CyberSource Secure Acceptance Web/Mobile

Configuration Guide

September 2014

CyberSource®

the power of payment

CyberSource Contact Information

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

For sales questions about any CyberSource Service, email sales@cybersource.com or
call 650-432-7350 or 888-330-2300 (toll free in the United States).

For support information about any CyberSource Service, visit the Support Center at
http://www.cybersource.com/support.

Copyright

Restricted Rights Legends

Trademarks

Contents

Recent Revisions to This Document

Release	Changes
September 2014	■ Updated the "Endpoints and Transactions Types" section. See page 40. ■ Updated the description for the **profile_id** field. See page 91.
July 2014	■ Updated a note to the "Customizing the Total Amount" section. See page 34. ■ Added a note to the "iFrame Implementation" section. See page 115.
June 2014	This revision contains only editorial changes and no technical updates.
May 2014	■ Updated the "Secure Acceptance Transaction Flow" section. See page 13. ■ Added the Used By column to the request API fields table. See page 75.
April 2014	■ Added "Custom Email Receipt" section. See page 29. ■ Added the "iFrame Implementation" appendix. See page 115.
March 2014	■ Updated the "Audience" section. See page 8. ■ Updated the "Related Documents" section. See page 9. ■ Added the "Secure Acceptance Transaction Flow" section. See page 13. ■ Added the "Level II and Level III Data" section. See page 16. ■ Added the "Go-Live with Secure Acceptance" section. See page 16. ■ Updated the "Reason Codes" table. See Table 6 on page 109.

About This Guide

Audience and Purpose

This guide is written for merchants who want to accept payments on a secure checkout hosted by CyberSource but who don't want to handle or store sensitive payment information on their own servers.

Using Secure Acceptance Web/Mobile requires minimal scripting skills. You must create a security script and modify your HTML form to invoke Secure Acceptance. You will also use the Business Center to review and manage orders. Your web site must meet the following requirements:

- Have shopping-cart or customer order creation software.
- Contain product pages in one of the supported scripting languages (see page 39).
- The IT infrastructure must be Public Key Infrastructure (PKI) enabled to use SSL-based form POST submissions.
- The IT infrastructure must be able to digitally sign customer data prior to submission to Secure Acceptance Web/Mobile.

Conventions

Note, Important, and Warning Statements

A *Note* contains helpful suggestions or references to material not contained in the document.

Note

	An *Important* statement contains information essential to successfully completing a task or learning a concept.
Important	

	A *Warning* contains information or instructions, which, if not heeded, can result in a security risk, irreversible loss of data, or significant cost in time or revenue or both.
Warning	

Text and Command Conventions

Convention	Usage
bold	■ Field and service names in text; for example: Include the **transaction_type** field.
	■ Items that you are instructed to act upon; for example: Click **Save**.
monospace	■ Code examples and samples.
	■ Text that you enter in an API environment; for example: Set the **transaction_type** field to create_payment_ token.

Related Documents

Refer to the Support Center for complete CyberSource technical documentation:

http://www.cybersource.com/support_center/support_documentation

Credit Card

The following documents describe how to integrate credit card processing into their order management system:

■ *Credit Card Services Using the SCMP API* (PDF | HTML)

■ *Credit Card Services Using the Simple Order API* (PDF | HTML)

Decision Manager

The following documents describe how to integrate and use the Decision Manager services:

- *Decision Manager Developer Guide Using the SCMP API* (PDF | HTML)
- *Decision Manager Developer Guide Using the Simple Order API* (PDF | HTML)

eCheck

The following documents describe how to integrate and use the eCheck services:

- *Electronic Check Services Using the SCMP API* (PDF | HTML)
- *Electronic Check Services Using the Simple Order API* (PDF | HTML)

Level II and Level III

Level II and Level III Processing Using Secure Acceptance (PDF | HTML)—describes each Level II and Level III API field and processing Level II and Level III transactions using Secure Acceptance.

Payer Authentication

The following documents describe how to integrate and use the payer authentication services:

- *Payer Authentication Using the SCMP API* (PDF | HTML)
- *Payer Authentication Using the Simple Order API* (PDF | HTML)

Payment Tokenization

The following documents describe how to create customer profiles and use payment tokens for on-demand payments:

- *Payment Tokenization Using the Business Center* (PDF | HTML)
- *Payment Tokenization Using the SCMP API* (PDF | HTML)
- *Payment Tokenization Using the Simple Order API* (PDF | HTML)

Recurring Billing

The following documents describe how to create customer subscriptions and use payment tokens for recurring and installment payments:

- *Recurring Billing Using the Business Center* (PDF | HTML)
- *Recurring Billing Using the SCMP API* (PDF | HTML)
- *Recurring Billing Using the Simple Order API* (PDF | HTML)

Reporting

Reporting Developer Guide (PDF | HTML)—describes how to view and configure Business Center reports.

Secure Acceptance

Secure Acceptance Silent Order POST Development Guide (PDF | HTML).

Payment Security Standards

Payment Card Industry Data Security Standard (PCI DSS)—web site offers standards and supporting materials to enhance payment card data security.

Customer Support

For support information about any CyberSource service, visit the Support Center:

http://www.cybersource.com/support

Using Secure Acceptance Web/Mobile

CyberSource Secure Acceptance Web/Mobile is your secure hosted customer checkout experience. It consists of securely managed payment forms or as a single page payment form for processing transactions, enabling you to decrease your Payment Card Industry Data Security Standard (PCI DSS) obligations and thereby reducing any risks associated with handling or storing sensitive payment information. You, the merchant, out-source payments to Secure Acceptance, which is designed to accept card payments. To create your customer's Secure Acceptance experience, you take these steps:

1 Create and configure Secure Acceptance profiles.

2 Update the code on your web site to invoke Secure Acceptance and immediately process card transactions (see "Rendering Secure Acceptance Web/Mobile," page 39). Sensitive card data bypasses your network and is accepted by Secure Acceptance directly from the customer. CyberSource processes the transaction on your behalf by sending an approval request to your payment processor in real time. See "Secure Acceptance Transaction Flow," page 13.

3 Use the reply information to display an appropriate transaction response page to the customer. You can view and manage all orders in the Business Center (see page 73).

Profile
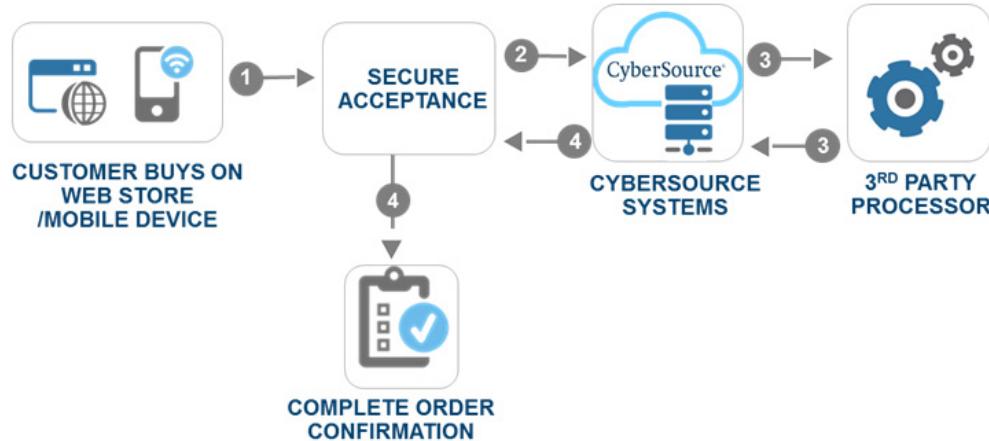
A Secure Acceptance profile consists of settings that you configure to create a customer checkout experience. You can create and edit multiple profiles, each offering a custom checkout experience (see page 33). For example, you might need multiple profiles for localized branding of your web sites. You can display a multi-step checkout process or a single page checkout (see page 23) to the customer as well as configure the appearance and branding, payment options, languages, and customer notifications.

Secure Acceptance Transaction Flow

The Secure Acceptance Web/Mobile transaction flow is illustrated in Figure 1 and described below.

Figure 1   Secure Acceptance Web/Mobile Transaction Flow

1   The customer clicks the Pay button on your payment form, which includes the Secure Acceptance request message, the signature, and the signed data fields. The customer browser interprets the code and renders the Secure Acceptance Web/Mobile checkout.

2   The customer enters and submits payment details (the unsigned data fields) and/or billing and shipping information. The transaction request message, the signature, and the signed and unsigned data fields are sent directly to the CyberSource servers. CyberSource reviews and validates the transaction request data to confirm that it has not been tampered with and that it contains valid authentication credentials.

3   CyberSource sends a transaction request for approval in real time to your payment processor. When the payment is approved, CyberSource processes the transaction and creates and signs the reply message. The HTTPS POST data contains the transaction result in addition to the masked payment data that was collected outside of your domain.

4   The HTTPS POST data can be used to display the appropriate message to the customer on whether the transaction was successful or not. You can configure your own customer response pages or you can use the default CyberSource hosted customer response pages. See page 29.

When the order is processed, it can be viewed in the Business Center (see page 69). If the transaction type was sale, it is immediately submitted for settlement. If the transaction type was authorization, you must submit a separate request for settlement such as when goods are shipped.

Payment Tokens

⚠ Important	Contact CyberSource Customer Support to activate your merchant account for the use of the payment tokenization services. You cannot use payment tokenization services until your account is activated and you have enabled payment tokenization for Secure Acceptance (see page 17).

Payment tokens are unique identifiers that replace sensitive card information and that cannot be mathematically reversed. CyberSource securely stores all the card information, replacing it with the payment token. The token is also known as a *subscription ID*, which you store on your server. The payment tokenization solution is compatible with the Visa and MasterCard Account Updater service. All payment information stored with CyberSource is automatically updated by participating banks, thereby reducing payment failures. See the *Account Updater User Guide*.

The payment token identifies the card and retrieves the associated billing, shipping, and card information. No sensitive card information is stored on your servers, thereby reducing your PCI DSS obligations.

Table 1 Types of Payment Tokens

Type	Description
22 digit	The default payment token.
16 digit	Displays the last 4 digits of the primary account number (PAN) and passes Luhn mod-10 checks.
16 digit	Displays *99* as the two leading digits and passes Luhn mod-10 checks. If your business rules prohibit using 99 as the leading digits, you must modify your system to accept the other 16-digit payment token.

Note	When you include the payment token, the billing, shipping, and card information is displayed on the Order Review page of Secure Acceptance.

one-click Checkout

With *one-click Checkout*, customers can buy products with a single click. Secure Acceptance is integrated to CyberSource Tokenization, so returning customers are not required to enter their payment details. Before a customer can use one-click Checkout, he or she must create a payment token during the first transaction on the merchant web site. See page 44. The payment token is an identifier for the payment details; therefore, no further purchases require that you enter any information. When the payment token is included in a payment request, it retrieves the card, billing, and shipping information related to the original payment request from the CyberSource database.

To use one-click Checkout, you must include the one-click Checkout endpoint to process the transaction. See page 61.

Subscription Payments

A customer subscription contains information that you store in the CyberSource database and use for future billing. At any time, you can send a request to bill the customer for an amount you specify, and CyberSource uses the payment token to retrieve the card, billing, and shipping information to process the transaction. You can also view the customer subscription in the CyberSource Business Center. See "Viewing Transactions in the Business Center," page 69.

A customer subscription includes:

- Customer contact information, such as billing and shipping information.
- Customer payment information, such as card type, masked account number, and expiration date.
- Customer order information, such as the transaction reference number and merchant-defined data fields.

Type of Subscription	Description
Recurring	A recurring billing service with no specific end date. You must specify the amount and frequency of each payment and the start date for processing the payments. CyberSource creates a schedule based on this information and automatically bills the customer according to the schedule. For example, you can offer an online service that the customer subscribes to and can charge a monthly fee for this service. See "Payment Token for Recurring Payments," page 48.

Type of Subscription	Description
Installment	A recurring billing service with a fixed number of scheduled payments. You must specify the number of payments, the amount and frequency of each payment, and the start date for processing the payments. CyberSource creates a schedule based on this information and automatically bills the customer according to the schedule. For example, you can offer a product for 75.00 and let the customer pay in three installments of 25.00. See "Payment Token for Installment Payments," page 50.

Level II and III Data

Secure Acceptance supports Level II and III data. Level II cards, also know as *Type II cards*, provide customers with additional information on their credit card statements. Business/corporate cards along with purchase/procurement cards are considered Level II cards.

Level III data can be provided for purchase cards, which are credit cards used by employees to make purchases for their company. You provide additional detailed information—the Level III data—about the purchase card order during the settlement process. The Level III data is forwarded to the company that made the purchase, and it enables the company to manage its purchasing activities.

For detailed descriptions of each Level II and Level III API field, see *Level II and Level III Processing Using Secure Acceptance* (PDF | HTML). This guide also describes how to request sale and capture transactions.

Go-Live with Secure Acceptance

⚠️ **Important**	CyberSource recommends that you submit all banking information and required integration services at least one month in advance of going live.

When you are ready to implement Secure Acceptance in your live environment, you must contact CyberSource Customer Support and request Go-Live. When all the banking information has been received by CyberSource the Go-Live procedure may require three days to complete. No Go-Live implementations take place on a Friday.

Creating a Web/Mobile Profile

![Important]

Important

Contact CyberSource Customer Support to enable your account for Secure Acceptance. You must activate a profile in order to use it (see page 38).

To create a Web/Mobile profile:

Step 1   Log in to the Business Center:

- Live transactions: https://ebc.cybersource.com
- Test transactions: https://ebctest.cybersource.com

Step 2   In the left navigation panel, choose **Tools & Settings > Secure Acceptance > Profiles**.

Step 3   Enter or check the following profile details.

Table 2   Profile Details

Profile Detail	Description
Profile Name	The Secure Acceptance profile name is required and cannot exceed 20 alphanumeric characters.
Description	The profile description cannot exceed 255 characters.
Integration Method	Check **Web/Mobile**.
Company Name	The company name is required and cannot exceed 40 alphanumeric characters.
Company Contact Name	Enter company contact information: name, email, and phone number.
Company Contact Email	
Company Phone Number	
Payment Tokenization	Check **Payment Tokenization.** For more information, see page 44.
Decision Manager	Check **Decision Manager**. For more information, see page 70.
Enable Verbose Data	Check **Enable Verbose Data**. For more information, see page 70.

Step 4   Click **Create**. The Configuring Payment Settings page appears. See "Configuring Payment Settings".

Configuring Payment Settings

> **Important**
>
> You must configure the payment settings before you can activate a profile.

On the Profile Settings page, click **Payment Settings**. The Payment Settings page appears. You must select the card types to offer to the customer as payment methods. For each card type you select, you can also manage currencies CVNs, and payer authentication options. Select only the types of credit cards and currencies that your merchant account provider authorizes.

