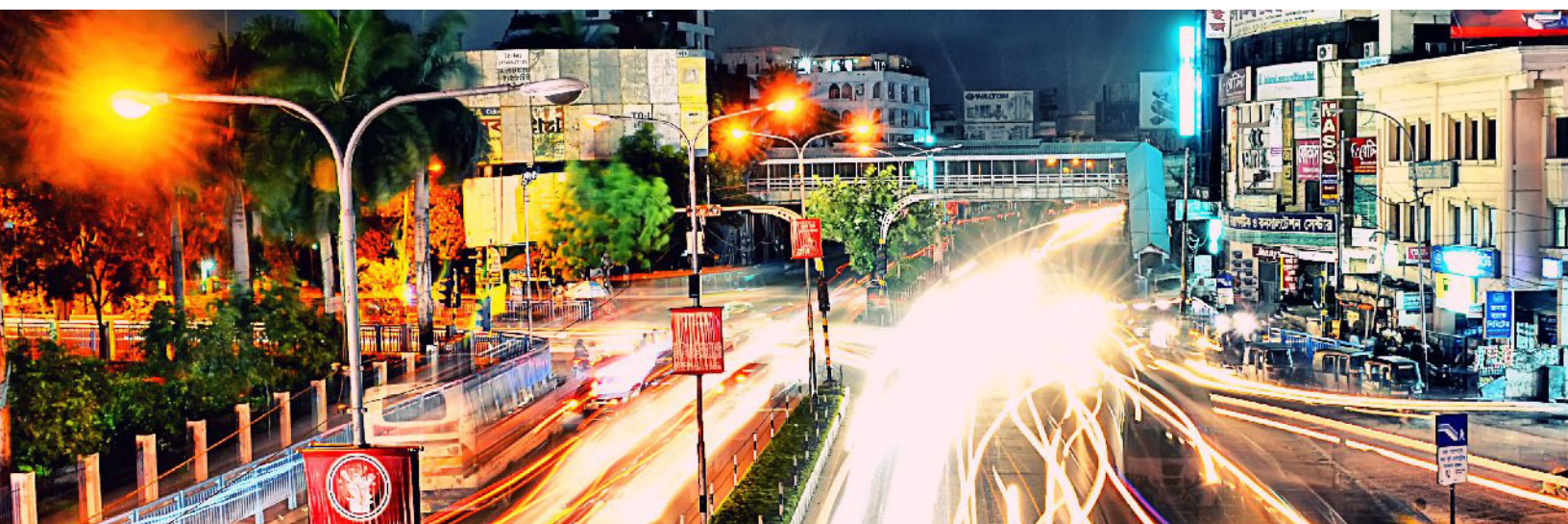


Secure Acceptance Hosted Checkout

Integration Guide



CyberSource®
A Visa Solution

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:

<http://www.cybersource.com/support>

Copyright

© 2020. CyberSource Corporation. All rights reserved. CyberSource Corporation ("CyberSource") furnishes this document and the software described in this document under the applicable agreement between the reader of this document ("You") and CyberSource ("Agreement"). You may use this document and/or software only in accordance with the terms of the Agreement. Except as expressly set forth in the Agreement, the information contained in this document is subject to change without notice and therefore should not be interpreted in any way as a guarantee or warranty by CyberSource. CyberSource assumes no responsibility or liability for any errors that may appear in this document. The copyrighted software that accompanies this document is licensed to You for use only in strict accordance with the Agreement. You should read the Agreement carefully before using the software. Except as permitted by the Agreement, You may not reproduce any part of this document, store this document in a retrieval system, or transmit this document, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written consent of CyberSource.

Restricted Rights Legends

For Government or defense agencies: Use, duplication, or disclosure by the Government or defense agencies is subject to restrictions as set forth the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and in similar clauses in the FAR and NASA FAR Supplement.

For civilian agencies: Use, reproduction, or disclosure is subject to restrictions set forth in subparagraphs (a) through (d) of the Commercial Computer Software Restricted Rights clause at 52.227-19 and the limitations set forth in CyberSource Corporation's standard commercial agreement for this software. Unpublished rights reserved under the copyright laws of the United States.

Trademarks

Authorize.Net, eCheck.Net, and The Power of Payment are registered trademarks of CyberSource Corporation. CyberSource, CyberSource Payment Manager, CyberSource Risk Manager, CyberSource Decision Manager, and CyberSource Connect are trademarks and/or service marks of CyberSource Corporation. Visa, Visa International, CyberSource, the Visa logo, and the CyberSource logo are the registered trademarks of Visa International in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Revision: July 2020

Contents

[Recent Revisions to This Document](#) 7

[About This Guide](#) 8

[Audience and Purpose](#) 8

[Web Site Requirements](#) 8

[Conventions](#) 9

[Important and Warning Statements](#) 9

[Text and Command Conventions](#) 9

[Related Documents](#) 10

[Customer Support](#) 11

Chapter 1 [Secure Acceptance Hosted Checkout](#) 12

[Required Browsers](#) 13

[Secure Acceptance Profile](#) 13

[Secure Acceptance Transaction Flow](#) 14

[Payment Tokens](#) 15

[Tokens That Represent a Card or Bank Account Only](#) 16

[One-click Checkout](#) 16

[Subscription Payments](#) 16

[Level II and III Data](#) 17

[BIN Lookup](#) 18

[Requirement](#) 18

[Request BIN Lookup](#) 18

[Payouts Payment Tokens](#) 18

[Go-Live with Secure Acceptance](#) 19

Chapter 2	Payment Configuration	20
	Create a Hosted Checkout Profile	20
	Configure Payment Methods	21
	Add Card Types and Currencies	22
	Enable Payer Authentication	23
	Enable Automatic Authorization Reversals	24
	Enable eChecks	25
	Enable Visa Checkout or Visa SRC	26
	Enable PayPal Express Checkout	27
	Create a Security Key	29
	Configure the Checkout	30
	Configure the Payment Form	30
	Display Billing Information Fields	31
	Display Shipping Information Fields	32
	Display eCheck Information	33
	Customize Order Review Details	34
	Receive Merchant Notifications	35
	Send a Customer Receipt	36
	Customer Notification Details	36
	Display a Response Page	37
	Display a Transaction Response Page	38
	CyberSource Hosted Response Page	38
	Display a Custom Hosted Response Page	38
	Custom Cancel Response Page	39
	CyberSource Hosted Response Page	39
	Custom Cancel Response Page	39
	Customize the Checkout Appearance	40
	Localize the Checkout Languages	44
	Activate a Profile	46
	Additional Profile Options	46
	Samples in Scripting Languages	47
	Sample Transaction Process Using JSP	47

Chapter 3	Portfolio Management for Resellers	48
	Create a Hosted Checkout Profile	48
	Configure Payment Methods	49
	Add Card Types and Currencies	50
	Enable Payer Authentication	51
	Enable Automatic Authorization Reversals	52
	Enable eChecks	53
	Enable Visa Checkout or Visa SRC	54
	Enable PayPal Express Checkout	55
	Enable the Service Fee	56
	Create a Security Key	57
	Configure the Checkout	58
	Configure the Payment Form	58
	Display and Edit Billing Information Fields	59
	Display and Edit Shipping Information Fields	60
	Display and Edit eCheck Information	61
	Display and Edit Order Review Details	62
	Receive Merchant Notifications	63
	Send a Customer Receipt	64
	Customer Notification Details	64
	Display a Response Page	65
	Display a Transaction Response Page	66
	CyberSource Hosted Response Page	66
	Display a Custom Hosted Response Page	66
	Display a Custom Cancel Response Page	67
	CyberSource Hosted Response Page	67
	Custom Cancel Response Page	67
	Customize the Checkout Appearance	68
	Activate a Profile	72
	Additional Profile Options	73

Chapter 4	Payment Transactions	74
	Endpoints and Transaction Types	74
	Required Signed Fields	76
	Create a Payment Token	76
	Payment Card	76
	eCheck	79
	Payment Token Transaction	81
	One-Click	81
	eCheck	83
	Recurring Payments	85

Installment Payments	87
Update a Payment Token	89
Payment Card	89
eCheck	91

Chapter 5 Decision Manager 93

Chapter 6	Test and View Transactions	95
	Testing Transactions	95
	View Transactions in the Business Center	96

Appendix A	API Fields	97
	Data Type Definitions	97
	Request Fields	98
	Reply Fields	132
	Reason Codes	168
	Types of Notifications	171
	AVS Codes	172
	International AVS Codes	172
	U.S. Domestic AVS Codes	173
	CVN Codes	175

Appendix B American Express SafeKey Response Codes 176

Appendix C	Iframe Implementation	177
	Clickjacking Prevention	178
	Endpoints	178

Appendix D Visa Secure Response Codes 179

Recent Revisions to This Document

Release	Changes
July 2020	Added endpoints and Business Center URLs for transactions in India.
February 2020	Updated Example 12, "Request: Create a Payment Token for Installment Payments," on page 87 and Example 12, "Request: Create a Payment Token for Installment Payments," on page 87 .
January 2020	Added Visa Secure Remote Commerce (SRC) wherever Visa Checkout occurs.
October 2019	Updated "Related Documents," page 10 . Updated data types for the reply fields auth_trans_ref_no, page 136 , bill_trans_ref_no, page 136 , and echeck_debit_ref_no, page 141 .
August 2019	Added required browsers. See "Required Browsers," page 13 . Updated Business Center procedures in the following chapters: <ul style="list-style-type: none"> ■ Chapter 2, "Payment Configuration," on page 20. (Previously called <i>Chapter 2, "Creating a Hosted Checkout Profile"</i> and <i>Chapter 3, "Updating a Secure Acceptance Profile"</i>) ■ Chapter 6, "Test and View Transactions," on page 95. Added a new chapter for resellers. See Chapter 3, "Portfolio Management for Resellers," on page 48 . Updated the description for the reason_code reply field. See reason_code, page 150 . Added an Important statement about iframes. See Appendix C, "Iframe Implementation," on page 177 .
July 2019	Updated transaction flow. See "Secure Acceptance Transaction Flow," page 14 . Added list of required signed fields. See "Required Signed Fields," page 76 . Added the override_customer_utc_offset request field. See override_customer_utc_offset, page 118 . Updated the payment_method field. See payment_method, page 120 .

About This Guide

Audience and Purpose

This guide is written for merchants who want to accept payments using Secure Acceptance Hosted Checkout and who do not want to handle or store sensitive payment information on their own servers.

Using Secure Acceptance Hosted Checkout 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.

Web Site Requirements

Your web site must meet the following requirements:

- It must have a shopping-cart, customer order creation software, or an application for initiating disbursements to send funds to payment accounts.
- It must contain product pages in one of the supported scripting languages. See ["Sample Transaction Process Using JSP," page 47](#).
- The IT infrastructure must be Public Key Infrastructure (PKI) enabled to use SSL-based form POST submissions.
- The IT infrastructure must be capable of digitally signing customer data prior to submission to Secure Acceptance Hosted Checkout.

Conventions

Important and Warning Statements



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



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.

Text and Command Conventions

Convention	Usage
Bold	<ul style="list-style-type: none">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.
Screen text	<ul style="list-style-type: none">Code examples and samples.Text that you enter in an API environment; for example: Set the transaction_type field to <code>create_payment_token</code>.

Related Documents

Refer to the Support Center for complete CyberSource technical documentation:

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

Table 1 Related Documents

Subject	Description
Business Center	<i>Business Center User Guide</i> (PDF HTML)—describes how to use the Business Center.
Decision Manager	The following documents describe how to integrate and use the Decision Manager services. <ul style="list-style-type: none"> ■ <i>Decision Manager Using the SCMP API Developer Guide</i> (PDF HTML) ■ <i>Decision Manager Using the Simple Order API Developer Guide</i> (PDF HTML)
Electronic checks	The following documents describe how to integrate and use the electronic check services: <ul style="list-style-type: none"> ■ <i>Electronic Check Services Using the SCMP API</i> (PDF HTML) ■ <i>Electronic Check Services Using the Simple Order API</i> (PDF HTML)
Level II and Level III	<i>Level II and Level III Processing Using Secure Acceptance</i> (PDF HTML)—describes each Level II and Level III 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: <ul style="list-style-type: none"> ■ <i>Payer Authentication Using the SCMP API</i> (PDF HTML) ■ <i>Payer Authentication Using the Simple Order API</i> (PDF HTML)
Payment cards	The following documents describe how to integrate payment card processing into an order management system: <ul style="list-style-type: none"> ■ <i>Credit Card Services Using the SCMP API</i> (PDF HTML) ■ <i>Credit Card Services Using the Simple Order API</i> (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.
Payouts	The following documents describe how to integrate and use the Payouts functionality: <ul style="list-style-type: none"> ■ <i>Payouts Using the SCMP API</i> (PDF HTML) ■ <i>Payouts Using the Simple Order API</i> (PDF HTML)
PayPal Express Checkout	The following documents describe how to integrate and use the PayPal Express Checkout services: <ul style="list-style-type: none"> ■ <i>PayPal Express Checkout Services Using the SCMP API</i> (PDF HTML) ■ <i>PayPal Express Checkout Services Using the Simple Order API</i> (PDF HTML).

Table 1 Related Documents (Continued)

Subject	Description
Recurring Billing	<p>The following documents describe how to create customer subscriptions and use payment tokens for recurring and installment payments:</p> <ul style="list-style-type: none"> ■ <i>Recurring Billing Using the Business Center</i> (PDF HTML) ■ <i>Recurring Billing Using the SCMP API</i> (PDF HTML) ■ <i>Recurring Billing Using the Simple Order API</i> (PDF HTML)
Reporting	<p><i>Business Center Reporting User Guide</i> (PDF HTML)—describes how to view and configure custom reports in the Business Center.</p>
Secure Acceptance	<p>The following documents describe how to integrate and use the Secure Acceptance Checkout API, along with processing a transaction with the service fee included:</p> <ul style="list-style-type: none"> ■ <i>Secure Acceptance Checkout API Integration Guide</i> (PDF HTML) ■ <i>Secure Acceptance Checkout API Service Fee Guide</i> (PDF)
Third-party tokens	<p>The following documents describe how to create tokens with a third-party provider and are available from CyberSource Customer Support:</p> <ul style="list-style-type: none"> ■ <i>Tokenization with a Third-Party Provider Using the SCMP API</i> ■ <i>Tokenization with a Third-Party Provider Using the Simple Order API</i>
Token Management Service	<p>The following documents describe how to integrate and use the token management service:</p> <ul style="list-style-type: none"> ■ <i>Token Management Service Using the SCMP API</i> (PDF HTML) ■ <i>Token Management Service Using the Simple Order API</i> (PDF HTML)
Visa Checkout	<p><i>Getting Started with Visa Checkout</i> (PDF HTML)—describes how to enroll in Visa Checkout and create a Visa Checkout profile.</p>
Visa Secure Remote Commerce	<p><i>Getting Started with Visa Secure Remote Commerce</i> (PDF HTML)—describes how to enroll in Visa Secure Remote Commerce and create a Visa Checkout profile.</p>

Customer Support

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

<http://www.cybersource.com/support>

Secure Acceptance Hosted Checkout

CyberSource Secure Acceptance Hosted Checkout is your secure hosted customer checkout experience. It consists of securely managed payment forms or as a single page payment form for capturing payment card data, 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 capturing and managing payment card data to Secure Acceptance, which is designed to accept card payments.



Secure Acceptance is designed to process transaction requests directly from the customer browser so that sensitive payment data does not pass through your servers. If you do intend to send payment data from your servers, use the [SOAP Toolkit API](#) or the [Simple Order API](#). Sending server-side payments using Secure Acceptance incurs unnecessary overhead and could result in the suspension of your merchant account and subsequent failure of transactions.

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 render the Secure Acceptance Hosted Checkout and immediately process card transactions (see "[Samples in Scripting Languages](#)," page 47). 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 14.
- 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 "[View Transactions in the Business Center](#)," page 96).

Required Browsers

You must use one of these browsers in order to ensure that the Secure Acceptance checkout flow is fast and secure:

Desktop browsers:

- IE 10 or later
- Edge 13 or later
- Firefox 42 or later
- Chrome 48 or later
- Safari 7.1 or later
- Opera 37 or later

Mobile browsers:

- iOS Safari 7.1 or later
- Android Browser 4.4 or later
- Chrome Mobile 48 or later

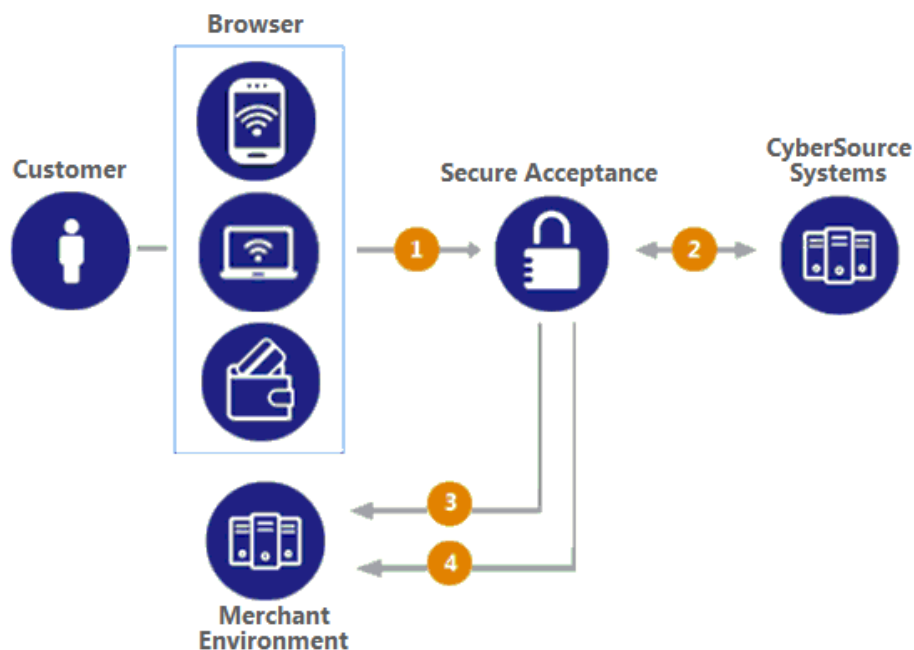
Secure Acceptance Profile

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 ["Customize the Checkout Appearance," page 40](#)). 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 ["Configure the Checkout," page 30](#)) to the customer as well as configure the appearance and branding, payment options, languages, and customer notifications.

Secure Acceptance Transaction Flow

The Secure Acceptance Hosted Checkout transaction flow is illustrated in [Figure 1](#) and described below.

Figure 1 Secure Acceptance Hosted Checkout Transaction Flow



- 1 The customer clicks the Pay button on your web site, which triggers an HTTPS POST that directs the customer to the hosted Secure Acceptance Hosted Checkout page that you configured in the Business Center. The HTTPS POST includes the signature and signed data fields containing the order information.

Secure Acceptance Hosted Checkout works best with JavaScript and cookies enabled in the customer browser.



Your system should sign only Secure Acceptance request fields. To prevent malicious actors from impersonating CyberSource, do not allow unauthorized access to the signing function.

- 2 Secure Acceptance verifies the signature to ensure that the order details were not amended or tampered with and displays the Secure Acceptance Hosted Checkout page. The customer enters and submits payment details and/or their billing and shipping information. The customer confirms the payment, and the transaction is processed.
- 3 CyberSource recommends that you configure a custom receipt page in the Business Center (see ["Receive Merchant Notifications," page 35](#)) so that the signed transaction response is sent back to your merchant server through the browser. You must validate the

reply signature to confirm that the reply data was not amended or tampered with. Secure Acceptance can also display a standard receipt page to your customer, and you can verify the result of the transaction using the Business Center search or the standard CyberSource reports.



If the reply signature in the reply field does not match the signature calculated based on the reply data, treat the POST as malicious and disregard it.

Secure Acceptance signs every response field. Ignore any reply fields in the POST that are not in the **signed_fields** field.

- 4 CyberSource recommends implementing the merchant POST URL notification (see ["Receive Merchant Notifications," page 35](#)) as a backup means of determining the transaction result. This method does not rely on your customer's browser. You receive the transaction result even if your customer lost connection after confirming the payment.

If the transaction type is sale, it is immediately submitted for settlement. If the transaction type is authorization, use the CyberSource Simple Order API to submit a capture request when goods are shipped.

Payment Tokens



Contact CyberSource Customer Support to activate your merchant account for Token Management Services. You cannot use payment tokens until your account is activated and you have enabled payment tokens for Secure Acceptance (see ["Create a Hosted Checkout Profile," page 20](#)).

Payment tokens are unique identifiers that replace sensitive payment 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. Card data stored with CyberSource is automatically updated by participating banks, thereby reducing payment failures. See the *Account Updater User Guide* ([PDF](#) | [HTML](#)).

The payment token replaces the card or electronic check bank account number, and optionally the associated billing, shipping, and card information. No sensitive card information is stored on your servers, thereby reducing your PCI DSS obligations.

For more information about tokens, see ["Related Documents," page 10](#).

Tokens That Represent a Card or Bank Account Only

Instrument identifier tokens created using the Token Management Service (TMS) and third-party tokens represent a payment card number or bank account number. The same card number or bank account number sent in multiple token creation calls results in the same payment token being returned. TMS instrument identifier and third-party tokens cannot be updated. If your merchant account is configured for one of these token types, you receive an error if you attempt to update a token.

When using Secure Acceptance with tokens that represent only the card number or bank account, you must include associated data, such as expiration dates and billing address data, in your transaction request.

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, they must create a payment token during the first transaction on the merchant web site. See ["Payment Token Transaction," page 81](#). 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 ["Endpoints and Transaction Types," page 74](#).

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 ["View Transactions in the Business Center," page 96](#).

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.

Table 2 Types of Subscriptions

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 "Recurring Payments," page 85 .
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 "Installment Payments," page 87 .

Level II and III Data

Secure Acceptance supports Level II and III data. Level II cards, also known as *Type II cards*, provide customers with additional information on their payment 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 payment 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 field, see *Level II and Level III Processing Using Secure Acceptance* ([PDF](#) | [HTML](#)). This guide also describes how to request sale and capture transactions.

BIN Lookup

The bank identification number (BIN) lookup service provides information about a payment card account based on first six digits of the account number. The information provided can be the country in which the card was issued, the domestic currency, and whether the card qualifies for the Payouts service. See ["Payouts Payment Tokens," page 18](#).

