before the"@" symbol).

customertelephone	The customer's telephone number.
	Valid characters:
	// Numbers 0-9
	// Spaces
	// Special characters: + - ( )

customertelephonetype	The type of telephone number entered.
	The options available are:
	// H = Home
	// M = Mobile
	// W = Work

9.1.4 Settlement fields

You can include the following optional fields in the POST to affect settlement.
Note: Please read section 1.11 and ensure you understand the settlement process before deferring settlement and/or modifying the settle status.

Field name	Description
settleduedate	Use this field to defer settlement until the date specified (in the format YYYY-MM-DD).
settlestatus	Leave blank or submit “0” to opt for standard settlement behaviour as described in section 1.11. Submit “1” to override fraud and duplicate checks, if these have been enabled on your account (see section 3). Submit "2" to manually suspend settlement. The transaction will remain in a suspended state until you update the settle status at a later date using MyST. **(Only supported by select acquirers)** Submit “100” to settle the transaction immediately after authorisation. Contact Support (section 8.1) to check if your acquirer supports this.

9.1.5 Charset

In order for data to be transmitted, the customer's browser encodes it using a character encoding. Our 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 we will assume the character encoding is ISO-8859-1. This is compatible with all browsers but can result in some characters (especially 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_" />
```

9.1.6 Request fields

Field name	Description
authmethod	To manually override the default auth method specified on your account (see section 7.3).
dcctype	This field is explained in section 6.4.
locale	By default, Payment Pages will be displayed to the customer in UK English, unless overridden using the values below: cy_GB = Welsh, United Kingdom da_DK = Danish, Denmark de_DE = German, Germany en_US = English, United States en_GB = English, United Kingdom es_ES = Spanish, Spain fr_FR = French, France nl_NL = Dutch, The Netherlands no_NO = Norwegian, Norway sv_SE = Swedish, Sweden
operatorname	You can use this field to record the name of the operator performing the payment via the Payment Pages. This is stored in our records and can be viewed later in MyST. If not submitted in the POST, this value defaults to "paymentpages". This value is not displayed on the Payment Pages (providing the account type is "ECOM"). If you opt to submit the **operatorname**, we recommend that you update your site security hash to include this field (see section 1.3), by contacting our Support team.
orderreference	Your own reference for the transaction. This can be useful when matching transactions to orders within your system.
paymenttypedescription	Allows you to choose the payment method for the transaction when using workflow B (see section 1.1.2.4).
requesttypedescriptions	Used to specify request types to be processed when enhanced post is enabled on your account (see section 7.1).
sitesecurity	Used to submit the request site security hash in the POST (see section 1.3).
sitesecuritytimestamp	As accurately as possible, the timestamp that reflects when the customer's browser is to be redirected to the Payment Pages. The customer will have 3 hours from the specified time to complete the payment (see section 1.3). The value submitted in this field must be in the format YYYY-MM-DD hh:mm:ss. The timestamp must be in UTC.

9.1.7 Custom fields

You can pass through custom fields in your POST. The field names do not need to be a specific case and will not be saved in the database. No additional configuration is required.

Custom fields can be posted back to your system after a transaction has been processed, by including them in a redirect (see section 1.3) and/or configuring a URL notification (see section 1.7).

While custom fields do not have a specification on valid values, it is important to ensure the value cannot be hijacked as part of a malicious attack. Wherever possible we recommend the following:

- **Use standard letters and numbers** within the ASCII character set without any special characters where possible, particularly with the field names.
- Any file references you may define should **use a full path rather than a relative path**.
- **Keep fields and values as short as possible**.

9.1.7.1 *Additional considerations*

- The maximum allowed length of custom fieldnames that can be submitted is 100 characters. Any custom fieldnames exceeding this limit will be truncated or cause an error.
- Fieldnames should not end with "_html".

9.1.8 Customisation fields

Field name	Description
stdefaultprofile	Two supported values: “st_paymentcardonly” – see section 2.1.1.2. “st_cardonly” - see section 2.1.1.4. “st_iframe_cardonly” - see section 2.1.1.5.
strequiredfields	Specify fields required to be entered by the customer (see section 2.5). *Multiple fields supported*

9.1.9 Apple Pay fields

You can submit the following optional fields in your POST to change how the customer is prompted for their address details while on the Payment Pages:

Field name	Description
billingcontact detailsoverride	**(Optional)** The billing address for the payment: “0” – Uses details entered (or posted) on the Payment Pages. “1” – Uses details specified on the customer’s Apple Pay account. If left blank, the address entered (or posted) on Payment Pages is used.
customercontact detailsoverride	**(Optional)** The customer (delivery) address for the payment: “0” – Uses details entered (or posted) on the Payment Pages. “1” – Uses details specified on the customer’s Apple Pay account. If left blank, the address entered (or posted) on Payment Pages is used.

9.1.10 PayPal fields

Field name	Description
paypaladdressoverride	Specify how the delivery address is entered when processing payments with PayPal (see section 4.13.2.2).
paypallocaleiso2a	The language of the PayPal login page. For the country code values that can be submitted, please refer to https://developer.paypal.com/docs/classic/api/locale_codes/

9.1.11 Rule fields

Field name	Description