> **Note**
>
> The Card Verification Number (CVN) is a three- or four-digit number printed on the back or front of a credit card. This number helps ensure that the customer has possession of the card at the time of the transaction.

Adding a Card Type

To add a card type and enable the CVN:

Step 1 Click **Add/Edit Card Types**. The Add/Edit Card Types window appears.

Step 2 Check each card type that you want to offer to the customer as a payment method. The card types must be supported by your payment processor.

Step 3 Click **Update**.

Step 4 Click the pencil icon in the column for each card type. The Edit Card Settings page appears.

Step 5 Check **CVN Display** to display the CVN field on Secure Acceptance. The customer decides whether to enter the CVN. CyberSource recommends displaying the CVN to reduce fraud.

Step 6 Check **CVN Required**. The CVN Display option must also be checked. If this option is checked, the customer is required to enter the CVN. CyberSource recommends requiring the CVN to reduce fraud.

Step 7 Click **Update**. The card types are added as an accepted payment type.

Step 8 Click **Save**.

Configuring Payer Authentication

⚠️ **Important**	Before you can use CyberSource Payer Authentication, you must contact CyberSource Customer Support to provide information about your company and your acquiring bank so that CyberSource can configure your account. Your merchant ID must be enabled for payer authentication. For more information about Payer Authentication, see "Related Documents," page 9.

Payer authentication enables you to add support for Verified by Visa, MasterCard SecureCode, American Express SafeKey, and J/Secure by JCB without running additional software on your own server. The payer authentication services deter unauthorized card use and provide added protection from fraudulent chargeback activity.

For each transaction, you receive detailed information in the replies and in the transaction details page of the Business Center. You can store this information for 12 months. CyberSource recommends that you store the payer authentication data because you may be required to display this information as enrollment verification for any payer authentication transaction that you re-present because of a chargeback. Your account provider may require that you provide all data in human-readable format. Make sure that you can decode the PAReq and PARes.

✏️ **Note**	The language used on each Payer Authentication page is determined by your issuing bank and overrides the locale you have specified. If you use the test card numbers for testing purposes the default language used on the Payer Authentication page is English and overrides the locale you have specified. See "Testing and Viewing Transactions," page 72.

To configure payer authentication:

Step 1   Click the pencil icon in the column for each card type. The **Edit Card Settings** page appears.

Step 2   Check **Payer Authentication** for each card type that you want to offer to the customer as a payment method. The card types that support payer authentication are:

- Amex
- MasterCard
- Maestro (UK Domestic or International)
- Visa

Step 3   Click **Update**.

Adding a Currency

> ⚠️ **Important** By default, all currencies are listed as disabled. You must select at least one currency. Contact your merchant account provider for a list of supported currencies.

To add a supported currency for each card type:

Step 1 Click the pencil icon in the column for each card type. The Edit Card Settings page appears.

Step 2 Click **Select All** or select a currency and use the arrow to move it from the Disabled list to the Enabled list.

Step 3 Click **Update**.

Enabling Automatic Authorization Reversals

For transactions that fail to return an Address Verification System (AVS) or a Card Verification Number (CVN) match, you can enable Secure Acceptance to perform an automatic authorization reversals. An automatic reversal releases the reserved funds held against a customer's card.

To enable automatic authorization reversals:

Step 1 Check **Fails AVS check**. Authorization is automatically reversed on a transaction that fails an AVS check.

Step 2 Check **Fails CVN check**. Authorization is automatically reversed on a transaction that fails a CVN check.

Step 3 Click **Save**.

Enabling eChecks

An eCheck is a payment made directly from your customer's U.S. or Canadian bank account. As part of the checkout process, you must display a terms and conditions statement for eChecks. Within the terms and conditions statement it is recommended to include a link to the table of returned item fees. The table lists by state the amount that your customer has to pay when a check is returned.

To enable the eCheck payment option:

Step 1   Check **eCheck payments enabled**.

Step 2   Click the pencil icon in the currencies table. The Electronic Check Settings page appears.

Step 3   Click **Select All** or select a currency and use the arrow to move it from the Disabled list to the Enabled list.

Step 4   Click **Update**.

Step 5   Click **Save**. You must configure the eCheck information fields. See "Displaying eCheck Information Fields," page 26.

Enabling the Service Fee

![Important] Contact CyberSource Customer Support to have your CyberSource account configured for this feature. Service fees are supported only if Wells Fargo is your acquiring bank and FDC Nashville Global is your payment processor.

As part of the checkout process, you must display a terms and conditions statement for the service fee. A customer must accept the terms and conditions before submitting an order.

To enable the service fee:

Step 1   Check **Service Fee applies on transactions using this profile**. The service fee terms and conditions URL and the service fee amount are added to the customer review page.

![Warning] Transactions fail if you disable this feature. Do not disable this feature unless instructed to do so by your account manager.

Step 2   Click **Save**.

> ⚠ **Important**   After you save the profile you cannot disable the service fee functionality for that profile. All transactions using the profile will include the service fee amount.

Creating a Security Key

> ⚠ **Important**   You must create a security key before you can activate a profile.

> ✎ **Note**   You cannot use the same security key for both test and live transactions. You must download a security key for both versions of Secure Acceptance:
>
> - For live transactions: https://ebc.cybersource.com
> - For test transactions: https://ebctest.cybersource.com

On the Profile Settings page, click **Security**. The Security Keys page appears. The security script signs the request fields using the secret key and the HMAC SHA256 algorithm. To verify data, the security script generates a signature to compare with the signature returned from the Secure Acceptance server. You must have an active security key to activate a profile. A security key expires in two years and protects each transaction from data tampering.

To create and activate a security key:

Step 1   Click **Create New Key**. The Create New Key page appears.

Step 2   Enter a key name (required).

Step 3   Choose signature version **Version 1**.

Step 4   Choose signature method **HMAC-SHA256**.

Step 5   Click **Generate Key**. The Create New Key window expands and displays the new access key and secret key. This window closes after 30 seconds.

Step 6   Copy and save the access key and secret key.

- Access key: Secure Sockets Layer (SSL) authentication with Secure Acceptance. You can have many access keys per profile. See page 39.
- Secret key: signs the transaction data and is required for each transaction. Copy and paste this secret key into your security script. See page 39.

By default, the new security key is active. The other options for each security key are:

- Deactivate: deactivates the security key. The security key is inactive.
- Activate: activates an inactive security key.
- View: displays the access key and security key.

> **Note** When you create a security key, it is displayed in the security keys table. You can select a table row to display the access key and the secret key for that specific security key.

Step 7   Click **Return to Profile home**. The Configuring Profile Settings page appears.

Configuring the Payment Form

On the Configuring Profile Settings page, click **Payment Form**. The Payment Form page appears. The payment form is the customer's checkout experience. It consists of either a series of pages or as a single checkout page in which the customer enters or reviews information before submitting a transaction. Select the fields that you want displayed on the single checkout page or on each page of the multi-step checkout process: billing, shipping, payment, and order review.

Configuring the Payment Form Flow

To configure the payment form flow:

Step 1   Check the payment form flow that you want for your checkout:

- Multi-step payment form—the checkout process consists of a sequence of pages on which the customer enters or reviews information before submitting a transaction. The default sequence is billing, shipping, payment, review, and receipt.
- Single page form—the checkout process consists of one page on which the customer enters or reviews information before submitting a transaction.

> **Note** Do not click **Save** until you have selected the billing or shipping fields, or both

Step 2   Click **Save**. The Configuring Profile Settings page appears.

Displaying the Tax Amount

Follow these steps to display the total tax amount of the transaction as a separate line on each window of the checkout process. The total tax amount must be included in each transaction.

To display the tax amount:

Step 1   Check Display the total tax amount in each step of the checkout process.

> ⚠️
> **Important**
> Calculate and include the total tax amount in the **tax_amount** API field.

> ✏️
> **Note**
> Do not click Save until you have selected the billing or shipping fields, or both.

Step 2   Click **Save**. The Configuring Profile Settings page appears.

Displaying Billing Information Fields

> ⚠️
> **Important**
> Select the billing information fields that are required by your merchant provider.

Select the customer billing information fields that you want displayed on Secure Acceptance. If these fields are captured at an earlier stage of the order process (for example on your web site), they can be passed into Secure Acceptance as hidden form fields (see page 76). Not selecting billing information allows you to shorten the checkout process.

To display and edit the billing information fields

Step 1   Check Billing Information. The billing information fields appear.

Step 2   Check the billing information fields that are required by your merchant provider. The options for each field are:

- Display: the customer can view the information displayed in this field. Choose this option if you want to pre-populate the billing information fields when Secure Acceptance Web/Mobile is rendered—these fields must be passed into Secure Acceptance as hidden form fields.

- Edit: the customer can view and edit the billing information on the Secure Acceptance Web/Mobile checkout. When you select this option, the display option is automatically selected.

- Require: the customer is required to enter the billing information on the Secure Acceptance Web/Mobile checkout before they submit the transaction. When you select this option, all other options are automatically selected.

> **Note**   Do not click **Save** until you have selected the shipping and order review fields.

Step 3   Click **Save**. The Configuring Profile Settings page appears.

Displaying Shipping Information Fields

> **Important**   Select the shipping information fields that are required by your merchant provider.

Select the customer shipping information fields that you want displayed on Secure Acceptance. These fields are optional. If you do not add these fields, the shipping information step is removed from Secure Acceptance. If these fields are captured at an earlier stage of the order process (for example, on your web site), they can be passed into Secure Acceptance as hidden form fields (see page 76). Not selecting shipping information shortens the checkout process.

To display and edit shipping information fields:

Step 1   Check **Shipping Information**.

Step 2 Check the shipping information fields that are required by your merchant provider. The options for each field are:

- Display: the customer can view the information displayed in this field. Choose this option if you want to pre-populate the shipping information fields when Secure Acceptance Web/Mobile is rendered—these fields must be passed into Secure Acceptance as hidden form fields.

- Edit: the customer can view and edit the shipping information on the Secure Acceptance Web/Mobile checkout. When you select this option, the display option is automatically selected.

- Require: the customer is required to enter the shipping information on the Secure Acceptance Web/Mobile checkout before they submit the transaction. When you select this option, all other options are automatically selected.

> **Note**
> Do not click **Save** until you have selected the shipping and order review fields.

Step 3 Click Save. The Configuring Profile Settings page appears.

Displaying eCheck Information Fields

> **Important**
> Select the eCheck account information fields that are required by your merchant provider.

Select the customer eCheck account information fields that you want displayed on Secure Acceptance.

To display and edit eCheck information fields:

Step 1 Check the eCheck account information to be included in Secure Acceptance. The options for each field are:

- Display: the customer can view the information displayed in this field. Choose this option if you want to pre-populate the eCheck information fields when Secure Acceptance Web/Mobile is rendered.

- Edit: the customer can view and edit the eCheck information on the Secure Acceptance Web/Mobile checkout. When you select this option, the display option is automatically selected.

- Require: the customer is required to enter the eCheck information on the Secure Acceptance Web/Mobile checkout before they submit the transaction. When you select this option, all other options are automatically selected.

> **Note** Do not click **Save** until you have selected the shipping and order review fields.

Step 2 Click **Save**. The Configuring Profile Settings page appears.

Customizing Order Review Details

Select the fields that you want displayed on the Order Review page of Secure Acceptance Web/Mobile. The customer reviews this information before submitting a transaction.

To display and edit order review fields:

Step 1 Check the fields that you want displayed on the Order Review page of Secure Acceptance Web/Mobile. The options for each field are:

- Display: the customer can view the information contained in this field. Available only for billing and shipping information.
- Edit: the customer can view and edit the information contained in this field.

Step 2 Click Save. The Configuring Profile Setting page appears.

Configuring Notifications

On the Profile Settings page, click **Notifications**. The Notifications page appears. Secure Acceptance sends merchant and customer notifications in response to transactions.

Configuring Merchant Notifications

You can receive a merchant notification by email or as an HTTP POST to a URL for each transaction processed. Both notifications contain the same transaction result data.

> **Important** CyberSource recommends that you implement the merchant POST URL to receive notification of each transaction. You need to parse the transaction response sent to the merchant POST URL and store the data within your systems. This ensures the accuracy of the transactions and informs you if the transaction was successfully processed.

To configure merchant notifications:

Step 1 Choose a merchant notification in one of two ways:

■ Check **Merchant POST URL**. Enter the URL. CyberSource sends transaction information to this URL. For more information, see "API Reply Fields," page 97.

> ⚠️ **Important** — Use ports 80, 443, or 8080 in the URL. Contact CyberSource Customer Support if you encounter problems using an HTTPS-based URL.

■ Check **Merchant POST Email**. Enter your email address.

> ✏️ **Note** — CyberSource sends transaction response information to this email address including payment information, return codes, and all relevant order information. See "API Reply Fields," page 97.

Step 2 Choose the card number digits that you want displayed in the merchant or customer receipt:

■ Return credit card BIN: displays the card's Bank Identification Number (BIN), which is the first six digits of the card number. All other digits are masked: 123456xxxxxxxxxx

■ Return last four digits of credit card number: displays the last four digits of the card number. All other digits are masked: xxxxxxxxxxxx1234

■ Return BIN and last four digits of credit card number: displays the BIN and the last four digits of the card number. All other digits are masked: 123456xxxxxx1234

Step 3 Continue to configure the customer notifications (see page 29) or click **Save**. The Profile Settings page appears.

Configuring Customer Notifications

You can send a purchase receipt email to your customer and a copy to your own email address. Both are optional. Customers may reply with questions regarding their purchases, so use an active email account. The email format is HTML unless your customer email is rich text format (RTF).

Customer Notification Details

To configure customer notifications:

Step 1   Check **Email Receipt to Customer.**

Step 2   Enter the email address to be displayed on the customer receipt. The customer will reply to this email with any queries.

Step 3   Enter the name of your business. It is displayed on the customer receipt.

Step 4   Check **Send a copy to**. This setting is optional.

Step 5   Enter your email address to receive a copy of the customer's receipt.

Note	Your copy of the customer receipt will contain additional transaction response information.

Step 6   Click **Save**. The Configuring Profile Settings page appears.

Company Logo

You can upload a company logo to display on customer notifications.

To add a company logo to the customer receipt and email:

Step 1   Check **Email Receipt to Customer.**

Step 2   Check **Display Notification Logo**.

Step 3 Click **Upload Company Logo**. Find and upload the image that you want to display on the customer receipt and email.

> ⚠️ **Important** For preview, an image must not exceed 200 (w) x 60 (h) pixels. The image file type must be GIF, JPEG, or PNG. The logo filename must not contain any special characters, such as a hyphen (-).

