CyberSource

Secure Acceptance Web/Mobile Quick Start Guide

i. Confidential Information

All material contained in this document is confidential information. The confidential information may not be disclosed to third parties other than employees and authorized contractors on behalf of and/or CyberSource.

ii. CyberSource Contact Information

For general information about our company, products and services, go to http://www.cybersource.com

Contents

1. Introduction to Secure Acceptance Web/Mobile

1.1. What Is It?

Secure Acceptance Web/Mobile enables you to quickly and easily accept card payments online, without handling payment data. Secure Acceptance Web/Mobile is a CyberSource hosted payment interface. Customers are directed to enter their payment details for payment processing and secure storage. After completing the transaction, CyberSource redirects customers back to your site with details of the payment transaction and a success, review or failure code. Optionally, CyberSource sends a direct response back to your site for verification.

Once a transaction has been processed it can be reviewed in the CyberSource Enterprise Business Centre. This is our central web management portal for reporting and follow on transaction processing.

Secure Acceptance is fully hosted by CyberSource therefore the customer payment data is not handled directly by the merchant. This will significantly help in decreasing the Payment Card Industry Data Security Standard (PCI-DSS) scope that you will face when processing Card-Not-Present type transactions.

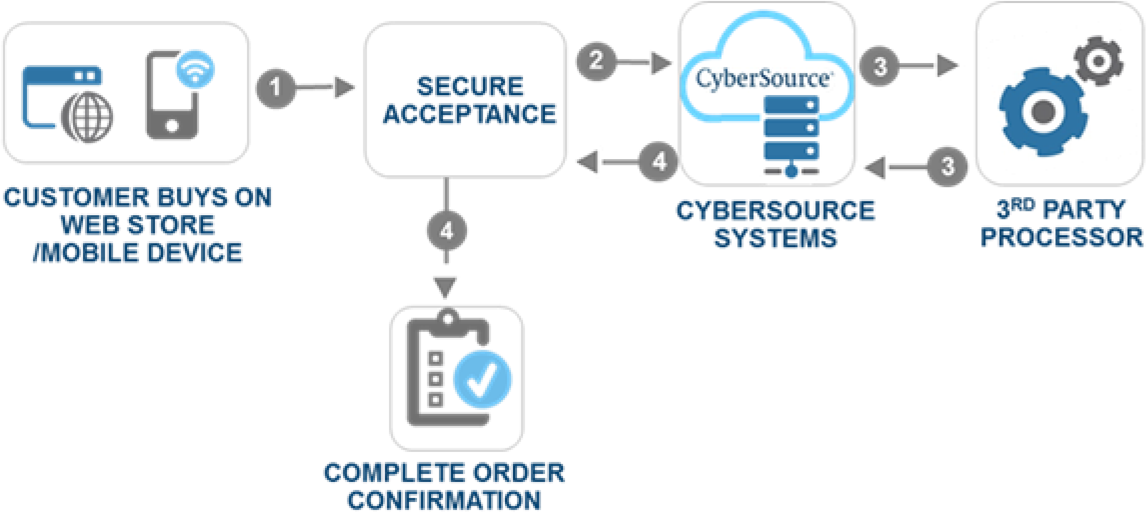
Please visit https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml for more information regarding PCI-DSS regulations.

Should you have any further enquiries or have specific questions around PCI-DSS compliancy, then please email VPSSAIS@VISA.COM who will be able to advise.

1.2. Secure Acceptance Web/Mobile Features

- **Security Compliance** – a hosted service, meaning it is faster and easier to achieve PCI-DSS certification
- **Reduced Risk** – no handling or storage of sensitive customer account data
- **Low Maintenance** – leave compliance and order page maintenance to CyberSource
- **Speed** – faster and easier than implementing in-house order pages
- **Customisation** – customize basic visual elements and messaging for customers
- **Virtually Transparent** – customers move seamlessly from web store to CyberSource's Secure Acceptance pages & back to web store confirmation page
- **Language Support** – checkout pages and email receipts can be translated into your customer's native language (37 languages and dialects as of July 2013)
- **Mobile Acceptance** – single integration supporting many channels of payment
- **Easy Transaction Management** – CyberSource Business Centre is used to review and manage all transactions from any computer with Internet access

1.3. How It Works



Step 1

Your web store directs customers who are ready to check out to Secure Acceptance: a CyberSource hosted PCI-compliant order form. The customer enters their own payment details on these pages, outside of your system.

You can use the CyberSource default layout to get started, or customize the payments steps, basic content and look of Secure Acceptance.

Step 2
The customer clicks 'Submit' on the hosted Secure Acceptance payment page to confirm their purchase.

Step 3
CyberSource sends a request for approval to the appropriate payment network in real time.

Once the payment is processed CyberSource will receive the response information from the payment network. We will store the response data and initiate a response via Secure Acceptance.

You can also use Secure Acceptance to create and update payment tokens and Recurring Billing subscriptions, with or without a payment request.

Step 4

The response information is sent back to you through the device's browser, and directly to your ecommerce infrastructure (see steps 14 and 15 of the step-by-step configuration guide for details on how to set this up). This data can be used to display an appropriate message to the customer, whether the transaction was approved or not.

Alternatively, you can use the default CyberSource hosted response page to display the result of the transaction.

Conclusion
When an order is processed it can be viewed in the Business Centre. If you have specified a 'Sale', the transaction will immediately be submitted for settlement. If you have specified 'Authorization', you will need to submit a separate request for settlement, for example when the goods are shipped.

2. Prerequisite Implementation Requirements

2.1. Technical Requirements

You **must** be able to create web pages that will gather customer and order information (excluding card data) for payment and fraud screening services. This data needs to be included in requests to Secure Acceptance, and you must be able to process the response information to fulfill the customer's order.

Your site must meet the following requirements:

- Shopping-cart or custom order creation software
- Product pages in one of the supported scripting languages (see next section)
- The IT infrastructure used for Secure Acceptance must be PKI enabled to use SSL based Form POST submissions.
- IT infrastructure used for Secure Acceptance must be able to digitally sign customer data prior to submission to Secure Acceptance Web/Mobile

2.2. Web Developers

To implement Secure Acceptance Web/Mobile, you should be competent in one of the following supported programming languages and have a basic understanding of HTML:

- Ruby
- PHP
- Perl
- JSP
- VB
- ASP.NET (C#)

Please note that the above languages are supported by CyberSource. Support through the CyberSource Professional Services team may be available for other languages.

2.3. Use of iframes

CyberSource recommends that if you implement our services within an iframe, please do so with the following PCI DSS Best Practices* in mind:

- iframes should be developed securely to ensure that unauthorized code is not executed inside of the iFrame.
- iframes should not expose internal network address ranges.
- iframes should be configured to prevent clickjacking (this occurs when a user is tricked into performing unsecure actions by clicking on hidden links within a browser).

*** PCI DSS E-commerce Guidelines – Information Supplement – January 2013**

3. Registering Test Accounts

To utilize the CyberSource payment gateway services, all merchants are required to obtain and activate a CyberSource test Merchant ID for integration and testing, or enable an existing Merchant ID.

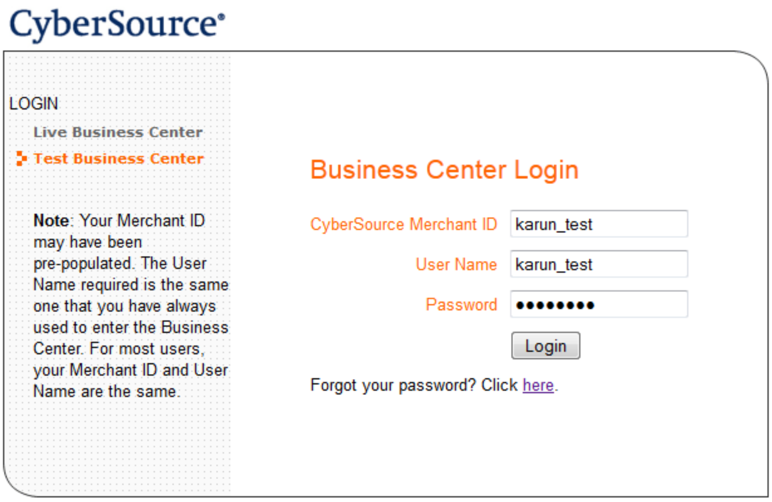
Please contact CyberSource Sales or Support who will be able to provide further guidance on how to obtain a test account. If necessary your account will be configured with the appropriate payment methods, currencies, and payment processor(s). Additionally if desired CyberSource will enable your test account for our value added services such as Tokenization, Recurring Billing and Decision Manager.