Requirement

To enable BIN lookup, contact CyberSource Customer Support to have your account configured for this feature.

Request BIN Lookup

You can request the BIN Lookup service with Secure Acceptance in the General Settings of your Secure Acceptance profile in the Business Center. You can set the BIN Lookup service to one of two modes:

- Free: verifies that the card is eligible for sending funds through the Payouts service.
- Paid: premium service that returns all data available for the BIN.

The BIN Lookup response is sent to the merchant notifications URL and email. See ["Receive Merchant Notifications," page 35](#). For security reasons it is not sent to the receipt URL.

The BIN Lookup results are detailed in the reply fields with the **bin_lookup** prefix. See ["Reply Fields," page 132](#).

Payouts Payment Tokens

Use Secure Acceptance to create a payment token that can be used with the Payouts API or batch submissions.

To create a payment token for Payouts:

- Step 1** Create a Secure Acceptance Profile and define your checkout page. See [Chapter 2, "Payment Configuration," on page 20](#) or [Chapter 3, "Portfolio Management for Resellers," on page 48](#).
- Step 2** Enable BIN Lookup to verify that the card used is eligible for sending funds using the Payouts service. See ["BIN Lookup," page 18](#).

Step 3 For transaction processing, create a payment token. See ["Create a Payment Token," page 76](#).

Step 4 Set the Payouts subscription ID field to the value of the payment token.

See *Payouts Using the Simple Order API* ([PDF](#) | [HTML](#)) or *Payouts Using the SCMP API* ([PDF](#) | [HTML](#)).

Go-Live with Secure Acceptance

CyberSource recommends that you submit all banking information and required integration services before going live. Doing so will speed up your merchant account configuration.

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 can require three days to complete. No Go-Live implementations occur on Fridays.

Payment Configuration

Create a Hosted Checkout Profile



Contact CyberSource Customer Support to enable your account for Secure Acceptance. You must activate a profile in order to use it (see "[Activate a Profile](#)," page 46).

To create a Hosted Checkout profile:

- Step 1** Log in to the Business Center:
- Live transactions: <https://ebc2.cybersource.com/ebc2/>
 - Live transactions in India: <https://ebc2.in.cybersource.com/ebc2/>
 - Test transactions: <https://ebctest.cybersource.com/ebc2/>
- Step 2** In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
- Step 3** Click **New Profile**. The Create Profile page appears.
- Step 4** Enter or verify the following profile details.

Table 3 Profile Details

Profile Detail	Description
Profile Name	The Secure Acceptance profile name is required and cannot exceed 40 alphanumeric characters.
Profile Description	The profile description cannot exceed 255 characters.
Integration Method	Check Hosted Checkout .
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	

Table 3 Profile Details (Continued)

Profile Detail	Description
Payment Tokenization	Check Payment Tokenization . For more information, see Chapter 4, "Payment Transactions," on page 74 .
Decision Manager	Check Decision Manager . For more information, see Chapter 5, "Decision Manager," on page 93 .
Verbose Data	Check Verbose Data . For more information, see Chapter 5, "Decision Manager," on page 93 .
Generate Device Fingerprint	Check Generate Device Fingerprint . For more information, see Chapter 5, "Decision Manager," on page 93 .
BIN Lookup	Choose Perform checks on card eligibility for Original Credit Transfer (OCT) for Payouts or Enable full BIN Lookup service . For more information, see "BIN Lookup," page 18 .

Step 5 Click **Submit**.

Configure Payment Methods

You must configure at least one payment method before you can activate a profile.

A payment method selection page is displayed as part of the checkout process for any of the following scenarios:

- Multiple payment methods are enabled for the profile, and no **payment_method** field is included in the request.
- **payment_method=visacheckout** is included in the request.
- Visa Checkout or Visa Secure Remote Commerce (SRC) is the only enabled payment method for the profile (see ["Enable Visa Checkout or Visa SRC," page 26](#)).



Visa SRC uses Visa Checkout services, Business Center labels, and API fields.

You can skip displaying the payment method selection page by specifying card or eCheck as the only available payment method (see ["Enable eChecks," page 25](#)).

Customers can change the payment method during the checkout process.

Add Card Types and Currencies

For each card type you choose, you can also manage currencies and payer authentication options. Choose only the types of payment cards and currencies that your merchant account provider authorizes.

The Card Verification Number (CVN) is a three- or four-digit number that helps ensure that the customer possess the card at the time of the transaction.

To add a card type and enable the CVN:

- Step 1** In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
 - Step 2** Select a profile. The General Settings page appears.
 - Step 3** Click **Payment Settings**. The Payment Settings page appears.
 - Step 4** Click **Add Card Types**. The list of card types appear.
 - Step 5** Check each card type that you want to offer to the customer as a payment method. Your payment processor must support the card types.
 - Step 6** Click the settings icon for each card type. The card settings and currencies lists appear.
 - Step 7** 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 8** 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 9** Check **Payer Authentication**.
 - Step 10** Check the currencies for each card.
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. If you select the Elo or Hipercard card type, only the Brazilian Real currency is supported.
 - Step 11** Click **Submit**. The card types are added as an accepted payment type.
 - Step 12** Click **Save**.
-

Enable Payer Authentication

Before you can use CyberSource Payer Authentication, you must contact CyberSource Customer Support so that CyberSource can configure your account. Your merchant ID must be enabled for payer authentication. For more information about payer authentication, see *Payer Authentication Using the SCMP API* ([PDF](#) | [HTML](#)) and *Payer Authentication Using the Simple Order API* ([PDF](#) | [HTML](#)).

Payer authentication is the CyberSource implementation of 3D Secure. It prevents unauthorized card use and provides added protection from fraudulent chargeback activity. Secure Acceptance supports 3D Secure 1.0 and 2.0.

For Secure Acceptance, CyberSource supports the following kinds of payer authentication:

- American Express SafeKey
- Mastercard Identity Check
- Visa Secure
- J/Secure by JCB

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 can be required to display this information as enrollment verification for any payer authentication transaction that you re-present because of a chargeback.

Your merchant account provider can require that you provide all data in human-readable format.

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 "[Test and View Transactions](#)," page 95.

To configure payer authentication:

- Step 1** In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
- Step 2** Select a profile. The General Settings page appears.
- Step 3** Click **Payment Settings**. The Payment Settings page appears.
- Step 4** Choose a 3D Secure version. If you choose 3D Secure 2.0 and the card issuer is not 3D Secure 2.0 ready, some transactions might still authenticate over 3D Secure 1.0. The **payer_authentication_specification_version** reply field indicates which version was used.

Step 5 Click **Save**. The card types that support payer authentication are:

- Amex
 - Cartes Bancaires
 - Diners Club
 - Discover
 - JCB
 - Mastercard
 - Maestro (UK Domestic or International)
 - Visa
-

Enable 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 reversal. An automatic reversal releases the reserved funds held against a customer's card.

To enable automatic authorization reversals:

- Step 1** In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
- Step 2** Select a profile. The General Settings page appears.
- Step 3** Click **Payment Settings**. The Payment Settings page appears.
- Step 4** Check **Fails AVS check**. Authorization is automatically reversed on a transaction that fails an AVS check.
- Step 5** Check **Fails CVN check**. Authorization is automatically reversed on a transaction that fails a CVN check.
- Step 6** Click **Save**.



When the AVS and CVN options are disabled and the transaction fails an AVS or CVN check, the customer is notified that the transaction was accepted. You are notified to review the transaction details (see ["Types of Notifications," page 171](#)).

Enable 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. For more information, see the [TeleCheck activation guide](#).

A customer must accept the terms and conditions before submitting an order. 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 method:

- Step 1** In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
 - Step 2** Select a profile. The General Settings page appears.
 - Step 3** Click **Payment Settings**. The Payment Settings page appears.
 - Step 4** Check **Enable eCheck Payments**. The list of account types appears.
 - Step 5** Check the account type(s):
 - Checking
 - Savings
 - Corporate Checking
 - General Ledger
 - Step 6** Click **Add Currencies**. The eCheck Settings page appears.
 - Step 7** Check **Select All** or check each currency.
 - Step 8** Click **Save**.

You must configure the eCheck information fields. See "[Display eCheck Information](#)," [page 33](#).
-

Enable Visa Checkout or Visa SRC

You must enroll in Visa Checkout or Visa SRC and create a Visa Checkout profile before you can enable it as a payment method. See *Getting Started with Visa Checkout* ([PDF](#) | [HTML](#)) or *Getting Started with Visa Secure Remote Commerce* ([PDF](#) | [HTML](#)). Only the authorization and sale transaction types are supported for Visa Checkout and Visa SRC transactions.



Visa SRC uses Visa Checkout services, Business Center labels, and API fields.

The payment methods selection page is displayed as part of the checkout process for the following scenarios:

- Multiple payment methods are enabled for the profile, and no **payment_method** field is included in the request.
- Visa Checkout is the only enabled payment method for the profile.
- **payment_method=visacheckout** is included in the request.

Visa Checkout and Visa SRC require the customer to enter only a username and password to pay for goods. It eliminates the need to enter account, shipping, and billing information. The customer logs in to their Visa Checkout or Visa SRC account and chooses the card with which they would like to pay. If the Secure Acceptance profile is enabled to request the payer authentication service for a specific card type, the customer is redirected to the relevant payer authentication screen before Secure Acceptance processes the transaction and redirects the customer to your web site.

To enable Visa Checkout or Visa SRC:

- Step 1** In the left navigation panel, choose **Payment Configuration > Digital Payment Solutions**. The Digital Payment Solutions page appears.
 - Step 2** Click **Configure**. The Visa Merchant Services Agreement appears.
 - Step 3** Review the Visa Checkout Services Agreement, then click **Agree and Create Account**. The Visa Checkout Configuration panel opens to the Merchant Configuration section.
 - Step 4** Enter your payment details.
 - Step 5** Click **Submit**.
-

To enable the payment method for Visa Checkout or Visa SRC:

- Step 1** In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
- Step 2** Select a profile. The General Settings page appears.
- Step 3** Click **Payment Settings**. The Payment Settings page appears.
- Step 4** Check **Enable Visa Checkout**.
- Step 5** Enter the name of the Visa Checkout profile to be used. If no profile name is entered, the default Visa Checkout profile is used.
- Step 6** Check the card types to request the payer authentication service for:
- Visa—the Visa Secure service is requested.
 - Mastercard—the Mastercard Identity Check service is requested.
 - American Express—the American Express SafeKey service is requested.
- See ["Enable Payer Authentication," page 23](#).
- Step 7** Indicate when to reject transactions based on a certain criterion:
- Billing address details are incorrect (AVS fail).
 - Security code is incorrect (CVV/CVN fail).
 - The Visa Checkout risk score is above your specified score. Select the risk score to use with your fraud model. A value of 0 indicates that a risk score will not be taken into account, and a higher risk score indicates a higher perceived fraud risk.
- Step 8** Click **Save**.
-

To configure the payment method for Visa Checkout or Visa SRC, log in to the [New Business Center](#) and go to [Configuring Visa Checkout](#).

Enable PayPal Express Checkout

PayPal Express Checkout is not supported on a Secure Acceptance iframe integration.

Contact CyberSource Customer Support to have your CyberSource account configured for this feature. You must also create a PayPal business account; see *PayPal Express Checkout Services Using the SCMP API* ([PDF](#) | [HTML](#)) or *PayPal Express Checkout Services Using the Simple Order API* ([PDF](#) | [HTML](#)).

Add the PayPal Express Checkout payment method to the Secure Acceptance Hosted Checkout payment methods selection page. Redirect the customer to their PayPal

account login. When logged in to their PayPal account they can review orders and edit shipping or payment details before completing transactions.

The payment methods selection page is displayed as part of the checkout process when multiple payment methods are enabled for the profile and no **payment_method** field is included in the request. If you include **payment_method=paypal** in the request, the payment methods selection page is not displayed, and the customer is redirected to PayPal.

To enable the PayPal Express Checkout payment method:

- Step 1** In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
- Step 2** Select a profile. The General Settings page appears.
- Step 3** Click **Payment Settings**. The Payment Settings page appears.
- Step 4** Check **Enable PayPal Express Checkout**.
- Step 5** Check **Allow customers to select or edit their shipping address within PayPal** to allow customers to edit the shipping address details that they provided in the transaction request to Secure Acceptance. Customers select a new address or edit the address when they are logged in to their PayPal account.
- Step 6** When the transaction type is authorization, check one of the following options:

- **Request a PayPal authorization and include the authorization reply values in the response**—check this option to create and authorize the PayPal order.



The customer funds are not captured using this option. You must request a PayPal capture; see *PayPal Express Checkout Services Using the SCMP API* ([PDF](#) | [HTML](#)) or *PayPal Express Checkout Services Using the Simple Order API* ([PDF](#) | [HTML](#)). If the transaction type is **sale**, Secure Acceptance authorizes and captures the customer funds.

- **Request a PayPal order setup and include the order setup reply values in the response**—check this option to create the PayPal order.



The customer funds are not authorized or captured using this option. You must request a PayPal authorization followed by a PayPal capture request; see *PayPal Express Checkout Services Using the SCMP API* ([PDF](#) | [HTML](#)) or *PayPal Express Checkout Services Using the Simple Order API* ([PDF](#) | [HTML](#)). If the transaction type is **sale**, Secure Acceptance authorizes and captures the customer funds.

Step 7 Click **Save**.

Create a Security Key

You must create a security key before you can activate a profile.

You cannot use the same security key for both test and live transactions. You must download a security key for each version of Secure Acceptance:

- For live transactions: <https://ebc2.cybersource.com/ebc2/>
- For live transactions in India: <https://ebc2.in.cybersource.com/ebc2/>
- For test transactions: <https://ebctest.cybersource.com/ebc2/>

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. A security key expires in two years and protects each transaction from data tampering.

To create and activate a security key:

- Step 1** In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
- Step 2** Select a profile. The General Settings page appears.
- Step 3** Click **Security**. The security keys page appears.
- Step 4** Click the Create Key plus sign (+).
- Step 5** Enter a key name (required).
- Step 6** Choose signature version **1** (default).
- Step 7** Choose signature method **HMAC-SHA256** (default).
- Step 8** Click **Create**.
- Step 9** Click **Confirm**. The Create New Key window expands and displays the new access key and secret key. This panel closes after 30 seconds.

Step 10 Copy and save or download 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 ["Samples in Scripting Languages," page 47.](#)
- Secret key: signs the transaction data and is required for each transaction. Copy and paste this secret key into your security script. See ["Samples in Scripting Languages," page 47.](#)



Remember to delete the copied keys from your clipboard or cached memory.

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.

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.

Configure the Checkout

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.

Configure the Payment Form

To configure the payment form:

- Step 1** In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Payment Form**. The Payment Form page appears.

Step 4 Choose the payment form flow:

- **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 payment selection (if multiple payment methods are enabled), 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.

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

Step 5 Check **Display the total tax amount in each step of the checkout process**.

The total tax amount must be included in each transaction. Calculate and include the total tax amount in the **tax_amount** field.

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

Step 6 Click **Save**.

Display Billing Information Fields



Select the billing information fields that your merchant provider requires. If the billing country is U.S. or Canada, you can select the state code field as a required field. CyberSource recommends that if the billing country is U.S. or Canada, the state code and the postal code fields be selected as required. If the billing country is located in the rest of the world, you can also select the state code field as a required field.

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 "[Request Fields](#)," [page 98](#)). You can shorten the checkout process by not selecting billing information.

To display and edit the billing information fields:

Step 1 In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.

Step 2 Choose a profile. The General Settings page appears.

Step 3 Click **Payment Form**. The Payment Form page appears.

Step 4 Check **Billing Information**. The billing information fields appear.

Step 5 Check the billing information fields that your merchant provider requires. 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 Hosted Checkout 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 Hosted 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 Hosted Checkout before they submit the transaction. When you select this option, all other options are automatically selected.

Do not click **Save** until you have selected the billing and order review fields.

Step 6 Indicate whether to mask sensitive fields.

Step 7 Click **Save**.

Display Shipping Information Fields

Select the shipping information fields that your merchant provider requires.

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 "[Request Fields](#)," [page 98](#)). You can shorten the checkout process by not selecting shipping information.

To display and edit shipping information fields:

Step 1 In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.

Step 2 Choose a profile. The General Settings page appears.

Step 3 Click **Payment Form**. The Payment Form page appears.

Step 4 Check **Shipping Information**.

Step 5 Check the shipping information fields that your merchant provider requires. 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 Hosted Checkout 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 Hosted 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 Hosted Checkout before they submit the transaction. When you select this option, all other options are automatically selected.

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

Step 6 Indicate whether to mask sensitive fields.

Step 7 Click **Save**.

Display eCheck Information

Select the eCheck account information fields that your merchant provider requires.

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

To display and edit eCheck information:

Step 1 In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.

Step 2 Choose a profile. The General Settings page appears.

Step 3 Click **Payment Form**. The Payment Form page appears.

Step 4 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 Hosted Checkout is rendered.

- **Edit:** the customer can view and edit the eCheck information on Secure Acceptance Hosted 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 Hosted Checkout before they submit the transaction. When you select this option, all other options are automatically selected.

Step 5 Indicate whether to mask sensitive fields.

Step 6 Click **Save**.

Customize Order Review Details

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

To display and edit order review fields:

Step 1 In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.

Step 2 Choose a profile. The General Settings page appears.

Step 3 Click **Payment Form**. The Payment Form page appears.

Step 4 Check the fields that you want displayed on the Order Review page of Secure Acceptance Hosted Checkout. 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 5 Click **Save**.

Receive Merchant Notifications

Secure Acceptance sends merchant and customer notifications in response to transactions. You can receive a merchant notification by email or as an HTTPS POST to a URL for each transaction processed. Both notifications contain the same transaction result data.

Ensure that your system acknowledges POST notifications (even when under load) as quickly as possible. Delays of more than 10 seconds might result in delays to future POST notifications.



CyberSource recommends that you implement the merchant POST URL to receive notification of each transaction. Parse the transaction response sent to the merchant POST URL and store the data within your order management system. This ensures the accuracy of the transactions and informs you when the transaction was successfully processed.

To configure merchant notifications:

- Step 1** In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Notifications**. The Notifications page appears.
- Step 4** Choose a merchant notification in one of two ways:
 - Check **Merchant POST URL**. Enter the HTTPS URL. CyberSource sends transaction information to this URL. For more information, see ["Reply Fields," page 132](#).

Only an HTTPS URL supporting TLS 1.2 or higher should be used for the merchant POST URL. If you encounter any problems, contact CyberSource Customer Support.
 - Check **Merchant POST Email**. Enter your email address.

CyberSource sends transaction response information to this email address including payment information, return codes, and all relevant order information. See ["Reply Fields," page 132](#).

- Step 5** Choose the card number digits that you want displayed in the merchant or customer receipt:
- Return payment 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 payment card number: displays the last four digits of the card number. All other digits are masked: xxxxxxxxxxxx1234
 - Return BIN and last four digits of payment card number: displays the BIN and the last four digits of the card number. All other digits are masked: 123456xxxxxx1234
- Step 6** Continue to configure the customer notifications (see ["Send a Customer Receipt," page 36](#)) or click **Save**.
-

Send a Customer Receipt

You can send a purchase receipt email to your customer and a copy to your own email address. Both are optional. Customers can 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** In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Notifications**. The Notifications page appears.
- Step 4** Check **Email Receipt to Customer**.
- Step 5** Enter the sender email address to be displayed on the customer receipt. The customer will reply to this email with any queries.
- Step 6** Enter the sender name of your business. It is displayed on the customer receipt.
- Step 7** Check **Send a copy to**. This setting is optional.
- Step 8** Enter your email address to receive a copy of the customer's receipt. Your copy of the customer receipt will contain additional transaction response information.

Step 9 Check **Display Notification Logo**.

Step 10 Click **Upload Company Logo**. Find and upload the image that you want to display on the customer receipt and email.

The image file must not exceed 840 (w) x 60 (h) pixels and must be GIF, JPEG, or PNG. The logo filename must not contain any special characters, such as a hyphen (-).

Step 11 Check **Custom Email Receipt**.

CyberSource recommends that you implement a DNS configuration to enable CyberSource to send email receipts on your behalf.

Step 12 Check the type of email receipt you want to send to a customer:

- Standard email receipt: this email is automatically translated based on the locale used for the transaction.
- Custom email receipt: 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 you use different locales.

Step 13 Check **custom email subject** and enter up to 998 characters. When the maximum number of characters is exceeded, the subject heading defaults to *Order Confirmation*.

You can insert email smart tags in the email subject, header, and footer sections to include specific information. Select each smart tag from the drop-down list and click **Insert**.

Step 14 Click **Save**.

Display a Response Page

You must configure the customer response page before you can activate a profile.

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 might be able to correct problems related to address or card verification, or you might 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.

Display a Transaction Response Page

CyberSource Hosted Response Page

To display a CyberSource hosted response page:

- Step 1** In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
 - Step 2** Choose a profile. The General Settings page appears.
 - Step 3** Click **Customer Response**. The Customer Response page appears.
 - Step 4** Under the Transaction Response Page heading, check **Hosted by CyberSource**.
 - Step 5** Under the Transaction Response Message heading, choose a number from the **Retry Limit** drop-down list. The maximum number of times a customer can retry a declined transaction is five.
 - Step 6** 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 7** Click **Save**. The Profile Settings page appears.
-

Display a Custom Hosted Response Page

To display your custom response page:

- Step 1** In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Customer Response**. The Customer Response page appears.
- Step 4** Under the Transaction Response Page heading, check **Hosted by You**.
- Step 5** Enter the URL for your customer response page. Use port 80, 443, or 8080 in your URL. Only port 443 should be used with a HTTPS URL. Parse the transaction results from the URL according to the reason code (), and redirect your customer to the appropriate response page. See ["Reason Codes," page 168](#).

- Step 6** Under the Transaction Response Message heading, choose a number from the **Retry Limit** drop-down list. The maximum number of times a customer can retry a declined transaction is 5.
- Step 7** 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 8** Click **Save**.
-

Custom Cancel Response Page

CyberSource Hosted Response Page

To display a CyberSource hosted response page:

- Step 1** In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Customer Response**. The Customer Response page appears.
- Step 4** Under the Custom Cancel Response Page heading, check **Hosted by CyberSource**.
- Step 5** Click **Save**.
-

Custom Cancel Response Page

To display your custom cancel response page:

- Step 1** In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Customer Response**. The Customer Response page appears.
- Step 4** Under the Custom Cancel Response Page heading, check **Hosted by You**.