Step 4 Click **Save**.

Custom Email Receipt

To create a customer email receipt:

Step 1 Check **Email Receipt to Customer.**

Step 2 Check which email receipt you would like to send to a customer:

- Standard email: this email is automatically translated based on the locale used for the transaction.
- Custom email: this email can be customized with text and data references. The email body section containing the transaction detail appears between the header and footer. Custom text is not translated when using different locales.

    You can insert email smart tags to both the email header and footer sections to include specific information.

Step 3 Select each specific smart tag from the drop-down list and click **Insert**.

Step 4 Click **Save**.

Displaying a Customer Response Page

> ⚠️ **Important**
>
> You must configure the customer response page before you can activate a profile.

On the Profile Settings page, click **Customer Response Pages**. The Customer Response Pages page appears. You can choose to have a transaction response page displayed to the customer at the end of the checkout process, and a cancel response page displayed during the checkout process. Enter a URL for your own customer response page or use the CyberSource hosted response pages.

Depending upon the transaction result, the CyberSource hosted response pages are Accept, Decline, or Error. Review declined orders as soon as possible because you may be able to correct problems related to address or card verification, or you may be able to obtain a verbal authorization. You can also choose to display a web page to the customer after the checkout process is completed.

Transaction Response Page

CyberSource Hosted Response Page

To display a CyberSource hostedresponse page:

Step 1 Under the Transaction Response Page heading, check **Hosted by CyberSource**.

Step 2 Choose a number from the **Decline Retry Limit** drop-down list. The maximum number of times a customer can retry a declined transaction is 5.

Step 3 Under the Customer Redirect after Checkout heading, enter the redirect URL of the web page. This web page is displayed to the customer after the checkout process is completed.

Step 4 Under the heading Transaction Response Page, check **Hosted by you**.

Step 5 Enter the redirect URL of the web page. This web page is displayed to the customer after the checkout process is completed.

Step 6 Click **Save**. The Profile Settings page appears.

Custom Hosted Response Page

To display your custom response page:

Step 1   Under the Transaction Response Page heading, check **Hosted by You**.

Step 2   Enter the URL for your customer response page. Use port 80, 443, or 8080 in your URL.

> **Note**   Parse the transaction results from the URL according to the reason code (see page 109), and redirect your customer to the appropriate response page.

Step 3   Choose a number from the Decline Retry Limit drop-down list. The maximum number od times a customer can retry a declined transaction is 5.

Step 4   Click **Save**. The Configuring Profile Settings page appears.

Cancel Response Page

CyberSource Hosted Response Page

To display a CyberSource hosted response page:

Step 1   Under the Transaction Response Page heading, check **Hosted by CyberSource**.

Step 2   Click **Save**. The Configuring Profile Settings page appears.

Custom Hosted Response Page

To display your custom response page:

Step 1   Under the Custom Cancel Response Page heading, check **Hosted by You**.

Step 2   Enter the URL for your customer response page. Use port 80, 443, or 8080 in your URL.

> **Note**   Parse the transaction results from the URL according to the reason code (see page 109), and redirect your customer to the appropriate response page.

Step 3   Click Save. The Configuring Profile Settings page appears.

Customizing Appearance and Branding

On the Configuring Profile Settings page, click **Appearance and Branding**. The Appearance and Branding page appears. Customize the appearance and branding of the Secure Acceptance checkout pages by choosing a background color, font, and text color. Upload a logo or image, and align it within the header or footer.

> ⚠️
> **Important**
> CyberSource recommends that you preview your changes in the Image Preview window. For preview, the image must not exceed 200 (w) x 60 (h) pixels.

To change the header color and upload an image:

Step 1   Check **Display Header.**

Step 2   Choose a color in one of two ways:

- Enter a hexadecimal value for the header color of teh payment form.
- Click within the header color palette to choose a color. Click the icon at the bottom right to confirm your selection.

Step 3   Click **Upload Header Image**. Upload the image to display as the header banner or as a logo within the header banner.

> ⚠️
> **Important**
> To display an image as the header banner of the payment form, the image dimensions must not exceed 840 (w) x 60 (h) pixels and the image size must not exceed 100Kb. To display a small logo within the header banner, the logo height must not exceed 60 pixels. The image file must be GIF, JPEG, or PNG.

Step 4   Check the alignment option for the image or logo: left-aligned, centered, or right-aligned.

Step 5   Click **Save**.

Step 6   Click **Set to Default** to restore all the default settings on this page.

To change the main body color and font settings:

Step 1   Choose a background color for the main body in one of two ways:

- Enter a hexadecimal value for the background color.
- Click within the header color palette to choose a color. Click the icon at the bottom right to confirm your selection.

Step 2   Select a text font from the drop-down list.

Step 3   Choose a text color in one of two ways:

- Enter a hexadecimal value for the background color.
- Click within the header color palette to choose a color. Click the icon at the bottom right to confirm your selection.

Step 4   Click **Save**.

Step 5   Click **Set to Default** to restore all the default settings on this page.

To change the background color and text color of the total amount:

![Important] If you are implementing the iFrame embedded version of Secure Acceptance Web/Mobile, the total amount figure is not displayed within the iFrame. Any settings you select below are ignored.

Step 1   Choose a background color in one of two ways:

- Enter a hexadecimal value for the background color.
- Click within the header color palette to choose a color. Click the icon at the bottom right to confirm your selection.

Step 2   Choose a text color in one of two ways:

- Enter a hexadecimal value for the text color of the total amount.
- Click within the header color palette to choose a color. Click the icon at the bottom right to confirm your selection.

Step 3   Click **Save**.

Step 4   Click **Set to Default** to restore all the default settings on this page.

To change the color of the progress bar:

Step 1 Choose a color in one of two ways:

- Enter a hexadecimal value for the color of the progress bar.
- Click within the header color palette to choose a color. Click the icon at the bottom right to confirm your selection.

Step 2 Click **Save**.

Step 3 Click **Set to Default** to restore all the default settings on this page.

To change the color and text displayed on the pay button:

Step 1 Choose a background color of the pay button in one of two ways:

- Enter a hexadecimal value for the background color.
- Click within the header color palette to choose a color. Click the icon at the bottom right to confirm your selection.

Step 2 Choose a color of the pay button text in one of two ways:

- Enter a hexadecimal value for the text.
- Click within the header color palette to choose a color. Click the icon at the bottom right to confirm your selection.

Step 3 Check **Change Button text.** A text box appears. Enter the text you want displayed on the button. The default is *Pay.*

Step 4 Click **Save**.

Step 5 Click **Set to Default** to restore all the default settings on this page.

To change the footer color and upload a small logo or image:

Step 1 Check Display Footer.

Step 2 Choose a color in one of two ways:

- Enter a hexadecimal value for the footer color of the payment form.
- Click within the header color palette to choose a color. Click the icon at the bottom right to confirm your selection.

Step 3 Click Upload Footer Image. Upload the image that you want displayed within the footer of the payment form.

> ⚠️ **Important**
> To display a small logo or image in the footer of the payment form, the file must not exceed 840 (w) x 60 (h) pixels. The image file must be GIF, JPEG, or PNG.

Step 4   Check the alignment option for the image: left-aligned, centered, or right-aligned.

Important   For preview, an image must not exceed 200 (w) x 60 (h) pixels.

Step 5   Click Save.

Step 6   Click Set to Default to restore all the default settings on this page.

Localization

Secure Acceptance supports 41 languages for localization purposes. The table below lists all the supported languages and the locale code you must include in your payment form.

To specify and display the local language on Secure Acceptance:

Step 1   Include the **locale** API field in your payment form.

Step 2   Enter the locale code in the API field. See "Rendering Secure Acceptance Web/Mobile," page 39.

Example   American English

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

Table 3   Locale Codes

Language	Locale Code
Arabic	ar-xn
Cambodia	km-kh
Chinese - Hong Kong	zh-hk
Chinese - Maco	zh-mo
Chinese - Mainland	zh-cn
Chinese - Singapore	zh-sg
Chinese - Taiwan	zh-tw
Czech	cz-cz
Dutch	nl-nl
English - American	en-us
English - Australia	en-au

Table 3   Locale Codes (Continued)

Language	Locale Code
English - Britain	en-gb
English - Canada	en-ca
English - Ireland	en-ie
English - New Zealand	en-nz
French	fr-fr
French - Canada	fr-ca
German	de-de
German - Austria	de-at
Hungary	hu-hu
Indonesian	id-id
Italian	it-it
Japanese	ja-jp
Korean	ko-kr
Lao People's Democratic Republic	lo-la
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 - Colombia	es-co
Spanish - Mexico	es-mx
Spanish - Peru	es-pe
Spanish - American	es-us
Thai	th-th
Turkish	tr-tr
Vietnamese	vi-vn

Activating a Profile

	You must complete the required settings in each of these sections before activating a profile:
Important	■ "Configuring Payment Settings"
	■ "Creating a Security Key"
	■ "Displaying a Customer Response Page"

To activate a profile:

Step 1   On the Profile Settings page, click **Promote to Active**. The profile is now active and listed as an active profile on the Manage Profiles page.

	The All Profiles link appears on the Profile Settings page. Click **All Profiles** to view the Manage Profiles list. See "Updating a Secure Acceptance Profile," page 42.
Note	

Additional Options for a Profile

- Deactivate—deactivates the active profile. The profile is now listed in the inactive profile list. Available only for an active profile.

- Create Editable Version—duplicates the active profile. The editable version is listed in the inactive profile list. Available only for an active profile.

- Promote to Active—activates the inactive profile. Available only for an inactive profile.

Rendering Secure Acceptance Web/Mobile

Web/Mobile can support any dynamic scripting language that supports HMAC256 hashing algorithms.

Select to download the sample script for the scripting language that you use:

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

To render Secure Acceptance Web/Mobile:

Step 1   The security script must be modified to include the Secret Key that you generated on page 22. In the security script sample, enter your security key into the **SECRET_KEY** field. See "Creating a Security Key," page 22.

The security algorithm in each security script sample is responsible for:

- Request authentication—the signature is generated on the merchant server by the keyed-hash message authentication code (HMAC) signing the request parameters using the shared secret key. This process is also carried out on the Secure Acceptance server, and the two signatures are compared for authenticity.

- Response authentication—the signature is generated on the Secure Acceptance server by HMAC signing the response parameters, using the shared secret key. This process is also carried out on the merchant server, and the two signatures are compared for authenticity.

Step 2   The payment form represents the payment information section of an e-commerce site. The sample payment form script contains some fields which you can hide from the view of the customer and pass through in the POST message.

In the payment form, paste your access key and profile ID into their respective fields. See "Creating a Security Key," page 22. Additional API fields can be added to this form if you want the fields pre-populated when Secure Acceptance is rendered. See page 76.

Step 3   The payment confirmation script represents the review of the payment and the order information prior to proceeding with making a payment.

In the payment confirmation page, enter the endpoint for processing either test or live transactions. See "Endpoints and Transaction Types," page 40.

Endpoints and Transaction Types

Standard Transaction Endpoints

Test Transactions	https://testsecureacceptance.cybersource.com/pay
Live Transactions	https://secureacceptance.cybersource.com/pay
Supported transaction types	■ authorization
	■ authorization,create_payment_token
	■ authorization,update_payment_token
	■ sale
	■ sale,create_payment_token
	■ sale,update_payment_token

One-click Transaction Endpoints

Test Transactions	https://testsecureacceptance.cybersource.com/oneclick/pay
Live Transactions	https://secureacceptance.cybersource.com/oneclick/pay
Supported transaction types	■ authorization
	■ authorization,update_payment_token
	■ sale
	■ sale,update_payment_token

Create Standalone Payment Token Endpoints

Test Transactions	https://testsecureacceptance.cybersource.com/token/create
Live Transactions	https://secureacceptance.cybersource.com/token/create
Supported transaction type	create_payment_token

Update Payment Token Endpoints

Test Transactions	https://testsecureacceptance.cybersource.com/token/update
Live Transactions	https://secureacceptance.cybersource.com/token/update
Supported transaction type	update_payment_token

iFrame Standard Transaction Endpoints (see "iFrame Implementation," page 115).

Test Transactions	https://testsecureacceptance.cybersource.com/embedded/pay
Live Transactions	https://secureacceptance.cybersource.com/embedded/pay
Supported transaction type	■ authorization
	■ authorization,create_payment_token
	■ authorization,update_payment_token
	■ sale
	■ sale,create_payment_token
	■ sale,update_payment_token

iFrame Create Payment Token Endpoints (see "iFrame Implementation," page 115).	
Test Transactions	https://testsecureacceptance.cybersource.com/embedded/token/create
Live Transactions	https://secureacceptance.cybersource.com/embedded/token/create
Supported transaction type	create_payment_token
iFrame Update Payment Token Endpoints (see "iFrame Implementation," page 115).	
Test Transactions	https://testsecureacceptance.cybersource.com/embedded/token/update
Live Transactions	https://secureacceptance.cybersource.com/embedded/token/update
Supported transaction type	update_payment_token

Updating a Secure Acceptance Profile

Profile status can be active or inactive:

- Active: the live Secure Acceptance profile. This is your current profile, and it is read-only. You can have more than one active profile.

- Inactive: the version of a new profile before activation, or the editable version of an active profile. Update and activate this profile to replace the current active profile.

> ⚠️ **Important** If you have multiple profiles the Manage Profiles page appears by default when you log in to the Business Center.

To update a profile:

Step 1 Log in to the Business Center:

- Live transactions: https://ebc.cybersource.com

- Test transactions: https://ebctest.cybersource.com

Step 2 In the left navigation panel, choose **Tools & Settings > Secure Acceptance > Profiles**.

Step 3 Check the active or inactive profile.

The options for an active profile are:

- Deactivate: deactivates the active profile. The profile is then listed in the inactive profile list.

- Edit: select edit and update the active profile. An editable version of the active profile appears in the inactive profile list. To activate this inactive profile, click **Promote to Active**.

- Copy: duplicates the active profile. The duplicate profile (editable version) is listed in the inactive profile list.

The options for an inactive profile are:

- Promote to Active: promotes the inactive profile to the active profile list. It replaces the current active profile, and it is removed from the inactive profile list.

- Delete: deletes the inactive profile.

- Copy: duplicates the inactive profile. The duplicate profile (editable version) is listed in the inactive profile list.

Note   You can also click the pencil icon to edit an inactive profile.

Step 4   Click **Continue**. The Profile Settings page appears.

Step 5   Update the inactive profile (editable version). See "Creating a Web/Mobile Profile," page 17.

Step 6   Activate the inactive profile. See "Activating a Profile," page 38.

Important   When you activate an inactive profile, it replaces the current active profile and is removed from the inactive profile list on the Manage Profiles page.