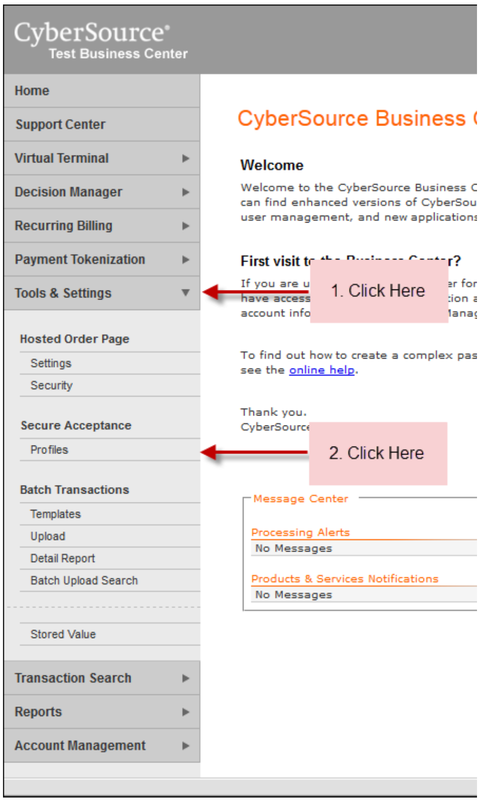
For more information on any of the above services, please contact your Sales Account representative.

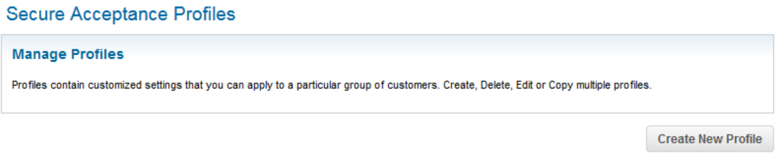
4. Implementation of Secure Acceptance

4.1. Step-by-Step Configuration

Before being able to deploy and send transactions via Secure Acceptance, the solution needs to be configured to your requirements. Use Step-By-Step Configuration Guide below:

1. Login to the Enterprise Business Centre (EBC) a. Open a web browser and navigate to https://ebctest.cybersource.com b. Enter your CyberSource Merchant ID * c. Enter your Username * d. Enter your Password * e. Click Login button and accept the notification of being in the TEST environment *** Provided by registering a CyberSource test account**	 CyberSource LOGIN Live Business Center Test Business Center Business Center Login Login **Note**: Your Merchant ID may have been pre-populated. The User Name required is the same one that you have always used to enter the Business Center. For most users, your Merchant ID and User Name are the same. CyberSource Merchant ID karun_test User Name karun_test Password •••••••• Forgot your password? Click here.

<table>
<tr>
<td>2. Click “Tools & Settings” on the left-hand menu followed by “Profiles” under the “Secure Acceptance” heading</td>
<td>


</td>
</tr>
<tr>
<td>3. Click “Create New Profile” Button</td>
<td>


Secure Acceptance Profiles

Manage Profiles

Profiles contain customized settings that you can apply to a particular group of customers. Create, Delete, Edit or Copy multiple profiles.

</td>
</tr>
</table>

4. Complete the form as per the screenshot. Mandatory fields are denoted by a red asterisks. Click the “Create” button once completed.

<u>Please note the following:</u>

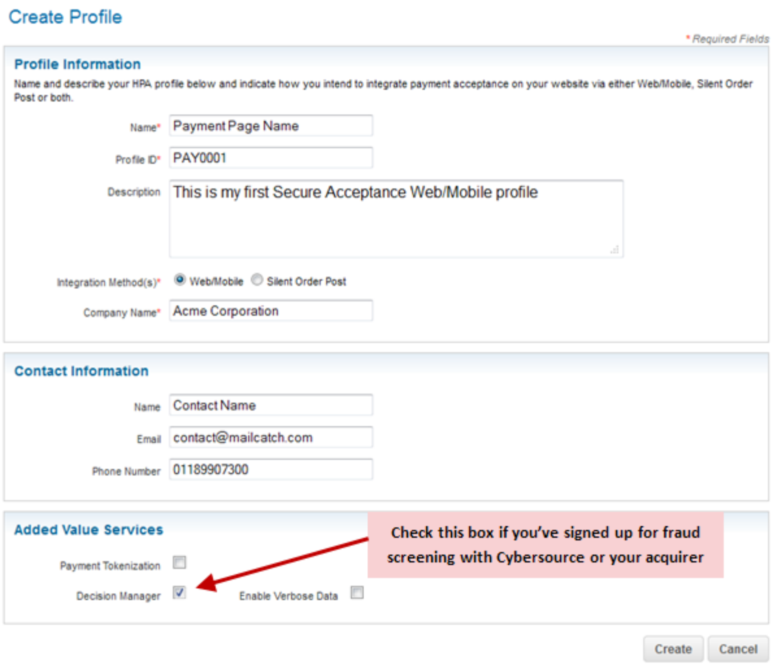
Name: max. 20 characters

Profile ID: 7 characters exactly. It is used in every transaction.

Description: max. 255 characters

Company Name: max 40 characters

Note: please ensure valid contact information is entered.



Create Profile

* Required Fields

Profile Information

Name and describe your HPA profile below and indicate how you intend to integrate payment acceptance on your website via either Web/Mobile, Silent Order Post or both.

Name*: Payment Page Name

Profile ID*: PAY0001

Description: This is my first Secure Acceptance Web/Mobile profile

Integration Method(s)*: ● Web/Mobile ○ Silent Order Post

Company Name*: Acme Corporation

Contact Information

Name: Contact Name

Email: contact@mailcatch.com

Phone Number: 01189907300

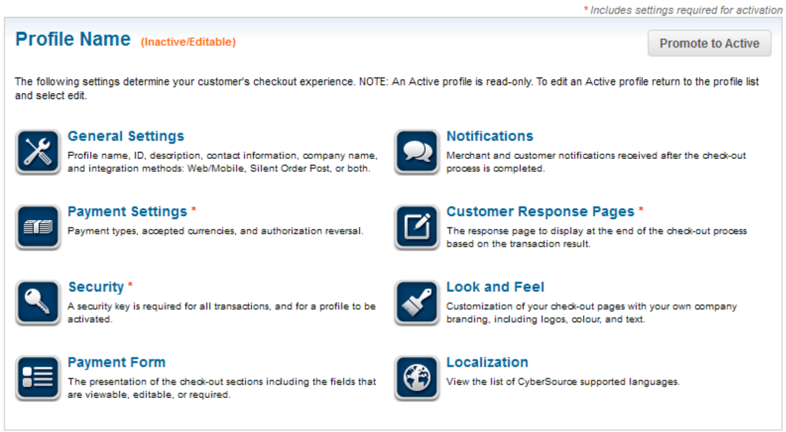
Added Value Services

Payment Tokenization □

Decision Manager ☑ Enable Verbose Data □

Check this box if you’ve signed up for fraud screening with Cybersource or your acquirer

5. When the profile is successfully created, the settings menu will be displayed. Click “Payment Settings”.



* Includes settings required for activation

Profile Name (Inactive/Editable)

The following settings determine your customer's checkout experience. NOTE: An Active profile is read-only. To edit an Active profile return to the profile list and select edit.

General Settings
Profile name, ID, description, contact information, company name, and integration methods: Web/Mobile, Silent Order Post, or both.

Notifications
Merchant and customer notifications received after the check-out process is completed.

Payment Settings *
Payment types, accepted currencies, and authorization reversal.

Customer Response Pages *
The response page to display at the end of the check-out process based on the transaction result.

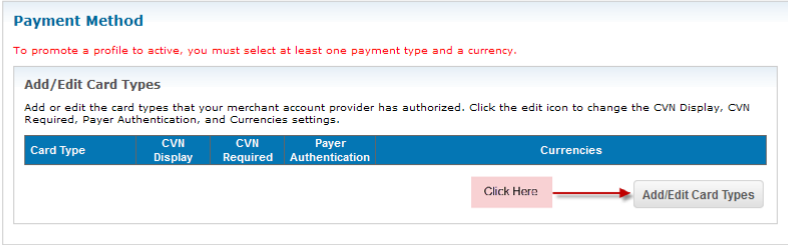
Security *
A security key is required for all transactions, and for a profile to be activated.

Look and Feel
Customization of your check-out pages with your own company branding, including logos, colour, and text.

Payment Form
The presentation of the check-out sections including the fields that are viewable, editable, or required.

Localization
View the list of CyberSource supported languages.

