Secure Acceptance Checkout API

Developer Guide

cybersource
A Visa Solution

Version: 24.02

Contents

Recent Revisions to This Document 6
About This Guide 8
Website Requirements 10
Secure Acceptance Checkout API Overview 11
Required Browsers 12
Secure Acceptance Profile 12
Secure Acceptance Transaction Flow 13
Payment Tokens 14
Tokens That Represent a Card or Bank Account Only 15
Subscription Payments 15
Level II and III Data 16
Payouts Payment Tokens 17
Creating a Payment Token for Payouts 17
Go-Live with Secure Acceptance 17
Payment Acceptance Configuration 18
Creating a Secure Acceptance Profile 18
Payment Method Configuration 19
Adding Card Types and Currencies 20
Payer Authentication3-D Secure Configuration 21
Enabling Automatic Authorization Reversals 22
Enabling ACH Payments 23
Enabling PayPal Express Checkout 24
Security Keys 25
Creating Security Keys 26
Merchant Notifications 27
Configuring Merchant Notifications 28
Customer Receipts 29
Configuring Customer Notifications 29
Customer Response Page 30
Configuring a Transaction Response Page 30
Activating a Profile 31
Additional Profile Options 32

Portfolio Management for Resellers 33
Creating a Hosted Checkout IntegrationCheckout API Profile 33
Payment Method Configuration 34
Reseller: Adding Card Types and Currencies 34
Payer Authentication 3-D Secure Configuration 35
Reseller: Enabling ACH Payments 37
Reseller: Enabling PayPal Express Checkout 38
Service Fees 39
Security Keys 40
Merchant Notifications 41
Customer Receipts 43
Customer Response Page 44
Reseller: Activating a Profile 45
Scripting Language Samples 46
Sample Transaction Process Using JSP 46
Payment Transactions 48
Endpoints and Transaction Types 48
Required Signed Fields 52
Payment Tokens 53
Creating a Payment Card Token 53
Creating an ACH Token 57
Payment Token Transactions 59
Requesting a Payment Card Transaction with a Token 59
ACH Payment with a Token 61
Recurring Payments 63
Installment Payments 65
Payment Token Updates 68
Updating a Payment Card Token 68
Updating an ACH Token 72
Decision Manager 75
Test and View Transactions 77
Testing Transactions 77
Viewing Transactions in the Business CenterYour Merchant Services Account 78
Hosted Checkout IntegrationCheckout API Fields 79
Data Type Definitions 79

Request Fields 80
Response Fields 159
SEC Codes 209
Reason Codes 211
Types of Notifications 215
AVS Codes 217
International AVS Codes 217
U.S. Domestic AVS Codes 217
CVN Codes 220
American Express SafeKey Response Codes 221
Iframe Implementation 222
Clickjacking Prevention 222
Iframe Transaction Endpoints 223
Visa Secure Response Codes 224

Recent Revisions to This Document

24.02

Updated request field **transaction_ reason** and added **transaction_agreement_id** request field. See Request Fields (on page 80).

Updated possible values for the **payer_authentication_eci** response field for China UnionPay cards. See Response Fields (on page 159).

24.01

Updated references to "echeck" with "ACH payments" where applicable.

This revision contains only editorial changes and no technical updates.

23.06

In the section Payment Acceptance Configuration (on page 18), the card number digits that you can choose to be displayed in the merchant or customer receipt has been corrected for these options:

- Return payment card BIN
- Return BIN and last four digits of payment card number

See Configuring Merchant Notifications (on page 28).

In the sections Payment Acceptance Configuration (on page 18) and Portfolio Management for Resellers (on page 33), the card number digits that you can choose to be displayed in the merchant or customer receipt has been corrected for these options:

- Return payment card BIN
- Return BIN and last four digits of payment card number

See Configuring Merchant Notifications (on page 28) and Reseller: Configuring Merchant Notifications (on page 42).

23.05

Initial release.

Added new request field **transaction_reason** for Recurring Payments. See Recurring Payments (on page 63) and Request Fields (on page 80).

23.04

Updated the descriptions for the SEC codes CCD and PPD. See SEC Codes (on page 209).

23.03

Added the new request field **payer_authentication_message_category** (on page 130).

23.02

Updated information about signed fields in a warning note at Secure Acceptance Transaction Flow (on page)Secure Acceptance Transaction Flow (on page 13), at Required Signed Fields (on page 52), and in an important note at Request Fields (on page 80).

Updated the values in the field **signed_field_names** in code examples throughout this guide.

Added a statement that your merchant ID must be enabled to process recurring and installment payments. See Recurring Payments (on page 63) and Installment Payments (on page 65).

Updated these tasks:

- Configuring a Custom Hosted Response Page (on page)
- Configuring a Custom Cancel Response Page (on page)
- Reseller: Configuring a Custom Hosted Response Page (on page)
- Reseller: Configuring a Custom Cancel Response Page (on page)

Updated these tasks:

- Configuring a Transaction Response Page (on page 30)
- Reseller: Configuring a Transaction Response Page (on page 44)

About This Guide

This section describes how to use this guide and where to find further information.