Step 7   Click **All Profiles** to view the active and inactive profiles you have created.

Important   If you have multiple profiles the Manage Profiles page appears by default when you log in to the Business Center and choose **Tools & Settings > Secure Acceptance > Profiles**.

Creating a Payment Token

Standalone Payment Token

For a Credit Card Customer

To create a standalone payment token for a credit card customer:

Step 1 Include the appropriate endpoint that supports **create_payment_token**. See page 40.

Step 2 Include the following required API fields on your payment form. For detailed descriptions of all request fields, see page 76.

```
reference_number=123456789
transaction_type=create_payment_token
currency=usd
locale=en
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
profile_id=demoid
transaction_uuid=02815b4f08e56882751a043839b7b481
signed_date_time=2013-07-11T15:16:54Z
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
```

Step 3 Depending on the payment settings you configured for Secure Acceptance Web/Mobile (see page 23), you can hide or pre-populate API fields when Secure Acceptance is rendered.

> ⚠️ **Important** Include all optional request fields in the required **signed_field_names** field (recommended) or the **unsigned_field_names** field. The **signed_field_names** field is used to generate a signature that is used to verify the content of the transaction to prevent data tampering.

Example 1   Pre-Populated API request fields

```
payment_method=card
card_type=001
card_number=4111111111111111
card_expiry_date=12-2022
card_cvn=005
bill_to_forename=Joe
bill_to_surname=Smith
bill_to_email=joesmith@example.com
bill_to_address_line1=1 My Apartment
bill_to_address_state=CA
bill_to_address_country=US
```

Below are the transaction reply fields (see for detailed descriptions of all reply fields). It includes the new payment token value.

```
req_reference_number=123456789
req_transaction_type=create_payment_token
req_locale=en
req_payment_method=card
req_card_type=001
req_card_number=xxxxxxxxxxxx1111
req_card_expiry_date=12-2022
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=joesmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
req_profile_id=demoid
req_transaction_uuid=02815b4f08e56882751a043839b7b481
signed_date_time=2013-07-11T15:16:54Z
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
decision=ACCEPT
reason_code=100
transaction_id=3735553783662130706689
payment_token=3529893314302230706689
```

For an eCheck Customer

To create a standalone payment token for an eCheck customer:

Step 1   Include the appropriate endpoint that supports **create_payment_token**. See page 40.

Step 2   Include the following required fields on your payment form. For detailed descriptions of all request fields, see page 76.

```
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p1
profile_id=demoid
transaction_type=create_payment_token
currency=USD
locale=en
reference_number=1730560013735542024294683
transaction_uuid=02815b4f08e56882751a043839b7b481
signed_date_time=2013-07-11T15:16:54Z
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
```

Step 3   Depending on the settings you configured for Secure Acceptance Web/Mobile (see page 23), you can hide, pre-populate, or allow the customer to edit the API fields when Secure Acceptance is rendered.

> ⚠️ **Important**   Include all optional request fields in the required **signed_field_names** field (recommended) or the **unsigned_field_names** field. The **signed_field_names** field is used to generate a signature that is used to verify the content of the transaction to prevent data tampering.

Example 2   Pre-Populated API request fields

```
bill_to_forename=Joe
bill_to_surname=Smith
bill_to_email=joesmith@example.com
bill_to_address_line1=1 My Apartment
bill_to_address_state=CA
bill_to_address_country=US
payment_method=echeck
driver_license_state=NY
driver_license_number=34-78239-396
date_of_birth=19901001
echeck_account_type=c
company_tax_id=123456789

echeck_sec_code=WEB
echeck_account_number=452894100
echeck_routing_number=672302882
```

Below are the transaction reply fields (see page 97 for detailed descriptions of all reply fields).

```
req_bill_to_address_country=US
req_driver_license_state=NY
req_driver_license_number=xx-xxxxx-xxx
req_date_of_birth=19901001
decision=ACCEPT
req_bill_to_address_state=CA
signed_field_names=comma separated list of signed fields
req_payment_method=echeck
req_transaction_type=create_payment_token
req_echeck_account_type=c
signature=NuxlJilx5YbvKoXlt0baB5hUj5gk4+OozqJnyVF390s=
req_locale=en
reason_code=100
req_bill_to_address_postal_code=94043
req_echeck_account_number=xxxxx4100
req_bill_to_address_line1=1 My Apartment
req_echeck_sec_code=WEB
req_bill_to_address_city=San Francisco
signed_date_time=2013-07-11T15:11:41Z
req_currency=USD
req_reference_number=1730560013735542024294683
req_echeck_routing_number=xxxxx2882
transaction_id=3735553783662130706689
req_amount=100.00
req_profile_id=demoid
req_company_tax_id=123456789
req_transaction_uuid=38f2efe650ea699597d325ecd7432b1c
payment_token=3529893314302130706689
req_bill_to_surname=Soap
req_bill_to_forename=Joe
req_bill_to_email=joesoap@yahoo.com
req_access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p1
```

Payment Token for Recurring Payments

You must specify the amount and frequency of each payment and the start date for processing recurring payments. CyberSource creates a schedule based on this information and automatically bills the customer according to the schedule.

To create a payment token for a recurring payment:

Step 1   Include the appropriate endpoint that supports **authorization,create_payment_token** or **sale,create_payment_token**. See page 40.

> ⚠️ **Important**
>
> The **amount** field is an optional field that indicates the setup fee for processing recurring payments. To charge this fee, include the **amount** field and ensure that the **transaction_type** field is set to **authorization,create_payment_token** or **sale,create_payment_token**.

Step 2   Include the following required API fields on your payment form. For detailed descriptions of all request fields, see page 76.

Depending on the settings you configured for Secure Acceptance Web/Mobile (see

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=demoid
transaction_type=authorization,create_payment_token
locale=en
currency=USD
amount=5.00
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2013-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
```

page 23), you can hide, pre-populate, or allow the customer to edit the API fields when Secure Acceptance is rendered.

> ⚠️ **Important**
>
> Include all optional request fields in the required **signed_field_names** field (recommended) or the **unsigned_field_names** field. The **signed_field_names** field is used to generate a signature that is used to verify the content of the transaction to prevent data tampering.

Example 3   Pre-Populated API request fields

```
bill_to_forename=Joe
bill_to_surname=Smith
bill_to_email=joesmith@example.com
bill_to_address_line1=1 My Apartment
bill_to_address_state=CA
bill_to_address_country=US
recurring_frequency=monthly
recurring_amount=25.00
payment_method=card
```

Below are the transaction reply fields (see for detailed descriptions of all reply fields).

```
transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=demoid
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization,create_payment_token
req_reference_number=1350029885978
req_tax_amount=15.00
req_currency=USD
req_locale=en
req_payment_method=card
req_payment_token_comments=These are my token comments
req_payment_token_title=This is my payment token title
req_consumer_id=1239874561
req_recurring_frequency=monthly
req_recurring_amount=25.00
req_recurring_start_date=20130125
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=jsmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_card_number=xxxxxxxxxxxx4242
req_card_type=001
req_card_expiry_date=11-2020
reason_code=100
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
```

```
auth_amount=100.00
auth_time==2012-08-14T134608Z
payment_token=342707583000181552556
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

Payment Token for Installment Payments

You must specify the number of payments, the amount and frequency of each payment, and the start date for processing the payments. CyberSource creates a schedule based on this information and automatically bills the customer according to the schedule.

To create a payment token for an installment payment:

Step 1   Include the appropriate endpoint that supports **authorization,create_payment_token** or **sale,create_payment_token**. See page 40.

> ⚠ **Important**   The **amount** field is an optional field that indicates the setup fee for processing recurring payments. To charge this fee, include the **amount** field and ensure the **transaction_type** field is set to **authorization,create_payment_token** or **sale,create_payment_token**.

Step 2   Include the following required API fields on your payment form. For detailed descriptions of all request fields, see page 76.

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=demoid
transaction_type=authorization,create_payment_token
locale=en
currency=USD
amount=5.00
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2013-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
```

Step 3   Depending on the settings you configured for Secure Acceptance Web/Mobile (see page 23), you can hide, pre-populate, or allow the customer to edit the API fields when Secure Acceptance is rendered.

> ⚠️ **Important**
>
> Include all optional request fields in the required **signed_field_names** field (recommended) or the **unsigned_field_names** field. The **signed_field_names** field is used to generate a signature that is used to verify the content of the transaction to prevent data tampering.

Example 4   Pre-Populated API request fields

```
bill_to_forename=Joe
bill_to_surname=Smith
bill_to_email=joesmith@example.com
bill_to_address_line1=1 My Apartment
bill_to_address_state=CA
bill_to_address_country=US
recurring_frequency=monthly
recurring_number_of_installments=6
recurring_amount=25.00
payment_method=card
```

Below are the transaction reply fields (see page 97 for detailed descriptions of all reply fields).

```
transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=demoid
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization,create_payment_token
req_reference_number=1350029885978
req_tax_amount=15.00
req_currency=USD
req_locale=en
req_payment_method=card
req_payment_token_comments=These are my token comments
req_payment_token_title=This is my payment token title
req_consumer_id=1239874561
req_recurring_frequency=monthly
req_recurring_amount=25.00
req_recurring_start_date=20130125
req_recurring_number_of_installments=6
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=jsmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_card_number=xxxxxxxxxxxx4242
req_card_type=001
```

```
req_card_expiry_date=11-2020
reason_code=100
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
auth_amount=100.00
auth_time==2012-08-14T134608Z
payment_token=3427075830000181552556
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

Updating Payment Token Details

For a Credit Card Customer

![!] **Important**
You must configure the billing, shipping, and payment details to allow a customer to edit their details on the Order Review page. See "Customizing Order Review Details," page 27.

To update payment token details for a credit card customer:

Step 1 Include the appropriate endpoint that supports **update_payment_token**. See page 40. This updates the token without processing a transaction.

Or, include the appropriate endpoint that supports **authorization,update_payment_ token** (updates the token and authorizes the transaction) or **sale,update_payment_ token** (updates the token and processes the transaction). See page 40.

Step 2 Include the **allow_payment_token_update** field and set to **true**.

Step 3 Include the following required API fields on your payment form. For detailed descriptions of required or optional request fields, see page 76.

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=demoid
reference_number=1350029885978
payment_token=3427075830000181552556
amount=100.00
currency=USD
locale=en
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2013-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
```

Step 4 The **payment_token** field identifies the card and retrieves the associated billing, shipping, and payment information. The customer is directed to the Order Review page.

Step 5 The customer clicks **Edit Address** or **Edit Details** to return to the relevant checkout page.

Step 6 The customer updates their details and clicks **Next**. The Order Review page appears.

Step 7   The customer clicks **Pay** to confirm the transaction.

Below is an example card update reply. It includes the new payment token.

```
transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=demoid
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization,update_payment_token
req_reference_number=1350029885978
req_amount=100.00
req_tax_amount=15.00
req_currency=USD
req_locale=en
req_payment_method=card
req_consumer_id=1239874561
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=jsmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_card_number=xxxxxxxxxxxx1111
req_card_type=001
req_card_expiry_date=12-2022
reason_code=100
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
auth_amount=100.00
auth_time==2012-08-14T134608Z
payment_token=3427075830000181552556
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

For detailed descriptions of all reply fields, see .

For an eCheck Customer

![Important] You must configure the billing, shipping, and payment details to allow a customer to edit their details on the Order Review page. See "Customizing Order Review Details," page 27.

Important

To update payment token details for an eCheck customer:

Step 1   Include the appropriate endpoint that supports **update_payment_token**. See page 40. This updates the token without processing a transaction.

Or, include the appropriate endpoint that supports **sale,update_payment_token** (updates the token and processes the transaction). See page 40.

Step 2   Include the **allow_payment_token_update** field and set to **true**.

Step 3   Include the following required API fields on your payment form. For detailed descriptions of required request fields, see page 76.

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=demoid
reference_number=1350029885978
payment_token=3427075830000181552556
amount=100.00
currency=USD
locale=en
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2013-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
```

Step 4   The **payment_token** field identifies the eCheck account and retrieves the associated billing, shipping, and payment information. The customer is directed to the Order Review page.

Step 5   The customer clicks **Edit Address** or **Edit Details** to return to the relevant checkout page.

Step 6   The customer updates their details and clicks **Next**. The Order Review page appears.

Step 7   The customer clicks **Pay** to confirm the transaction.

Below is an example eCheck update reply. It includes the new payment token.

```
req_bill_to_address_country=US
req_driver_license_state=NY
req_driver_license_number=xx-xxxxx-xxx
req_date_of_birth=19901001
decision=ACCEPT
req_bill_to_address_state=CA
signed_field_names=comma separated list of signed fields
req_payment_method=echeck
req_transaction_type=sale,update_payment_token
req_echeck_account_type=c
signature=NuxlJilx5YbvKoXlt0baB5hUj5gk4+OozqJnyVF390s=
req_locale=en
reason_code=100
req_bill_to_address_postal_code=94043
req_echeck_account_number=xxxxx4100
req_bill_to_address_line1=1 My Apartment
req_echeck_sec_code=WEB
req_bill_to_address_city=San Francisco
signed_date_time=2013-07-11T15:11:41Z
req_currency=USD
req_reference_number=173056001373554 2024294683
req_echeck_routing_number=xxxxx2882
transaction_id=3735553783662130706689
req_amount=100.00
req_profile_id=demoid
req_company_tax_id=123456789
req_transaction_uuid=38f2efe650ea699597d325ecd7432b1c
payment_token=3529893314302130706689
req_bill_to_surname=Soap
req_bill_to_forename=Joe
req_bill_to_email=joesoap@yahoo.com
req_access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p1
```

For detailed descriptions of all reply fields, see .

Payment Token for Recurring Payments

> **⚠ Important** You must configure the billing, shipping, and payment details to allow a customer to edit their details on the Order Review page. See "Customizing Order Review Details," page 27.

To update payment token details for a recurring payment:

Step 1   Include the appropriate endpoint that supports **update_payment_token**. See page 40. This updates the token without processing a transaction.

Or, include the appropriate endpoint that supports **authorization,update_payment_ token** (updates the token and authorizes the transaction) or **sale,update_payment_ token** (updates the token and processes the on-demand transaction). See page 40.

Step 2   Include the **allow_payment_token_update** field and set to **true**.

Step 3   Include the following required API fields on your payment form. For detailed descriptions of required request fields, see page 76.

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=HPA0002
reference_number=1350029885978
payment_token=3427075830000181552556
amount=100.00
currency=USD
locale=en
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2013-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
```

Step 4   The **payment_token** field identifies the card and retrieves the associated billing, shipping, and payment information. The customer is directed to the Order Review page.

Step 5   The customer clicks **Edit Address** or **Edit Details** to return to the relevant checkout page.