Step 5 Enter the URL for your customer response page. Use port 80, 443, or 8080 in your URL. Only port 443 should be used with a HTTPS URL. Parse the transaction results from the URL according to the reason code (), and redirect your customer to the appropriate response page. See "[Reason Codes](#)," page 168.

Step 6 Click **Save**.

Customize the Checkout Appearance

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.

CyberSource recommends that you preview your changes in the Image Preview window.

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 100 kB. 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.

To change the header content:

Step 1 In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.

Step 2 Choose a profile. The General Settings page appears.

Step 3 Click **Branding**. The Branding page appears.

Step 4 Check **Display Header**.

Step 5 Click the header color icon.

Step 6 Choose a color in one of two ways:

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

Step 7 Click **Browse** to upload the image to display as the header banner or as a logo within the header banner.

Step 8 Choose the alignment option for the image or logo: left-aligned, centered, or right-aligned.

Step 9 Click **Save**.

To change the body color and font settings:

Step 1 In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.

Step 2 Choose a profile. The General Settings page appears.

Step 3 Click **Branding**. The Branding page appears.

Step 4 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 color icon to confirm your selection.

Step 5 Select a text font from the drop-down list.

Step 6 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 color icon to confirm your selection.

Step 7 Click **Save**.

Step 8 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:



If you are implementing the iframe embedded version of Secure Acceptance Hosted Checkout, the total amount figure is not displayed within the iframe. Any settings you select below are ignored.

Step 1 In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.

Step 2 Choose a profile. The General Settings page appears.

Step 3 Click **Branding**. The Branding page appears.

- Step 4** 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 color icon to confirm your selection.
- Step 5** 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 color icon to confirm your selection.
- Step 6** Click **Save**.
- Step 7** Click **Set to Default** to restore all the default settings on this page.
-

To change the color of the progress bar:

- Step 1** In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Branding**. The Branding page appears.
- Step 4** 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 color icon to confirm your selection.
- Step 5** Click **Save**.
- Step 6** Click **Set to Default** to restore all the default settings on this page.
-

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

- Step 1** In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Branding**. The Branding page appears.

- Step 4** Choose a background color of the pay or the finish 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 color icon to confirm your selection.
- Step 5** Choose a color of the pay or the finish 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 6** Check **Change Button text**. A text box appears for the pay button.
- Step 7** Enter the text you want displayed on the pay button. This button text is required.
- Step 8** Enter the text you want displayed on the finish button. This button text is required.
- Step 9** Click **Save**.
- Step 10** 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** In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Branding**. The Branding page appears.
- Step 4** Check **Display Footer**.
- Step 5** 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 color icon to confirm your selection.
- Step 6** Click **Browse** to upload a footer logo. Upload the image that you want displayed within the footer of the payment form.
- 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 7** Choose the alignment option for the image: left-aligned, centered, or right-aligned.
- Step 8** Click **Save**.

Step 9 Click **Set to Default** to restore all the default settings on this page.

Localize the Checkout Languages

Secure Acceptance supports multiple languages. [Table 4](#) lists all the supported languages and the locale code that you must include in your payment form.

From the list, include the locale code in the **locale** request field on your payment form. See ["Sample Transaction Process Using JSP," page 47](#).

Example 1 American English

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

Table 4 **Locale Codes**

Language	Locale Code
Arabic	ar-xn
Catalan	ca-es
Chinese—Hong Kong	zh-hk
Chinese—Macau	zh-mo
Chinese—Mainland	zh-cn
Chinese—Singapore	zh-sg
Chinese—Taiwan	zh-tw
Croatian	hr-hr
Czech	cz-cz
Danish	da-dk
Dutch	nl-nl
English—United States of America	en-us
English—Australia	en-au
English—Great Britain	en-gb
English—Canada	en-ca
English—Ireland	en-ie
English—New Zealand	en-nz
Finnish	fi-fi
French	fr-fr
French—Canada	fr-ca
German	de-de

Table 4 Locale Codes (Continued)

Language	Locale Code
German—Austria	de-at
Greek	el-gr
Hebrew	he-il
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
Norwegian (Bokmal)	nb-no
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—United States of America	es-us
Swedish	sv-se
Thai	th-th
Turkish	tr-tr
Vietnamese	vi-vn

Activate a Profile

You must complete the required settings described in each of these sections before you can activate a profile:

- ["Configure Payment Methods"](#)
- ["Create a Security Key"](#)
- ["Display a Response Page"](#)

To activate a profile:

Step 1 On the left navigation pane, click the **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.

Step 2 Perform one of the following steps:

- On the Active Profiles tab, select the profile that you want to activate, and click the **Promote Profile** icon.
- On the Edit Profile page, click the **Promote Profile** icon.

Step 3 Click **Confirm**.

Additional Profile Options

- **Deactivate**—deactivates the active profile. The profile is now listed in the inactive profile list. This option is available only for an active profile.
- **Create Editable Version**—duplicates the active profile and creates an editable version. The editable version is listed in the inactive profile list. This option is available only for an active profile.
- **Promote to Active**—activates the inactive profile. This option is available only for an inactive profile.

Samples in Scripting Languages

Secure Acceptance 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

Sample Transaction Process Using JSP

- 1 **payment_form.jsp** file—represents the customer's product selection on a web site. Enter your access key and profile ID into their respective fields. POST the fields to your server to sign and create the signature. All the fields must be included in the **signed_field_names** field as a CSV list.
- 2 **security.jsp** file—security algorithm signs fields and creates a signature using the **signed_field_names** field. Enter your security key in the **SECRET_KEY** field. Modify the security script to include the Secret Key that you generated in ["Create a Security Key," page 29](#).

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.
- 3 **payment_confirmation.jsp** file—represents the customer order review page on a web site, before the customer makes a payment. POST transaction to the Secure Acceptance endpoint () and render the Secure Acceptance Hosted Checkout. See [Chapter 4, "Payment Transactions," on page 74](#).

Portfolio Management for Resellers

Create a Hosted Checkout Profile

Contact CyberSource Customer Support to enable your account for Secure Acceptance. You must activate a profile in order to use it (see ["Activate a Profile," page 72](#)).

To create a Hosted Checkout profile:

- Step 1** Log in to the Business Center:
- Live transactions: <https://ebc2.cybersource.com/ebc2/>
 - Live transactions in India: <https://ebc2.in.cybersource.com/ebc2/>
 - Test transactions: <https://ebctest.cybersource.com/ebc2/>
- Step 2** In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
- Step 3** Click **New Profile**.
- Step 4** Enter or verify the following profile details.

Table 5 Profile Details

Profile Detail	Description
Profile Name	The Secure Acceptance profile name is required and cannot exceed 40 alphanumeric characters.
Profile Description	The profile description cannot exceed 255 characters.
Integration Method	Check Hosted Checkout .
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 Chapter 4, "Payment Transactions," on page 74 .

Table 5 Profile Details (Continued)

Profile Detail	Description
Decision Manager	Check Decision Manager . For more information, see Chapter 5, "Decision Manager," on page 93.
Verbose Data	Check Verbose Data . For more information, see Chapter 5, "Decision Manager," on page 93.
Generate Device Fingerprint	Check Generate Device Fingerprint . For more information, see Chapter 5, "Decision Manager," on page 93.
BIN Lookup	Choose Perform checks on card eligibility for Original Credit Transfer (OCT) for Payouts or Enable full BIN Lookup service . For more information, see "BIN Lookup," page 18.

Step 5 Click **Submit**.

Configure Payment Methods

You must configure at least one payment method before you can activate a profile.



Visa SRC uses Visa Checkout services, Business Center labels, and API fields.

A payment method selection page is displayed as part of the checkout process for any of the following scenarios:

- Multiple payment methods are enabled for the profile, and no **payment_method** field is included in the request.
- **payment_method=visacheckout** is included in the request.
- Visa Checkout or Visa SCR is the only enabled payment method for the profile (see ["Enable Visa Checkout or Visa SRC,"](#) page 54).

You can skip the payment method selection page by specifying card or echeck as the only available payment method (see ["Enable eChecks,"](#) page 53).

Customers can change the payment method during the checkout process.

Add Card Types and Currencies

For each card type you choose, you can also manage currencies and payer authentication options. Choose only the types of payment cards and currencies that your merchant account provider authorizes.

The Card Verification Number (CVN) is a three- or four-digit number that helps ensure that the customer possesses the card at the time of the transaction.

To add a card type and enable the CVN:

- Step 1** In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Payment Settings**. The Payment Settings page appears.
- Step 4** Click **Add Card Types**. The list of card types appear.
- Step 5** Check each card type that you want to offer to the customer as a payment method. Your payment processor must support the card types.
- Step 6** Click **Settings** for each card type. The card settings and currencies lists appear.
- Step 7** 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 8** 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 9** Check the currencies for each card.



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. If you select the Elo or Hipercard card type, only the Brazilian Real currency is supported.

- Step 10** Click **Submit**. The card types are added as an accepted payment type.
 - Step 11** Click **Save**.
-

Enable Payer Authentication

Before you can use CyberSource Payer Authentication, you must contact CyberSource Customer Support so that CyberSource can configure your account. Your merchant ID must be enabled for payer authentication. For more information about payer authentication, see *Payer Authentication Using the SCMP API* ([PDF](#) | [HTML](#)) and *Payer Authentication Using the Simple Order API* ([PDF](#) | [HTML](#)).

Payer authentication is the CyberSource implementation of 3D Secure. It deters unauthorized card use and provides added protection from fraudulent chargeback activity. Secure Acceptance supports 3D Secure 1.0 and 2.0.

For Secure Acceptance, CyberSource supports the following kinds of payer authentication:

- American Express SafeKey
- Mastercard Identity Check
- Visa Secure
- J/Secure by JCB

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 can be required to display this information as enrollment verification for any payer authentication transaction that you re-present because of a chargeback.

Your merchant account provider can require that you provide all data in human-readable format.

The language used on each payer authentication page is determined by your issuing bank and overrides the locale that you specified. If you use the test card numbers, the default language used on the payer authentication page is English and overrides the locale you have specified. See "[Test and View Transactions](#)," [page 95](#).

To configure payer authentication:

- Step 1** In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Payment Settings**. The Payment Settings page appears.
- Step 4** Choose the 3D Secure version that you want to use. If you choose 3D Secure 2.0 and the card issuer is not 3D Secure 2.0 ready, some transactions might still authenticate over 3D Secure 1.0. The **payer_authentication_specification_version** reply field indicates which version was used.

Step 5 Click **Save**. The card types that support payer authentication are:

- Amex
 - Cartes Bancaires
 - Diners Club
 - Discover
 - JCB
 - Mastercard
 - Maestro (UK Domestic or International)
 - Visa
-

Enable 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 reversal. An automatic reversal releases the reserved funds held against a customer's card.

To enable automatic authorization reversals:

- Step 1** In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Payment Settings**. The Payment Settings page appears.
- Step 4** Check **Fails AVS check**. Authorization is automatically reversed on a transaction that fails an AVS check.
- Step 5** Check **Fails CVN check**. Authorization is automatically reversed on a transaction that fails a CVN check.
- Step 6** Click **Save**.



When the AVS and CVN options are disabled and the transaction fails an AVS or CVN check, the customer is notified that the transaction was accepted. You are notified to review the transaction details (see "[Types of Notifications](#)," [page 171](#)).

Enable 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. For more information, see the [TeleCheck activation guide](#).

A customer must accept the terms and conditions before submitting an order. 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 method:

- Step 1** In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
 - Step 2** Choose a profile. The General Settings page appears.
 - Step 3** Click **Payment Settings**. The Payment Settings page appears.
 - Step 4** Check **Enable eCheck Payments**. The list of account types appears.
 - Step 5** Check the account type(s):
 - Checking
 - Savings
 - Corporate Checking
 - General Ledger
 - Step 6** Click **Add Currencies**. The eCheck Settings page appears.
 - Step 7** Check **Select All** or select a currency.
 - Step 8** Click **Save**.
You must configure the eCheck information fields. See "[Display and Edit eCheck Information](#)," page 61.
-

Enable Visa Checkout or Visa SRC

You must enroll in Visa Checkout or Visa SRC and create a Visa Checkout profile before you can enable it as a payment method. See *Getting Started with Visa Checkout* ([PDF](#) | [HTML](#)) or *Getting Started with Visa Secure Remote Commerce* ([PDF](#) | [HTML](#)). Only the authorization and sale transaction types are supported for Visa Checkout and Visa SRC transactions.



Visa SRC uses Visa Checkout services, Business Center labels, and API fields.

The payment methods selection page is displayed as part of the checkout process for either of the following scenarios:

- Multiple payment methods are enabled for the profile and no **payment_method** field is included in the request.
- Visa Checkout is the only enabled payment method for the profile.
- **payment_method=visacheckout** is included in the request.

Visa Checkout and Visa SRC require the customer to enter only a username and password to pay for goods. It eliminates the need to enter account, shipping, and billing information. The customer logs in to their Visa Checkout or Visa SRC account and chooses the card with which they would like to pay. If the Secure Acceptance profile is enabled to request the payer authentication service for a specific card type, the customer is redirected to the relevant payer authentication screen before Secure Acceptance processes the transaction and redirects the customer to your web site.

To enable the payment method for Visa Checkout or Visa SRC:

- Step 1** In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Payment Settings**. The Payment Settings page appears.
- Step 4** Check **Enable Visa Checkout**.
- Step 5** Click **Save**.
- Step 6** In the left navigation panel, choose **Payment Configuration > Digital Payment Solutions**.

Step 7 Click **Save**.

To configure the payment method for Visa Checkout or Visa SRC, log in to the [New Business Center](#) and go to [Configuring Visa Checkout](#).

Enable PayPal Express Checkout

PayPal Express Checkout is not supported on a Secure Acceptance iframe integration.

Contact CyberSource Customer Support to have your CyberSource account configured for this feature. You must also create a PayPal business account; see *PayPal Express Checkout Services Using the SCMP API* ([PDF](#) | [HTML](#)) or *PayPal Express Checkout Services Using the Simple Order API* ([PDF](#) | [HTML](#)).

Add the PayPal Express Checkout payment method to the Secure Acceptance Hosted Checkout payment methods selection page. Redirect the customer to their PayPal account login. When logged in to their PayPal account they can review orders and edit shipping or payment details before completing transactions.

The payment methods selection page is displayed as part of the checkout process when multiple payment methods are enabled for the profile and no **payment_method** field is included in the request. If you include **payment_method=paypal** in the request, the payment methods selection page is not displayed and the customer is redirected to PayPal.

To enable the PayPal Express Checkout payment method:

- Step 1** In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
 - Step 2** Choose a profile. The General Settings page appears.
 - Step 3** Click **Payment Settings**. The Payment Settings page appears.
 - Step 4** Check **Enable PayPal Express Checkout**.
 - Step 5** Click **Save**.
-

Enable the Service Fee

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.

The service fee setting applies to the card and eCheck payment methods. To apply the service fee to only one payment method, create two Secure Acceptance profiles with the appropriate payment methods enabled on each: one with the service fee feature enabled and one with the service fee feature disabled.

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** In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Payment Settings**. The Payment Settings page appears.
- Step 4** 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.



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

- Step 5** Click **Save**.



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.

Create a Security Key



You must create a security key before you can activate a profile.

You cannot use the same security key for both test and live transactions. You must download a security key for each versions of Secure Acceptance:

- For live transactions: <https://ebc2.cybersource.com/ebc2/>
- For live transactions in India: <https://ebc2.in.cybersource.com/ebc2/>
- For test transactions: <https://ebctest.cybersource.com/ebc2/>

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** In the left navigation panel, choose **Payment Configuration > Key Management**.
- Step 2** Click **Generate Key**.
- Step 3** Select a key type.
- Step 4** Click **Next Step**.
- Step 5** Select the key subtype **Secure Acceptance**.
- Step 6** Click **Next Step**.
- Step 7** Enter a key name (required).
- Step 8** Choose signature version **1**.
- Step 9** Choose signature method **HMAC-SHA256**.
- Step 10** Select a security profile.
- Step 11** Click **Submit**.
- Step 12** 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 13 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 ["Samples in Scripting Languages," page 47.](#)
- Secret key: signs the transaction data and is required for each transaction. Copy and paste this secret key into your security script. See ["Samples in Scripting Languages," page 47.](#)



Remember to delete the copied keys from your clipboard or cached memory.

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.

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 14 Click **Key Management**. The Key Management page appears.

Configure the Checkout

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.

Configure the Payment Form

To configure the payment form:

Step 1 In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.

Step 2 Choose a profile. The General Settings page appears.

Step 3 Click **Payment Form**. The Payment Form page appears.

Step 4 Choose the payment form flow:

- 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 payment selection (if multiple payment methods are enabled), 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.

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

Step 5 Check **Display the total tax amount in each step of the checkout process**.

The total tax amount must be included in each transaction. Calculate and include the total tax amount in the **tax_amount** field.

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

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

Display and Edit Billing Information Fields



Select the billing information fields that your merchant provider requires. If the billing country is U.S. or Canada, you can select the state code field as a required field. CyberSource recommends that if the billing country is U.S. or Canada, the state code and the postal code fields be selected as required. If the billing country is located in the rest of the world, you can also select the state code field as a required field.

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 "[Request Fields](#)," page 98). You can shorten the checkout process by not selecting billing information.

To display and edit the billing information fields:

Step 1 In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.

Step 2 Choose a profile. The General Settings page appears.

Step 3 Click **Payment Form**. The Payment Form page appears.

Step 4 Check **Billing Information**. The billing information fields appear.

Step 5 Check the billing information fields that your merchant provider requires. 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 Hosted Checkout 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 Hosted 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 Hosted Checkout before they submit the transaction. When you select this option, all other options are automatically selected.

Do not click **Save** until you have selected the billing and order review fields.

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

Display and Edit Shipping Information Fields

Select the shipping information fields that your merchant provider requires.

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 ["Request Fields," page 98](#)). You can shorten the checkout process by not selecting billing information.

To display and edit shipping information fields:

Step 1 In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.

Step 2 Choose a profile. The General Settings page appears.

Step 3 Click **Payment Form**. The Payment Form page appears.

Step 4 Check **Shipping Information**.

- Step 5** 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 Hosted Checkout 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 Hosted 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 Hosted Checkout before they submit the transaction. When you select this option, all other options are automatically selected.

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

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

Display and Edit eCheck Information

Select the eCheck account information fields that your merchant provider requires.

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

To display and edit eCheck information:

- Step 1** In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Payment Form**. The Payment Form page appears.
- Step 4** 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 the Secure Acceptance Hosted Checkout is rendered.
 - **Edit:** the customer can view and edit the eCheck information on the Secure Acceptance Hosted 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 Hosted Checkout before they submit the transaction. When you select this option, all other options are automatically selected.
- Do not **Save** until you have selected the eCheck account information and order review fields.

Step 5 Click **Save**.

Display and Edit Order Review Details

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

To display and edit order review fields:

- Step 1** In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Payment Form**. The Payment Form page appears.
- Step 4** Check the fields that you want displayed on the Order Review page of Secure Acceptance Hosted Checkout. 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 5** Click **Save**. The Configuring Profile Setting page appears.
-

Receive Merchant Notifications

Secure Acceptance sends merchant and customer notifications in response to transactions. You can receive a merchant notification by email or as an HTTPS POST to a URL for each transaction processed. Both notifications contain the same transaction result data.

Ensure that your system acknowledges POST notifications (even when under load) as quickly as possible. Delays of more than 10 seconds might result in delays to future POST notifications.



CyberSource recommends that you implement the merchant POST URL to receive notification of each transaction. Parse the transaction response sent to the merchant POST URL and store the data within your order management system. This ensures the accuracy of the transactions and informs you when the transaction was successfully processed.

To configure merchant notifications:

- Step 1** In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Notifications**. The Notifications page appears.
- Step 4** Choose a merchant notification in one of two ways:
 - Check **Merchant POST URL**. Enter the HTTPS URL. CyberSource sends transaction information to this URL. For more information, see ["Reply Fields," page 132](#).

Only an HTTPS URL supporting TLS 1.2 or higher should be used for the merchant POST URL. If you encounter any problems, contact CyberSource Customer Support.
 - Check **Merchant POST Email**. Enter your email address.

CyberSource sends transaction response information to this email address including payment information, return codes, and all relevant order information. See ["Reply Fields," page 132](#).
- Step 5** Choose the card number digits that you want displayed in the merchant or customer receipt:
 - Return payment 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 payment card number: displays the last four digits of the card number. All other digits are masked: xxxxxxxxxxx1234
- Return BIN and last four digits of payment card number: displays the BIN and the last four digits of the card number. All other digits are masked: 123456xxxxxx1234

Step 6 Continue to configure the customer notifications (see ["Send a Customer Receipt," page 64](#)) or click **Save**. The Profile Settings page appears.

Send a Customer Receipt

You can send a purchase receipt email to your customer and a copy to your own email address. Both are optional. Customers can 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** In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Notifications**. The Notifications page appears.
- Step 4** Check **Email Receipt to Customer**.
- Step 5** Enter the sender email address to be displayed on the customer receipt. The customer will reply to this email with any queries.
- Step 6** Enter the sender name of your business. It is displayed on the customer receipt.
- Step 7** Check **Send a copy to**. This setting is optional.
- Step 8** Enter your email address to receive a copy of the customer's receipt.
Your copy of the customer receipt will contain additional transaction response information.
- Step 9** Check **Display Notification Logo**.

Step 10 Click **Upload Company Logo**. Find and upload the image that you want to display on the customer receipt and email.

The image file must not exceed 840 (w) x 60 (h) pixels and must be GIF, JPEG, or PNG. The logo filename must not contain any special characters, such as a hyphen (-).

Step 11 Check **Custom Email Receipt**.

CyberSource recommends that you implement a DNS configuration to enable CyberSource to send email receipts on your behalf.

Step 12 Check the type of email receipt that you want to send to a customer:

- Standard email receipt: this email is automatically translated based on the locale used for the transaction.
- Custom email receipt: 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 are used.

Step 13 Check **custom email subject** and enter up to 998 characters. When the maximum number of characters is exceeded, the subject heading defaults to *Order Confirmation*.

You can insert email smart tags in the email subject, header, and footer sections to include specific information. Select each smart tag from the drop-down list and click **Insert**.

Step 14 Click **Save**.

Display a Response Page

You must configure the customer response page before you can activate a profile.

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 might be able to correct problems related to address or card verification, or you might 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.