allurlnotification	This is the URL the notification is sent to following any request, when STR-10 is enabled (see section 1.7.3).
declinedurlredirect	This is the URL the customer's browser is redirected to following a declined transaction, when STR-7 is enabled (see section 1.5.2).
declinedurlnotification	This is the URL the notification is sent to following a declined transaction, when STR-9 is enabled (see section 1.7.2).
ruleidentifier	Used to enable rules on a request-by-request basis (see section 7.6). *Multiple fields supported*
stextraurlredirectfields	This is used to include additional fields in redirects (see section 1.5.4).
stextraurlnotifyfields	This is used to include additional fields in URL notifications (see section 1.7.5).
successfulurlredirect	This is the URL the customer's browser is redirected to following a successful transaction, when STR-6 is enabled (see section 1.5.1).
successfulurlnotification	This is the URL the notification is sent to following a successful transaction, when STR-8 is enabled (see section 1.7.1).

9.1.12 Protect Plus fields

The following optional fields can be posted to the Payment Pages to improve the Protect Plus checks:

Field name	Description
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: **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

9.1.13 Additional Authorisation Data Merchant Category Code (MCC) 6012 fields

Visa and Mastercard have mandated that all UK-based merchants with a Merchant Category Code (MCC) of 6012 are required to send the following fields. **Failing to submit these fields may result in the customer being displayed an invalid request error.**

Field name	Description
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.
customeraccountnumbertype	Either “CARD” or “ACCOUNT”.
customerdob	The account holder’s date of birth. Must be in the format YYYY-MM-DD.
customerlastname	The account holder’s last name.

customerpostcode	The account holder’s postcode.
	
	We perform the following validation for addresses in United States, Great Britain and Canada (where 'T' represents text A-Z or a-z and 'N' represents numbers 0-9):
	
	Great Britain:
	// TN NTT
	// TNT NTT
	// TNN NTT
	// TTN NTT
	// TTNN NTT
	// TTNT NTT
	
	United States:
	// NNNNN
	// NNNNNNNNN
	
	Canada:
	// TNT NTN
	// TNTNTN
	
	British Forces Post Office (BFPO)
	// “BFPO” N
	// “BFPO” NN
	// “BFPO” N
	// “BFPO” NN
	
	We also accept 3-4 digit ZIP codes for US addresses. These will be automatically preceded with zeroes, e.g. “123” will be changed to “00123”,
	
	If the country provided is not United States, Great Britain or Canada, or if no country is provided, the postcode field is not validated.

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 the Support team (see section 8.1).

Once you have processed a payment or account check (see section 3.1.7) containing these required fields, they are automatically included in future re-authorisations and account checks performed in MyST, and passed onto the acquiring bank.

9.1.14 Debt repayment fields

Visa and Mastercard have mandated that all merchants processing debt repayments submit the following fields in the POST (when the data has been made available).

This mandate only applies to merchants with certain acquiring banks.
Please contact our Support team for further information (see section 8.1).

Requirement: Your merchant category code must be either 6012, 6051 or 7299.

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 the Support team (see section 8.1).

Field name	Description
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.
customeraccountnumbertype	Either “CARD” or “ACCOUNT”.
customerdob	The account holder’s date of birth. Must be in the format YYYY-MM-DD.
customerlastname	The account holder’s last name.

customerpostcode	The account holder’s postcode.
	
	We perform the following validation for addresses in United States, Great Britain and Canada (where 'T' represents text A-Z or a-z and 'N' represents numbers 0-9):
	
	Great Britain:
	// TN NTT
	// TNT NTT
	// TNN NTT
	// TTN NTT
	// TTNN NTT
	// TTNT NTT
	
	United States:
	// NNNNN
	// NNNNNNNNN
	
	Canada:
	// TNT NTN
	// TNTNTN
	
	British Forces Post Office (BFPO)
	// “BFPO” N
	// “BFPO” NN
	// “BFPO” N
	// “BFPO” NN
	
	We also accept 3-4 digit ZIP codes for US addresses. These will be automatically preceded with zeroes, e.g. “123” will be changed to “00123”,
	
	If the country provided is not United States, Great Britain or Canada, or if no country is provided, the postcode field is not validated.

debtrepayment	Indicates if transaction is flagged as debt repayment: 1 – Transaction is flagged as debt repayment. 0 – Transaction is **not** flagged as debt repayment. **Note:** Your site can be configured to automatically submit this flag with value 0 or 1 in every transaction by default. (Contact Support to make this change – see section 8.1).

9.2 Supported domains

When connecting to Secure Trading, you will need to ensure you specify a supported domain in the URL.

Please contact our Support Team (see section 8.1) to confirm the gateway your account has been configured to use.

These are the supported values:

	European Gateway	US Gateway
Payment Pages	https://payments.securetrading.net	https://payments.securetrading.us
MyST	https://myst.securetrading.net	https://myst.securetrading.us
Web App	https://webapp.securetrading.net	https://webapp.securetrading.us

9.3 Custom URL redirect rule that excludes default fields

Use the MyST Rule manager to add the following rules:

Action type: Payment pages redirect

Rule for successful AUTH:

- **Condition:** Request “AUTH”, Settle status 0, 1, 2, 10 & 100, Account type “ECOM”, Error code 0.
- **Action:** URL for redirect (use “Field selection” tab to select additional fields)

Rule for declined AUTH:

- **Condition:** Request “AUTH”, Settle status 3, Account type “ECOM”, Error code 70000.
- **Action:** URL for redirect (use “Field selection” to select additional fields)

9.4 Generating the request site security hash

Use the following examples to assist in developing your own code, for generating the request site security hash (see section 1.3) that is included in requests to the Payment Pages.

9.4.1 Python example