Step 6   The customer updates their details and clicks **Next**. The Order Review page appears.

Step 7   The customer clicks **Pay** to confirm the transaction.

Below is an example recurring billing update reply. It includes the new payment token value.

```
transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=demoid
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization,update_payment_token
req_reference_number=1350029885978
req_tax_amount=2.50
req_currency=USD
req_locale=en
req_payment_method=card
req_consumer_id=1239874561
req_recurring_frequency=monthly
req_recurring_amount=25.00
req_recurring_start_date=20130125
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=joesmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_card_number=xxxxxxxxxxxx1111
req_card_type=001
req_card_expiry_date=12-2022
reason_code=100
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
auth_amount=100.00
auth_time==2012-08-14T134608Z
payment_token=6739075830290181556723
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

For detailed descriptions of all request and reply fields, see .

Payment Token for Installment Payments

> **⚠ Important**
>
> You must configure the billing, shipping, and payment details to allow a customer to edit their details on the Order Review page. See "Customizing Order Review Details," page 27.

To update payment token details for an installment subscription:

Step 1   Include the appropriate endpoint that supports **update_payment_token**. See page 40. This updates the token without processing a transaction.

Or, include the appropriate endpoint that supports **authorization,update_payment_token** (updates the token and authorizes the transaction) or **sale,update_payment_token** (updates the token and processes the on-demand transaction). See page 40.

Step 2   Include the **allow_payment_token_update** field and set to **true**.

Step 3   Include the following required API fields on your payment form. For detailed descriptions of required request fields, see page 76.

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=HPA0002
reference_number=1350029885978
payment_token=3427075830000181552556
amount=100.00
currency=USD
locale=en
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2013-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
```

Step 4   The **payment_token** field identifies the card and retrieves the associated billing, shipping, and payment information. The customer is directed to the Order Review page.

Step 5   The customer clicks **Edit Address** or **Edit Details** to return to the relevant checkout page.

Step 6   The customer updates their details and clicks **Next**. The Order Review page appears.

Step 7   The customer clicks **Pay** to confirm the transaction.

Below is an example installment payment update reply. It includes the new payment token value.

```
transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=demoid
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization,update_payment_token
req_reference_number=1350029885978
req_tax_amount=15.00
req_currency=USD
req_locale=en
req_payment_method=card
req_payment_token_comments=These are my token comments
req_payment_token_title=This is my payment token title
req_consumer_id=1239874561
req_recurring_frequency=monthly
req_recurring_amount=25.00
req_recurring_start_date=20130125
req_recurring_number_of_installments=6
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=jsmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_card_number=xxxxxxxxxxxx1111
req_card_type=001
req_card_expiry_date=12-2022
reason_code=100
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
auth_amount=100.00
auth_time==2012-08-14T134608Z
payment_token=6739075830290181556723
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00
```

For detailed descriptions of all request and reply fields, see .

Processing Transactions Using a Payment Token

For one-click Payments

To process one-click payments:

Step 1 Include the appropriate one-click endpoint that supports **authorization** or **sale**. See page 40.

Step 2 Include the following required API fields on your payment form. For detailed descriptions of all request fields, see page 76.

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=HPA0002
reference_number=1350029885978
payment_token=3427075830000181552556
transaction_type=authorization
amount=100.00
currency=USD
locale=en
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2013-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
```

Step 3 The **payment_token** field identifies the card and retrieves the associated billing, shipping, and payment information.

Step 4 The customer is directed to the Order Review page. Depending on the settings you configured for Secure Acceptance Web/Mobile (see page 23), the customer can view or update their billing, shipping, and payment details (see page 53).

Step 5 The customer clicks **Pay**.

Below is the transaction reply.

```
transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=HPA0002
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization
req_reference_number=1350029885978
req_amount=100.00
req_tax_amount=15.00
req_currency=USD
req_locale=en
req_payment_method=card
req_consumer_id=1239874561
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=jsmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_card_number=xxxxxxxxxxxx4242
req_card_type=001
req_card_expiry_date=11-2020
reason_code=100
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
auth_amount=100.00
auth_time==2012-08-14T134608Z
payment_token=3427075830000181552556
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
req_amount=100.00
req_tax_amount=15.00
req_currency=USD
req_locale=en
req_payment_method=card
req_consumer_id=1239874561
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=jsmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_card_number=xxxxxxxxxxxx4242
req_card_type=001
req_card_expiry_date=11-2020
reason_code=100
```

```
reason_code=100
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
auth_amount=100.00
auth_time==2012-08-14T134608Z
payment_token=3427075830000181552556
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

For detailed descriptions of all reply fields, see page 97.

For eCheck Payments

To process eCheck payments:

Step 1   Include the appropriate endpoint that supports the **transaction_type** sale. See page 40.

Step 2   Include the following required API fields on your payment form. For detailed descriptions of required request fields, see page 76.

```
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
profile_id=ECP0003
reference_number=1845864013783060468573616
transaction_type=sale
currency=USD
amount=100.00
locale=en
payment_token=3644783643210170561946
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2013-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

Step 3   The **payment_token** field identifies the eCheck account and retrieves the associated billing, shipping, and payment information.

Step 4   The customer is directed to the Order Review page. Depending on the settings you configured for Secure Acceptance Web/Mobile (see page 23) the customer can view or update their billing, shipping, and payment details (see page 63).

Step 5   The customer clicks **Pay**.

Below is the transaction reply.

```
req_bill_to_address_country=US
req_driver_license_state=NY
req_driver_license_number=xx-xxxxx-xxx
req_date_of_birth=19901001
decision=ACCEPT
req_bill_to_address_state=CA
signed_field_names=comma separated list of signed fields
req_payment_method=echeck
req_transaction_type=sale
req_echeck_account_type=c
signature=ZUk7d99c/yb+kidvVUbz10JtykmjOt8LMPgkllRaZR8=
req_locale=en
reason_code=100
req_echeck_account_number=xxxxx4100
req_bill_to_address_line1=1 My Apartment
req_echeck_sec_code=WEB
signed_date_time=2013-06-12T09:59:50Z
req_currency=USD
req_reference_number=77353001371031080772693
req_echeck_routing_number=xxxxx2882
transaction_id=3710311877042130706689
req_amount=100.00
message=Request was processed successfully.
echeck_debit_ref_no=1
echeck_debit_submit_time=2013-03-25T104341Z
req_profile_id=demoid
req_company_tax_id=123456789
req_transaction_uuid=bdc596506c2677b79133c9705e5cf77c
req_bill_to_surname=Smith
req_bill_to_forename=Joe
req_bill_to_email=jsmith@example.com
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
```

For detailed descriptions of all reply fields, see page 97.

For Recurring Payments

To process recurring payments:

Step 1   Include the appropriate endpoint that supports the **transaction_type** authorization or sale. See page 40.

Step 2   Include the following required API fields on your payment form. For detailed descriptions of required request fields, see page 76.

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=HPA0002
reference_number=1350029885978
payment_token=3427075830000181552556
transaction_type=authorization
amount=100.00
currency=USD
locale=en
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2013-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
```

Step 3   The **payment_token** field identifies the card and retrieves the associated billing, shipping, and payment information.

Step 4   The customer is directed to the Order Review page. Depending on the settings you configured for Secure Acceptance Web/Mobile (see page 23), the customer can view or update their billing, shipping, and payment details (see page 57).

Step 5   The customer clicks **Pay**.

Below is the transaction reply.

```
transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=demoid
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization
req_reference_number=1350029885978
req_tax_amount=2.50
req_currency=USD
req_locale=en
req_payment_method=card
req_consumer_id=1239874561
req_recurring_frequency=monthly
req_recurring_amount=25.00
req_amount=100
req_recurring_start_date=20130125
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=joesmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_card_number=xxxxxxxxxxxx4242
req_card_type=001
req_card_expiry_date=11-2020
reason_code=100
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
auth_amount=100.00
auth_time==2012-08-14T134608Z
payment_token=3427075830000181552556
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

For detailed descriptions of all reply fields, see .

For Installment Payments

To process installment payments:

Step 1 Include the appropriate endpoint that supports the **transaction_type** authorization or sale. See page 40.

Step 2 Include the following required API fields on your payment form. For detailed descriptions of required request fields, see page 76.

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=demoid
reference_number=1350029885978
payment_token=3427075830000181552556
transaction_type=authorization
amount=100.00
currency=USD
locale=en
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2013-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
```

Step 3 The **payment_token** field identifies the card and retrieves the associated billing, shipping, and payment information.

Step 4 The customer is directed to the Order Review page. Depending on the settings you configured for Secure Acceptance Web/Mobile (see page 23), the customer can view or update their billing, shipping, and payment details (see page 59).

Step 5 The customer clicks **Pay**.