Display a Transaction Response Page

CyberSource Hosted Response Page

To display a CyberSource hosted response page:

- Step 1** In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
 - Step 2** Choose a profile. The General Settings page appears.
 - Step 3** Click **Customer Response**. The Customer Response page appears.
 - Step 4** Under the Transaction Response Page heading, check **Hosted by CyberSource**.
 - Step 5** Under the Transaction Response Message heading, choose a number from the **Retry Limit** drop-down list. The maximum number of times a customer can retry a declined transaction is five.
 - Step 6** 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 7** Click **Save**. The Profile Settings page appears.
-

Display a Custom Hosted Response Page

To display your custom response page:

- Step 1** In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Customer Response**. The Customer Response page appears.
- Step 4** Under the Transaction Response Page heading, check **Hosted by You**.
- Step 5** Enter the URL for your customer response page. Use port 80, 443, or 8080 in your URL.

Only port 443 should be used with a HTTPS URL. Parse the transaction results from the URL according to the reason code (see ["Reason Codes," page 168](#)), and redirect your customer to the appropriate response page.

- Step 6** Under the Transaction Response Message heading, choose a number from the **Retry Limit** drop-down list. The maximum number of times a customer can retry a declined transaction is 5.
- Step 7** 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 8** Click **Save**. The Configuring Profile Settings page appears.
-

Display a Custom Cancel Response Page

CyberSource Hosted Response Page

To display a CyberSource hosted response page:

- Step 1** In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Customer Response**. The Customer Response page appears.
- Step 4** Under the Custom Cancel Response Page heading, check **Hosted by CyberSource**.
- Step 5** Click **Save**.
-

Custom Cancel Response Page

To display your custom cancel response page:

- Step 1** In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Customer Response**. The Customer Response page appears.
- Step 4** Under the Custom Cancel Response Page heading, check **Hosted by You**.

Step 5 Enter the URL for your customer response page. Use port 80, 443, or 8080 in your URL.

Only port 443 should be used with a HTTPS URL. Parse the transaction results from the URL according to the reason code (see ["Reason Codes," page 168](#)), and redirect your customer to the appropriate response page.

Step 6 Click **Save**.

Customize the Checkout Appearance

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.



CyberSource recommends that you preview your changes in the Image Preview window.

To change the header content:

Step 1 In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.

Step 2 Choose a profile. The General Settings page appears.

Step 3 Click **Branding**. The Branding page appears.

Step 4 Check **Display Header**.

Step 5 Click the header color.

Step 6 Choose a color in one of two ways:

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

Step 7 Click **Browse** to upload the image to display as the header banner or as a logo within the header banner.

Step 8 Choose the alignment option for the image or logo: left-aligned, centered, or right-aligned.

Step 9 Click **Save**.



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 100 kB. 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.

To change the main body color and font settings:

Step 1 In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.

Step 2 Choose a profile. The General Settings page appears.

Step 3 Click **Branding**. The Branding page appears.

Step 4 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 color to confirm your selection.

Step 5 Select a text font from the drop-down list.

Step 6 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 color to confirm your selection.

Step 7 Click **Save**.

Step 8 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:



If you are implementing the iframe embedded version of Secure Acceptance Hosted Checkout, the total amount figure is not displayed within the iframe. Any settings you select below are ignored.

- Step 1** In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
 - Step 2** Choose a profile. The General Settings page appears.
 - Step 3** Click **Branding**. The Branding page appears.
 - Step 4** 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 color to confirm your selection.
 - Step 5** 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 color to confirm your selection.
 - Step 6** Click **Save**.
 - Step 7** Click **Set to Default** to restore all the default settings on this page.
-

To change the color of the progress bar:

- Step 1** In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Branding**. The Branding page appears.
- Step 4** 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 color to confirm your selection.
- Step 5** Click **Save**.

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

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

- Step 1** In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Branding**. The Branding page appears.
- Step 4** Choose a background color of the pay or the finish 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 color to confirm your selection.
- Step 5** Choose a color of the pay or the finish 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 at the bottom right to confirm your selection.
- Step 6** Check **Change Button text**. A text box appears for the pay button.
- Step 7** Enter the text you want displayed on the pay button. This button text is required.
- Step 8** Enter the text you want displayed on the finish button. This button text is required.
- Step 9** Click **Save**.
- Step 10** 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** In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
- Step 2** Choose a profile. The General Settings page appears.
- Step 3** Click **Branding**. The Branding page appears.
- Step 4** Check **Display Footer**.

- Step 5** 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 color to confirm your selection.

- Step 6** Click **Browse** to upload a footer logo. Upload the image that you want displayed within the footer of the payment form.



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 7** Choose the alignment option for the image: left-aligned, centered, or right-aligned.

- Step 8** Click Save.

- Step 9** Click **Set to Default** to restore all the default settings on this page.
-

Activate a Profile



You must complete the required settings described in each of these sections before activating a profile:

- ["Configure Payment Methods"](#)
 - ["Create a Security Key"](#)
 - ["Display a Response Page"](#)
-

To activate a profile:

- Step 1** In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
- Step 2** Perform one of the following steps:
- On the Active Profiles tab, choose a profile and click **Publish Profile**.
 - On the Edit Profile page, click **Publish Profile**.
- Step 3** Click **Confirm**.
-

Additional Profile Options

- **Copy**—duplicates the active profile and creates an editable version. The editable version is listed in the inactive profile list. This option is available only for an active profile.
- **Deactivate**—deactivates the active profile. The profile is now listed in the inactive profile list. This option is available only for an active profile.
- **Publish to Active**—activates the inactive profile. This option is available only for an inactive profile.

Payment Transactions

Endpoints and Transaction Types

Table 6 Endpoints

Create Payment Token Endpoints	
Test Transactions	https://testsecureacceptance.cybersource.com/token/create
Live Transactions	https://secureacceptance.cybersource.com/token/create
Live Transactions in India	https://secureacceptance.in.cybersource.com/token/create
Supported transaction type	create_payment_token
Iframe Create Payment Token Endpoints (see "Iframe Implementation," page 177).	
Test Transactions	https://testsecureacceptance.cybersource.com/embedded/token/create
Live Transactions	https://secureacceptance.cybersource.com/embedded/token/create
Live Transactions in India	https://secureacceptance.in.cybersource.com/embedded/token/create
Supported transaction type	create_payment_token
Iframe Transaction Endpoints (see "Iframe Implementation," page 177).	
Test Transactions	https://testsecureacceptance.cybersource.com/embedded/pay
Live Transactions	https://secureacceptance.cybersource.com/embedded/pay
Live Transactions in India	https://secureacceptance.in.cybersource.com/embedded/pay
Supported transaction type	<ul style="list-style-type: none"> ■ authorization ■ authorization,create_payment_token ■ authorization,update_payment_token ■ sale ■ sale,create_payment_token ■ sale,update_payment_token
Iframe Update Payment Token Endpoints (see "Iframe Implementation," page 177).	
Test Transactions	https://testsecureacceptance.cybersource.com/embedded/token/update
Live Transactions	https://secureacceptance.cybersource.com/embedded/token/update
Live Transactions in India	https://secureacceptance.in.cybersource.com/embedded/token/update
Supported transaction type	update_payment_token

Table 6 Endpoints (Continued)

One-click Endpoints	
Test Transactions	https://testsecureacceptance.cybersource.com/oneclick/pay
Live Transactions	https://secureacceptance.cybersource.com/oneclick/pay
Live Transactions in India	https://secureacceptance.in.cybersource.com/oneclick/pay
Supported transaction types	<ul style="list-style-type: none"> ■ authorization ■ authorization,update_payment_token ■ sale ■ sale,update_payment_token
Process Transaction Endpoints	
Test Transactions	https://testsecureacceptance.cybersource.com/pay
Live Transactions	https://secureacceptance.cybersource.com/pay
Live Transactions in India	https://secureacceptance.in.cybersource.com/pay
Supported transaction types	<ul style="list-style-type: none"> ■ authorization ■ authorization,create_payment_token ■ authorization,update_payment_token ■ sale ■ sale,create_payment_token ■ sale,update_payment_token
Update Payment Token Endpoints	
Test Transactions	https://testsecureacceptance.cybersource.com/token/update
Live Transactions	https://secureacceptance.cybersource.com/token/update
Live Transactions in India	https://secureacceptance.in.cybersource.com/token/update
Supported transaction type	update_payment_token
Visa Checkout and Visa SRC Endpoints	
Test Transactions	https://testsecureacceptance.cybersource.com/pay
Live Transactions	https://secureacceptance.cybersource.com/pay
Live Transactions in India	https://secureacceptance.in.cybersource.com/pay
Supported transaction types	<ul style="list-style-type: none"> ■ authorization ■ sale

Required Signed Fields

The following signed fields are required in all Secure Acceptance requests:

- `access_key`
- `amount`
- `currency`
- `locale`
- `profile_id`
- `reference_number`
- `signed_date_time`
- `signed_field_names`
- `transaction_type`
- `transaction_uuid`
- `unsigned_field_names`

For descriptions of signed request fields, see ["Request Fields," page 98](#).

Create a Payment Token

Payment Card



Include the appropriate endpoint that supports the **create_payment_token** transaction type (see ["Endpoints and Transaction Types," page 74](#)). For descriptions of all request and reply fields, see ["API Fields," page 97](#).

Include all request fields in the **signed_field_names** field with the exception of the **card_number** field. The **signed_field_names** field is used to generate a signature that is used to verify the content of the transaction in order to prevent data tampering.

Example 2 Request: Create a Standalone Payment Token

```

reference_number=123456789
transaction_type=create_payment_token
currency=usd
amount=100.00
locale=en
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
profile_id=0FFEAFB-8171-4F34-A22D-1CD38A28A384
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=
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_city=Mountain View
bill_to_address_postal_code=94043
bill_to_address_state=CA
bill_to_address_country=US

```

Example 3 Reply: Create a Standalone Payment Token

```

req_reference_number=123456789
req_transaction_type=create_payment_token
req_locale=en
req_amount=100.00
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_city=Mountain View
req_bill_to_address_postal_code=94043
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
req_profile_id=0FFEAFB-8171-4F34-A22D-1CD38A28A384
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
req_payment_token=3529893314302230706689

```

eCheck



Include the appropriate endpoint that supports the **create_payment_token** transaction type (see ["Endpoints and Transaction Types," page 74](#)). For descriptions of all request and reply fields, see ["API Fields," page 97](#).

Include all request fields in the **signed_field_names** field. The **signed_field_names** field is used to generate a signature that is used to verify the content of the transaction in order to prevent data tampering.

Example 4 Request: Create a Standalone Payment Token

```
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p1
profile_id=0FFEAFfB-8171-4F34-A22D-1CD38A28A384
transaction_type=create_payment_token
amount=100.00
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
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_postal_code=94043
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
```

Example 5 Reply: Create a Standalone 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_amount=100.00
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=0FFEAFB-8171-4F34-A22D-1CD38A28A384
req_company_tax_id=123456789
req_transaction_uuid=38f2efe650ea699597d325ecd7432b1c
req_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 Transaction

One-Click

The customer is directed to the Order Review page. Depending on the settings you configured for Secure Acceptance Hosted Checkout (see ["Configure the Checkout," page 30](#)), the customer can view or update billing, shipping, and payment details before confirming to pay.



Include the appropriate endpoint that supports the **authorization** or **sale** transaction types (see ["Endpoints and Transaction Types," page 74](#)). For descriptions of all request and reply fields, see ["API Fields," page 97](#).

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

Example 6 Request: One-Click Transaction

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
reference_number=1350029885978
payment_token=3427075830000181552556
consumer_id=1239874561
transaction_type=authorization
amount=100.00
currency=USD
locale=en
transaction_uuid=fccfc212e92d23be881d1299ef3c3b314
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=
```

Example 7 Reply: One-Click Transaction

```

transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=0FFEAFB-8171-4F34-A22D-1CD38A28A384
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
req_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

```

```

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=

```

eCheck

The customer is directed to the Order Review page. Depending on the settings you configured for Secure Acceptance Hosted Checkout (see ["Configure the Checkout," page 30](#)), the customer can view or update billing, shipping, and payment details before confirming to pay.



Include the appropriate endpoint that supports the **authorization** or **sale** transaction types (see ["Endpoints and Transaction Types," page 74](#)). For descriptions of all request and reply fields, see ["API Fields," page 97](#).

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

Example 8 Request: Process eCheck Payment Token

```

access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
profile_id=0FFEAFB-8171-4F34-A22D-1CD38A28A384
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=

```

Example 9 Reply: Process eCheck 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
req_echeck_account_type=c
signature=ZUk7d99c/yb+kidvVUbz10JtykmjOt8LMPgk1lRaZR8=
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=0FFEAFB-8171-4F34-A22D-1CD38A28A384
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

```

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.



Include the appropriate endpoint that supports the **authorization,create_payment_token** or **sale,create_payment_token** transaction types (see ["Endpoints and Transaction Types," page 74](#)). For descriptions of all request and reply fields, see ["API Fields," page 97](#).

Example 10 Request: Create a Payment Token for Recurring Payments

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
transaction_type=authorization,create_payment_token
locale=en
amount=5.00
transaction_uuid=fcf212e92d23be881d1299ef3c3b314
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=
consumer_id=1239874561
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
card_type=001
card_number=4111111111111111
card_expiry_date=12-2022
card_cvn=005
recurring_frequency=monthly
recurring_amount=25.00
recurring_start_date=20130125
payment_method=card
```

Example 11 Reply: Create a Payment Token for Recurring Payments

```

transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=0FFEAFB-8171-4F34-A22D-1CD38A28A384
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization,create_payment_token
req_reference_number=1350029885978
req_amount=5.00
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
req_payment_token=3427075830000181552556
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=

```

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.



Include the appropriate endpoint that supports the **authorization,create_payment_token** or **sale,create_payment_token** transaction types (see ["Endpoints and Transaction Types," page 74](#)). For descriptions of all request and reply fields, see ["API Fields," page 97](#).

Example 12 Request: Create a Payment Token for Installment Payments

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=0FFEAFB-8171-4F34-A22D-1CD38A28A384
transaction_type=authorization,create_payment_token
amount=5.00
locale=en
transaction_uuid=fcf0212e92d23be881d1299ef3c3b314
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=
consumer_id=1239874561
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
card_type=001
card_number=4111111111111111
card_expiry_date=12-2022
card_cvn=005
recurring_frequency=monthly
recurring_number_of_installments=6
recurring_amount=25.00
recurring_start_date=20130125
payment_method=card
```

Example 13 Reply: Create a Payment Token for Installment Payments

```

transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=0FFEAFB-8171-4F34-A22D-1CD38A28A384
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization,create_payment_token
req_reference_number=1350029885978
req_amount=5.00
req_currency=USD
req_locale=en
req_payment_method=card
req_consumer_id=1239874561
req_recurring_frequency=monthly
req_recurring_number_of_installments=6
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
req_payment_token=3427075830000181552556
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=

```

Update a Payment Token

Payment Card

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 and clicks **Edit Address** or **Edit Details** to return to the relevant checkout page. The customer clicks **Pay** to confirm the transaction.

You must configure the billing, shipping, and payment details so that a customer can edit their details on the Order Review page. See ["Customize Order Review Details," page 34](#).



Include the endpoint that supports **update_payment_token** or the 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 ["Sample Transaction Process Using JSP," page 47](#). You must include the **allow_payment_token_update** field and set it to `true`.

Example 14 Request: Updating a Payment Token for a Card

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
reference_number=1350029885978
payment_token=3427075830000181552556
amount=100.00
currency=USD
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
locale=en
transaction_uuid=fcfcc212e92d23be881d1299ef3c3b314
signed_date_time=2013-01-17T10:46:39Z
consumer_id=1239874561
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
signature=WrxOhTzhBjYmZROwiCug2My3jiZHOqATimcz5EBA07M=
```

Example 15 Reply: Updating a Payment Token for a Card

```

transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
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=

```

eCheck

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 and clicks Edit Address or Edit Details to return to the relevant checkout page. The customer clicks Pay to confirm the transaction.

You must configure the billing, shipping, and payment details so that a customer can edit their details on the Order Review page. See ["Customize Order Review Details," page 34](#).



Include the endpoint that supports **update_payment_token** or the endpoint that supports **sale,update_payment_token** (updates the token and processes the transaction). You must include the **allow_payment_token_update** field and set to **true**.

Example 16 Request: Updating an eCheck Payment Token

```
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
profile_id=0FFEAFfB-8171-4F34-A22D-1CD38A28A384
reference_number=1845864013783060468573616
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=
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
```

Example 17 Reply: Updating an eCheck Payment Token