6. By default, no payment types are selected. In order to accept a card type, click the “Add/Edit Card Types” button.



Payment Method

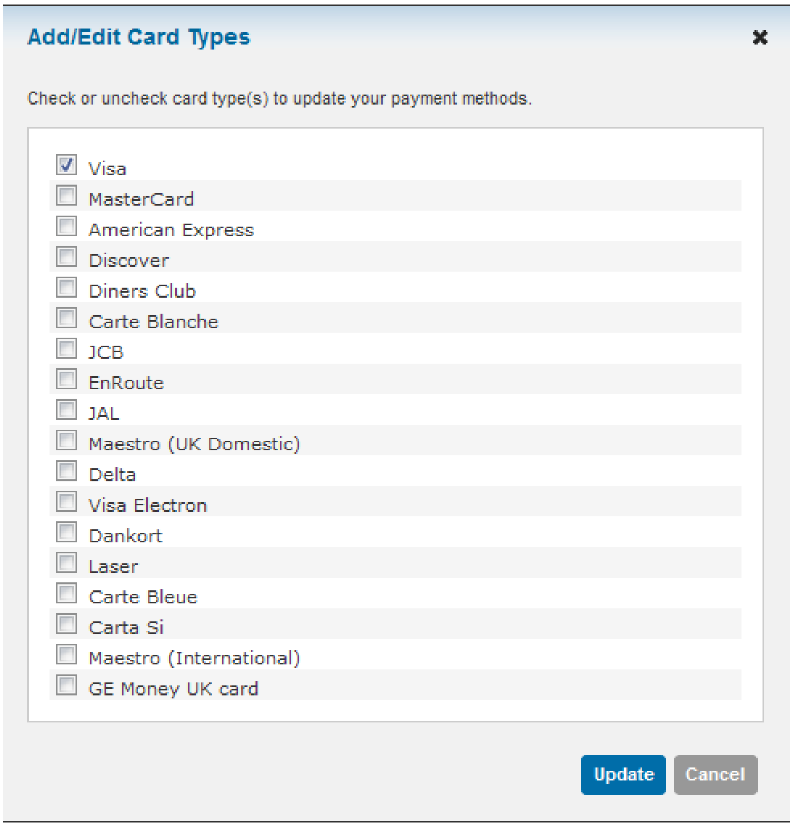
To promote a profile to active, you must select at least one payment type and a currency.

Add/Edit Card Types

Add or edit the card types that your merchant account provider has authorized. Click the edit icon to change the CVN Display, CVN Required, Payer Authentication, and Currencies settings.

Card Type	CVN Display	CVN Required	Payer Authentication	Currencies

Select the card types you wish to accept. Ensure that the card types you select are supported by your processor. Click “Update” when you have finished.

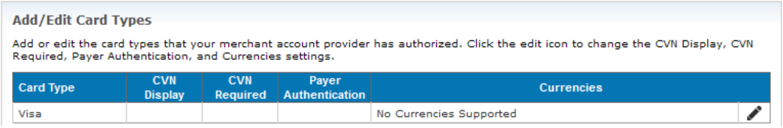


Add/Edit Card Types

Check or uncheck card type(s) to update your payment methods.

☑ Visa
□ MasterCard
□ American Express
□ Discover
□ Diners Club
□ Carte Blanche
□ JCB
□ EnRoute
□ JAL
□ Maestro (UK Domestic)
□ Delta
□ Visa Electron
□ Dankort
□ Laser
□ Carte Bleue
□ Carta Si
□ Maestro (International)
□ GE Money UK card

8. Click the “pencil” edit button to the right of each card type row.



Add/Edit Card Types

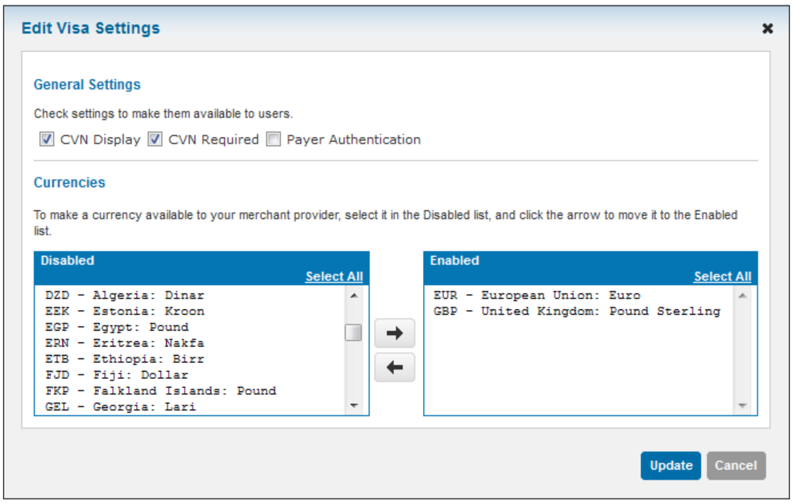
Add or edit the card types that your merchant account provider has authorized. Click the edit icon to change the CVN Display, CVN Required, Payer Authentication, and Currencies settings.

Card Type	CVN Display	CVN Required	Payer Authentication	Currencies
Visa				No Currencies Supported

9. Chose the currencies that you wish this profile to use. You can select multiple currencies by holding down the Ctrl button whilst selecting. Move them between the boxes by using the arrow buttons in the center.

   It is advised you display and require Card Verification Number (CVN) to reduce fraud. Card Scheme Payer Authentication (3DSecure) options can also be enabled here for further fraud protection.

   Click the “Update” button once complete.



Edit Visa Settings

General Settings

Check settings to make them available to users.

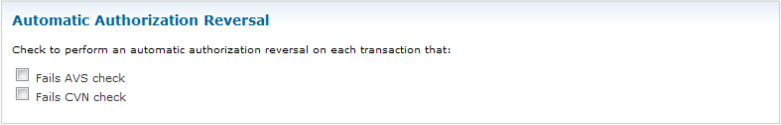
☑ CVN Display ☑ CVN Required ☐ Payer Authentication

Currencies

To make a currency available to your merchant provider, select it in the Disabled list, and click the arrow to move it to the Enabled list.

Disabled	Enabled
DZD - Algeria: Dinar	EUR - European Union: Euro
EEK - Estonia: Kroon	GBP - United Kingdom: Pound Sterling
EGP - Egypt: Pound	
ERN - Eritrea: Nakfa	
ETB - Ethiopia: Birr	
FJD - Fiji: Dollar	
FKP - Falkland Islands: Pound	
GEL - Georgia: Lari	

10. Select these boxes to release a customer’s reserved funds (perform an Authorization Reversal) in the event of the AVS (Address Verification Service) or CVN checks failing.



Automatic Authorization Reversal

Check to perform an automatic authorization reversal on each transaction that:

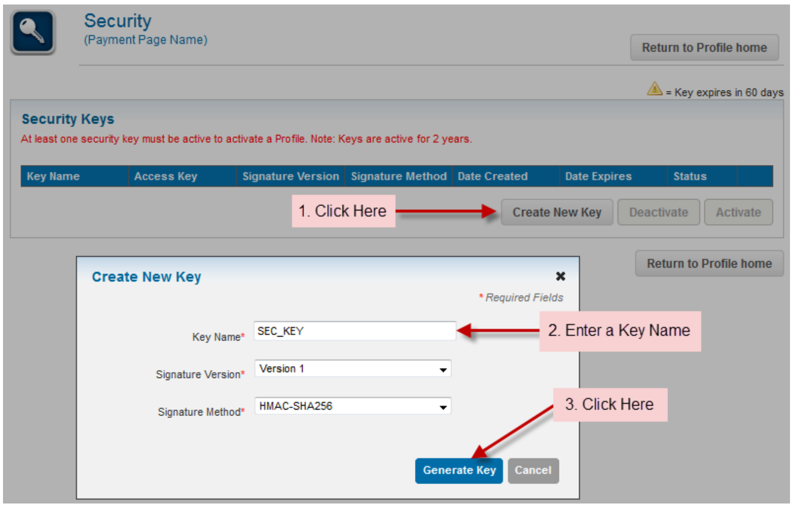
☐ Fails AVS check
☐ Fails CVN check

11. At the Profile Settings Menu, click the “Security” button.

    Click the “Create New Key” button to generate a Security Key for your Secure Acceptance profile.

    Give the New Key a name and click the “Generate Key” button.

    Note: Do not change the other settings.



Security
(Payment Page Name)

⚠ = Key expires in 60 days

Security Keys

At least one security key must be active to activate a Profile. Note: Keys are active for 2 years.