```
#!/usr/bin/python

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

9.4.2 PHP example

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

9.4.3 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("UTF-8"));
      String merchantHash = String.format("%064x",new
BigInteger(1,digestObj.digest()));
      System.out.println(merchantHash);
    }
}
```

9.4.4 Perl example

```
#!/usr/bin/perl

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

9.5 Handling iframes on iOS devices

To avoid compatibility issues when rendering the Payment Pages in iframes on iOS devices, include the following in your HTML mark-up:

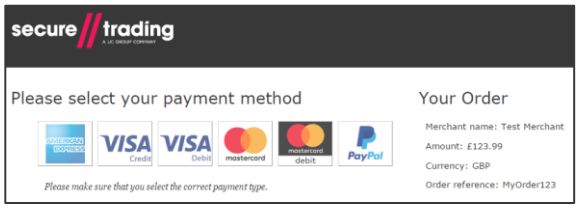
```
<div style="overflow:hidden; min-width:100%">
<iframe class="zonalIframe" scrolling="no" src="WIDGETURL"
style="width:1px; min-width:100%;">
</iframe>
</div>
```

And the following CSS:

```
overflow:hidden;
min-width:100%
```

9.6 Migrating from version 1

If your Payment Pages looks like:

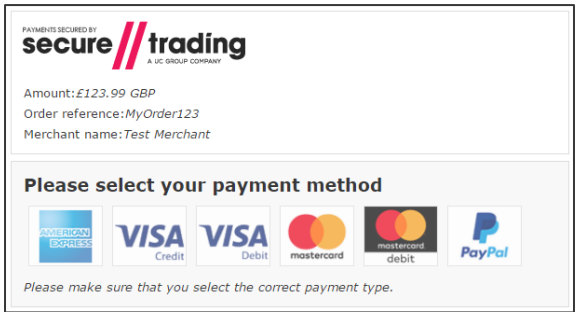


Or if your HTTPS POST includes *version=1*

You're on version 1

Please follow the steps below to benefit from the new features available.

If your Payment Pages looks like:



Or if your HTTPS POST includes *version=2*

You're on version 2

You're all set!

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="<DOMAIN>/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>
```

See section 9.2 for a full list of supported domains for the <DOMAIN> placeholder.

9.6.1 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 make changes to your CSS to support version 2. To get started, see section 2.1.