```

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=1730560013735542024294683
req_echeck_routing_number=xxxxx2882
transaction_id=3735553783662130706689
req_amount=100.00
req_profile_id=0FFEAFB-8171-4F34-A22D-1CD38A28A384
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

```

Decision Manager



Contact CyberSource Customer Support to enable the Decision Manager verbose data mode for your merchant account and to obtain 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 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 payment 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 an 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.

Optional Decision Manager fields are:

- consumer_id
- complete_route
- customer_cookies_accepted
- customer_gift_wrap
- customer_ip_address
- departure_time
- date_of_birth
- device_fingerprint_id—the device fingerprint ID generated by CyberSource overrides the merchant-generated device fingerprint ID. See [device_fingerprint_id](#), page 107.
- journey_leg#_orig
- journey_leg#_dest
- journey_type

- merchant_defined_data#
- item_#_passenger_forename
- item_#_passenger_email
- item_#_passenger_id
- item_#_passenger_surname
- item_#_passenger_status
- item_#_passenger_type
- returns_accepted

For detailed descriptions of all request fields, see [Table 8, "Request Fields," on page 98](#).
For detailed descriptions of all Decision Manager reply fields, see the *Decision Manager Using the SCMP API Developer Guide* in the [Business Center](#).

Test and View Transactions



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 but must recreate the profile.

Testing Transactions

To test Secure Acceptance transactions:

- Step 1** Log in to the Business Center test environment: <https://ebctest.cybersource.com/ebc2/>
- Step 2** Create a Secure Acceptance profile. See "[Create a Hosted Checkout Profile](#)," page 20, for merchants or "[Create a Hosted Checkout Profile](#)," page 48, for resellers.
- Step 3** Integrate with Secure Acceptance. See "[Samples in Scripting Languages](#)," page 47.
-



Include the test transactions endpoint in your HTML form. See "[Sample Transaction Process Using JSP](#)," page 47.

- Step 4** You can use the following test payment card numbers for transactions. Remove spaces when sending to CyberSource.

Table 7Test Credit Card Numbers

Payment Card Type	Test Account Number
Visa	4111 1111 1111 1111
Mastercard	5555 5555 5555 4444
American Express	3782 8224 6310 005
Discover	6011 1111 1111 1117
JCB	3566 1111 1111 1113
Diners Club	3800 0000 0000 0006
Maestro International (16 digits)	6000 3400 0000 9859
Maestro Domestic (16 digits)	6759 1800 0000 5546

View Transactions in the Business Center

To view a transaction in the Business Center:

- Step 1** Log in to the Business Center:
- Live transactions: <https://ebc2.cybersource.com/ebc2/>
 - Live transactions in India: <https://ebc2.in.cybersource.com/ebc2/>
 - Test transactions: <https://ebctest.cybersource.com/ebc2/>
- Step 2** In the left navigation panel, choose **Transaction Management > Secure Acceptance**. The Secure Acceptance Search page appears.
- Step 3** Search transactions search using your preferred methods.
- Step 4** Click the Request ID link of the transaction that you want to view. The Details page opens.



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

For more information about managing transactions, go to [Transaction Management in the Business Center](#).

API Fields

Data Type Definitions



Unless otherwise noted, all fields are order and case sensitive. CyberSource recommends that you not include URL-encoded characters in any request field prior to generating a signature.

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 (.)
ASCIISAlphaNumericPunctuation	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:mm z
Email	Valid email address.
Enumerated String	Comma-separated alphanumeric string
IP	Valid IP address
ISO 8601 Date	YYYY-MM-DDThh:mm:ssZ
Locale	[a-z] including a hyphen (-)
Numeric	0123456789
Phone	(), +, -, * x 1234567890
URL	Valid URL (http or https)

Request Fields



To prevent data tampering, sign all request fields with the exception of the **card_number** field, the **card_cvn** field, and the **signature** field.

Table 8 Request Fields

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
access_key	Required for authentication with Secure Acceptance. See "Create a Security Key," page 29 . Important To prevent data tampering, sign this field.	Required by the Secure Acceptance application.	Alphanumeric String (32)
aggregator_id	Value that identifies you as a payment aggregator. Obtain this value for the processor. CyberSource through VisaNet The value for this field corresponds to the following data in the TC 33 capture file ¹ : <ul style="list-style-type: none"> Record: CP01 TCR6 Position: 95-105 Field: Mastercard Payment Facilitator ID FDC Compass This value must consist of upper-case characters. Field Length American Express Direct: 20 CyberSource through VisaNet: 11 FDC Compass: 20 FDC Nashville Global: 15 Required/Optional American Express Direct: R for all aggregator transactions. CyberSource through VisaNet: R for Mastercard aggregator authorizations; otherwise, not used. FDC Compass: R for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	authorization (See description)	String (See description)

¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
allow_payment_token_update	Indicates whether the customer can update the billing, shipping, and payment information on the order review page. Possible values: <ul style="list-style-type: none"> ■ <code>true</code>: Customer can update details. ■ <code>false</code>: Customer cannot update details. 	update_payment_token (R)	Enumerated 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.	<ul style="list-style-type: none"> ■ 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)
auth_indicator	Flag that specifies the purpose of the authorization. Possible values: <ul style="list-style-type: none"> ■ 0: Preauthorization ■ 1: Final authorization Mastercard requires European merchants to indicate whether the authorization is a final authorization or a preauthorization. To set the default for this field, contact CyberSource Customer Support.	authorization (See description)	String (1)
auth_type	Authorization type. Possible values: <ul style="list-style-type: none"> ■ <code>AUTOCAPTURE</code>: Automatic capture. ■ <code>STANDARDCAPTURE</code>: Standard capture. ■ <code>verbal</code>: Forced capture. Asia, Middle East, and Africa Gateway; Cielo; Comercio Latino; and CyberSource Latin American Processing Set this field to <code>AUTOCAPTURE</code> and include it in a bundled request to indicate that you are requesting an automatic capture. If your account is configured to enable automatic captures, set this field to <code>STANDARDCAPTURE</code> and include it in a standard authorization or bundled request to indicate that you are overriding an automatic capture.	ics_auth (See description.) ics_bill (Required for a verbal authorization; otherwise, not used.)	Cielo, Comercio Latino, and CyberSource Latin American Processing: String (15) All other processors: String (11)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
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: <ul style="list-style-type: none"> ■ <code>true</code>: Bill payment or loan payment. ■ <code>false</code> (default): Not a bill payment or loan payment. 	This field is optional.	Enumerated String (5)
bill_to_address_city	City in the billing address. 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 "Display Billing Information Fields," page 31 .	<ul style="list-style-type: none"> ■ create_payment_token (R) ■ authorization or sale (R) ■ authorization, create_payment_token (R) ■ sale, create_payment_token (R) ■ update_payment_token (O) 	AlphaNumeric Punctuation Atos: String (32) All other processors: String (50)
bill_to_address_country	Country code for the billing address. Use the two-character ISO country codes . 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 "Display Billing Information Fields," page 31 .	<ul style="list-style-type: none"> ■ 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. On JCN Gateway, this field is required when the authorization or sale request includes create_payment_token or Decision Manager. This field is optional when requesting an authorization or a sale without create_payment_token or Decision Manager. 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 "Display Billing Information Fields," page 31 .	<ul style="list-style-type: none"> ■ create_payment_token (R) ■ authorization or sale (R) ■ authorization, create_payment_token (R) ■ sale, create_payment_token (R) ■ update_payment_token (O) 	AlphaNumeric Punctuation Atos: String (29) CyberSource through VisaNet: String (40) Moneris: String (50) Worldpay VAP: String (35) All other processors: String (60)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
bill_to_address_line2	<p>Second line of the billing address.</p> <p>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 "Display Billing Information Fields," page 31.</p>	This field is optional.	<p>AlphaNumeric Punctuation</p> <p>Atos: String (29)</p> <p>CyberSource through VisaNet: String (40)</p> <p>Moneris: String (50)</p> <p>Worldpay VAP: String (35)</p> <p>All other processors: String (60)</p>
bill_to_address_postal_code	<p>Postal code for the billing address.</p> <p>This field is required if bill_to_address_country is U.S. or Canada.</p> <p>When the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits]</p> <p>Example 12345-6789</p> <p>When the billing country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space][numeric][alpha][numeric]</p> <p>Example A1B 2C3</p> <p>For the rest of the world countries, the maximum length is 10.</p> <p>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 "Display Billing Information Fields," page 31.</p>	See description.	<p>AlphaNumeric Punctuation</p> <p>See description.</p>

¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
bill_to_address_state	<p>State or province in the billing address. Use the two-character ISO state and province code.</p> <p>This field is required if bill_to_address_country is U.S. or Canada.</p> <p>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 "Display Billing Information Fields," page 31.</p>	See description.	AlphaNumeric Punctuation String (2)
bill_to_company_name	<p>Name of the customer's company.</p> <p>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 "Display Billing Information Fields," page 31.</p>	This field is optional.	AlphaNumeric Punctuation String (40)
bill_to_email	<p>Customer email address, including the full domain name.</p> <p>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 "Display Billing Information Fields," page 31.</p>	<ul style="list-style-type: none"> ■ 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	<p>Customer first name. This name must be the same as the name on the card.</p> <p>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 "Display Billing Information Fields," page 31.</p>	<ul style="list-style-type: none"> ■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O) 	AlphaNumeric Punctuation String (60)
<p>¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>			

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
bill_to_phone	<p>Customer phone number. CyberSource recommends that you include the country code if the order is from outside the U.S.</p> <p>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 "Display Billing Information Fields," page 31.</p> <p>This field is optional for card payments. For eCheck payments this field is required if your processor is CyberSource ACH Service or TeleCheck.</p>	See description.	<p>Phone</p> <p>String (6 to 15)</p> <p>String (10) if using TeleCheck for eCheck payments.</p>
bill_to_surname	<p>Customer last name. This name must be the same as the name on the card.</p> <p>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 "Display Billing Information Fields," page 31.</p>	<ul style="list-style-type: none"> ■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O) 	<p>AlphaNumeric Punctuation</p> <p>String (60)</p>
card_cvn	<p>Card verification number.</p> <p>For American Express card types, the CVN must be 4 digits.</p> <p>This field can be configured as required or optional. See "Configure Payment Methods," page 21.</p>	See description.	<p>Numeric</p> <p>String (4)</p>
card_expiry_date	<p>Card expiration date.</p> <p>Format: MM-YYYY</p>	<ul style="list-style-type: none"> ■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O) 	<p>Date (a)</p> <p>String (7)</p>
<p>1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>			

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
card_number	Card number. Use only numeric values. Be sure to include valid and well-formed data for this field.	<ul style="list-style-type: none"> ■ 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)
card_type	Type of card to authorize. Use one of these values: <ul style="list-style-type: none"> ■ 001: Visa ■ 002: Mastercard ■ 003: American Express ■ 004: Discover ■ 005: Diners Club: cards starting with 54 or 55 are rejected. ■ 006: Carte Blanche ■ 007: JCB ■ 014: EnRoute ■ 021: JAL ■ 024: Maestro UK Domestic ■ 031: Delta ■ 033: Visa Electron ■ 034: Dankort ■ 036: Carte Bancaire ■ 037: Carta Si ■ 042: Maestro International ■ 043: GE Money UK card ■ 050: Hipercard (sale only) ■ 054: Elo 	<ul style="list-style-type: none"> ■ 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)

¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
card_type_selection_indicator	Identifies whether the card type is the result of the default acquirer parameter settings or the selection of the cardholder. Possible values: <ul style="list-style-type: none"> 0: Card type selected by default acquirer settings. 1: Card type selected by cardholder. This field is supported only on Credit Mutuel-CIC. The default value is 1.	ics_auth (O)	String (1)
company_tax_id	Company's tax identifier. Contact your TeleCheck representative to find out whether this field is required or optional. 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 "Display eCheck Information," page 33 .	<ul style="list-style-type: none"> sale (See description) create_payment_token (See description) sale,create_payment_token (See description) update_payment_token (See description) 	AlphaNumeric Punctuation String (9)
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 "Decision Manager," page 93 .	AlphaNumeric Punctuation String (255)
conditions_accepted	Indicates whether the customer accepted the service fee amount. Possible values: <ul style="list-style-type: none"> false: Customer did not accept. true: Customer did accept. 	This is a required field when service fee is enabled for the profile. See "Enable the Service Fee," page 56 .	Enumerated String String (5)
1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.			

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
consumer_id	Identifier for the customer's account. This field is defined when you create a subscription.	<ul style="list-style-type: none"> ■ create_payment_token (O) ■ authorization,create_payment_token (O) ■ sale,create_payment_token (O) ■ update_payment_token (O) 	AlphaNumeric Punctuation String (100)
currency	Currency used for the order. For the possible values, see the ISO currency codes . Important To prevent data tampering, sign this field.	<ul style="list-style-type: none"> ■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O) 	Alpha String (3)
customer_cookies_accepted	Indicates whether the customer's browser accepts cookies. This field can contain one of the following values: <ul style="list-style-type: none"> ■ true: Customer browser accepts cookies. ■ false: Customer browser does not accept cookies. 	This field is optional. See "Decision Manager," page 93 .	Enumerated String String (5)
customer_gift_wrap	Indicates whether the customer requested gift wrapping for this purchase. This field can contain one of the following values: <ul style="list-style-type: none"> ■ true: Customer requested gift wrapping. ■ false: Customer did not request gift wrapping. 	This field is optional. See "Decision Manager," page 93 .	Enumerated String String (5)
customer_ip_address	Customer's IP address reported by your web server via socket information.	This field is optional. See "Decision Manager," page 93 .	IP String (15)
date_of_birth	Date of birth of the customer. Use the format: YYYYMMDD. 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 "Display eCheck Information," page 33 .	This is an optional field.	Date (b) String (8)
1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.			

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
debt_indicator	<p>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:</p> <ul style="list-style-type: none"> ■ <code>false</code> (default): Not a loan payment. ■ <code>true</code>: Loan payment. 	This field is optional.	<p>Enumerated String</p> <p>String (5)</p>
departure_time	<p>Departure date and time of the first leg of the trip. Use one of the following formats:</p> <ul style="list-style-type: none"> ■ <code>yyyy-MM-dd HH:mm z</code> ■ <code>yyyy-MM-dd hh:mm a z</code> ■ <code>yyyy-MM-dd hh:mma z</code> ■ <code>HH</code> = 24-hour format ■ <code>hh</code> = 12-hour format ■ <code>a</code> = am or pm (case insensitive) ■ <code>z</code> = time zone of the departing flight. <p>Examples</p> <ul style="list-style-type: none"> ■ 2019-01-20 23:30 GMT ■ 2019-01-20 11:30 PM GMT ■ 2019-01-20 11:30pm GMT 	<p>This field is optional.</p> <p>See "Decision Manager," page 93.</p>	<p>Date (c)</p> <p>DateTime (29)</p>
device_fingerprint_id	<p>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 (_)</p> <p>However, do not use the same uppercase and lowercase letters to indicate different session IDs.</p> <p>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.</p> <p>Important The CyberSource-generated device fingerprint ID overrides the merchant-generated device fingerprint ID.</p> <p>See skip_decision_manager, page 127.</p>	<p>This field is optional.</p> <p>See "Decision Manager," page 93.</p>	<p>AlphaNumeric Punctuation</p> <p>String (88)</p>
<p>¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>			

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
driver_license_number	<p>Driver's license number of the customer.</p> <p>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.</p> <p>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 "Display eCheck Information," page 33.</p>	<ul style="list-style-type: none"> ■ sale (See description) ■ create_payment_token (See description) ■ sale,create_payment_token (See description) ■ update_payment_token (See description) 	<p>AlphaNumeric</p> <p>String (30)</p>
driver_license_state	<p>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.</p> <p>Contact your TeleCheck representative to find out whether this field is required or optional.</p> <p>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 "Display eCheck Information," page 33.</p>	<ul style="list-style-type: none"> ■ sale (See description) ■ create_payment_token (See description) ■ sale,create_payment_token (See description) ■ update_payment_token (See description) 	<p>Alpha</p> <p>String (2)</p>
e_commerce_indicator	<p>The commerce indicator for the transaction type.</p> <p>Value: <code>install</code></p> <p>This field is required only for installment payments on CyberSource Latin American Processing.</p>	<p>authorization (See description)</p>	<p>String (20)</p>
echeck_account_number	<p>Account number.</p> <p>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 "Display eCheck Information," page 33.</p>	<ul style="list-style-type: none"> ■ sale (R) ■ create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O) 	<p>Numeric</p> <p>Non-negative integer (8 to 17)</p>

¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
echeck_account_type	Account type. Possible values: <ul style="list-style-type: none"> ■ C: Checking ■ S: Savings (USD only) ■ X: Corporate checking (USD only) ■ G: General Ledger ■ 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 "Display eCheck Information," page 33. 	<ul style="list-style-type: none"> ■ sale (R) ■ create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O) 	<p>Enumerated String</p> <p>String (1)</p>
echeck_check_number	Check number. If your payment processor is TeleCheck, you should include this field. 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 "Display eCheck Information," page 33.	<ul style="list-style-type: none"> ■ sale (See description) ■ create_payment_token (See description) ■ sale,create_payment_token (See description) ■ update_payment_token (See description) 	<p>Numeric</p> <p>Integer (8)</p>
echeck_effective_date	Effective date for the transaction. This date must be within 45 days of the current date. Format: MMDDYYYY	<ul style="list-style-type: none"> ■ sale (O) ■ sale,create_payment_token (O) 	<p>Date (b)</p> <p>String (8)</p>
echeck_routing_number	Bank routing number. If the currency being used is CAD, the maximum length of the routing number is 8 digits. If the currency being used is USD, the maximum length of the routing number is 9 digits. 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 "Display eCheck Information," page 33.	<ul style="list-style-type: none"> ■ sale (R) ■ create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O) 	<p>Numeric</p> <p>Non-negative integer (See description)</p>
<p>1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>			

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
echeck_sec_code	<p>If your payment processor is TeleCheck, then this field is required.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ 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. 	<ul style="list-style-type: none"> ■ sale (See description) ■ create_payment_token (See description) ■ sale,create_payment_token (See description) ■ update_payment_token (See description) 	<p>Enumerated String</p> <p>String (3)</p>
ignore_avs	<p>Ignore the results of AVS verification.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ true ■ false <p>Important To prevent data tampering, sign this field.</p>	This field is optional.	<p>Enumerated String</p> <p>String (5)</p>

¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
ignore_cvn	Ignore the results of CVN verification. Possible values: <ul style="list-style-type: none"> ■ true ■ false Important To prevent data tampering, sign this field.	This field is optional.	Enumerated String String (5)
installment_amount	Amount for the current installment payment. This field is required only for installment payments on CyberSource Latin American Processing or CyberSource through VisaNet.	authorization (See description)	Amount (12)
installment_frequency	Frequency of the installment payments. Possible values: <ul style="list-style-type: none"> ■ B: Biweekly ■ M: Monthly ■ W: Weekly This field is supported only on CyberSource through VisaNet.	authorization (See description)	AlphaNumeric (2)
installment_plan_type	Flag that indicates the type of funding for the installment plan associated with the payment. Possible values: <ul style="list-style-type: none"> ■ 1: Merchant-funded installment plan ■ 2: Issuer-funded installment plan If you do not include this field in the request, CyberSource uses the value that is in your CyberSource account. To change this value contact CyberSource Customer Service. CyberSource through VisaNet American Express-defined code that indicates the type of installment plan for this transaction. Contact American Express for: <ul style="list-style-type: none"> ■ Information about the types of installment plans that American Express provides ■ Values for this field 	authorization (See description)	CyberSource Latin American Processing: String (1) CyberSource through VisaNet: String (2)

¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
installment_sequence	<p>Installment number when making payments in installments. Used along with installment_total_count to keep track of which payment is being processed. For example, the second of five payments would be passed to CyberSource as installment_sequence = 2 and installment_total_count = 5.</p> <p>This field is required only for installment payments on CyberSource through VisaNet.</p>	authorization (See description)	Integer (2)
installment_total_amount	<p>Total amount of the loan that is being paid in installments.</p> <p>This field is required only for installment payments on CyberSource Latin American Processing or CyberSource through VisaNet.</p>	authorization (see description)	Amount (12)
installment_total_count	<p>Total number of installment payments as part of an authorization.</p> <p>Possible values: 1 to 99</p> <p>This field is required only for installment payments on CyberSource Latin American Processing or CyberSource through VisaNet.</p>	authorization (See description)	Numeric String (2)
issuer_additional_data	<p>Data defined by the issuer.</p> <p>See the “Formats for Discretionary Data” section in Credit Card Services Using the SCMP API or Credit Card Services Using the Simple Order API.</p>	authorization (O)	Alphanumeric String (256)
item_#_code	Type of product. # can range from 0 to 199.	<p>This field is optional.</p> <p>If you include this field, you must also include the line_item_count field.</p>	AlphaNumeric Punctuation String (255)
item_#_name	<p>Name of the item. # can range from 0 to 199.</p> <p>This field is required when the item_#_code value is not default nor related to shipping or handling.</p>	<p>See description.</p> <p>If you include this field, you must also include the line_item_count field.</p>	AlphaNumeric Punctuation String (255)
item_#_passenger_email	Passenger's email address.	<p>This field is optional.</p> <p>See "Decision Manager," page 93.</p>	String (255)
<p>1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>			

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
item_#_passenger_forename	Passenger's first name.	This field is optional. See "Decision Manager," page 93.	String (60)
item_#_passenger_id	ID of the passenger to whom the ticket was issued. For example, you can use this field for the frequent flyer number.	This field is optional. See "Decision Manager," page 93.	String (32)
item_#_passenger_phone	Passenger's phone number. If the order is from outside the U.S., include the country code.	This field is optional. See "Decision Manager," page 93.	String (15)
item_#_passenger_status	Your company's passenger classification, such as with a frequent flyer number. In this case, you might use values such as standard, gold, or platinum.	This field is optional. See "Decision Manager," page 93.	String (32)
item_#_passenger_surname	Passenger's last name.	This field is optional. See "Decision Manager," page 93.	String (60)
item_#_passenger_type	Passenger classification associated with the price of the ticket. You can use one of the following values: <ul style="list-style-type: none"> ■ ADT: Adult ■ CNN: Child ■ INF: Infant ■ YTH: Youth ■ STU: Student ■ SCR: Senior Citizen ■ MIL: Military 	This field is optional. See "Decision Manager," page 93.	String (32)

¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
item_#_quantity	<p>Quantity of line items. The default value is 1.</p> <p>Required field when one of the following product codes is used:</p> <ul style="list-style-type: none"> ■ adult_content ■ coupon ■ electronic_good ■ electronic_software ■ gift_certificate ■ service ■ subscription <p># can range from 1 to 199.</p> <p>This field is required when the item_#_code value is not default nor related to shipping or handling.</p>	<p>See description.</p> <p>If you include this field, you must also include the line_item_count field.</p>	<p>Numeric</p> <p>String (10)</p>
item_#_sku	<p>Identification code for the product.</p> <p>Required field when one of the following product codes is used:</p> <ul style="list-style-type: none"> ■ adult_content ■ coupon ■ electronic_good ■ electronic_software ■ gift_certificate ■ service ■ subscription <p># can range from 0 to 199.</p>	<p>See description.</p> <p>If you include this field, you must also include the line_item_count field.</p>	<p>AlphaNumeric Punctuation</p> <p>String (255)</p>
item_#_tax_amount	<p>Tax amount to apply to the line item. # can range from 0 to 199. This value cannot be negative. The tax amount and the offer amount must be in the same currency.</p>	<p>This field is optional.</p> <p>If you include this field, you must also include the line_item_count field.</p>	<p>Amount</p> <p>String (15)</p>
item_#_unit_price	<p>Price of the line item. # can range from 0 to 199. This value cannot be negative.</p> <p>Important You must include either this field or the amount field in the request.</p>	<p>See description.</p> <p>If you include this field, you must also include the line_item_count field.</p>	<p>Amount</p> <p>String (15)</p>
<p>¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>			

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
journey_leg#_dest	<p>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.</p> <p>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.</p>	<p>This field is optional.</p> <p>See "Decision Manager," page 93.</p>	<p>Alpha</p> <p>String (3)</p>