Below is the transaction reply.

```
transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=demoid
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization
req_reference_number=1350029885978
req_tax_amount=2.50
req_currency=USD
req_locale=en
req_payment_method=card
req_consumer_id=1239874561
req_recurring_frequency=monthly
req_recurring_amount=25.00
req_recurring_start_date=20130125
req_recurring_number_of_installments=6
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=jsmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_card_number=xxxxxxxxxxxx4242
req_card_type=001
req_card_expiry_date=11-2020
reason_code=100
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
auth_amount=100.00
auth_time==2012-08-14T134608Z
payment_token=3427075830000181552556
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

For detailed descriptions of all reply fields, see .

Viewing Transactions in the Business Center

To view a transaction in the Business Center:

Step 1   Log in to the Business Center:

- Live transactions: https://ebc.cybersource.com
- Test transactions: https://ebctest.cybersource.com

Step 2   In the left navigation panel, choose **Transaction Search > Secure Acceptance Search**. The Secure Acceptance Search page appears. The search options are:

- Account suffix
- Cardholder's surname
- Merchant reference number
- Request ID

Step 3   Select the date range for your search. The dates can range from the current day to a maximum of 6 months past.

Step 4   Select the number of results to be displayed, from 10 to 100 transactions per page.

Step 5   Click **Search**. The Secure Acceptance Transaction Search Results page appears.

> ![Important] If a transaction has missing or invalid data, it is displayed in the Secure Acceptance Transaction Search Results page without a request ID link.

Step 6   The additional search options for each transaction are:

- Click the **request ID** link of the transaction. The Transaction Search Details page appears.

- Click the magnifying glass icon in the Log column for each transaction. The Secure Acceptance Transaction Search Details page appears. The search results are:
  - Summary information—includes the merchant ID, request ID, profile ID, the transaction decision, and the message for the transaction.
  - Request log—includes all the request API fields for the transaction.
  - Reply log—includes all the reply API fields for the transaction.

Using Decision Manager

⚠ **Important**	Contact CyberSource Customer Support to enable the Decision Manager verbose data mode for your merchant account and for detailed information regarding the device fingerprint.

Decision Manager is a hosted fraud management tool that enables you to identify legitimate orders quickly and that reduces the need to manually intervene in your order review process. You can accurately identify and review potentially risky transactions while minimizing the rejection of valid orders. With Secure Acceptance, you can use Decision Manager to screen orders containing travel data. Include the complete route or the individual legs of the trip, or both. If you include both, the value for the complete route is used.

Decision Manager also obtains data about the geographical location of a customer by linking the IP address extracted from the customer's browser to the country and the credit card. Add the customer's IP address to the **customer_ip_address** field and include it in the request.

Verbose mode returns detailed information about the order, and it returns the decision of each rule that the order triggered. Rules that are evaluated as true are returned with the appropriate results and field names, but rules that are evaluated as false are not returned.

Include the following fields in the request:
- consumer_id
- complete_route
- customer_cookies_accepted
- customer_gift_wrap
- customer_ip_address
- departure_time
- date_of_birth
- device_fingerprint_id
- journey_leg#_orig
- journey_leg#_dest
- journey_type
- merchant_defined_data#

■   returns_accepted

For detailed descriptions of all request fields, see page 76. For detailed descriptions of all the Decision Manager reply fields, see *Decision Manager Developer Guide Using the SCMP API* (PDF | HTML) or *Decision Manager Developer Guide Using the Simple Order API* (PDF | HTML).

Testing and Viewing Transactions

<table>
<tr><td>

⚠️

Important</td><td>You must create a profile in both the test and live versions of Secure Acceptance. You cannot copy a profile from the test version to the live version. You must recreate the profile.</td></tr>
</table>

Testing Transactions

To test Secure Acceptance transactions:

Step 1   Log in to the Test Business Center: https://ebctest.cybersource.com

Step 2   Create a Secure Acceptance profile. See "Creating a Web/Mobile Profile," page 17.

Step 3   Integrate with Secure Acceptance. See page 39.

<table>
<tr><td>

⚠️

Important</td><td>Include the test transactions endpoint in your HTML form. See "Rendering Secure Acceptance Web/Mobile," page 39.</td></tr>
</table>

Step 4   You may use the following test credit card numbers for transactions:

Credit Card Type	Test Account Number
Visa	4111111111111111
MasterCard	5555555555554444
American Express	378282246310005
Discover	6011111111111117
JCB	3566111111111113
Diners Club	38000000000006
Maestro International (16 digits)	6000340000009859
Maestro Domestic (16 digits)	6759180000005546

To simulate processor-specific error messages, choose your payment processor here:

http://www.cybersource.com/developers/test_and_manage/testing/legacy_scmp_api/

Viewing Transactions in the Business Center

To view a transaction in the Business Center:

Step 1   Log in to the Business Center:

- Live transactions: https://ebc.cybersource.com
- Test transactions: https://ebctest.cybersource.com

Step 2   In the left navigation panel, choose **Transaction Search > Secure Acceptance Search**. The Secure Acceptance Search page appears. The search options are:

- Account suffix
- Cardholder's surname
- Merchant reference number
- Request ID

Step 3   Select the date range for your search. The dates can range from the current day to a maximum of 6 months past.

Step 4   Select the number of results to be displayed, from 10 to 100 transactions per page.

Step 5   Click **Search**. The Secure Acceptance Transaction Search Results page appears.

> ⚠️ **Important**   If a transaction has missing or invalid data, it is displayed in the Secure Acceptance Transaction Search Results page without a request ID link.

Step 6   The additional search options for each transaction are:

- Click the **request ID** link of the transaction. The Transaction Search Details page appears.

■ Click the magnifying glass icon in the Log column for each transaction. The Secure Acceptance Transaction Search Details page appears. The search results are:

- Summary information—includes the merchant ID, request ID, profile ID, the transaction decision, and the message for the transaction.

- Request log—includes all the request API fields for the transaction.

- Reply log—includes all the reply API fields for the transaction.

API Fields

Data Type Definitions

Data Type	Permitted Characters and Formats
Alpha	Any letter from any language
AlphaNumeric	Alpha with any numeric character in any script
AlphaNumericPunctuation	Alphanumeric including ! "#$%&'()*+,-./:;=?@^_~
Amount	0123456789 including a decimal point (.)
ASCIIAlphaNumericPunctuation	Any ASCII alphanumeric character including ! "#$%&'()*+,-.\/:;=?@^_~
Date (a)	MM-YYYY
Date (b)	YYYYMMDD
Date (c)	yyyy-MM-dd HH:mm z yyyy-MM-dd hh:mm a z yyyy-MM-dd hh:mma z
Email	Valid email address
Enumerated String	Comma-separated alphanumeric string
IP	Valid IP address
ISO 8601 Date	2013-09-17T08:17:07Z
Locale	[a-z] including a hyphen (-)
Numeric	0123456789
Phone	( ),+-.*#xX1234567890
URL	Valid URL (http or https)

Request Fields

Table 4   Request Fields

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
access_key	Required for authentication with Secure Acceptance. See "Creating a Security Key," page 22.	Required by the Secure Acceptance application.	Alphanumeric String (32)
allow_payment_ token_update	Indicates whether the customer can update the billing, shipping, and payment information on the order review page. This field can contain one of the following values: ■ true: customer can update details. ■ false: customer cannot update details.	update_payment_token (R)	Enumerated String String (5)
amount	Total amount for the order. Must be greater than or equal to zero and must equal the total amount of each line item including the tax amount.	■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_payment_ token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	Amount String (15)
bill_payment	Flag that indicates a payment for a bill or for an existing contractual loan.Visa provides a Bill Payment program that enables customers to use their Visa cards to pay their bills. Possible values: ■ true: bill payment or loan payment. ■ false (default): not a bill payment or loan payment.	This field is optional.	Enumerated String String (5)
bill_to_address_city	City in the billing address. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying Billing Information Fields," page 24.	■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_payment_ token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	AlphaNumericPunctuation String (50)

Table 4   Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
bill_to_address_ country	Country code for the billing address. Use the two-character ISO country codes. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying Billing Information Fields," page 24.	▪ create_payment_token (R) ▪ authorization or sale (R) ▪ authorization,create_payment_ token (R) ▪ sale,create_payment_token (R) ▪ update_payment_token (O)	Alpha String (2)
bill_to_address_ line1	First line of the billing address. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying Billing Information Fields," page 24.	▪ create_payment_token (R) ▪ authorization or sale (R) ▪ authorization,create_payment_ token (R) ▪ sale,create_payment_token (R) ▪ update_payment_token (O)	AlphaNumericPunctuation String (60)
bill_to_address_ line2	Second line of the billing address. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying Billing Information Fields," page 24.	This field is optional.	AlphaNumericPunctuation String (60)
bill_to_address_ postal_code	Postal code for the billing address. **Note** This field is optional if the bill_ to_address_country is not U.S. or CA. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying Billing Information Fields," page 24.	▪ create_payment_token (R) ▪ authorization or sale (R) ▪ authorization,create_payment_ token (R) ▪ sale,create_payment_token (R) ▪ update_payment_token (O)	AlphaNumericPunctuation String (10)
bill_to_address_ state	State or province in the billing address. Use the two-character ISO state and province code. **Note** This field is required for U.S. and Canada. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying Billing Information Fields," page 24.	See description.	AlphaNumericPunctuation String (2 for U.S. and Canada, otherwise 60)

Table 4   Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
bill_to_company_ name	Name of the customer's company. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying Billing Information Fields," page 24.	This field is optional.	AlphaNumericPunctuation String (40)
bill_to_email	Customer email address, including the full domain name. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying Billing Information Fields," page 24.	■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_payment_ token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	Email String (255)
bill_to_forename	Customer first name. This name must be the same as the name on the card. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying Billing Information Fields," page 24.	■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_payment_ token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	AlphaNumericPunctuation String (60)
bill_to_phone	Customer phone number. CyberSource recommends that you include the country code if the order is from outside the U.S. **Note** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying Billing Information Fields," page 24. **Important** This field is optional for card payments. For eCheck payments this field is required if your processor is CyberSource ACH Service or Telecheck.	See description.	Phone String (15) String (10) if using Telecheck for echeck payments.

Table 4   Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
bill_to_surname	Customer last name. This name must be the same as the name on the card. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying Billing Information Fields," page 24.	■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	AlphaNumericPunctuation String (60)
card_cvn	Card verification number. This field can be configured as required or optional.	See description.	Numeric String (4)
card_expiry_date	Card expiration date. Format: MM-YYYY	■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	Date (a) String (7)
card_number	Card number. **Important** Use only numeric values. Make sure to include valid and well formed data for this field.	■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	Numeric String (20)

Table 4   Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
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 ■ 036: Carte Bleue ■ 037: Carta Si ■ 042: Maestro (International) ■ 043: GE Money UK card	■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_payment_ token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	Enumerated String String (3)
company_tax_id	Company's tax identifier. **Note** Contact your TeleCheck representative to find out whether this field is required or optional. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying eCheck Information Fields," page 26.	■ sale (See description) ■ create_payment_token (See description) ■ sale,create_payment_token (See description) ■ update_payment_token (See description)	AlphaNumericPunctuation String (9)

Table 4   Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
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. In your request, send either the complete route or the individual legs (**journey_leg#_orig** and **journey_ leg#_dest**). If you send all the fields, the value of **complete_route** takes precedence over that of the **journey_ leg#** fields.	This field is optional. See "Using Decision Manager," page 70.	AlphaNumericPunctuation String (255)
conditions_ accepted	Indicates whether the customer accepted the service fee amount. Possible values: ■ false: the customer did not accept. ■ true: the customer did accept.	This is a required field if service fee is enabled for the profile. See "Enabling the Service Fee," page 21.	Enumerated String String (5)
consumer_id	Identifier for the customer's account. This field is defined when you create a subscription.	■ create_payment_token (O) ■ authorization,create_payment_ token (O) ■ sale,create_payment_token (O) ■ update_payment_token (O)	AlphaNumericPunctuation String (50)
currency	Currency used for the order. For the possible values, see the ISO currency codes.	■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_payment_ token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	Alpha String (5)
customer_cookies_ accepted	Indicates whether the customer's browser accepts cookies. This field can contain one of the following values: ■ true: customer browser accepts cookies. ■ false: customer browser does not accept cookies.	This field is optional. See "Using Decision Manager," page 70.	Enumerated String String (5)

Table 4   Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
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.	This field is optional. See "Using Decision Manager," page 70.	Enumerated String String (5)
customer_ip_ address	Customer's IP address reported by your web server via socket information.	This field is optional. See "Using Decision Manager," page 70.	IP String (15)
date_of_birth	Date of birth of the customer. Use the format: YYYYMMDD. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying eCheck Information Fields," page 26.	This is an optional field.	Date (b) String (8)
debt_indicator	Flag that indicates a payment for an existing contractual loan under the VISA Debt Repayment program. Contact your processor for details and requirements. Possible formats: ■ false (default): not a loan payment ■ true: loan payment	This field is optional.	Enumerated String String (5)

Table 4   Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
departure_time	Departure date 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. **Example** ■ 2014-01-20 11:30 GMT ■ 2014-01-20 11:30 PM GMT ■ 2014-01-20 11:30pm GMT	This field is optional. See "Using Decision Manager," page 70.	Date (c) DateTime (29)
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.	This field is optional. See "Using Decision Manager," page 70.	AlphaNumericPunctuation String (88)

Table 4   Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
driver_license_number	Driver's license number of the customer. **Note** Contact your TeleCheck representative to find out whether this field is required or optional. If you include this field in your request then you must also include the **driver_license_state** field. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying eCheck Information Fields," page 26.	■ sale (See description) ■ create_payment_token (See description) ■ sale,create_payment_token (See description) ■ update_payment_token (See description)	AlphaNumericPunctuation String (30)
driver_license_state	State or province where the customer's driver's license was issued. Use the two-character *State, Province, and Territory Codes for the United States and Canada*. **Note** Contact your TeleCheck representative to find out whether this field is required or optional. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying eCheck Information Fields," page 26.	■ sale (See description) ■ create_payment_token (See description) ■ sale,create_payment_token (See description) ■ update_payment_token (See description)	Alpha String (2)
echeck_account_number	Account number. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying eCheck Information Fields," page 26.	■ sale (R) ■ create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	Numeric Non-negative integer (17)

Table 4   Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
echeck_account_ type	Account type. Possible values: ■ C: checking ■ S: savings (USD only) ■ X: corporate checking (USD only) **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying eCheck Information Fields," page 26.	■ sale (R) ■ create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	Enumerated String String (1)
echeck_check_ number	Check number. **Note** If you payment processor is TeleCheck then it is recommended to include this field. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying eCheck Information Fields," page 26.	■ sale (See description) ■ create_payment_token (See description) ■ sale,create_payment_token (See description) ■ update_payment_token (See description)	Numeric Integer (8)
echeck_routing_ number	Bank routing number. This is also called the transit number. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying eCheck Information Fields," page 26.	■ sale (R) ■ create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	Numeric Non-negative integer (9)

Table 4   Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
echeck_sec_code	**Note** If you payment processor is TeleCheck then this field is required. Possible values: ▪ CCD: Corporate cash disbursement—charge or credit against a business checking account. You can use one-time or recurring CCD transactions to transfer funds to or from a corporate entity. A standing authorization is required for recurring transactions. ▪ PPD: Prearranged payment and deposit entry—charge or credit against a personal checking or savings account. You can originate a PPD entry only when the payment and deposit terms between you and the customer are prearranged. A written authorization from the customer is required for one-time transactions and a written standing authorization is required for recurring transactions. ▪ TEL: Telephone-initiated entry— one-time charge against a personal checking or savings account. You can originate a TEL entry only when there is a business relationship between you and the customer or when the customer initiates a telephone call to you. For a TEL entry, you must obtain an authorization from the customer over the telephone. ▪ WEB: Internet-initiated entry— charge against a personal checking or savings account. You can originate a one-time or recurring WEB entry when the customer initiates the transaction over the Internet. You must obtain an authorization from the customer over the Internet.	▪ sale (See description) ▪ create_payment_token (See description) ▪ sale,create_payment_token (See description) ▪ update_payment_token (See description)	Enumerated String String (3)

Table 4   Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
ignore_avs	Ignore the results of AVS verification. Possible values: ■ true ■ false **Important** To prevent data tampering CyberSource recommends signing this field.	This field is optional.	Enumerated String String (5)