Key Name	Access Key	Signature Version	Signature Method	Date Created	Date Expires	Status

Create New Key

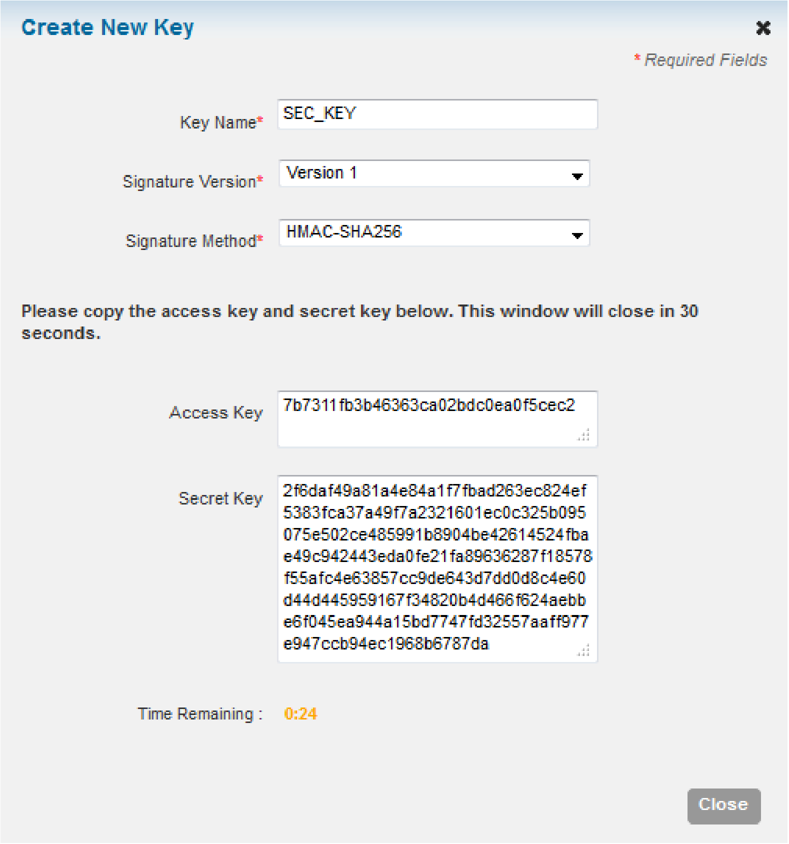
* Required Fields

Key Name* SEC_KEY

Signature Version* Version 1

Signature Method* HMAC-SHA256

12. The “Access Key” and “Secret Key” **are displayed for 30 seconds.** Copy both into a safe location for the time being; both keys will be required during implementation of the code (See Section 4.2 of this document).



Create New Key

* Required Fields

Key Name*: SEC_KEY

Signature Version*: Version 1

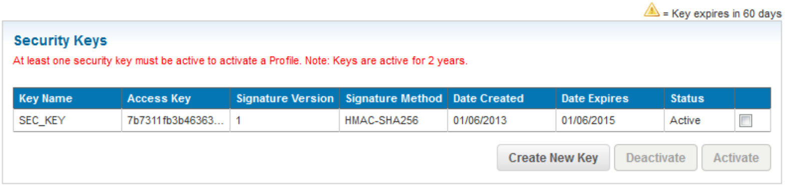
Signature Method*: HMAC-SHA256

Please copy the access key and secret key below. This window will close in 30 seconds.

Access Key: 7b7311fb3b46363ca02bdc0ea0f5cec2

Secret Key:
```
2f6daf49a81a4e84a1f7fbad263ec824ef
5383fca37a49f7a2321601ec0c325b095
075e502ce485991b8904be42614524fba
e49c942443eda0fe21fa89636287f18578
f55afc4e63857cc9de643d7dd0d8c4e60
d44d445959167f34820b4d466f624aebb
e6f045ea944a15bd7747fd32557aaff977
e947ccb94ec1968b6787da
```

Time Remaining : 0:24



⚠ = Key expires in 60 days

Security Keys

At least one security key must be active to activate a Profile. Note: Keys are active for 2 years.

Key Name	Access Key	Signature Version	Signature Method	Date Created	Date Expires	Status	
SEC_KEY	7b7311fb3b46363...	1	HMAC-SHA256	01/06/2013	01/06/2015	Active	□

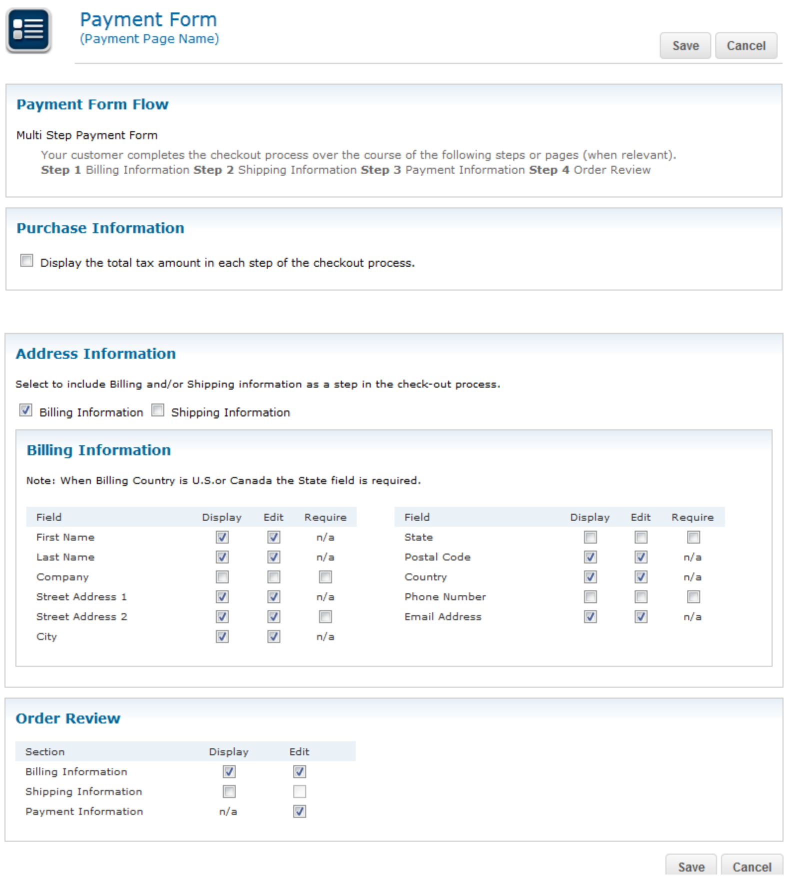
It is possible to view these keys again by clicking the key in the Security Key table.

13. At the Profile Settings Menu, click the “Payment Form” button.

The screenshot showcases the default fields to be displayed in the Secure Acceptance payment pages and can be customized to suit your needs.

Should the billing and/or shipping address be captured at an earlier stage of the order process (e.g. on the merchant’s website), these fields can be passed in hidden form fields (See Section 4.4 of this document). This allows you to shorten the checkout process, by disabling the Billing and Shopping information steps.

Click the “Save” button when complete.



Payment Form
(Payment Page Name)

Payment Form Flow

Multi Step Payment Form

Your customer completes the checkout process over the course of the following steps or pages (when relevant).
Step 1 Billing Information **Step 2** Shipping Information **Step 3** Payment Information **Step 4** Order Review

Purchase Information

□ Display the total tax amount in each step of the checkout process.

Address Information

Select to include Billing and/or Shipping information as a step in the check-out process.

☑ Billing Information □ Shipping Information

Billing Information

Note: When Billing Country is U.S.or Canada the State field is required.

Field	Display	Edit	Require	Field	Display	Edit	Require
First Name	☑	☑	n/a	State	□	□	□
Last Name	☑	☑	n/a	Postal Code	☑	☑	n/a
Company	□	□	□	Country	☑	☑	n/a
Street Address 1	☑	☑	n/a	Phone Number	□	□	□
Street Address 2	☑	☑	□	Email Address	☑	☑	n/a
City	☑	☑	n/a				

Order Review

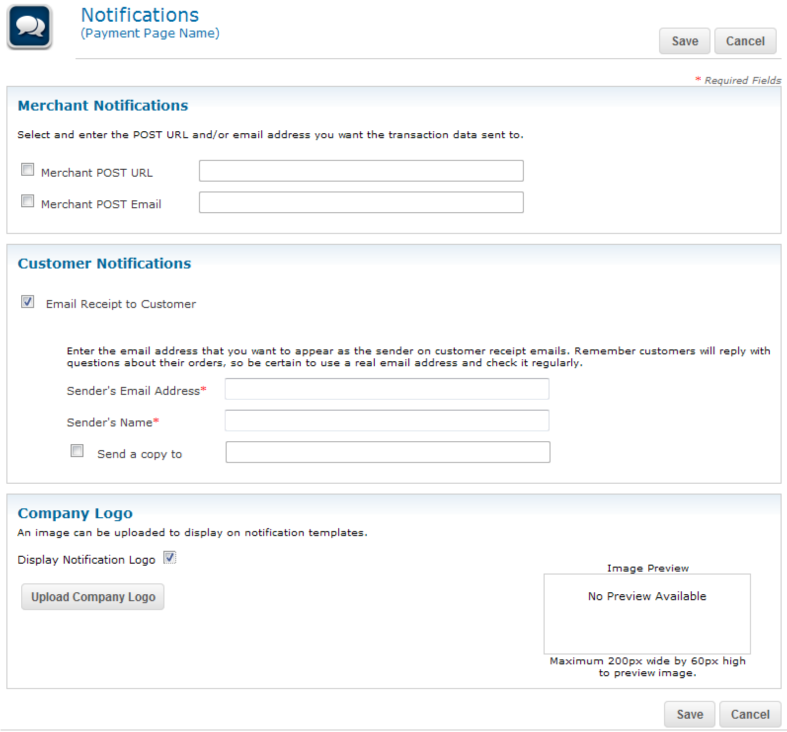
Section	Display	Edit
Billing Information	☑	☑
Shipping Information	□	□
Payment Information	n/a	☑

14. At the Profile Settings Menu, click the “Notifications” button.

    It is recommended that you implement the Merchant POST URL to directly receive notification of each transaction. You need to programmatically capture the response sent to the Merchant POST URL and store the data within your systems. This ensures the accuracy of transactions and lets you know if the transaction was successfully processed in the case of a timeout when communicating to the customer’s browser.