journey_leg#_orig	<p>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.</p> <p>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.</p>	<p>This field is optional.</p> <p>See "Decision Manager," page 93.</p>	<p>Alpha</p> <p>String (3)</p>
journey_type	Type of travel, such as one way or round trip.	<p>This field is optional.</p> <p>See "Decision Manager," page 93.</p>	<p>AlphaNumeric Punctuation</p> <p>String (32)</p>
line_item_count	Total number of line items. Maximum number is 200.	This field is required if you include any item fields in the request.	<p>Numeric</p> <p>String (2)</p>
locale	<p>Indicates the language to use for customer-facing content. Possible value: en-us. See "Activate a Profile," page 46.</p> <p>Important To prevent data tampering, sign this field.</p>	Required by the Secure Acceptance application.	<p>Locale</p> <p>String (5)</p>

¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
merchant_defined_data#	<p>Optional fields that you can use to store information (see "Customer Notification Details," page 36). # can range from 1 to 100.</p> <p>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 through to Decision Manager as part of the initial payment request and are not stored against the payment token.</p> <p>Important 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 and any Secure Acceptance field that is not specifically designed to capture personally identifying information. 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, 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.</p>	<p>This field is optional.</p> <p>See "Decision Manager," page 93.</p>	<p>AlphaNumeric Punctuation String (100)</p>
<p>1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>			

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
merchant_descriptor merchant_descriptor_ alternate merchant_descriptor_ city merchant_descriptor_ contact merchant_descriptor_ country merchant_descriptor_ state merchant_descriptor_ postal_code merchant_descriptor_ street	For the descriptions, used-by information, data types, and lengths for these fields, see the “Merchant Descriptors” section in either Credit Card Services Using the SCMP API or Credit Card Services Using the Simple Order API .	authorization (See description)	
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.	AlphaNumeric Punctuation String (2000)
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.	AlphaNumeric Punctuation String (100)
override_backoffice_ post_url	Overrides the backoffice post URL profile setting with your URL. URL must be HTTPS and support TLS 1.2 or later.	This field is optional.	URL String (255)
override_custom_ cancel_page	Overrides the custom cancel page profile setting with your URL. URL must be HTTPS and support TLS 1.2 or later.	This field is optional.	URL String (255)
override_custom_ receipt_page	Overrides the custom receipt profile setting with your URL. URL must be HTTPS and support TLS 1.2 or later. Important To prevent data tampering, sign this field.	This field is optional.	URL String (255)
1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.			

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
override_customer_utc_offset	Overrides the transaction date and time with the number of minutes the customer is ahead of or behind UTC. Use this field to override the local browser time detected by Secure Acceptance. This time determines the date on receipt pages and emails. For example, if the customer is 2 hours ahead, the value is 120; if 2 hours behind, then -120; if UTC, the value is 0.	This field is optional.	Integer (5)
override_paypal_order_setup	Overrides the PayPal order setup profile setting. Possible values: <ul style="list-style-type: none">■ include_authorization: The PayPal order is created and authorized.■ exclude_authorization: The PayPal order is created but not authorized.	This field is optional. See "," page 27 .	String (21)
payer_authentication_challenge_code	Possible values: <ul style="list-style-type: none">■ 01: No preference■ 02: No challenge request■ 03: Challenge requested (3D Secure requestor preference)■ 04: Challenge requested (mandate)	This field is optional.	Integer (2)
payer_authentication_customer_annual_transaction_count	Number of transactions (successful and abandoned) for this cardholder account within the past year. Recommended for Discover ProtectBuy.	This field is optional.	Integer (3)
payer_authentication_customer_daily_transaction_count	Number of transaction (successful or abandoned) for this cardholder account within the past 24 hours. Recommended for Discover ProtectBuy.	This field is optional.	Integer (3)
payer_authentication_marketing_source	Indicates origin of the marketing offer. Recommended for Discover ProtectBuy.	This field is optional.	String (40)
payer_authentication_mobile_phone	Cardholder's mobile phone number. Important Required for Visa Secure transactions in Brazil. Do not use this request field for any other types of transactions.	This field is optional.	Integer (25)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
payer_authentication_new_customer	Indicates whether the customer is a new or existing customer with the merchant. Possible values: <ul style="list-style-type: none">■ true■ false	This field is optional.	String (5)
payer_authentication_pre_order	Indicates whether cardholder is placing an order with a future availability or release date. Possible values: <ul style="list-style-type: none">■ 01: Merchandise available■ 02: Future availability	This field is optional.	Integer (2)
payer_authentication_pre_order_date	Expected date that a pre-ordered purchase will be available. Format: YYYYMMDD	This field is optional.	Integer (8)
payer_authentication_recurring_end_date	The date after which no further recurring authorizations should be performed. Format: YYYYMMDD. This field is required for recurring transactions. If recurring_frequency and recurring_number_of_installments are included in the request, Secure Acceptance will automatically populate this field. Specify a value to override this logic.	This field is optional.	Integer (8)
payer_authentication_recurring_frequency	Integer value indicating the minimum number of days between recurring authorizations. A frequency of monthly is indicated by the value 28. Multiple of 28 days will be used to indicate months. Example: 6 months= 168 This field is required for recurring transactions. If recurring_frequency is included in the request, Secure Acceptance will automatically populate this field. Specify a value to override this logic.	This field is optional.	Integer (3)
1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.			

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
payer_authentication_reorder	Indicates whether the cardholder is reordering previously purchased merchandise. Possible values: <ul style="list-style-type: none"> 01: First time ordered 02: Reordered 	This field is optional.	Integer (2)
payer_authentication_ship_to_address_first_used	Date on which this shipping address was first used. Possible values: <ul style="list-style-type: none"> -1: Guest account 0: First used during this transaction If neither value applies, enter the date in YYYYMMDD format. Recommended for Discover ProtectBuy.	This field is optional.	Integer (8)
payer_authentication_transaction_mode	Transaction mode identifier. Identifies the channel from which the transaction originates. Possible values: <ul style="list-style-type: none"> M: MOTO (Mail Order Telephone Order) R: Retail S: E-commerce P: Mobile Device T: Tablet 	Required by the Secure Acceptance application.	String (1)
payment_method	Method of payment. Possible values: <ul style="list-style-type: none"> card echeck paypal visacheckout 	This field is optional.	Enumerated String String (30)
¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.			

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
payment_token	<p>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.</p> <p>You must be currently using Token Management Services. Populate this field with the customer subscription ID.</p> <p>This field is required for token-based transactions.</p>	<ul style="list-style-type: none"> ■ authorization or sale (R) ■ authorization,update_payment_token (R) ■ sale,update_payment_token (R) ■ update_payment_token (R) 	<p>Numeric</p> <p>String (26)</p>
payment_token_comments	Optional comments you can add for the customer subscription.	This field is optional.	<p>AlphaNumeric Punctuation</p> <p>String (255)</p>
payment_token_title	Name or title for the customer subscription.	This field is optional.	<p>AlphaNumeric Punctuation</p> <p>String (60)</p>
profile_id	<p>Identifies the profile to use with each transaction.</p> <p>Important To prevent data tampering, sign this field.</p>	Assigned by the Secure Acceptance application.	<p>ASCIIAlphaNumericPunctuation</p> <p>String (36)</p>
promotion_code	Promotion code for a transaction.	This field is optional.	String (100)
recipient_account_id	Identifier for the recipient's account. Use the first six digits and last four digits of the recipient's account number.	authorization (R for recipient transactions, otherwise not used)	<p>Numeric</p> <p>String (10)</p>
recipient_date_of_birth	<p>Recipient's date of birth.</p> <p>Format: YYYYMMDD.</p>	authorization (R for recipient transactions, otherwise not used)	<p>Date (b)</p> <p>String (8)</p>
recipient_postal_code	<p>Partial postal code for the recipient's address.</p> <p>For example, if the postal code is NN5 7SG, the value for this field should be the first part of the postal code: NN5.</p>	authorization (R for recipient transactions, otherwise not used)	<p>Alphanumeric</p> <p>String (6)</p>
recipient_surname	Recipient's last name.	authorization (R for recipient transactions, otherwise not used)	<p>Alpha</p> <p>String (6)</p>
<p>¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>			

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
recurring_amount	Payment amount for each installment or recurring subscription payment.	<ul style="list-style-type: none"> ■ create_payment_token (R) ■ authorization,create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O) 	Amount String (15)
recurring_automatic_renew	Indicates whether to automatically renew the payment schedule for an installment subscription. Possible values: <ul style="list-style-type: none"> ■ true (default): Automatically renew. ■ false: Do not automatically renew. 	<ul style="list-style-type: none"> ■ create_payment_token (O) ■ authorization,create_payment_token (O) ■ sale,create_payment_token (O) ■ update_payment_token (O) 	Enumerated String String (5)
recurring_frequency	Frequency of payments for an installment or recurring subscription. Possible values: <ul style="list-style-type: none"> ■ 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 	<ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ■ 261: Weekly ■ 130: Bi-weekly ■ 65: Quad-weekly ■ 60: Monthly ■ 120: Semi-monthly ■ 20: Quarterly ■ 10: Semi-annually ■ 5: Annually 	<ul style="list-style-type: none"> ■ create_payment_token (R) ■ authorization,create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O) 	Numeric String (3)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
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.	<ul style="list-style-type: none"> ■ 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. Important To prevent data tampering, sign this field.	Required by the Secure Acceptance application.	AlphaNumeric Punctuation Asia, Middle East, and Africa Gateway: String (40) Atos: String (32) All other processors: String (50)
returns_accepted	Indicates whether product returns are accepted. This field can contain one of the following values: <ul style="list-style-type: none"> ■ true ■ false 	This field is optional. See "Decision Manager," page 93 .	Enumerated String (5)
sales_organization_id	Company ID assigned to an independent sales organization. Obtain this value from Mastercard. CyberSource through VisaNet The value for this field corresponds to the following data in the TC 33 capture file ¹ : <ul style="list-style-type: none"> ■ Record: CP01 TCR6 ■ Position: 106-116 ■ Field: Mastercard Independent Sales Organization ID 	authorization (Required for Mastercard aggregator transactions on CyberSource through VisaNet)	Nonnegative integer (11)
ship_to_address_city	City of shipping address. 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 "Display Shipping Information Fields," page 32 .	This field is optional.	AlphaNumeric Punctuation String (50)

¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
ship_to_address_country	Country code for the shipping address. Use the two-character ISO country codes . 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 "Display Shipping Information Fields," page 32 .	This field is optional.	Alpha String (2)
ship_to_address_line1	First line of shipping address. 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 "Display Shipping Information Fields," page 32 .	This field is optional.	AlphaNumeric Punctuation String (60)
ship_to_address_line2	Second line of shipping address. 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 "Display Shipping Information Fields," page 32 .	This field is optional.	AlphaNumeric Punctuation String (60)
ship_to_address_postal_code	Postal code for the shipping address. This field is required if bill_to_address_country is U.S. or Canada. When the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits] Example 12345-6789 When the billing country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space] [numeric][alpha][numeric] Example A1B 2C3 For the rest of the world countries, the maximum length is 10. 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 "Display Shipping Information Fields," page 32 .	This field is optional.	AlphaNumeric Punctuation See description.

- 1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
ship_to_address_state	<p>State or province of shipping address. Use the two-character ISO state and province codes.</p> <p>This field is required if shipping address is U.S. or Canada.</p> <p>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 "Display Shipping Information Fields," page 32.</p>	This field is optional.	<p>AlphaNumeric Punctuation</p> <p>String (2)</p>
ship_to_company_name	<p>Name of the company receiving the product.</p> <p>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 "Display Shipping Information Fields," page 32.</p>	This field is optional.	<p>AlphaNumeric Punctuation</p> <p>String (40)</p>
ship_to_forename	<p>First name of the person receiving the product.</p> <p>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 "Display Shipping Information Fields," page 32.</p>	This field is optional.	<p>AlphaNumeric Punctuation</p> <p>String (60)</p>
ship_to_phone	<p>Phone number of the shipping address.</p> <p>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 "Display Shipping Information Fields," page 32.</p>	This field is optional.	<p>Phone</p> <p>String (6 to 15)</p>
ship_to_surname	<p>Last name of the person receiving the product.</p> <p>This can be entered by your customer during the checkout process, or you can include this in your request to Secure Acceptance. See "Display Shipping Information Fields," page 32.</p>	This field is optional.	<p>AlphaNumeric Punctuation</p> <p>String (60)</p>
<p>1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>			

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
shipping_method	<p>Shipping method for the product. Possible values:</p> <ul style="list-style-type: none"> ■ 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.	<p>Enumerated String</p> <p>String (10)</p>
signature	<p>Merchant-generated Base64 signature. This is generated using the signing method for the access_key field supplied.</p>	Required by the Secure Acceptance application.	AlphaNumeric Punctuation
signed_date_time	<p>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.</p> <p>Format: YYYY-MM-DDThh:mm:ssZ</p> <p>Example 2019-08-11T22:47:57Z equals August 11, 2019, at 22:47:57 (10:47:57 p.m.). The T separates the date and the time. The Z indicates UTC.</p> <p>Your system time must be accurate to avoid payment processing errors related to the signed_date_time field.</p> <p>Important To prevent data tampering, sign this field.</p>	Required by the Secure Acceptance application.	<p>ISO 8601 Date String (20)</p>
signed_field_names	<p>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.</p> <p>Important All request fields should be signed to prevent data tampering, with the exception of the card_number field and the signature field.</p>	Required by the Secure Acceptance application.	<p>AlphaNumeric Punctuation</p> <p>Variable</p>
<p>¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>			

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
skip_auto_auth	Indicates whether to skip or perform the preauthorization check when creating this token. Possible values: <ul style="list-style-type: none"> ■ <code>true</code> (skip the preauthorization check) ■ <code>false</code> (perform the preauthorization check) 	This field is optional.	Enumerated String String (5)
skip_bin_lookup	Indicates whether to skip the BIN lookup service. See "BIN Lookup," page 18 . This field can contain one of the following values: <ul style="list-style-type: none"> ■ <code>true</code> ■ <code>false</code> 	This field is optional.	Enumerated String String (5)
skip_decision_manager	Indicates whether to skip Decision Manager. See Chapter 5, "Decision Manager," on page 93 . This field can contain one of the following values: <ul style="list-style-type: none"> ■ <code>true</code> (Decision Manager is not enabled for this transaction, and the device fingerprint ID will not be displayed) ■ <code>false</code> 	This field is optional.	Enumerated String String (5)
submerchant_city	Sub-merchant's city. FDC Compass This value must consist of uppercase characters.	authorization American Express Direct: R for all aggregator transactions. CyberSource through VisaNet: not used. FDC Compass: R for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	American Express Direct: String (15) FDC Compass: String (21) FDC Nashville Global: String (11)
¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.			

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
submerchant_country	<p>Sub-merchant's country. Use the two-character ISO Standard Country Codes.</p> <p>FDC Compass This value must consist of uppercase characters.</p>	<p>authorization</p> <p>American Express Direct: R for all aggregator transactions.</p> <p>CyberSource through VisaNet: not used.</p> <p>FDC Compass: O for all aggregator transactions.</p> <p>FDC Nashville Global: R for all aggregator transactions.</p>	String (3)
submerchant_email	<p>Sub-merchant's email address.</p> <p>CyberSource through VisaNet With American Express, the value for this field corresponds to the following data in the TC 33 capture file¹:</p> <ul style="list-style-type: none"> Record: CP01 TCRB Position: 25-64 Field: American Express Seller E-mail Address 	<p>authorization</p> <p>American Express Direct: R for all aggregator transactions.</p> <p>CyberSource through VisaNet: O for all aggregator transactions with American Express; otherwise, not used.</p> <p>FDC Compass: O for all aggregator transactions.</p> <p>FDC Nashville Global: R for all aggregator transactions.</p>	<p>American Express Direct: String (40)</p> <p>CyberSource through VisaNet: String (40)</p> <p>FDC Compass: String (40)</p> <p>FDC Nashville Global: String (19)</p>
<p>¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>			

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
submerchant_id	<p>The ID you assigned to your sub-merchant.</p> <p>FDC Compass</p> <ul style="list-style-type: none"> This value must consist of uppercase characters. <p>CyberSource through VisaNet</p> <p>With American Express, the value for this field corresponds to the following data in the TC 33 capture file¹:</p> <ul style="list-style-type: none"> Record: CP01 TCRB Position: 65-84 Field: American Express Seller ID <p>With Mastercard, the value for this field corresponds to the following data in the TC 33 capture file¹:</p> <ul style="list-style-type: none"> Record: CP01 TCR6 Position: 117-131 Field: Mastercard Sub-Merchant ID 	<p>authorization</p> <p>American Express Direct: R for all aggregator transactions.</p> <p>CyberSource through VisaNet:</p> <ul style="list-style-type: none"> O for all American Express aggregator transactions; R for all Mastercard aggregator authorizations; otherwise, not used. <p>FDC Compass: R for all aggregator transactions.</p> <p>FDC Nashville Global: R for all aggregator transactions.</p>	<p>American Express Direct: String (20)</p> <p>CyberSource through VisaNet with American Express: String (20)</p> <p>CyberSource through VisaNet with Mastercard: String (15)</p> <p>FDC Compass: String (20)</p> <p>FDC Nashville Global: String (14)</p>
submerchant_name	<p>Sub-merchant's business name.</p> <p>FDC Compass</p> <p>This value must consist of uppercase characters.</p>	<p>authorization</p> <p>American Express Direct: R for all aggregator transactions.</p> <p>CyberSource through VisaNet: not used.</p> <p>FDC Compass: R for all aggregator transactions.</p> <p>FDC Nashville Global: R for all aggregator transactions.</p>	<p>American Express Direct: String (37)</p> <p>FDC Compass with American Express: String (19)</p> <p>FDC Compass with Mastercard: String (37)</p> <p>FDC Nashville Global: String (12)</p>
<p>¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>			

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
submerchant_phone	<p>Sub-merchant's telephone number.</p> <p>CyberSource through VisaNet With American Express, the value for this field corresponds to the following data in the TC 33 capture file¹:</p> <ul style="list-style-type: none"> Record: CP01 TCRB Position: 5-24 Field: American Express Seller Telephone Number <p>FDC Compass This value must consist of uppercase characters. Use one of these recommended formats: NNN-NNN-NNNN NNN-AAAAAAA</p>	<p>authorization</p> <p>American Express Direct: R for all aggregator transactions.</p> <p>CyberSource through VisaNet: O for all aggregator transactions with American Express; otherwise, not used.</p> <p>FDC Compass: R for all aggregator transactions.</p> <p>FDC Nashville Global: R for all aggregator transactions.</p>	<p>American Express Direct: String (20)</p> <p>CyberSource through VisaNet: String (20)</p> <p>FDC Compass: String (13)</p> <p>FDC Nashville Global: String (10)</p>
submerchant_postal_code	<p>Partial postal code for the sub-merchant's address.</p> <p>FDC Compass This value must consist of uppercase characters.</p>	<p>authorization</p> <p>American Express Direct: R for all aggregator transactions.</p> <p>CyberSource through VisaNet: not used.</p> <p>FDC Compass: O for all aggregator transactions.</p> <p>FDC Nashville Global: R for all aggregator transactions.</p>	<p>American Express Direct: String (9)</p> <p>FDC Compass: String (15)</p> <p>FDC Nashville Global: String (9)</p>
submerchant_state	<p>Sub-merchant's state or province. Use the State, Province, and Territory Codes for the United States and Canada.</p> <p>FDC Compass This value must consist of uppercase characters.</p>	<p>authorization</p> <p>American Express Direct: R for all aggregator transactions.</p> <p>CyberSource through VisaNet: not used.</p> <p>FDC Compass: O for all aggregator transactions.</p> <p>FDC Nashville Global: R for all aggregator transactions.</p>	<p>String (2)</p>

¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
submerchant_street	<p>First line of the sub-merchant's street address.</p> <p>FDC Compass This value must consist of uppercase characters.</p>	<p>authorization American Express Direct: R for all aggregator transactions. CyberSource through VisaNet: not used. FDC Compass: O for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.</p>	<p>American Express Direct: String (30) FDC Compass: String (38) FDC Nashville Global: String (25)</p>
tax_amount	<p>Total tax amount to apply to the order. This value cannot be negative.</p> <p>Important To prevent data tampering, sign this field.</p>	This field is optional.	<p>Amount String (15)</p>
transaction_type	<p>The type of transaction. Possible values:</p> <ul style="list-style-type: none"> ■ authorization ■ authorization,create_payment_token ■ authorization,update_payment_token ■ sale ■ sale,create_payment_token ■ sale,update_payment_token ■ create_payment_token ■ update_payment_token <p>Only authorization and sale are supported for Visa Checkout and Visa SRC transactions.</p> <p>Important To prevent data tampering, sign this field.</p>	Required by the Secure Acceptance application.	<p>Enumerated String String (60)</p>
transaction_uuid	<p>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.</p> <p>Important To prevent data tampering, sign this field.</p>	Required by the Secure Acceptance application.	<p>ASCIIAlphaNumericPunctuation String (50)</p>

¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 8 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
unsigned_field_names	<p>A comma-separated list of request fields that are not signed.</p> <p>Important To prevent data tampering, sign this field even if no value is included in this field.</p>	Required by the Secure Acceptance application.	<p>AlphaNumeric Punctuation</p> <p>Variable</p>
<p>1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>			

Reply Fields

Reply fields are sent using the following notification methods:

- Merchant POST URL (see ["Receive Merchant Notifications," page 35](#))
- Merchant POST Email (see ["Receive Merchant Notifications," page 35](#))
- POST to the URL specified in the Transaction or Custom Cancel Response page (see ["Display a Transaction Response Page," page 38](#))

Notification methods are enabled on the Notifications and Customer Response pages of your Secure Acceptance profile.

To ensure the integrity of the reply fields, a signature is included in the response. This signature is generated using the same **secret_key** value that was used to generate the request signature.

To verify that the reply fields have not been tampered with, create a signature using the fields listed in the **signed_field_names** reply field. This signature must be the same value that is included in the signature response field. Refer to the receipt page that is included in the sample scripts (see ["Samples in Scripting Languages," page 47](#)).



Because CyberSource can add reply fields and reason codes at any time, proceed as follows:

- Parse the reply data according to the names of the fields instead of their order in the reply. For more information on parsing reply fields, see the documentation for your scripting language.
- The signature that you generate must be the same value that is included in the signature response field.
- Your error handler should use the **decision** field to determine the transaction result if it receives a reason code that it does not recognize.

If configured, these reply fields are sent back to your Merchant POST URL or email. See ["Receive Merchant Notifications," page 35](#). Your error handler should use the **decision** field to obtain the transaction result if it receives a reason code that it does not recognize.

Table 9 Reply Fields

Field	Description	Data Type & Length
auth_affluence_indicator	<p>Chase Paymentech Solutions Indicates whether a customer has high credit limits. This information enables you to market high cost items to these customers and to understand the kinds of cards that high income customers are using.</p> <p>This field is supported for Visa, Mastercard, Discover, and Diners Club.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ Y: Yes ■ N: No ■ X: Does not apply/unknown <p>Worldpay VAP Flag that indicates that a Visa cardholder or Mastercard cardholder is in one of the affluent categories. Possible values:</p> <ul style="list-style-type: none"> ■ AFFLUENT: High income customer with high spending pattern (>100k USD annual income and >40k USD annual card usage). ■ MASS AFFLUENT: High income customer (>100k USD annual income). 	<p>Chase Paymentech Solution: String (1)</p> <p>Worldpay VAP: String (13)</p>
auth_amount	Amount that was authorized.	String (15)
auth_avs_code	AVS result code. See "AVS Codes," page 172 .	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_card_commercial	<p>Indicates whether the card is a commercial card, which enables you to include Level II data in your transaction requests.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ Y: Yes ■ N: No ■ X: Does not apply/unknown <p>This field is supported for Visa and Mastercard on Chase Paymentech Solutions.</p>	String (1)

¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
auth_card_healthcare	<p>Indicates whether the card is a healthcare card.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ Y: Yes ■ N: No ■ X: Does not apply/unknown <p>This field is supported for Visa and Mastercard on Chase Paymentech Solutions.</p>	String (1)
auth_card_issuer_country	<p>Country in which the card was issued. This information enables you to determine whether the card was issued domestically or internationally. Use the two-character ISO Standard Country Codes.</p> <p>This field is supported for Visa, Mastercard, Discover, Diners Club, JCB, and Maestro (International) on Chase Paymentech Solutions.</p>	String (3)