ignore_cvn	Ignore the results of CVN verification. Possible values: ■ true ■ false **Important** To prevent data tampering CyberSource recommends signing this field.	This field is optional.	Enumerated String String (5)
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 # can range from 0 to 49.	This field is optional. If you include this field, you must also include the **line_item_count** field.	Enumerated String String (255)
item_#_name	Name of the item. # can range from 0 to 49. **Note** This field is required when the **item_#_code** value is not default or relating to shipping or handling.	See description. If you include this field, you must also include the **line_item_count** field.	AlphaNumericPunctuation String (255)

Table 4   Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
item_#_quantity	Quantity of line items.	See description.	Numeric
	Required field if one of the following product codes is used:	If you include this field, you must also include the **line_item_count** field.	String (10)
	■ adult_content		
	■ coupon		
	■ electronic_good		
	■ electronic_software		
	■ gift_certificate		
	■ service		
	■ subscription		
	# can range from 0 to 49.		
	Note This field is required when the **item_#_code** value is not default or relating to shipping or handling.		
item_#_sku	Identification code for the product.	See description.	AlphaNumericPunctuation
	Required field if one of the following product codes is used:	If you include this field, you must also include the **line_item_count** field.	String (255)
	■ adult_content		
	■ coupon		
	■ electronic_good		
	■ electronic_software		
	■ gift_certificate		
	■ service		
	■ subscription		
	# can range from 0 to 49.		
item_#_tax_amount	Tax amount to apply to the line item. # can range from 0 to 49. This value cannot be negative. The tax amount and the offer amount must be in the same currency.	This field is optional.	Amount
		If you include this field, you must also include the **line_item_count** field.	String (15)
item_#_unit_price	Price of the line item. # can range from 0 to 49. This value cannot be negative.	See description.	Amount
		If you include this field, you must also include the **line_item_count** field.	String (15)
	Important You must include either this field or the **amount** field in the request.		

Table 4   Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
journey_leg#_dest	Airport code for the destination 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. In your request, send either the **complete_route** field or the individual legs (**journey_leg#_orig** and **journey_leg#_dest**). If you send all the fields, the complete route takes precedence over the individual legs.	This field is optional. See "Using Decision Manager," page 70.	Alpha String (3)
journey_leg#_orig	Airport code for the origin 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. In your request, send either the **complete_route** field or the individual legs (**journey_leg#_orig** and **journey_leg#_dest**). If you send all the fields, the complete route takes precedence over the individual legs.	This field is optional. See "Using Decision Manager," page 70.	Alpha String (3)
journey_type	Type of travel, such as: one way or round trip.	This field is optional. See "Using Decision Manager," page 70.	AlphaNumericPunctuation String (32)
line_item_count	Total number of line items. Maximum number is 50.	This field is required if you include any item fields in the request.	Numeric String (2)
locale	Indicates the language to use for customer-facing content. Possible value: en-us. See "Activating a Profile," page 38.	Required by the Secure Acceptance application.	Locale String (5)

Table 4   Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
merchant_defined_ data#	Optional fields that you can use to store information. # can range from 1 to 100. Merchant defined data fields 1 to 4 are stored against the payment token and are used for subsequent token based transactions. Merchant defined data fields 5 to 100 are passed trough to Decision Manager as part of the initial payment request and are not stored against the payment token. Merchant-defined data fields are not intended to and MUST NOT be used to capture personally identifying information. Accordingly, merchants are prohibited from capturing, obtaining, and/or transmitting any personally identifying information in or via the merchant-defined data fields. Personally identifying information includes, but is not limited to, card number, bank account number, social security number, driver's license number, state-issued identification number, passport number, and card verification numbers (CVV, CVC2, CVV2, CID, CVN). In the event CyberSource discovers that a merchant is capturing and/or transmitting personally identifying information via the merchant-defined data fields, whether or not intentionally, CyberSource WILL immediately suspend the merchant's account, which will result in a rejection of any and all transaction requests submitted by the merchant after the point of suspension.	This field is optional. See "Using Decision Manager," page 70.	AlphaNumericPunctuation String (100)
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.	This field is optional.	AlphaNumericPunctuation String (100)

Table 4   Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
merchant_secure_data4	Optional field that you can use to store information. CyberSource encrypts the data before storing it in the database.	This field is optional.	AlphaNumericPunctuation String (2000)
override_custom_cancel_page	Overrides the custom cancel page setting with your own URL.	This field is optional.	URL String (255)
override_custom_receipt_page	Overrides the custom receipt profile setting with your own URL. **Important** CyberSource recommends signing this field.	This field is optional.	URL String (255)
payment_method	Method of payment. Possible values: - card - echeck	Required by the Secure Acceptance application.	Enumerated String String (30)
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. You must be currently using CyberSource Payment Tokenization services. Populate this field with the customer subscription ID. **Important** This field is required for token-based transactions.	- authorization or sale (R) - authorization,update_payment_token (R) - sale,update_payment_token (R) - update_payment_token (R)	Numeric String (26)
payment_token_comments	Optional comments you have for the customer subscription.	This field is optional.	AlphaNumericPunctuation String (255)
payment_token_title	Name or title for the customer subscription.	This field is optional.	AlphaNumericPunctuation String (60)
profile_id	Identifies the profile to use with each transaction.	Assigned by the Secure Acceptance application.	ASCIIAlphaNumericPunctuation String (36)
recurring_amount	Payment amount for each installment or recurring subscription payment.	- create_payment_token (R) - authorization,create_payment_token (R) - sale,create_payment_token (R) - update_payment_token (O)	Amount String (15)

Table 4 Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
recurring_frequency	Frequency of payments for an installment or recurring subscription. Possible values: ■ weekly: every 7 days. ■ bi-weekly: every 2 weeks. ■ quad-weekly: every 4 weeks. ■ monthly ■ semi-monthly: twice every month (1st and 15th). ■ quarterly ■ semi-annually: twice every year. ■ annually ■ on demand	■ create_payment_token (R) ■ authorization,create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	Enumerated String String (20)
recurring_number_of_installments	Total number of payments set up for an installment subscription. Maximum values: ■ 156: weekly ■ 130: bi-weekly ■ 65: quad-weekly ■ 60: monthly ■ 24: semi-monthly ■ 20: quarterly ■ 10: semi-annually ■ 5: annually ■ 0: on demand. No recurring frequency.	■ create_payment_token (R) ■ authorization,create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	Numeric String (3)
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 defaults to the day after the date was entered.	■ create_payment_token (O) ■ authorization,create_payment_token (O) ■ sale,create_payment_token (O) ■ update_payment_token (O)	Date (b) String (8)
reference_number	Unique merchant-generated order reference or tracking number for each transaction.	Required by the Secure Acceptance application.	AlphaNumericPunctuation String (50)

Table 4   Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
returns_accepted	Indicates whether product returns are accepted. This field can contain one of the following values: ■ true ■ false	This field is optional. See "Using Decision Manager," page 70.	Enumerated String String (5)
ship_to_address_ city	City of shipping address. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying Shipping Information Fields," page 25.	This field is optional.	AlphaNumericPunctuation String (50)
ship_to_address_ country	Country code for the shipping address. Use the two-character ISO country codes. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying Shipping Information Fields," page 25.	This field is optional.	Alpha String (2)
ship_to_address_ line1	First line of shipping address. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying Shipping Information Fields," page 25.	This field is optional.	AlphaNumericPunctuation String (60)
ship_to_address_ line2	Second line of shipping address. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying Shipping Information Fields," page 25.	This field is optional.	AlphaNumericPunctuation String (60)

Table 4   Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
ship_to_address_ postal_code	Postal code for the shipping address. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying Shipping Information Fields," page 25.	This field is optional.	AlphaNumericPunctuation String (10)
ship_to_address_ state	State or province of shipping address. Use the two-character ISO state and province codes. **Important** This field is required if shipping address is U.S. and Canada. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying Shipping Information Fields," page 25.	This field is optional.	AlphaNumericPunctuation String (2)
ship_to_company_ name	Name of the company receiving the product. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying Shipping Information Fields," page 25.	This field is optional.	AlphaNumericPunctuation String (40)
ship_to_forename	First name of the person receiving the product. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying Shipping Information Fields," page 25.	This field is optional.	AlphaNumericPunctuation String (60)

Table 4   Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
ship_to_phone	Phone number of the shipping address. **Important** This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Displaying Shipping Information Fields," page 25.	This field is optional.	Phone String (15)
ship_to_surname	Last name of the person receiving the product. **Important** This can be entered by your customer during the checkout process, or you can include this in your request to Secure Acceptance. See "Displaying Shipping Information Fields," page 25.	This field is optional.	AlphaNumericPunctuation String (60)
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	This field is optional.	Enumerated String String (10)
signature	Merchant-generated Base64 signature. This is generated using the signing method for the **access_key** field supplied.	Required by the Secure Acceptance application.	AlphaNumericPunctuation
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. **Important** Your system time must be accurate to avoid payment processing errors related to the **signed_date_time** field.	Required by the Secure Acceptance application.	ISO 8601 Date String (20)

Table 4   Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
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** All request fields should be signed to prevent data tampering, with the exception of the **card_ number** field and the signature field.	Required by the Secure Acceptance application.	AlphaNumericPunctuation Variable
skip_decision_ manager	Indicates whether to skip Decision Manager. See page 70. This field can contain one of the following values: ■ true ■ false	This field is optional.	Enumerated String String (5)
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.	This field is optional.	Amount String (15)
transaction_type	The type of transactions: ■ authorization ■ authorization,create_payment_ token ■ authorization,update_payment_ token ■ sale ■ sale,create_payment_token ■ sale,update_payment_token ■ create_payment_token ■ update_payment_token	Required by the Secure Acceptance application.	Enumerated String String (60)
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.	Required by the Secure Acceptance application.	ASCIIAlphaNumericPunct uation String (50)
unsigned_field_ names	A comma-separated list of request fields that are not signed.	Required by the Secure Acceptance application.	AlphaNumericPunctuation Variable

API Reply Fields

	If configured, these API reply fields are sent back to your Merchant POST URL or email. See page 27. Your error handler should use the **decision** field to obtain the transaction result if it receives a reason code that it does not recognize.
Important	

Table 5   API Reply Fields

Field Name	Description	Data Type and Length
auth_amount	Amount that was authorized.	String (15)
auth_avs_code	AVS result code. See "AVS Codes."	String (1)
auth_avs_code_raw	AVS result code sent directly from the processor. Returned only if a value is returned by the processor.	String (10)
auth_code	Authorization code. Returned only if a value is returned by the processor.	String (7)
auth_cv_result	CVN result code. See "CVN Codes."	String (1)
auth_cv_result_raw	CVN result code sent directly from the processor. Returned only if a value is returned by the processor.	String (10)
auth_response	For most processors, this is the error message sent directly from the bank. Returned only if a value is returned by the processor.	String (10)
auth_time	Time of authorization in UTC.	String (20)
auth_trans_ref_no	Reference number that you use to reconcile your CyberSource reports with your processor reports.	String (60)
bill_trans_ref_no	Reference number that you use to reconcile your CyberSource reports with your processor reports.	String (60)
decision	The result of your request. Possible values: ■ ACCEPT ■ DECLINE ■ REVIEW ■ ERROR See "CVN Codes."	String (7)
echeck_debit_ref_no	Reference number for the transaction.	String (60)

Table 5   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
echeck_debit_submit_time	Time when the debit was requested in UTC.	Date and Time (20)
invalid_fields	Indicates which request fields were invalid.	Variable
message	Reply message from the payment gateway.	String (255)
payer_authentication_cavv	Cardholder authentication verification value (CAVV). Transaction identifier generated by the issuing bank. This field is used by the payer authentication validation service.	String (50)
payer_authentication_eci	Electronic commerce indicator (ECI). Numeric indicator returned only for Verified by Visa transactions. This field is used by payer authentication validation and enrollment services. Possible values: Enrollment Service: ■ 06: Card can be enrolled. You are protected. ■ 07: Card cannot be enrolled. You are not protected. ■ Validation Service: ■ 00: Failed authentication ■ 05: Successful authentication. ■ 06: Authentication attempted. ■ 07: Failed authentication.	String (3)
payer_authentication_proof_xml	XML element containing proof of enrollment checking. For cards not issued in the U.S. or Canada, your bank may require this data as proof of enrollment validation for any payer authentication transaction that you re-present because of a chargeback. For cards issued in the U.S. or Canada, Visa may require this data for specific merchant category codes.	String (1024)
payer_authentication_uad	MasterCard SecureCode UCAF authentication data. Returned only for MasterCard SecureCode transactions.	String (32)

Table 5   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
payer_authentication_uci	MasterCard SecureCode UCAF collection indicator. This field indicates whether authentication data is collected at your web site. Possible values: ■ 0: Authentication data was not collected and customer authentication not completed. ■ 1: Authentication data was not collected because customer authentication not completed. ■ 2: Authentication data was collected. Customer completed authentication.	String (1)
payer_authentication_xid	Transaction identifier generated by CyberSource Payer Authentication. Used to match an outgoing PA request with an incoming PA response.	String (28)
reason_code	Numeric value corresponding to the result of the credit card authorization request. See "CVN Codes."	String (5)
req_access_key	Authenticates the merchant with the application.	String (32)
req_allow_payment_token_update	Indicates whether the customer can update the billing, shipping, and payment information on the order review page. This field can contain one of the following values: true: customer can update details. false: customer cannot update details.	String (5)
req_amount	Total amount for the order. Must be greater than or equal to zero.	String (15)

Table 5   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_bill_payment	Flag that indicates a payment for a bill or for an existing contractual loan.Visa provides a Bill Payment program that enables customers to use their Visa cards to pay their bills. Possible values: true: Bill payment or loan payment. false (default): Not a bill payment or loan payment.	String (1)
req_bill_to_address_city	City in the billing address.	String (50)
req_bill_to_address_country	Country code for the billing address. Use the two-character ISO country codes.	String (2)
req_bill_to_address_line1	First line of the street address in the billing address.	String (60)
req_bill_to_address_line2	Second line of the street address in the billing address.	String (60)
req_bill_to_address_postal_code	Postal code for the billing address.	String (10)
req_bill_to_address_state	State or province in the billing address. The two-character ISO state and province code. This field is required for U.S and Canada.	String (2 for U.S. and Canada, otherwise 60)
req_bill_to_company_name	Name of the customer's company.	String (40)
req_bill_to_email	Customer email address.	String (255)
req_bill_to_forename	Customer first name.	String (60)
req_bill_to_phone	Customer phone number.	String (15)
req_bill_to_surname	Customer last name.	String (60)
req_card_expiry_date	Card expiration date.	String (7)
req_card_number	Card number.	String (20)
req_card_type	Type of card. See page 18.	String (3)
req_company_tax_id	Company's tax identifier. The the last four digits are not masked.	String (9)
req_consumer_id	Identifier for the customer account. This value is defined when creating a customer subscription.	String (50)

Table 5   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_complete_route	Concatenation of individual travel legs in the format: SFO-JFK:JFK-LHR:LHR-CDG. For a complete list of airport codes, see IATA's City Code Directory. In your request, send either the complete route field or the individual legs (**journey_leg#_orig** and **journey_leg#_dest**). If you send all the fields, the value of **complete_ route** takes precedence over that of the **journey_leg#** fields.	String (255)
req_currency	Currency used for the order. See ISO currency codes.	String (5)
req_customer_cookies_accepted	Indicates whether the customer's browser accepts cookies. This field can contain one of the following values: ▪ true: customer browser accepts cookies. ▪ false: customer browser does not accept cookies.	String (5)
req_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.	String (5)
req_customer_ip_address	Customer's IP address reported by your web server using socket information.	
req_date_of_birth	Date of birth of the customer. Use the format: YYYYMMDD.	String (8)
req_debt_indicator	Flag that indicates a payment for an existing contractual loan under the VISA Debt Repayment program. Contact your processor for details and requirements. Possible formats: ▪ false (default): not a loan payment ▪ true: loan payment	String (5)

Table 5 API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_departure_time	Departure date 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.	String (29)
req_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 sessions 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.	String (88)
req_driver_license_number	Driver's license number of the customer. The the last four digits are not masked.	String (30)
req_driver_license_state	State or province from which the customer's driver's license was issued. Use the two-character *State, Province, and Territory Codes for the United States and Canada*.	String (2)
req_echeck_account_number	Account number. This number is masked.	Non-negative integer (17)
req_echeck_account_type	Account type. Possible values: ■ C: checking ■ S: savings (USD only) ■ X: corporate checking (USD only)	String (1)
req_echeck_check_number	Check number.	Integer (8)
req_echeck_routing_number	Bank routing number. It is also called the *transit number*.	Non-negative integer (9)

Table 5   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_echeck_sec_code	The authorization method for the transaction. Possible values: ■ CCD ■ PPD ■ TEL ■ WEB	String (3)