    Please note – For the Merchant POST URL use port 80, 443 or 8080.

    Click the “Save” button when complete.



Notifications
(Payment Page Name)

Merchant Notifications

Select and enter the POST URL and/or email address you want the transaction data sent to.

□ Merchant POST URL

□ Merchant POST Email

Customer Notifications

☑ Email Receipt to Customer

Enter the email address that you want to appear as the sender on customer receipt emails. Remember customers will reply with questions about their orders, so be certain to use a real email address and check it regularly.

Sender's Email Address*

Sender's Name*

□ Send a copy to

Company Logo

An image can be uploaded to display on notification templates.

Display Notification Logo ☑

Maximum 200px wide by 60px high to preview image.

15. At the Profile Settings Menu, click the “Response Page Views” button.

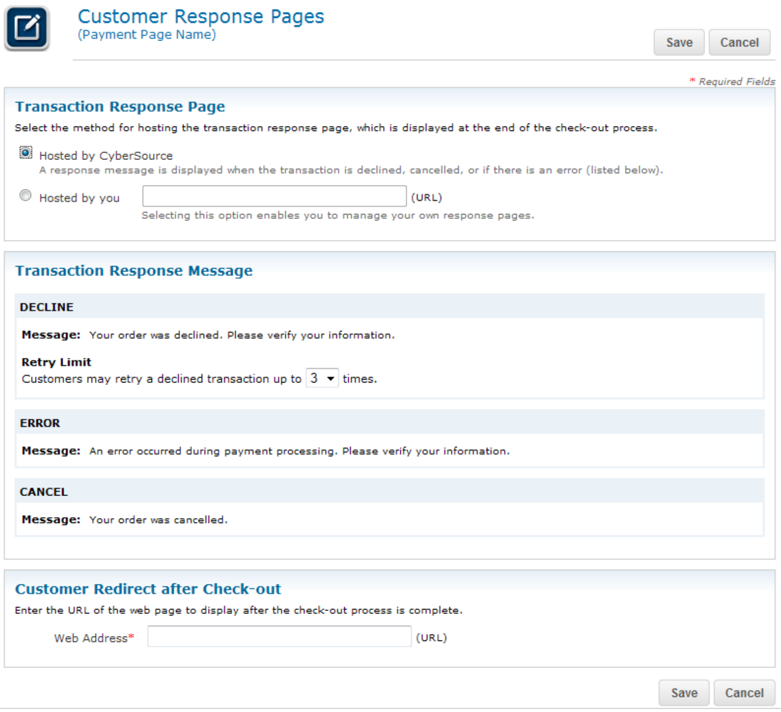
    By default, the use of CyberSource’s own response pages is selected. CyberSource recommends that you host a custom page where the responses are interpreted and displayed to the customer for the following Transaction Decisions:

    - Accept
    - Decline
    - Error
    - Cancel
    - Fraud Processing

    For the “Customer Redirect after Check-out” section please supply a fully qualified web address here e.g.

    http://www.cybersource.com/

    Click the “Save” button when complete.



Customer Response Pages
(Payment Page Name)

* Required Fields

Transaction Response Page

Select the method for hosting the transaction response page, which is displayed at the end of the check-out process.

● Hosted by CyberSource
A response message is displayed when the transaction is declined, cancelled, or if there is an error (listed below).

○ Hosted by you (URL)
Selecting this option enables you to manage your own response pages.

Transaction Response Message

DECLINE

Message: Your order was declined. Please verify your information.

Retry Limit
Customers may retry a declined transaction up to 3 times.

ERROR

Message: An error occurred during payment processing. Please verify your information.

CANCEL

Message: Your order was cancelled.

Customer Redirect after Check-out

Enter the URL of the web page to display after the check-out process is complete.

Web Address* (URL)

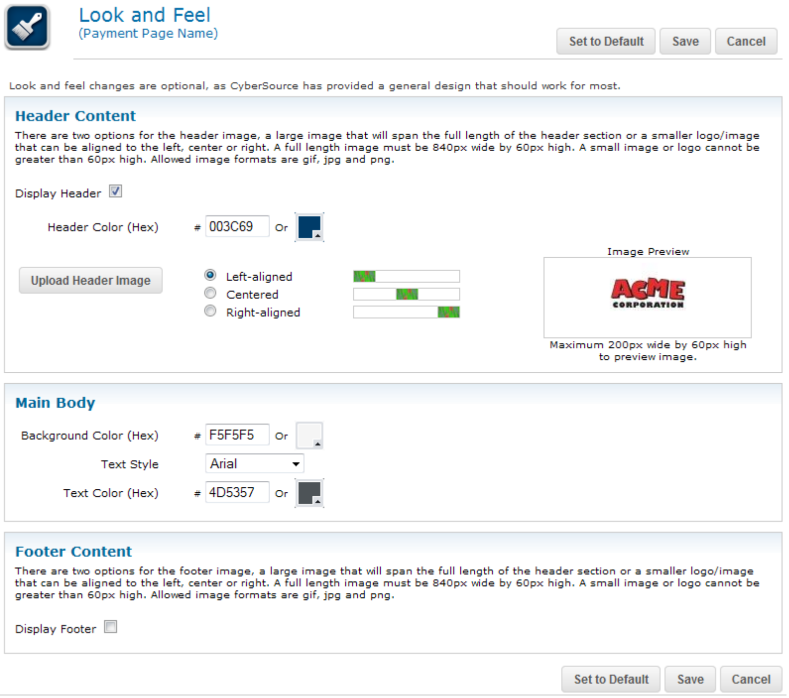
16. At the Profile Settings Menu, click the “Appearance and Branding” button.

    By default, CyberSource has pre-configured the “Header” and “Body” of the Secure Acceptance payment pages.

    You can change the colors of all sections, along with the alignment and display of your company logo in the Header and Footer section.

    To ensure correct rendering on mobile devices, a full width header logo can be no larger than 840px by 60px.

    Click the “Save” button when complete.



Look and Feel
(Payment Page Name)

Look and feel changes are optional, as CyberSource has provided a general design that should work for most.

Header Content

There are two options for the header image, a large image that will span the full length of the header section or a smaller logo/image that can be aligned to the left, center or right. A full length image must be 840px wide by 60px high. A small image or logo cannot be greater than 60px high. Allowed image formats are gif, jpg and png.

Display Header ☑

Header Color (Hex) # 003C69 Or

● Left-aligned
○ Centered
○ Right-aligned

Image Preview

Maximum 200px wide by 60px high to preview image.

Main Body

Background Color (Hex) # F5F5F5 Or

Text Style Arial

Text Color (Hex) # 4D5357 Or

Footer Content

There are two options for the footer image, a large image that will span the full length of the header section or a smaller logo/image that can be aligned to the left, center or right. A full length image must be 840px wide by 60px high. A small image or logo cannot be greater than 60px high. Allowed image formats are gif, jpg and png.