auth_card_level_3_eligible	<p>Indicates whether the card is eligible for Level III interchange fees, which enables you to include Level III data in your transaction requests.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ Y: Yes ■ N: No ■ X: Does not apply/unknown <p>This field is supported for Visa and Mastercard on Chase Paymentech Solutions.</p>	String (1)
auth_card_payroll	<p>Indicates whether the card is a payroll card.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ Y: Yes ■ N: No ■ X: Does not apply/unknown <p>This field is supported for Visa, Discover, Diners Club, and JCB on Chase Paymentech Solutions.</p>	String (1)
<p>¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>		

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
auth_card_pinless_debit	<p>Indicates whether the card is a PINless debit card.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ Y: Yes ■ N: No ■ X: Does not apply/unknown <p>This field is supported for Visa and Mastercard on Chase Paymentech Solutions.</p>	String (1)
auth_card_prepaid	<p>Indicates whether the card is a prepaid card. This information enables you to determine when a gift card or prepaid card is presented for use when establishing a new recurring billing or installment billing relationship.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ Y: Yes ■ N: No ■ X: Does not apply/unknown <p>This field is supported for Visa, Mastercard, Discover, Diners Club, and JCB on Chase Paymentech Solutions.</p>	String (1)
auth_card_regulated	<p>Indicates whether the card is regulated according to the Durbin Amendment. If the card is regulated, the card issuer is subject to price caps and interchange rules.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ Y: Yes (assets greater than \$10B) ■ N: No (assets less than \$10B) ■ X: Does not apply/unknown <p>This field is supported for Visa, Mastercard, Discover, Diners Club, and JCB on Chase Paymentech Solutions.</p>	String (1)
auth_card_signature_debit	<p>Indicates whether the card is a signature debit card. This information enables you to alter the way an order is processed.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ Y: Yes ■ N: No ■ X: Does not apply/unknown <p>This field is supported for Visa, Mastercard, and Maestro (International) on Chase Paymentech Solutions.</p>	String (1)

¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
auth_cavv_result	<p>Mapped response code for the Visa Secure and American Express SafeKey:</p> <ul style="list-style-type: none"> ■ See Appendix D, "Visa Secure Response Codes," on page 179. ■ See Appendix B, "American Express SafeKey Response Codes," on page 176. 	String (3)
auth_cavv_result_raw	Raw response code sent directly from the processor for Visa Secure and American Express SafeKey.	String (3)
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," page 175.	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.	AlphaNumeric (60)
bill_trans_ref_no	<p>Reference number that you use to reconcile your CyberSource reports with your processor reports.</p> <p>This field is not supported on CyberSource through VisaNet.</p>	AlphaNumeric (60)
bin_lookup_billing_currency	<p>Cardholder's billing currency. For the possible values, see ISO Standard Currency Codes.</p> <p>For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).</p>	(3)String
bin_lookup_billing_currency_minor_digits	<p>Number of decimal positions for amounts in the cardholder's billing currency.</p> <p>For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).</p>	String (1)
bin_lookup_billing_currency_numeric_code	Three-digit numeric ISO code for the cardholder's billing currency. Use the three-character ISO Standard Currency Codes .	String (3)
<p>¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>		

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
bin_lookup_card_product_category	<p>Category of product, such as business, commercial, or consumer.</p> <p>For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).</p>	String (no maximum length)
bin_lookup_card_sub_type	<p>Kind of card. Possible values:</p> <ul style="list-style-type: none"> ■ Charge ■ Credit ■ Credit/debit ■ Debit ■ Deferred debit ■ Prepaid <p>For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).</p>	String (no maximum length)
bin_lookup_card_type	<p>Three-digit value that indicates the card type. For the possible values, see the appendix “Card Types” in Credit Card Services Using the SCMP API or Credit Card Services Using the Simple Order API.</p> <p>For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).</p>	String (3)
bin_lookup_card_type_name	<p>Name of the card type.</p> <p>For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).</p>	String (50)
bin_lookup_cross_border_eligible	<p>Indicates whether cross-border transactions are supported. <i>Cross border</i> means that the issuer and acquirer are in different countries. Possible values:</p> <ul style="list-style-type: none"> ■ Y: Supported ■ N: Not supported <p>For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).</p>	String (1)
<p>¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant’s acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>		

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
bin_lookup_issuer_country	Country of the issuing bank. For the possible values, see ISO Standard Country Codes . For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).	String (2)
bin_lookup_issuer_country_numeric_code	Three-digit numeric ISO code for the issuer's country. See the appendix "Numeric Country and Currency Codes" in Credit Card Services Using the SCMP API or Credit Card Services Using the Simple Order API . For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).	String (3)
bin_lookup_issuer_name	Bank that issued the card, such as Bank of America, Chase, or Wells Fargo. For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).	String (no maximum length)
bin_lookup_issuer_phone	Customer service phone number for the issuing bank. For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).	String (no maximum length)
bin_lookup_level_2_eligible	Indicates whether Level II transactions are supported. Possible values: <ul style="list-style-type: none">■ Y: Supported■ N: Not supported For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).	String (1)
bin_lookup_level_3_eligible	Indicates whether Level III transactions are supported. Possible values: <ul style="list-style-type: none">■ Y: Supported■ N: Not supported For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).	String (1)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
bin_lookup_network#_aft_cross_border_eligible	<p>Indicates whether cross-border AFT transactions are supported on network specified by the network ID value. <i>Cross border</i> means that the issuer and acquirer are in different countries. Possible values:</p> <ul style="list-style-type: none"> ■ Y: Supported ■ N: Not supported <p>This field is returned only for debit networks that are supported for the card number submitted in the request.</p> <p>For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).</p>	String (1)
bin_lookup_network#_aft_domestic_eligible	<p>Indicates whether domestic AFT transactions are supported on network specified by the network ID value. <i>Domestic</i> means that the issuer and acquirer are in the same country. Possible values:</p> <ul style="list-style-type: none"> ■ Y: Supported ■ N: Not supported <p>This field is returned only for debit networks that are supported for the card number submitted in the request.</p> <p>For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).</p>	String (1)
bin_lookup_network#_network_id	<p>Network identifier for the related elements in the array. For detailed information, see the appendix “Network IDs and Sharing Group Codes” in Credit Card Services Using the SCMP API or Credit Card Services Using the Simple Order API.</p> <p>This field is returned only for debit networks that are supported for the card number submitted in the request.</p> <p>For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).</p>	String (4)
bin_lookup_network#_network_order	<p>One or more codes that indicate which networks are supported for the card.</p> <p>For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).</p>	String (5)
<p>¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant’s acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>		

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
bin_lookup_network#_oct_cross_border_eligible	<p>Indicates whether cross-border OCT transactions are supported on network specified by the network ID value. <i>Cross border</i> means that the issuer and acquirer are in different countries. Possible values:</p> <ul style="list-style-type: none"> ■ Y: Supported ■ N: Not supported <p>This field is returned only for debit networks that are supported for the card number submitted in the request.</p> <p>For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).</p>	String (1)
bin_lookup_network#_oct_domestic_eligible	<p>Indicates whether domestic OCT transactions are supported on network specified by the network ID value. <i>Domestic</i> means that the issuer and acquirer are in the same country. Possible values:</p> <ul style="list-style-type: none"> ■ Y: Supported ■ N: Not supported <p>This field is returned only for debit networks that are supported for the card number submitted in the request.</p> <p>For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).</p>	String (1)
bin_lookup_oct_fast_funds_indicator	<p>Indicates the issuer's level of support for Fast Funds transactions. A Fast Funds transaction makes funds available to the recipient within 30 minutes. An issuer that supports original credit transactions (OCTs) but not Fast Funds transactions makes funds available within two business days.</p> <ul style="list-style-type: none"> ■ B: Issuer supports Fast Funds for all transactions. ■ D: Issuer supports Fast Funds only for domestic transactions. ■ N: Issuer does not support Fast Funds. <p>For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).</p>	String (1)
<p>¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>		

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
bin_lookup_oct_gambling_eligible	<p>Indicates whether the account can receive original credit transactions (OCTs) for gambling transactions. Possible values:</p> <ul style="list-style-type: none"> ■ Y: Original credit transactions (OCTs) for gambling transactions are blocked. ■ N: Original credit transactions (OCTs) for gambling transactions are not blocked. <p>For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).</p>	String (1)
bin_lookup_oct_indicator	<p>Indicates whether the account can receive Visa Direct transactions. Possible values:</p> <ul style="list-style-type: none"> ■ A: Accepts Visa Direct transactions. ■ B: Accepts Visa Direct transactions. ■ C: Accepts Visa Direct transactions. ■ N: Does not accept Visa Direct transactions. <p>For information about Visa Direct, see "Payouts Payment Tokens," page 18.</p> <p>For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser).</p>	String (1)
decision	<p>The result of your request. Possible values:</p> <ul style="list-style-type: none"> ■ ACCEPT ■ DECLINE ■ REVIEW ■ ERROR ■ CANCEL <p>See "Types of Notifications," page 171.</p>	String (7)
echeck_debit_ref_no	Reference number for the transaction.	AlphaNumeric (60)
echeck_debit_submit_time	Time when the debit was requested in UTC.	Date and Time (20)
exchange_rate	<p>Exchange rate if a currency conversion occurred.</p> <p>The 17 characters include the decimal point.</p>	Decimal (17)
invalid_fields	Indicates which request fields were invalid.	Variable
message	Reply message from the payment gateway.	String (255)
<p>¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>		

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
payer_authentication_cavv	Cardholder authentication verification value (CAVV). Transaction identifier generated by the issuing bank, Visa Checkout, or Visa SRC. This field is used by the payer authentication validation service.	String (50)
payer_authentication_eci	Electronic commerce indicator (ECI). This field is used by payer authentication validation and enrollment services. Possible values for Visa, American Express, and JCB: <ul style="list-style-type: none"> ■ 05: Successful authentication. ■ 06: Authentication attempted. ■ 07: Failed authentication. Possible values for Mastercard: <ul style="list-style-type: none"> ■ 01: Merchant is liable. ■ 02: Card issuer is liable. 	String (3)
payer_authentication_enroll_e_commerce_indicator	Commerce indicator for cards not enrolled. This field contains one of these values: <ul style="list-style-type: none"> ■ internet: Card not enrolled or card type not supported by payer authentication. No liability shift. ■ js_attempted: JCB card not enrolled, but attempt to authenticate is recorded. Liability shift. ■ js_failure: J/Secure directory service is not available. No liability shift. ■ spa: Mastercard card not enrolled in the Identity Check program. No liability shift. ■ vbv_attempted: Visa card not enrolled, but attempt to authenticate is recorded. Liability shift. ■ vbv_failure: For payment processor Barclays, Streamline, AIBMS, or FDC Germany, you receive this result if Visa's directory service is not available. No liability shift. 	String (255)

¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
payer_authentication_enroll_veres_enrolled	<p>Result of the enrollment check. This field can contain one of these values:</p> <ul style="list-style-type: none"> ■ Y: Card enrolled or can be enrolled; you must authenticate. Liability shift. ■ N: Card not enrolled; proceed with authorization. Liability shift. ■ U: Unable to authenticate regardless of the reason. No liability shift. <p>This field applies only to the Asia, Middle East, and Africa Gateway. If you are configured for this processor, you must send the value of this field in your authorization request.</p> <p>The following value can be returned if you are using rules-based Payer Authentication:</p> <ul style="list-style-type: none"> ■ B: Indicates that authentication was bypassed. <p>For Rules-Based Payer Authentication information see the <i>Payer Authentication Using the SCMP API</i> (PDF HTML) or <i>Payer Authentication Using the Simple Order API</i> (PDF HTML).</p>	String (255)
payer_authentication_pares_status	<p>Raw result of the authentication check. This field can contain one of these values:</p> <ul style="list-style-type: none"> ■ A: Proof of authentication attempt was generated. ■ N: Customer failed or cancelled authentication. Transaction denied. ■ U: Authentication not completed regardless of the reason. ■ Y: Customer was successfully authenticated. 	String (255)
payer_authentication_pares_timestamp	Decrypted time stamp for the payer authentication result. Visa Checkout and Visa SRC generate this value. Format: Unix time, which is also called <i>epoch time</i> .	String
<p>¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>		

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
payer_authentication_proof_xml	<p>XML element containing proof of enrollment checking.</p> <p>For cards not issued in the U.S. or Canada, your bank can require this data as proof of enrollment validation for any payer authentication transaction that you represent because of a chargeback.</p> <p>For cards issued in the U.S. or Canada, Visa can require this data for specific merchant category codes.</p> <p>This field is not returned for 3D Secure 2.0 transactions.</p>	String (1024)
payer_authentication_reason_code	<p>Numeric value corresponding to the result of the payer authentication request.</p> <p>See "Reason Codes," page 168.</p>	String (5)
payer_authentication_specification_version	This field contains the 3D Secure version that was used to process the transaction. For example, 1.0.2 or 2.0.0.	String (20)
payer_authentication_transaction_id	Payer authentication transaction identifier used by Secure Acceptance to link the enrollment check and validate authentication messages.	String (20)
payer_authentication_uad	Mastercard Identity Check UCAF authentication data. Returned only for Mastercard Identity Check transactions.	String (32)
payer_authentication_uci	<p>Mastercard Identity Check UCAF collection indicator. This field indicates whether authentication data is collected at your web site. Possible values:</p> <ul style="list-style-type: none"> ■ 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)
<p>¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>		

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
payer_authentication_validate_e_commerce_indicator	<p>Indicator that distinguishes Internet transactions from other types. The authentication failed if this field is not returned. For Visa, if your payment processor is Streamline, Barclays, AIBMS, or FDC Germany, you receive the value <code>vbv_failure</code> instead of <code>internet</code> when payer_authentication_eci is not present.</p> <p>The value of this field is passed automatically to the authorization service if you request the services together. This field contains one of these values:</p> <ul style="list-style-type: none"> ■ <code>aesk</code>: American Express SafeKey authentication verified successfully. ■ <code>aesk_attempted</code>: Card not enrolled in American Express SafeKey, but the attempt to authenticate was recorded. ■ <code>internet</code>: Authentication was not verified successfully. ■ <code>js</code>: J/Secure authentication verified successfully. ■ <code>js_attempted</code>: JCB card not enrolled in J/Secure, but the attempt to authenticate was recorded. ■ <code>spa</code>: Mastercard Identity Check authentication verified successfully. ■ <code>spa_failure</code>: Mastercard Identity Check failed authentication. ■ <code>vbv</code>: Visa Secure authentication verified successfully. ■ <code>vbv_attempted</code>: Card not enrolled in Visa Secure, but the attempt to authenticate was recorded. ■ <code>vbv_failure</code>: Visa Secure authentication unavailable. 	String (255)
<p>1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>		

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
payer_authentication_validate_result	Raw authentication data that comes from the card-issuing bank that indicates whether authentication was successful and whether liability shift occurred. This field contains one of these values: <ul style="list-style-type: none"> ■ -1: Invalid PAREs. ■ 0: Successful validation. ■ 1: Cardholder is not participating, but the attempt to authenticate was recorded. ■ 6: Issuer unable to perform authentication. ■ 9: Cardholder did not complete authentication. 	String (255)
payer_authentication_veres_timestamp	Decrypted time stamp for the verification response. Visa Checkout and Visa SRC generate this value. Format: Unix time, which is also called <i>epoch time</i> .	String
payer_authentication_xid	Transaction identifier generated by CyberSource Payer Authentication. Used to match an outgoing PA request with an incoming PA response.	String (28)
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 supersedes the previous payment token and is returned if: <ul style="list-style-type: none"> ■ The merchant is configured for a 16 digit payment token which displays the last four digits of the primary account number (PAN) and passes Luhn mod-10 check. See "Payment Tokens," page 15. ■ The consumer has updated the card number on their payment token. This payment token supersedes the previous payment token and should be used for subsequent transactions. You must be currently using Token Management Services.	String (26)
paypal_address_status	Status of the street address on file with PayPal. Possible values: <ul style="list-style-type: none"> ■ None ■ Confirmed ■ Unconfirmed 	String (12)
paypal_authorization_correlation_id	PayPal identifier that is used to investigate any issues.	String (20)
paypal_authorization_transaction_id	Unique identifier for the transaction.	String (17)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
paypal_customer_email	Email address of the customer as entered during checkout. PayPal uses this value to pre-fill the PayPal membership sign-up portion of the PayPal login page.	String (127)
paypal_do_capture_correlation_id	PayPal identifier that is used to investigate any issues.	String (20)
paypal_do_capture_transaction_id	Unique identifier for the transaction.	String (17)
paypal_ec_get_details_correlation_id	PayPal identifier that is used to investigate any issues.	String (20)
paypal_ec_get_details_request_id	Value of the request ID returned from a PayPal get details service request.	String (26)
paypal_ec_get_details_transaction_id	Unique identifier for the transaction.	String (17)
paypal_ec_order_setup_correlation_id	PayPal identifier that is used to investigate any issues.	String (20)
paypal_ec_order_setup_transaction_id	Unique identifier for the transaction.	String (17)
paypal_ec_set_request_id	Value of the request ID returned from a PayPal set service request.	String (26)
paypal_fee_amount	PayPal fee charged for the transaction. This value does not exceed the equivalent of 10,000 USD in any currency and does not include a currency symbol. The decimal separator is a period (.), and the optional thousands separator is a comma (,).	String (9)
paypal_order_request_id	Value of the request ID returned from a PayPal order setup service request.	String (26)
paypal_payer_id	Customer's PayPal account identification number.	Alphanumeric String (13)
paypal_payer_status	Customer's status. Possible values: <ul style="list-style-type: none"> ■ verified ■ unverified 	String (10)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
paypal_pending_reason	<p>Indicates the reason that payment is pending. Possible values:</p> <ul style="list-style-type: none"> ■ address: Your customer did not include a confirmed shipping address, and your Payment Receiving preferences are set to manually accept or deny such payments. To change your preferences, go to the Preferences section of your PayPal profile. ■ authorization: The payment has been authorized but not settled. Capture the authorized amount. ■ echeck: Payment was made by an eCheck that has not yet cleared. ■ intl: You have a non-U.S. account and do not have a withdrawal mechanism. You must manually accept or deny this payment in your PayPal Account Overview. ■ multi-currency: You do not have a balance in the currency sent, and your Payment Receiving preferences are not set to automatically convert and accept this payment. You must manually accept or deny this payment in your PayPal Account Overview. ■ none: No pending reason. ■ order: The payment is part of an order that has been authorized but not settled. ■ paymentreview: The payment is being reviewed by PayPal for possible fraud. ■ unilateral: The payment was made to an email address that is not registered or confirmed. ■ verify: Your account is not yet verified. You must verify your account before you can accept this payment. 	String (14)
<p>1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>		

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
paypal_pending_status	<p>Status of the transaction. Possible values:</p> <ul style="list-style-type: none"> ■ Canceled-Reversal: PayPal canceled the reversal, which happens when you win a dispute, and the funds for the reversal are returned to you. ■ Completed: PayPal completed the payment and added the funds to your account. ■ Denied: You denied a payment, which happens only if the payment was pending for the reason indicated in the reason_code field. ■ Expired: The authorization expired. ■ Failed: The payment failed. This event can happen only when the payment is made from your customer's bank account. ■ In-Progress: The transaction is not complete yet. ■ None: No status. ■ Partially-Refunded: The payment was partially refunded. ■ Pending: The payment is pending for the reason indicated in the paypal_pending_reason field. ■ Processed: PayPal accepted the payment. ■ ReasonCode ■ Refunded: You refunded the payment. ■ Reversed: PayPal reversed the payment for the reason specified in the reason_code field. The funds were transferred from your account to the customer's account. ■ Voided: The authorization was voided 	String (20)
paypal_protection_eligibility	<p>Seller protection in force for the transaction. Possible values:</p> <ul style="list-style-type: none"> ■ Eligible: You are protected by the PayPal Seller Protection Policy for unauthorized payment and item not received. ■ PartiallyEligible: You are protected by the PayPal Seller Protection Policy for item not received. ■ Ineligible: You are not protected under the PayPal Seller Protection Policy. 	String (17)

¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
paypal_protection_eligibility_type	<p>Seller protection in force for the transaction. Possible values:</p> <ul style="list-style-type: none"> ■ Eligible: You are protected by the PayPal Seller Protection Policy for unauthorized payment and item not received. ■ ItemNotReceivedEligible: You are protected by the PayPal Seller Protection Policy for item not received. ■ UnauthorizedPaymentEligible: You are protected by the PayPal Seller Protection Policy for unauthorized payment. ■ Ineligible: You are not protected under the PayPal Seller Protection Policy. <p>To enable the paypal_protection_eligibility_type field, contact CyberSource Customer Support to have your account configured for this feature.</p>	String (32)
paypal_request_id	Identifier for the request generated by the client.	String (26)
paypal_token	Timestamped PayPal token which identifies that PayPal Express Checkout is processing the transaction. Save this value to send in future request messages.	String (20)
paypal_transaction_type	<p>Indicates the PayPal transaction type.</p> <p>Possible value: <code>expresscheckout</code></p>	String (16)
reason_code	<p>Numeric value corresponding to the result of the payment card transaction request.</p> <p>See "Reason Codes," page 168.</p>	String (5)
req_access_key	Authenticates the merchant with the application.	String (32)
<p>¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>		

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
req_aggregator_id	<p>Value that identifies you as a payment aggregator. Obtain this value for the processor.</p> <p>CyberSource through VisaNet The value for this field corresponds to the following data in the TC 33 capture file¹:</p> <ul style="list-style-type: none"> Record: CP01 TCR6 Position: 95-105 Field: Mastercard Payment Facilitator ID <p>FDC Compass This value must consist of upper-case characters.</p> <p>Field Length American Express Direct: 20 CyberSource through VisaNet: 11 FDC Compass: 20 FDC Nashville Global: 15</p> <p>Required/Optional American Express Direct: R for all aggregator transactions. CyberSource through VisaNet: R for Mastercard aggregator authorizations; otherwise, not used. FDC Compass: R for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.</p>	String (See description)
req_allow_payment_token_update	<p>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:</p> <ul style="list-style-type: none"> 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)
req_auth_indicator	<p>Flag that specifies the purpose of the authorization. Possible values:</p> <ul style="list-style-type: none"> 0: Preauthorization 1: Final authorization <p>Mastercard requires European merchants to indicate whether the authorization is a final authorization or a preauthorization.</p> <p>To set the default for this field, contact CyberSource Customer Support.</p>	String (1)

¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
req_auth_type	<p>Authorization type. Possible values:</p> <ul style="list-style-type: none"> ■ <code>AUTOCAPTURE</code>: Automatic capture. ■ <code>STANDARDCAPTURE</code>: Standard capture. ■ <code>verbal</code>: Forced capture. <p>Asia, Middle East, and Africa Gateway; Cielo; Comercio Latino; and CyberSource Latin American Processing</p> <p>Set this field to <code>AUTOCAPTURE</code> and include it in a bundled request to indicate that you are requesting an automatic capture. If your account is configured to enable automatic captures, set this field to <code>STANDARDCAPTURE</code> and include it in a standard authorization or bundled request to indicate that you are overriding an automatic capture.</p> <p>Forced Capture</p> <p>Set this field to <code>verbal</code> and include it in the authorization request to indicate that you are performing a forced capture; therefore, you receive the authorization code outside the CyberSource system.</p> <p>Verbal Authorization</p> <p>Set this field to <code>verbal</code> and include it in the capture request to indicate that the request is for a verbal authorization.</p>	<p>Cielo, Comercio Latino, and CyberSource Latin American Processing: String (15)</p> <p>All other processors: String (11)</p>
req_bill_payment	<p>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:</p> <ul style="list-style-type: none"> ■ <code>true</code>: Bill payment or loan payment. ■ <code>false</code> (default): Not a bill payment or loan payment. 	String (1)
req_bill_to_address_city	City in the billing address.	<p>String (50)</p> <p>Visa Checkout and Visa SRC: String (100)</p>
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.	<p>String (60)</p> <p>Visa Checkout and Visa SRC: String (100)</p>