req_ignore_avs	Ignore the results of AVS verification. Possible values: ■ true ■ false	String (5)
req_ignore_cvn	Ignore the results of CVN verification. Possible values: ■ true ■ false	String (5)
req_item_#_code	Type of product. # can range from 0 to 49.	
req_item_#_name	Name of the item. # can range from 0 to 49.	String (255)
req_item_#_quantity	Quantity of line items. # can range from 0 to 49.	String (10)
req_item_#_sku	Identification code for the product. # can range from 0 to 49.	String (255)
req_item_#_tax_amount	Tax amount to apply to the line item. # can range from 0 to 49. This value cannot be negative. The tax amount and the offer amount must be in the same currency.	String (15)
req_item_#_unit_price	Price of the line item. # can range from 0 to 49. This value cannot be negative.	String (15)

Table 5 API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_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. In your request, send either the **complete_route** field or the individual legs (**journey_leg#_orig** and **journey_leg#_dest**). If you send all the fields, the complete route takes precedence over the individual legs.	String (3)
req_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. In your request, send the **complete_route** field or the individual legs (**journey_leg#_orig** and **journey_leg#_dest**). If you send all the fields, the complete route takes precedence over the individual legs.	String (3)
req_journey_type	Type of travel, such as: one way or round trip.	String (32)
req_line_item_count	Total number of line items. Maximum amount is 50.	String (2)
req_locale	Indicates the language to use for customer content. See "Activating a Profile," page 38.	String (5)

Table 5   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_merchant_defined_data#	Optional fields that you can use to store information. # can range from 1 to 100.	String (100)
	Merchant defined data fields 1 to 4 are stored against the payment token and are used for subsequent token based transactions. Merchant defined data fields 5 to 100 are passed trough to Decision Manager as part of the initial payment request and are not stored against the payment token.	
	Merchant-defined data fields are not intended to and MUST NOT be used to capture personally identifying information. Accordingly, merchants are prohibited from capturing, obtaining, and/or transmitting any personally identifying information in or via the merchant-defined data fields. Personally identifying information includes, but is not limited to, card number, bank account number, social security number, driver's license number, state-issued identification number, passport number, and card verification numbers (CVV, CVC2, CVV2, CID, CVN). In the event CyberSource discovers that a merchant is capturing and/or transmitting personally identifying information via the merchant-defined data fields, whether or not intentionally, CyberSource WILL immediately suspend the merchant's account, which will result in a rejection of any and all transaction requests submitted by the merchant after the point of suspension.	
req_merchant_secure_data1 req_merchant_secure_data2 req_merchant_secure_data3	Optional fields that you can use to store information. CyberSource encrypts the data before storing it in the database.	String (100)

Table 5   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_merchant_secure_data4	Optional field that you can use to store information. CyberSource encrypts the data before storing it in the database.	String (2000)
req_override_custom_receipt_page	Overrides the custom receipt profile setting with your own URL.	String (255)
req_payment_method	Method of payment. Possible values: ■ card ■ echeck	String (30)
req_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. You must be currently using CyberSource Payment Tokenization services. Populate this field with the customer subscription ID.	String (26)
payment_token	Identifier for the payment details. The payment token retrieves the card data, billing information, and shipping information from the CyberSource database. This payment token super cedes the previous payment token and is returned if: the merchant is configured for a 16 digit payment token which displays the last 4 digits of the primary account number (PAN) and passes Luhn mod-10 check. See page 14. the consumer has updated the card number on their payment token. This payment token super cedes the previous payment token and should be used for subsequent transactions. You must be currently using CyberSource Payment Tokenization services. Populate this field with the customer subscription ID.	String (26)

Table 5   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_payment_token_comments	Optional comments about the customer subscription.	String (255)
req_payment_token_title	Name of the customer subscription.	String (60)
req_profile_id	Identifies the profile to use with each transaction. Assigned by the Secure Acceptance application.	String (36)
req_recurring_amount	Payment amount for each installment or recurring subscription payment.	String (15)
req_recurring_frequency	Frequency of payments for an installment or recurring subscription.	String (20)
req_recurring_number_of_ installments	Total number of payments set up for an installment subscription. Installments range from 1 to 156.	String (3)
req_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 defaults to the day after the date was entered.	String (8)
req_reference_number	Unique merchant-generated order reference or tracking number for each transaction.	String (50)
req_returns_accepted	Indicates whether product returns are accepted. This field can contain one of the following values: ▪ true ▪ false	String (5)
req_ship_to_address_city	City of shipping address.	String (50)
req_ship_to_address_country	The two-character country code.	String (2)
req_ship_to_address_line1	First line of shipping address.	String (60)
req_ship_to_address_line2	Second line of shipping address.	String (60)
req_ship_to_address_postal_code	Postal code for the shipping address.	String (10)
req_ship_to_address_state	The two-character ISO state and province code.	String (2)
req_ship_to_company_name	Name of the company receiving the product.	String (40)
req_ship_to_forename	First name of person receiving the product.	String (60)
req_ship_to_phone	Phone number for the shipping address.	String (15)

Table 5   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_ship_to_surname	Last name of person receiving the product.	String (60)
req_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	String (10)
req_skip_decision_manager	Indicates whether to skip Decision Manager. See page 70. This field can contain one of the following values: ■ true ■ false	String (5)
req_tax_amount	Total tax to apply to the product.	String (15)
req_transaction_type	The type of transaction requested.	String (60)
req_transaction_uuid	Unique merchant-generated identifier. Include with the **access_key** field for each transaction.	String (50)
required_fields	Indicates which of the request fields were required but not provided.	Variable
service_fee_amount	The service fee amount for the order.	String (15)
signature	The Base64 signature returned by the server.	String (44)
signed_date_time	The date and time of when the signature was generated by the server. UTC date and time format: 2011-12-31T11:59:59Z	String (20)
signed_field_names	A comma-separated list of response data that was signed by the server. All fields within this list should be used to generate a signature that can then be compared to the response signature to verify the response.	Variable

Table 5   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
transaction_id	The transaction identifier returned from the payment gateway.	String (26)

Reason Codes

The **reasonCode** field contains additional data regarding the decision response of the transaction. Depending on the decision of a transaction request, the CyberSource's default receipt page or your receipt page is displayed to the customer. Both you and your customer may also receive an email receipt. See "Configuring Notifications," page 27.

Table 6   Reason Codes

Reason Code	Description
100	Successful transaction.
102	One or more fields in the request contain invalid data.
	Possible action: see the reply fields **invalid_fields** for which fields are invalid. Resend the request with the correct information.
104	The **access_key** and **transaction_uuid** fields for this authorization request matches the **access_key** and **transaction_uuid** of another authorization request that you sent within the past 15 minutes.
	Possible action: resend the request with an unique **access_key** and **transaction_uuid** fields.
110	Only a partial amount was approved.
200	The authorization request was approved by the issuing bank but declined by CyberSource because it did not pass the Address Verification System (AVS) check.
	Possible action: you can capture the authorization, but consider reviewing the order for the possibility of fraud.
201	The issuing bank has questions about the request. You do not receive an authorization code programmatically, but you might receive one verbally by calling the processor.
	Possible action: call your processor to possibly receive a verbal authorization. For contact phone numbers, refer to your merchant bank information.
202	Expired card. You might also receive this value if the expiration date you provided does not match the date the issuing bank has on file.
	Possible action: request a different card or other form of payment.
203	General decline of the card. No other information was provided by the issuing bank.
	Possible action: request a different card or other form of payment.

Table 6   Reason Codes (Continued)

Reason Code	Description
204	Insufficient funds in the account.
	Possible action: request a different card or other form of payment.
205	Stolen or lost card.
	Possible action: review this transaction manually to ensure that you submitted the correct information.
207	Issuing bank unavailable.
	Possible action: wait a few minutes and resend the request.
208	Inactive card or card not authorized for card-not-present transactions.
	Possible action: request a different card or other form of payment.
210	The card has reached the credit limit.
	Possible action: request a different card or other form of payment.
211	Invalid CVN.
	Possible action: request a different card or other form of payment.
221	The customer matched an entry on the processor's negative file.
	Possible action: review the order and contact the payment processor.
222	Account frozen.
230	The authorization request was approved by the issuing bank but declined by CyberSource because it did not pass the CVN check.
	Possible action: you can capture the authorization, but consider reviewing the order for the possibility of fraud.
231	Invalid account number.
	Possible action: request a different card or other form of payment.
232	The card type is not accepted by the payment processor.
	Possible action: contact your merchant bank to confirm that your account is set up to receive the card in question.
233	General decline by the processor.
	Possible action: request a different card or other form of payment.
234	There is a problem with the information in your CyberSource account.
	Possible action: do not resend the request. Contact CyberSource Customer Support to correct the information in your account.
236	Processor failure.
	Possible action: wait a few minutes and resend the request.
240	The card type sent is invalid or does not correlate with the credit card number.
	Possible action: confirm that the card type correlates with the credit card number specified in the request, then resend the request.

Table 6   Reason Codes (Continued)

Reason Code	Description
475	The cardholder is enrolled for payer authentication. Possible action: authenticate cardholder before proceeding.
476	Payer authentication could not be authenticated.
520	The authorization request was approved by the issuing bank but declined by CyberSource based on your legacy Smart Authorization settings. Possible action: review the authorization request.

Table 7   Types of Notifications

Decision	Description	Type of Notification	CyberSource Hosted Page
ACCEPT	Successful Transaction. Reason codes 100 and 110.	▪ Customer receipt page ▪ Customer receipt email ▪ Merchant POST URL ▪ Merchant receipt email	Accept
REVIEW	Transaction was declined. Please review payment details. See reason codes 200, 201, 230, and 520.	▪ Customer receipt page ▪ Merchant receipt email	Accept
DECLINE	Transaction was declined. See reason codes 102, 200, 202, 203, 204, 205, 207, 208, 210, 211, 221, 222, 230, 231, 232, 233, 234, 236, 240, 475, and 476.	▪ Customer receipt page [1] ▪ Merchant POST URL [1] ▪ Merchant receipt email [1]	Decline
ERROR	Access denied, page not found, or internal server error. See reason codes 102 and 104.	▪ Customer receipt page ▪ Merchant POST URL	Error
CANCEL	The consumer did not accept the service fee conditions. The consumer cancelled the transaction.	▪ Customer receipt page ▪ Merchant POST URL	Cancel

1 The customer receives the decline message, "Your order was declined. Please verify your information." before the merchant receives the decline message. The decline message relates to either the processor declining the transaction or a payment processing error, or the customer entered their 3D Secure credentials incorrectly.

AVS Codes

An issuing bank uses the AVS code to confirm that your customer is providing the correct billing address. If the customer provides incorrect data, the transaction might be fraudulent. The international and U.S. domestic Address Verification Service (AVS) codes are the Visa standard AVS codes, except for codes 1 and 2, which are CyberSource AVS codes. The standard AVS return codes for other types of credit cards (including American Express cards) are mapped to the Visa standard codes. You receive the code in the **auth_avs_code** reply field. See .

⚠️ **Important**	When you populate billing street address 1 and billing street address 2, CyberSource through VisaNet concatenates the two values. If the concatenated value exceeds 40 characters, CyberSource through VisaNet truncates the value at 40 characters before sending it to Visa and the issuing bank. Truncating this value affects AVS results and therefore might impact risk decisions and chargebacks.

International AVS Codes

These codes are returned only for Visa cards issued outside the U.S.

Table 8   International AVS Codes

Code	Response	Description
B	Partial match	Street address matches, but postal code is not verified.
C	No match	Street address and postal code do not match.
D & M	Match	Street address and postal code match.
I	No match	Address not verified.
P	Partial match	Postal code matches, but street address not verified.

U.S. Domestic AVS Codes

Table 9   U.S. Domestic AVS Codes

Code	Response	Description
A	Partial match	Street address matches, but 5-digit and 9-digit postal codes do not match.
B	Partial match	Street address matches, but postal code is not verified.
C	No match	Street address and postal code do not match.
D & M	Match	Street address and postal code match.
E	Invalid	AVS data is invalid or AVS is not allowed for this card type.
F	Partial match	Card member's name does not match, but billing postal code matches. Returned only for the American Express card type.

Table 9   U.S. Domestic AVS Codes (Continued)

Code	Response	Description
H	Partial match	Card member's name does not match, but street address and postal code match. Returned only for the American Express card type.
I	No match	Address not verified.
J	Match	Card member's name, billing address, and postal code match. Shipping information verified and chargeback protection guaranteed through the Fraud Protection Program. Returned only if you are signed up to use AAV+ with the American Express Phoenix processor.
K	Partial match	Card member's name matches, but billing address and billing postal code do not match. Returned only for the American Express card type.
L	Partial match	Card member's name and billing postal code match, but billing address does not match. Returned only for the American Express card type.
M	Match	Street address and postal code match.
N	No match	One of the following: ■ Street address and postal code do not match. ■ Card member's name, street address, and postal code do not match. Returned only for the American Express card type.
O	Partial match	Card member's name and billing address match, but billing postal code does not match. Returned only for the American Express card type.
P	Partial match	Postal code matches, but street address not verified.
Q	Match	Card member's name, billing address, and postal code match. Shipping information verified but chargeback protection not guaranteed (Standard program). Returned only if you are signed to use AAV+ with the American Express Phoenix processor.
R	System unavailable	System unavailable.
S	Not supported	U.S.-issuing bank does not support AVS.
T	Partial match	Card member's name does not match, but street address matches. Returned only for the American Express card type.
U	System unavailable	Address information unavailable for one of these reasons: ■ The U.S. bank does not support non-U.S. AVS. ■ The AVS in a U.S. bank is not functioning properly.
V	Match	Card member's name, billing address, and billing postal code match. Returned only for the American Express card type.
W	Partial match	Street address does not match, but 9-digit postal code matches.
X	Match	Street address and 9-digit postal code match.
Y	Match	Street address and 5-digit postal code match.

Table 9   U.S. Domestic AVS Codes (Continued)

Code	Response	Description
Z	Partial match	Street address does not match, but 5-digit postal code matches.
1	Not supported	AVS is not supported for this processor or card type.
2	Unrecognized	The processor returned an unrecognized value for the AVS response.
3	Match	Address is confirmed. Returned only for PayPal Express Checkout.
4	No match	Address is not confirmed. Returned only for PayPal Express Checkout.

CVN Codes

Table 10   CVN Codes

Code	Description
D	The transaction was considered to be suspicious by the issuing bank.
I	The CVN failed the processor's data validation.
M	The CVN matched.
N	The CVN did not match.
P	The CVN was not processed by the processor for an unspecified reason.
S	The CVN is on the card but was not included in the request.
U	Card verification is not supported by the issuing bank.
X	Card verification is not supported by the card association.
1	Card verification is not supported for this processor or card type.
2	An unrecognized result code was returned by the processor for the card verification response.
3	No result code was returned by the processor.

iFrame Implementation

> **⚠ Important**
>
> There are a number of differences that you need to take in to account between a standard Web/Mobile implementation and an iFrame implementation. These differences relate to how Internet Explorer and Safari handle third-party content. Failure to address these differences can result in payment failures for customers using these browsers.

You must select the single page checkout option (see) for Web/Mobile iFrame implementation.

> **✎ Note**
>
> The total amount value and the transaction cancel button are not displayed within the iFrame. Any settings that you configured for the total amount figure (see) are ignored.

> **⚠ Important**
>
> CyberSource recommends that you manage the total amount value on your web site containing the inline frame. You must also provide customers the cancel order functionality on your web site containing the inline frame.

Clickjacking Prevention

Clickjacking (also known as user-interface redress attack and iframe overlay) is used by attackers to trick users into clicking on a transparent layer (with malicious code) above legitimate buttons or clickable content for a site. To prevent clickjacking, you must prevent third-party sites from including your web site within an iFrame.

While no security remediation can prevent every clickjacking, these are the minimum measures you must use for modern web browsers:

- Set HTTP response header X-FRAME_OPTIONS to either "DENY" or "SAMEORGIN".
- Provide frame-busting scripts to ensure your page is always the top level window or disabling code for older browsers that do not support X-FRAME_OPTIONS.

	Do not use double framing on the same page where the Web/Mobile iFrame implementation is used.
Note	

You are required to implement the recommended prevention techniques in your web site. See the OWASP clickjacking page and the Cross-site scripting page for up to date information.

Web application protections for Cross-site Scripting (XSS), Cross-site Request Forgery (CSRF), etc. must also be incorporated.

- For XSS protection, you need to implement comprehensive input validation and the OWASP recommended security encoding library to do output encoding on your website.

- For CSRF protection, you are strongly encouraged to use a synchronized token pattern. This measure requires generating a randomized token associating with the user session. The token will be inserted whenever a HTTP request is sent to the server. Your server application will verify if the token from the request is the same as the one associated with the user session.

Endpoints

For iFrame transaction endpoints and supported transaction types for each endpoint, see "Endpoints and Transaction Types," page 40.