Display Footer □

17. At the Profile Settings Menu, click the “Localization” button.

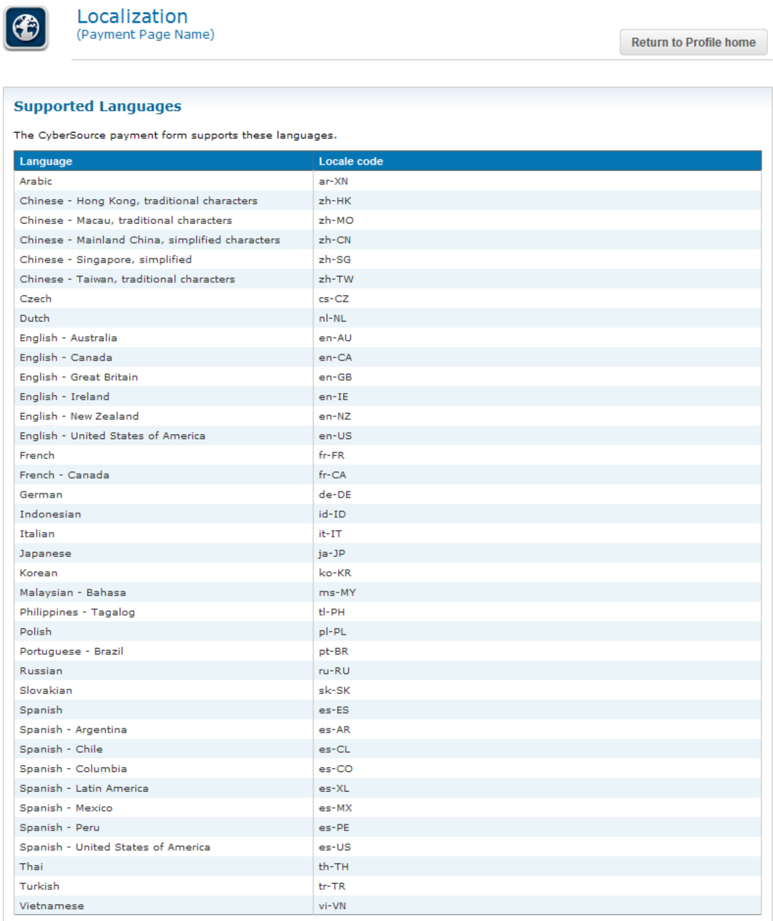
    This showcases the languages supported through Secure Acceptance Web/Mobile.

    The Locale parameter can be used within your website code to allow Secure Acceptance to display the screens and customer email receipts in the language and localization of your choosing.

    e.g.

    ```
    <input type="hidden"
    name="locale" value="en-
    us">
    ```

    Click the “Return to Profile home” button.

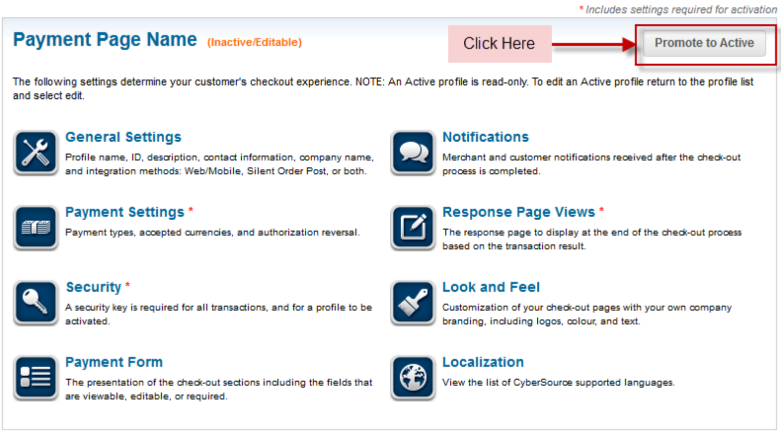


Supported Languages

The CyberSource payment form supports these languages.

Language	Locale code
Arabic	ar-XN
Chinese - Hong Kong, traditional characters	zh-HK
Chinese - Macau, traditional characters	zh-MO
Chinese - Mainland China, simplified characters	zh-CN
Chinese - Singapore, simplified	zh-SG
Chinese - Taiwan, traditional characters	zh-TW
Czech	cs-CZ
Dutch	nl-NL
English - Australia	en-AU
English - Canada	en-CA
English - Great Britain	en-GB
English - Ireland	en-IE
English - New Zealand	en-NZ
English - United States of America	en-US
French	fr-FR
French - Canada	fr-CA
German	de-DE
Indonesian	id-ID
Italian	it-IT
Japanese	ja-JP
Korean	ko-KR
Malaysian - Bahasa	ms-MY
Philippines - Tagalog	tl-PH
Polish	pl-PL
Portuguese - Brazil	pt-BR
Russian	ru-RU
Slovakian	sk-SK
Spanish	es-ES
Spanish - Argentina	es-AR
Spanish - Chile	es-CL
Spanish - Columbia	es-CO
Spanish - Latin America	es-XL
Spanish - Mexico	es-MX
Spanish - Peru	es-PE
Spanish - United States of America	es-US
Thai	th-TH
Turkish	tr-TR
Vietnamese	vi-VN

18. At the Profile Settings Menu, once all settings have been configured to your requirements, click the “Promote to Active” button.



* Includes settings required for activation

Payment Page Name (Inactive/Editable)

The following settings determine your customer's checkout experience. NOTE: An Active profile is read-only. To edit an Active profile return to the profile list and select edit.

General Settings
Profile name, ID, description, contact information, company name, and integration methods: Web/Mobile, Silent Order Post, or both.

Notifications
Merchant and customer notifications received after the check-out process is completed.

Payment Settings *
Payment types, accepted currencies, and authorization reversal.

Response Page Views *
The response page to display at the end of the check-out process based on the transaction result.

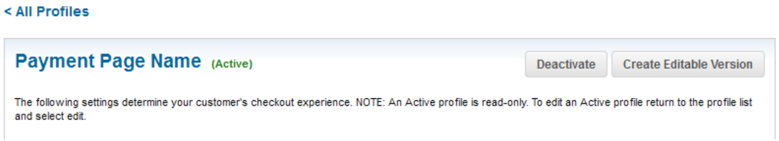
Security *
A security key is required for all transactions, and for a profile to be activated.

Look and Feel
Customization of your check-out pages with your own company branding, including logos, colour, and text.

Payment Form
The presentation of the check-out sections including the fields that are viewable, editable, or required.

Localization
View the list of CyberSource supported languages.

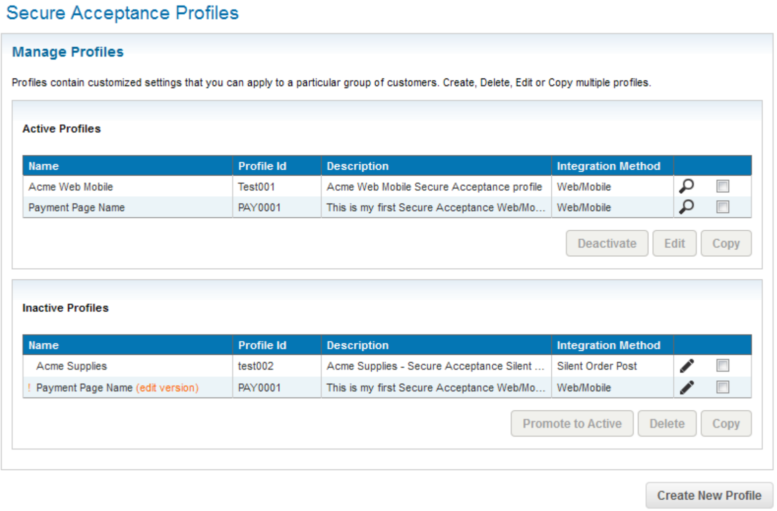
The profile can be deactivated. If you deactivate the profile it will make the Secure Acceptance Web/Mobile forms unavailable on your website.



Payment Page Name (Active)

The following settings determine your customer's checkout experience. NOTE: An Active profile is read-only. To edit an Active profile return to the profile list and select edit.

A Profile can be made editable. The original profile is still available on your website while you edit a copy. When you are finished editing you can “promote to active”. This will overwrite the original. In this way you can seamlessly update your website with no downtime.



Secure Acceptance Profiles

Manage Profiles

Profiles contain customized settings that you can apply to a particular group of customers. Create, Delete, Edit or Copy multiple profiles.

Active Profiles

Name	Profile Id	Description	Integration Method		
Acme Web Mobile	Test001	Acme Web Mobile Secure Acceptance profile	Web/Mobile	🔍	□
Payment Page Name	PAY0001	This is my first Secure Acceptance Web/Mo...	Web/Mobile	🔍	□

Inactive Profiles

Name	Profile Id	Description	Integration Method		
Acme Supplies	test002	Acme Supplies - Secure Acceptance Silent ...	Silent Order Post	✎	□
! Payment Page Name (edit version)	PAY0001	This is my first Secure Acceptance Web/Mo...	Web/Mobile	✎	□

4.2. Development of Secure Acceptance

Secure Acceptance Web/Mobile can be implemented very quickly by using and modifying the sample scripts provided by CyberSource (section 2.2 above). If you are migrating from our legacy Hosted Order Page or Silent Order Post, it is recommended you implement the sample code first to gain an understanding of how it works.