<p>¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>		

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
req_bill_to_address_line2	Second line of the street address in the billing address.	String (60) Visa Checkout and Visa SRC: String (100)
req_bill_to_address_postal_code	Postal code for the billing address. This field is returned if bill_to_address_country is U.S. or Canada.	String (10) Visa Checkout and Visa SRC: String (100)
req_bill_to_address_state	State or province in the billing address. The two-character ISO state and province code . This field is returned for U.S and Canada.	String (2)
req_bill_to_company_name	Name of the customer's company.	String (40)
req_bill_to_email	Customer email address.	String (255) Visa Checkout and Visa SRC: String (256)
req_bill_to_forename	Customer first name.	String (60) Visa Checkout and Visa SRC: String (256)
req_bill_to_phone	Customer phone number.	String (15) Visa Checkout and Visa SRC: String (30)
req_bill_to_surname	Customer last name.	String (60) Visa Checkout and Visa SRC: String (265)
¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.		

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
req_card_account_type	<p>Flag that specifies the type of account associated with the card. The cardholder provides this information during the payment process.</p> <p>Cielo and Comercio Latino Possible values:</p> <ul style="list-style-type: none"> ■ CR: Credit card ■ DB: Debit card <p>CyberSource through VisaNet Possible values:</p> <ul style="list-style-type: none"> ■ CH: Checking account ■ CR: Credit card account ■ SA: Savings account <p>This field is returned for:</p> <ul style="list-style-type: none"> ■ Debit transactions on Cielo and Comercio Latino. ■ Transactions with Brazilian-issued cards on CyberSource through VisaNet. <p>Combo cards in Brazil contain credit and debit functionality in a single card. Visa systems use a bank identification number (BIN) for this type of card. Using the BIN to determine whether a card is debit or credit can cause transactions with these cards to be processed incorrectly. CyberSource strongly recommends that you include this field for combo card transactions.</p>	String (2)
req_card_expiry_date	Card expiration date.	String (7)
req_card_number	Card number.	String (20)
req_card_type	Type of card.	String (3)
req_company_tax_id	Company's tax identifier. The the last four digits are not masked.	String (9)
<p>¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>		

Table 9 Reply Fields (Continued)

Field	Description	Data Type & 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_consumer_id	Identifier for the customer account. This value is defined when creating a customer subscription.	String (100)
req_currency	Currency used for the order. See ISO currency codes .	String (3)
req_customer_cookies_accepted	Indicates whether the customer's browser accepts cookies. This field can contain one of the following values: <ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ■ 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. 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: <ul style="list-style-type: none"> ■ false (default): Not a loan payment ■ true: Loan payment 	String (5)
¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.		

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
req_departure_time	<p>Departure date and time of the first leg of the trip. Use one of the following formats:</p> <ul style="list-style-type: none"> ■ yyyy-MM-dd HH:mm z ■ yyyy-MM-dd hh:mm a z ■ yyyy-MM-dd hh:mm 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	<p>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 (_).</p> <p>However, do not use the same uppercase and lowercase letters to indicate different sessions IDs.</p> <p>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.</p>	String (88)
req_driver_license_number	Driver's license number of the customer. 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_e_commerce_indicator	<p>The commerce indicator for the transaction type.</p> <p>Value: <code>install</code></p> <p>This field is returned only for installment payments on CyberSource Latin American Processing.</p>	String (13)
req_echeck_account_number	Account number. This number is masked.	Non-negative integer (17)
req_echeck_account_type	<p>Account type. Possible values:</p> <ul style="list-style-type: none"> ■ C: Checking ■ S: Savings (USD only) ■ X: Corporate checking (USD only) 	String (1)
req_echeck_check_number	Check number.	Integer (8)
<p>¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>		

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
req_echeck_effective_date	Effective date for the transaction.	Date (b) String (8)
req_echeck_routing_number	Bank routing number. It is also called the <i>transit number</i> .	Non-negative integer (9)
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_installment_total_amount	Total amount of the loan that is being paid in installments. This field is returned only for installment payments on CyberSource Latin American Processing or CyberSource through VisaNet.	Amount (12)
req_installment_total_count	Total number of installment payments as part of an authorization. Possible values: 1 to 99 This field is returned only for installment payments on CyberSource Latin American Processing.	Numeric String (2)
req_issuer_additional_data	Data defined by the issuer. See the “Formats for Discretionary Data” section in Credit Card Services Using the SCMP API or Credit Card Services Using the Simple Order API .	Alphanumeric String (256)
req_item_#_code	Type of product. # can range from 0 to 199.	String (255)
req_item_#_description	Description of the item. # can range from 0 to 199.	String (255)
req_item_#_name	Name of the item. # can range from 0 to 199.	String (255)
req_item_#_passenger_email	Passenger’s email address.	String (255)
req_item_#_passenger_forename	Passenger’s first name.	String (60)
req_item_#_passenger_id	ID of the passenger to whom the ticket was issued. For example, you can use this field for the frequent flyer number.	String (32)
req_item_#_passenger_phone	Passenger’s phone number. If the order is from outside the U.S., CyberSource recommends that you include the country code.	String (15)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant’s acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
req_item_#_passenger_status	Your company's passenger classification, such as with a frequent flyer classification. In this case, you might use values such as standard, gold, or platinum.	String (32)
req_item_#_passenger_surname	Passenger's last name.	String (60)
req_item_#_passenger_type	Passenger classification associated with the price of the ticket. You can use one of the following values: <ul style="list-style-type: none"> ■ ADT: Adult ■ CNN: Child ■ INF: Infant ■ YTH: Youth ■ STU: Student ■ SCR: Senior Citizen ■ MIL: Military 	String (32)
req_item_#_quantity	Quantity of line items. # can range from 0 to 199.	String (10)
req_item_#_sku	Identification code for the product. # can range from 0 to 199.	String (255)
req_item_#_tax_amount	Tax amount to apply to the line item. # can range from 0 to 199. 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 199. This value cannot be negative.	String (15)
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)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
req_journey_leg#_orig	<p>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.</p> <p>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.</p>	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 200.	String (2)
req_locale	<p>Indicates the language to use for customer content.</p> <p>See "Activate a Profile," page 46.</p>	String (5)
<p>1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>		

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
req_merchant_defined_data#	<p>Optional fields that you can use to store information. # can range from 1 to 100.</p> <p>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 through to Decision Manager as part of the initial payment request and are not stored against the payment token.</p> <p>Warning 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 and any Secure Acceptance field that is not specifically designed to capture personally identifying information.</p> <p>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, 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.</p>	String (100)
req_merchant_descriptor	<p>For the descriptions, used-by information, data types, and lengths for these fields, see the "Merchant Descriptors" section in either Credit Card Services Using the SCMP API or Credit Card Services Using the Simple Order API.</p>	
req_merchant_descriptor_alterate		
req_merchant_descriptor_city		
req_merchant_descriptor_contact		
req_merchant_descriptor_country		
req_merchant_descriptor_state		
req_merchant_descriptor_postal_code		
req_merchant_descriptor_street		
<p>1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.</p>		

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
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)
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_backoffice_post_url	Overrides the backoffice post URL profile setting with your own URL.	URL (255)
req_override_custom_cancel_page	Overrides the custom cancel page profile setting with your own URL.	URL (255)
req_override_custom_receipt_page	Overrides the custom receipt profile setting with your own URL.	URL (255)
req_payment_method	Method of payment. Possible values: <ul style="list-style-type: none"> ■ card ■ echeck ■ paypal ■ visacheckout 	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 Token Management Services. Populate this field with the customer subscription ID.	String (26)
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_promotion_code	Promotion code included in the transaction.	String (100)
req_recipient_account_id	Identifier for the recipient's account. Use the first six digits and last four digits of the recipient's account number.	Numeric String (10)
req_recipient_date_of_birth	Recipient's date of birth. Format: YYYYMMDD.	Date (b) String (8)
¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.		

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
req_recipient_postal_code	Partial postal code for the recipient's address. For example, if the postal code is NN5 7SG, the value for this field should be the first part of the postal code: NN5.	Alphanumeric String (6)
req_recipient_surname	Recipient's last name.	Alpha String (6)
req_recurring_amount	Payment amount for each installment or recurring subscription payment.	String (15)
req_recurring_automatic_renew	Indicates whether to automatically renew the payment schedule for an installment subscription. Possible values: <ul style="list-style-type: none"> ■ <code>true</code> (default): Automatically renew. ■ <code>false</code>: Do not automatically renew. 	Enumerated String String (5)
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.	String (3)
req_recurring_start_date	First payment date for an installment or recurring subscription payment.	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: <ul style="list-style-type: none"> ■ <code>true</code> ■ <code>false</code> 	String (5)
req_sales_organization_id	Company ID assigned to an independent sales organization. Obtain this value from Mastercard. CyberSource through VisaNet The value for this field corresponds to the following data in the TC 33 capture file ¹ : <ul style="list-style-type: none"> ■ Record: CP01 TCR6 ■ Position: 106-116 ■ Field: Mastercard Independent Sales Organization ID 	Nonnegative integer (11)

¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
req_ship_to_address_city	City of shipping address.	String (50) Visa Checkout and Visa SRC: String (100)
req_ship_to_address_country	The two-character country code.	String (2)
req_ship_to_address_line1	First line of shipping address.	String (60) Visa Checkout and Visa SRC: String (100)
req_ship_to_address_line2	Second line of shipping address.	String (60) Visa Checkout and Visa SRC: String (100)
req_ship_to_address_postal_code	Postal code for the shipping address.	String (10) Visa Checkout and Visa SRC: String (100)
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) Visa Checkout and Visa SRC: String (256)
req_ship_to_phone	Phone number for the shipping address.	String (15) Visa Checkout and Visa SRC: String (30)
req_ship_to_surname	Last name of person receiving the product.	String (60) Visa Checkout and Visa SRC: String (256)
¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.		

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
req_shipping_method	Shipping method for the product. Possible values: <ul style="list-style-type: none"> ■ 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_bin_lookup	Indicates whether the BIN lookup service was skipped. See "BIN Lookup," page 18 .	Enumerated String String (5)
req_skip_decision_manager	Indicates whether to skip Decision Manager. See Chapter 5, "Decision Manager," on page 93 . This field can contain one of the following values: <ul style="list-style-type: none"> ■ true ■ false 	String (5)
req_submerchant_city	Sub-merchant's city. FDC Compass This value must consist of uppercase characters.	American Express Direct: String (15) FDC Compass: String (21) FDC Nashville Global: String (11)
req_submerchant_country	Sub-merchant's country. Use the two-character ISO Standard Country Codes . FDC Compass This value must consist of uppercase characters.	String (3)
¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.		

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
req_submerchant_email	<p>Sub-merchant's email address.</p> <p>CyberSource through VisaNet With American Express, the value for this field corresponds to the following data in the TC 33 capture file¹:</p> <ul style="list-style-type: none"> Record: CP01 TCRB Position: 25-64 Field: American Express Seller E-mail Address 	<p>American Express Direct: String (40)</p> <p>FDC Compass: String (40)</p> <p>FDC Nashville Global: String (19)</p> <p>CyberSource through VisaNet: String (40)</p>
req_submerchant_id	<p>The ID you assigned to your sub-merchant.</p> <p>FDC Compass This value must consist of uppercase characters.</p> <p>CyberSource through VisaNet With American Express, the value for this field corresponds to the following data in the TC 33 capture file¹:</p> <ul style="list-style-type: none"> Record: CP01 TCRB Position: 65-84 Field: American Express Seller ID <p>With Mastercard, the value for this field corresponds to the following data in the TC 33 capture file¹:</p> <ul style="list-style-type: none"> Record: CP01 TCR6 Position: 117-131 Field: Mastercard Sub-Merchant ID 	<p>American Express Direct: String (20)</p> <p>FDC Compass: String (20)</p> <p>FDC Nashville Global: String (14)</p> <p>CyberSource through VisaNet with American Express: String (20)</p> <p>CyberSource through VisaNet with Mastercard: String (15)</p>
req_submerchant_name	<p>Sub-merchant's business name.</p> <p>FDC Compass This value must consist of uppercase characters.</p>	<p>American Express Direct: String (37)</p> <p>FDC Compass with American Express: String (19)</p> <p>FDC Compass with Mastercard: String (37)</p> <p>FDC Nashville Global: String (12)</p>

¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
req_submerchant_phone	<p>Sub-merchant's telephone number.</p> <p>FDC Compass This value must consist of uppercase characters. Use one of these recommended formats: NNN-NNN-NNNN NNN-AAAAAAA</p> <p>CyberSource through VisaNet With American Express, the value for this field corresponds to the following data in the TC 33 capture file¹:</p> <ul style="list-style-type: none"> Record: CP01 TCRB Position: 5-24 Field: American Express Seller Telephone Number 	<p>American Express Direct: String (20)</p> <p>FDC Compass: String (13)</p> <p>FDC Nashville Global: String (10)</p> <p>CyberSource through VisaNet: String (20)</p>
req_submerchant_postal_code	<p>Partial postal code for the sub-merchant's address.</p> <p>FDC Compass This value must consist of uppercase characters.</p>	<p>American Express Direct: String (9)</p> <p>FDC Compass: String (15)</p> <p>FDC Nashville Global: String (9)</p>
req_submerchant_state	<p>Sub-merchant's state or province. Use the State, Province, and Territory Codes for the United States and Canada.</p> <p>FDC Compass This value must consist of uppercase characters.</p>	String (2)
req_submerchant_street	<p>First line of the sub-merchant's street address.</p> <p>FDC Compass This value must consist of uppercase characters.</p>	<p>American Express Direct: String (30)</p> <p>FDC Compass: String (38)</p> <p>FDC Nashville Global: String (25)</p>
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	<p>Unique merchant-generated identifier. Include with the access_key field for each transaction.</p>	<p>String (50)</p> <p>Visa Checkout and Visa SRC: String (100)</p>

¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 9 Reply Fields (Continued)

Field	Description	Data Type & Length
request_token	Request token data created by CyberSource for each reply. This field is an encoded string that contains no confidential information. Atos You must store the request token value so that you can retrieve and send it in follow-on requests.	String (256)
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. Format: YYYY-MM-DDThh:mm:ssZ Example 2019-08-11T22:47:57Z equals August 11, 2019, at 22:47:57 (10:47:57 p.m.). The T separates the date and the time. The Z indicates UTC.	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
transaction_id	The transaction identifier returned from the payment gateway.	String (26)
utf8	Indicates whether the unicode characters are encoded. Possible value: ✓	String (3)
vc_avs_code_raw	Decrypted raw (unmapped) AVS code provided by Visa Checkout and Visa SRC.	String (10)
vc_risk_score	Decrypted risk score used with your fraud model. See "Enable Visa Checkout or Visa SRC," page 26 .	Positive Integer (2)
vc_wallet_reference_id	Decrypted order identifier generated by Visa Checkout and Visa SRC.	String (100)
¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.		

Reason Codes

The **reason_code** field contains additional data regarding the decision response of the transaction. Depending on the decision of a transaction request, the CyberSource default receipt page or your receipt page is displayed to the customer. Both you and your customer can also receive an email receipt. See ["Receive Merchant Notifications," page 35](#).

Table 10 Reason Codes

Reason Code	Description
100	Successful transaction.
102	One or more fields in the request contain invalid data. Possible action: see the reply field invalid_fields to ascertain which fields are invalid. Resend the request with the correct information.
104	The access_key and transaction_uuid fields for this authorization request match the access_key and transaction_uuid fields of another authorization request that you sent within the past 15 minutes. Possible action: resend the request with unique access_key and transaction_uuid fields. A duplicate transaction was detected. The transaction might have already been processed. Possible action: before resubmitting the transaction, use the single transaction query or search for the transaction using the Business Center (see "View Transactions in the Business Center," page 96) to confirm that the transaction has not yet been processed.
110	Only a partial amount was approved.
150	General system failure. Possible action: To avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status either directly in the Business Center or programmatically through the Single Transaction Query .
151	The request was received but a server timeout occurred. This error does not include timeouts between the client and the server. Possible action: To avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status either directly in the Business Center or programmatically through the Single Transaction Query .
152	The request was received, but a service timeout occurred. Possible action: To avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status either directly in the Business Center or programmatically through the Single Transaction Query .

Table 10 Reason Codes (Continued)

Reason Code	Description
200	<p>The authorization request was approved by the issuing bank but declined by CyberSource because it did not pass the Address Verification System (AVS) check.</p> <p>Possible action: you can capture the authorization, but consider reviewing the order for fraud.</p>
201	<p>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.</p> <p>Possible action: call your processor to possibly receive a verbal authorization. For contact phone numbers, refer to your merchant bank information.</p>
202	<p>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.</p> <p>Possible action: request a different card or other form of payment.</p>
203	<p>General decline of the card. No other information was provided by the issuing bank.</p> <p>Possible action: request a different card or other form of payment.</p>
204	<p>Insufficient funds in the account.</p> <p>Possible action: request a different card or other form of payment.</p>
205	<p>Stolen or lost card.</p> <p>Possible action: review this transaction manually to ensure that you submitted the correct information.</p>
207	<p>Issuing bank unavailable.</p> <p>Possible action: To avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status either directly in the Business Center or programmatically through the Single Transaction Query.</p>
208	<p>Inactive card or card not authorized for card-not-present transactions.</p> <p>Possible action: request a different card or other form of payment.</p>
210	<p>The card has reached the credit limit.</p> <p>Possible action: request a different card or other form of payment.</p>
211	<p>Invalid CVN.</p> <p>Possible action: request a different card or other form of payment.</p>
221	<p>The customer matched an entry on the processor's negative file.</p> <p>Possible action: review the order and contact the payment processor.</p>
222	<p>Account frozen.</p>
230	<p>The authorization request was approved by the issuing bank but declined by CyberSource because it did not pass the CVN check.</p> <p>Possible action: you can capture the authorization, but consider reviewing the order for the possibility of fraud.</p>

Table 10 Reason Codes (Continued)

Reason Code	Description
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: To avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status either directly in the Business Center or programmatically through the Single Transaction Query .
240	The card type sent is invalid or does not correlate with the payment card number. Possible action: confirm that the card type correlates with the payment card number specified in the request; then resend the request.
475	The cardholder is enrolled for payer authentication. Possible action: authenticate cardholder before proceeding.
476	Payer authentication could not be authenticated.
481	Transaction declined based on your payment settings for the profile. Possible action: review the risk score settings for the profile.
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.

Types of Notifications

Table 11 Types of Notifications

Decision	Description	Type of Notification	CyberSource Hosted Page
ACCEPT	Successful transaction. Reason codes 100 and 110.	<ul style="list-style-type: none"> ■ Custom receipt page ■ Customer receipt email ■ Merchant POST URL ■ Merchant receipt email 	Accept
REVIEW	Authorization was declined; however, a capture might still be possible. Review payment details. See reason codes 200, 201, 230, and 520.	<ul style="list-style-type: none"> ■ Custom receipt page ■ Customer receipt email ■ Merchant POST URL ■ 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, 476, and 481.	<ul style="list-style-type: none"> ■ Custom 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, 104, 150, 151 and 152.	<ul style="list-style-type: none"> ■ Custom receipt page ■ Merchant POST URL 	Error
CANCEL	<ul style="list-style-type: none"> ■ The customer did not accept the service fee conditions. ■ The customer cancelled the transaction. 	<ul style="list-style-type: none"> ■ Custom receipt page ■ Merchant POST URL 	Cancel
¹ If the retry limit is set to 0, the customer receives the decline message, <i>Your order was declined. Please verify your information.</i> before the merchant receives it. 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 payment cards (including American Express cards) are mapped to the Visa standard codes. You receive the code in the **auth_avs_code** reply field. See ["Reply Fields," page 132](#).



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 also affect risk decisions and chargebacks.

International AVS Codes

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

Table 12 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 13 U.S. Domestic AVS Codes

Code	Response	Description
A	Partial match	Street address matches, but five-digit and nine-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.
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: <ul style="list-style-type: none"> ■ 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.

Table 13 U.S. Domestic AVS Codes (Continued)

Code	Response	Description
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: <ul style="list-style-type: none"> ■ 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 nine-digit postal code matches.
X	Match	Street address and nine-digit postal code match.
Y	Match	Street address and five-digit postal code match.
Z	Partial match	Street address does not match, but five-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 14 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.

American Express SafeKey Response Codes

The American Express SafeKey response code is returned in **auth_cavv_result** in the reply message for an authorization request.

Table 15 American Express SafeKey Response Codes

Response Code	Description
1	CAVV failed validation and authentication.
2	CAVV passed validation and authentication.
3	CAVV passed the validation attempt.
4	CAVV failed the validation attempt.
7	CAVV failed the validation attempt and the issuer is available.
8	CAVV passed the validation attempt and the issuer is available.
9	CAVV failed the validation attempt and the issuer is not available.
A	CAVV passed the validation attempt and the issuer is not available.
U	Issuer does not participate or 3D Secure data was not used.
99	An unknown value was returned from the processor.

Iframe Implementation



Internet Explorer and Safari handle third-party content differently. Therefore, you must consider these differences when implementing a standard Secure Acceptance Hosted Checkout implementation or an iframe implementation. Otherwise, payments can fail for customers using these browsers.

PayPal Express Checkout is not supported on a Secure Acceptance iframe integration.



For the payer authentication 3D Secure 2.x process, ensure that the iframe is large enough to display the issuer's access control server (ACS) challenge content (at least 390 x 400 pixels). For more information about ACS, see *Payer Authentication Using the SCMP API* ([PDF](#) | [HTML](#)).

You must select the single page checkout option for the hosted checkout iframe implementation. See ["Configure the Checkout," page 30](#).

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 are ignored (see ["Customize the Checkout Appearance," page 40](#)).

CyberSource recommends that you manage the total amount value on your web site containing the inline frame. You must also provide customers a 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 "SAMEORIGIN".
- Provide frame-busting scripts to ensure that 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 hosted checkout iframe implementation is used.

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 must 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 associated with the user session. The token will be inserted whenever an HTTP request is sent to the server. Your server application will verify that 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 74](#).

Visa Secure Response Codes

The Visa Secure response code is returned in **auth_cavv_result** in the reply message for an authorization request.

Table 16 Visa Secure Response Codes

Response Code	Description
0	CAVV not validated because erroneous data was submitted.
1	CAVV failed validation and authentication.
2	CAVV passed validation and authentication.
3	CAVV passed the validation attempt.
4	CAVV failed the validation attempt.
6	CAVV not validated because the issuer does not participate.
7	CAVV failed the validation attempt and the issuer is available.
8	CAVV passed the validation attempt and the issuer is available.
9	CAVV failed the validation attempt and the issuer is not available.
A	CAVV passed the validation attempt and the issuer is not available.
B	CAVV passed the validation with information only; no liability shift.
C	CAVV attempted but not validated; issuer did not return CAVV code.
D	CAVV not validated or authenticated; issuer did not return CAVV code.
I	Invalid security data.
U	Issuer does not participate or 3D Secure data was not used.
99	An unknown value was returned from the processor.