Each example is provided with the following files:

- Security script
- Payment form
- Payment confirmation page
- Receipt page

4.2.1. Modifying the Security Script

The security script needs to be modified to include the Secret Key generated at point 12 of Section 4.1 of this document. In the PHP example, this will look something like:

```
define ('SECRET_KEY', '
2f6daf49a81a4e84a1f7fbad263ec824ef5383fca37a49f7a2321601ec0c32
5b095075e502ce485991b8904be42614524fbae49c942443eda0fe21fa8963
6287f18578f55afc4e63857cc9de643d7dd0d8c4e60d44d445959167f34820
b4d466f624aebbe6f045ea944a15bd7747fd32557aaff977e947ccb94ec196
8b6787da');
```

4.2.2. Modifying the Payment Form

The payment form represents the payment information section of an e-Commerce site. In the sample code for Secure Acceptance some fields are shown that you may wish to hide from the view of a customer and pass through in the POST message.

In the PHP example, the minimum that needs to be changed are the Access Key and Profile ID (as generated/created in Section 4.1 of this document):

```
<input type="hidden" name="access_key" value="
7b7311fb3b46363ca02bdc0ea0f5cec2">

<input type="hidden" name="profile_id" value="PAY0001">
```

4.2.3. Modifying the Payment Confirmation Page

The payment confirmation page represents the review of the payment, and the order information prior to proceeding with making a payment. In the sample code for Secure Acceptance all fields and data are shown prior to the POST message being made to CyberSource.

In the PHP example, the minimum that needs to be changed is the POST form URL for either TEST or PRODUCTION:

TEST

```
<form
```

```
action="https://testsecureacceptance.cybersource.com/pay"
method="post"/>
```

PRODUCTION

```
<form action="https://secureacceptance.cybersource.com/pay"
method="post"/>
```

4.3. CyberSource Decision Manager Device Fingerprinting

To successfully implement Device Fingerprinting, an invisible 1-pixel image file and two scripts need to be placed in the <body> tag your checkout page (the page prior to directing the customer to Secure Acceptance) at the top of the main body. This ensures a 3-5 second window in which the code segments can complete the data collection necessary to create a fingerprint for the device making the order.

Below are the code segments for implementing Device Fingerprinting:

PNG Image

<p style="background:url(https://h.online-metrix.net/fp/clear.png?org_id=***<org ID>***&amp;session_id=***<merchant id><session ID>***&amp;m=1)"></p> <img src="https://h.online-metrix.net/fp/clear.png?org_id=***<org ID>***&amp;session_ id=***<merchant id><session ID>***&amp;m=2" alt="">

Flash Code

<object type="application/x-shockwave-flash" data="https://h.online-metrix.net/fp/ fp.swf?org_id=***<org ID>***&amp;session_id=***<merchant id><session ID>***" width="1" height="1" id="thm_fp"> <param name="movie" value="https://h.online-metrix.net/fp/fp.swf?org_id=***<org ID>***&amp;session_id=***<merchant id><session ID>***" /> <div></div> </object>

JavaScript Code

<script src="https://h.online-metrix.net/fp/check.js?org_id=***<org ID>***&amp;session_ id=***<merchant id><session ID>***" type="text/javascript"> </script>

The following attributes need to be placed within the italic bold sections of the above code segments:

- Domain:
  - Testing – Use *h.online-metrix.net*, which is the DNS name of the fingerprint server as shown in the sample HTML tags above.
  - Production – Change the domain name to a local URL, and configure your Web server to redirect the URL to *h.online-metrix.net*
- <org ID>:

Test Ord ID:	**1snn5n9w**
Live Ord ID:	k8vif92e

- <merchant ID>: Merchants unique CyberSource merchant ID
- < session ID>: The session ID is a string variable (letters and numbers only) that must be unique for each merchant ID. Merchants can use any string that they are already generating, such as an order number or Web session ID. However, **do not use** the same uppercase and lowercase letters to indicate different session IDs.

4.4. Mandatory & Optional Fields

Below is a full list of Mandatory and Optional fields required for payments processing and fraud screening with CyberSource/Professional Services. This list of fields can be found in the Secure Acceptance Web/Mobile User's Guide (Section: API Fields).

Field Name	Description	Required or Optional	Data Type (Length)	Legacy HOP/SOP Field Name
access_key	Authentication with Secure Acceptance	R	String (32)	**n/a**
amount	Total amount for the order. Must be greater than or equal to zero. If line item quantity and prices are provided, this must equal the total amount of each line item multiplied by the line item quantity	R	String (15)	**amount**
currency	Currency used for the order (ISO Currency Codes)	R	String (5)	**currency**
locale	Indicates the language to use for customer-facing content	R	String (5)	**n/a**
profile_id	Identifies the profile to use with each transaction	R	String (7)	**n/a**
reference_number	Unique merchant-generated order reference or tracking number for each transaction	R	String (60)	**orderNumber**
signature	Merchant-generated Base64 signature. This is generated using the signing method for the access_key field supplied.			**n/a**
signed_date_time	The date and time that the signature was generated. Must be in UTC Date & Time format. This field is used to check for duplicate transaction attempts.	R	String (20)	**n/a**

signed_field_names	A comma-separated list of request fields that are signed. This field is used to generate a signature that is used to verify the content of the transaction to protect it from tampering. **Important** CyberSource recommends signing all request API fields except the signature field.	R	Variable	**n/a**
transaction_type	The type of transaction: - authorization - sale - authorization, create_payment_token	R	String (60)	**orderPage_transactionType**
transaction_uuid	Unique merchant-generated identifier. Include with the access_key field for each transaction. This identifier must be unique for each transaction. This field is used to check for duplicate transaction attempts.	R	String (50)	**n/a**
unsigned_field_names	A comma-separated list of request fields that are not signed.	R	Variable	**n/a**
bill_to_address_city	City in the billing address	O	String (50)	**billTo_city**
bill_to_address_country	Country code for the billing address (ISO Country Codes)	O	String (2)	**billTo_country**
bill_to_address_line1	First line of the billing address	O	String (60)	**billTo_street1**
bill_to_address_line2	Second line of the billing address	O	String (60)	**billTo_street2**
bill_to_address_postal_code	Postal code for the billing address	O	String (10)	**billTo_postalCode**
bill_to_address_state	State or province in the billing address (ISO State & Province Code)	O	String (2)	**billTo_state**
bill_to_company_name	Name of the customer's company.	O	String(40)	**billTo_company**
bill_to_email	Customer's email address, including the full domain name	O	String (255)	**billTo_email**
bill_to_forename	Customer's first name. This name must be the same as the name on the card	O	String (60)	**billTo_firstName**

bill_to_phone	Customer’s phone number	O	String (15)	**billTo_phoneNumber**
bill_to_surname	Customer’s last name. This name must be the same as the name on the card	O	String (60)	**billTo_lastName**
card_cvn	Card verification number	O	String (4)	**card_cvNumber**
card_expiry_date	Card expiration date. Format: MM-YYYY	O	String (7)	**n/a**
card_number	Card number	O	String (20)	**card_accountNumber**
card_type	Type of card to authorize. Use one of these values: - 001: Visa - 002: MasterCard - 003: American Express - 004: Discover - 005: Diners Club - 006: Carte Blanche - 007: JCB - 014: EnRoute - 021: JAL - 024: Maestro (UK Domestic) - 031: Delta - 033: Visa Electron - 034: Dankort - 035: Laser - 036: Carte Bleue - 037: Carta Si - 042: Maestro (International) - 043: GE Money UK card	O	String (3)	**card_cardType**
complete_route	Concatenation of individual travel legs in the format for example: SFO-JFK:JFK-LHR:LHR-CDG. For a complete list of airport codes, see IATA’s City Code Directory.	O	String(255)	**decisionManager_travelData_completeRoute**

consumer_id	Identifier for the customer's account. This field is defined when you create a subscription.	O	String (50)	**billTo_customerID**
customer_cookies_accepted	Indicates whether the customer's browser accepts cookies. This field can contain one of the following values: - true: customer's browser accepts cookies. - false: customer's browser does not accept cookies	O	String(5)	**billTo_httpBrowserCookiesAccepted**
customer_gift_wrap	Indicates whether the customer requested gift wrapping for this purchase. This field can contain one of the following values: - true: customer requested gift wrapping. - false: customer did not request gift wrapping.	O	String(5)	**invoiceHeader_isGift**
customer_ip_address	Customer's IP address reported by your web server via socket information.	O	String (15)	**billTo_ipAddress**
date_of_birth	Date of birth of the customer. Use the format: YYYYMMDD.	O	String (8)	**billTo_dateOfBirth**
departure_time	Departure data and time of the first leg of the trip. Use one of the following formats: - yyyy-MM-dd HH:mm z - yyyy-MM-dd hh:mm a z - yyyy-MM-dd hh:mma z HH = 24-hour format hh = 12-hour format a = am or pm (case insensitive) z = time zone of the departing flight, for example: If the airline is based in city A, but the flight departs from city B, z is the time zone of city B at the time of departure.	O	DateTime(25)	**decisionManager_travelData_departureDateTime**

device_fingerprint_id	Field that contains the session ID for the fingerprint. The string can contain uppercase and lowercase letters, digits, and these special characters: hyphen (-) and underscore (_). However, do not use the same uppercase and lowercase letters to indicate different session IDs. The session ID must be unique for each merchant ID. You can use any string that you are already generating, such as an order number or web session ID.	O	String (88)	**deviceFingerprintID**
ignore_avs	Ignore the results of AVS verification. Possible values: - true - false **Important** To prevent data tampering, CyberSource recommends signing this field.	O	String (5)	**orderPage_ignoreAVS**
ignore_cvn	Ignore the results of CVN verification. Possible values: - true - false **Important** To prevent data tampering, CyberSource recommends signing this field.	O	String (5)	**orderPage_ignoreCVN**

item_#_code	Type of product. If it is supplied, the item code must be one of the following values: - default - adult_content - coupon - electronic_good - electronic_software - gift_certificate - service - subscription - handling_only - service - shipping_and_handling - shipping_only - subscription # is the range of 0-49	O		**item_#_productCode**
item_#_name	Name of the item. # can range from 0-49	O	String (255)	**item_#_productName**
item_#_quantity	Quantity of line items. # can range from 0-49	O	String (10)	**item_#_quantity**
item_#_sku	Identification code for the product. # can range from 0-49	O	String (255)	**item_#_productSKU**
item_#_tax_amount	Tax amount to apply to the line item. # can range from 1- 49. This value cannot be negative. The tax amount and the offer amount must be in the same currency.	O	String (15)	**item_#_taxAmount**
item_#_unit_price	Price of the line item. # can range from 0-49	O	String (15)	**item_#_unitPrice**
journey_leg#_dest	Airport code for the origin of the leg of the trip designated by the pound (#) symbol in the field name. A maximum of 30 legs can be included in the request. This code is usually three digits long, for example: SFO = San Francisco. Do not use the colon (:) or the hyphen (-). For a complete list of airport codes, see IATA's City Code Directory.	O	String(3)	**decisionManager_travelData_legList (destination)**
journey_leg#_orig	Airport code for the origin of the leg of the trip designated by the pound (#) symbol in the field name. A maximum of 30 legs can be included in the request. This code is usually three digits long, for example: SFO = San Francisco. Do not use the colon (:) or the hyphen (-). For a complete list of airport codes, see IATA's City Code Directory.	O	String(3)	**decisionManager_travelData_leg#_orig**

journey_type	Type of travel, such as: one way or round trip.	O	String(32)	**decisionManager_travelData_journeyType**
line_item_count	Total number of line items. Maximum number is 50	O	String (2)	**lineItemCount**
merchant_defined_data#	Fields that you can use to store your business information. N.B. It must not be used for personally identifying information.	O	String(100)	**merchantDefinedData#**
merchant_secure_data1 **merchant_secure_data2** **merchant_secure_data3**	Optional fields that you can use to store information. CyberSource encrypts the data before storing it in the database.	O	String (100)	**n/a**
merchant_secure_data4	Optional field that you can use to store information. CyberSource encrypts the data before storing it in the database.	O	String (2000)	**n/a**
override_custom_receipt_page	Overrides the custom receipt profile setting with your own URL. Important To prevent data tampering CyberSource recommends signing this field.	O	String (255)	**orderPage_receiptResponseURL**
payment_method	Method of payment: card	O	String (30)	**paymentOption**
payment_token	Identifier for the payment details. The payment token retrieves the card data, billing information, and shipping information from the CyberSource database. When this field is included in the request, the card data, and billing and shipping information are optional. Important You must be currently using CyberSource Payment Tokenization services. Populate this field with the customer subscription ID.	O	String (26)	**paySubscriptionCreateReply_subscriptionID**
payment_token_comments	Optional comments you have for the customer subscription.	O	String (255)	**comments**
payment_token_title	Name or title for the customer subscription.	O	String (60)	**subscription_title**
recurring_amount	Payment amount for each installment or recurring subscription payment.	O	String (15)	**recurringSubscriptionInfo_amount**
recurring_frequency	Frequency of payments for an installment or recurring subscription.	O	String (20)	**recurringSubscriptionInfo_frequency**

recurring_start_date	First payment date for an installment or recurring subscription payment. Date must use the format YYYYMMDD. If a date in the past is supplied the start date will default to the day after the date was entered.	O	String (8)	**recurringSubscriptionInfo_startDate**
recurring_number_of_installments	Total number of payments set up for an installment subscription. # can range from 1-156.	O	String (3)	**recurringSubscriptionInfo_numberOfPayments**
returns_accepted	Indicates whether product returns are accepted. This field can contain one of the following values: - true - false	O	String (5)	
ship_to_address_city	City of shipping address	O	String (50)	**shipTo_city**
ship_to_address_country	Country code for the shipping address (ISO Country Codes)	O	String (2)	**shipTo_country**
ship_to_address_line1	First line of shipping address	O	String (60)	**shipTo_street1**
ship_to_address_line2	Second line of shipping address	O	String(60)	**shipTo_street2**
ship_to_address_postal_code	Postal code for the shipping address	O	String (10)	**shipTo_postalCode**
ship_to_address_state	State or province of shipping address (ISO State & Province Code)	O	String (2)	**shipTo_state**
ship_to_company_name	Name of the company receiving the product.	O	String (40)	**shipTo_company**
ship_to_forename	First name of the person receiving shipment	O	String (60)	**shipTo_firstName**
ship_to_phone	Phone number of the shipping address	O	String (15)	**shipTo_phoneNumber**
ship_to_surname	Last name of the person receiving the shipment	O	String (60)	**shipTo_lastName**

shipping_method	Shipping method for the product. Possible values: - sameday: Courier or same-day service - oneday: Next day or overnight service - twoday: Two-day service - threeday: Three-day service - lowcost: Lowest-cost service - pickup: Store pick-up - other: Other shipping method - none: No shipping method because	O	String (10)	**shipTo_shippingMethod**
skip_decision_manager	Indicates whether to skip Decision Manager when creating a subscription. This field can contain one of the following values: - true - false	O	String (5)	**n/a**
tax_amount	Total tax amount to apply to the order. This value cannot be negative. Important To prevent data tampering CyberSource recommends signing this field.	O	String (15)	**taxAmount**

5. Testing

5.1. How to Test Secure Acceptance

It is recommended to test the implementation of the Secure Acceptance extensively; here are the details that can be used for testing:

- Card Type – 001
- Credit Card Number – 4111111111111111
- Expiration Date – anything beyond the current month/year
- First Name – noreal
- Last Name – name
- Street 1 – 1295 Charleston Road
- City – Mountain View
- State - CA
- Postal Code – 94043
- Country – US
- Email – null@cybersource.com

CyberSource recommends that all facets of the implementation be tested including any additional CyberSource services such as:

- Payer Authentication – (3D Secure, Verified by Visa, Mastercard SecureCode, AMEX SafeKey)
- Decision Manager – CyberSource's Fraud Tool
- Tokenization – The ability to store card data on your systems securely
- Recurring Billing – The ability to schedule recurring and/or installment payments

6. Go-Live Procedure

6.1. How to Request a Go-Live

When you are ready to implement Secure Acceptance in your live environment, you will need to request Go-Live through CyberSource Support.

Please note that Go-Live requests take **three working days** to action once all relevant banking information has been received, and no Go-Live will take place on Fridays.

It is recommended that you submit all banking information and integration services required to CyberSource at least one month in advance of Go-Live.

6.2. Testing in Production

CyberSource recommends testing the implementation of Secure Acceptance in the production environment prior to fully releasing it to the general public.

In order to do this, the merchant will be required to use a **real valid card** with the associated billing details to the card. The merchant will then be able to verify the implementation and reverse the charge or refund through the CyberSource Enterprise Business Centre.

No dummy or test data can be used to perform tests in production

7. Additional Information and Documentation

CyberSource Business Center	Test - https://ebctest.cybersource.com Live – https://ebc.cybersource.com
CyberSource Account Registration	http://www.cybersource.com/register
CyberSource Support Center/Knowledgebase	https://support.cybersource.com
Secure Acceptance Web/Mobile User's Guide	Secure_Acceptance_WM.pdf
Secure Acceptance – Test Harness	https://emea-ps-hosted.cybshosting.com/SATestHarness/
Enterprise Business Centre Overview	EBC_Overview.pdf
Business Centre Tutorial	Business Centre Tutorial.html
PCI DSS 2.0 eCommerce Guidelines	PCI DSS 2.0 eCommerce Guidelines