Audience and Purpose

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

Using Secure Acceptance Hosted Checkout Integration 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.

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

Using Secure Acceptance Hosted Checkout Integration requires minimal scripting skills. You must create a security script and modify your HTML form to invoke Secure Acceptance. You will also use your merchant services account to review and manage orders.

This guide is written for merchants who want to customize and control their own customer checkout experience, including receipt and response pages. After the customization, you will have full control to store and control customer information before sending it to Cybersource to process transactions, and to use Business Center to review and manage all of your orders.

Using the Secure Acceptance Checkout API requires moderate scripting skills. You must create a security script and modify your HTML form to pass order information to Cybersource.

Conventions

These special statements are used in this document:

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

Warning: 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.

Customer Support

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

http://support.cybersource.com

Website Requirements

Your website must meet these 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 have a shopping cart or customer order creation software.
- It must contain product pages in one of the supported scripting languages. See "Sample Transaction Process Using JSP," (on page 46).
- 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.

Secure Acceptance Checkout API Overview

Cybersource Secure Acceptance Checkout API provides a seamless customer checkout experience that keeps your branding consistent. You can create a Secure Acceptance Checkout API profile and configure the required settings to set up your customer checkout experience.

Secure Acceptance Checkout API can significantly simplify your Payment Card Industry Security Standard (PCI DSS) compliance by sending sensitive payment card data directly from your customer's browser to Cybersource servers. Your web application infrastructure does not come into contact with the sensitive payment data and the transition is silent.

> **Important:** 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 REST API, 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 Secure Acceptance profilemerchant account and subsequent failure of transactions.

To create your customer's Secure Acceptance experience, you take these steps:

1. Create and configure Secure Acceptance Checkout API profiles.
2. Update the code on your web site to POST payment data directly to Cybersource from your secure payment form. See Sample Transaction Process Using JSP (on page 46). Cybersource processes the transaction on your behalf by sending an approval request to your payment processor in real time. See Secure Acceptance Transaction Flow (on page 13).
3. Use the response information to generate an appropriate transaction response page to display to the customer. You can view and manage all orders in the Business Center. You can configure the payment options, response pages, and customer notifications. See Creating a Secure Acceptance Profile (on page 18).

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:

- Internet Explorer 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

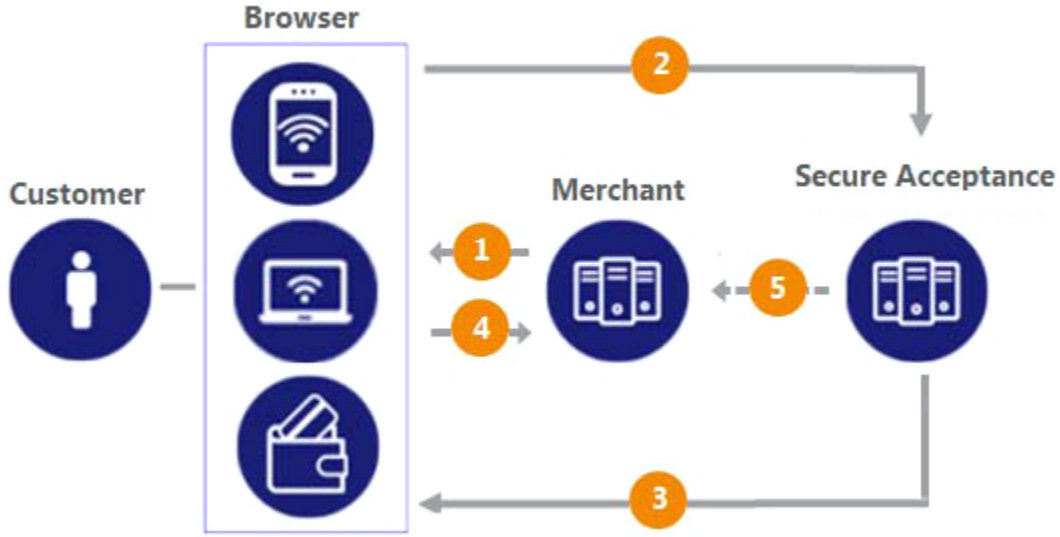
Throughout this document you will see references to Secure Acceptance. Secure Acceptance is the umbrella term for the Hosted Checkout Integration and Checkout API integration methods. Information about Secure Acceptance applies to Hosted Checkout Integration.

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 Custom Checkout Appearance (on page). For example, you might need multiple profiles for localized branding of your websites. You can display a multi-step checkout process or a single page checkout to the customer as well as configure the appearance and branding, payment options, languages, and customer notifications. See Checkout Configuration (on page).

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. For example, you might want to offer different payment options for different geographic locations.

Secure Acceptance Transaction Flow

Secure Acceptance Checkout API Transaction Flow



1. Display the checkout page on your customer's browser with a form to collect their payment information and include a signature to validate their order information (signed data fields).

   Warning: Your system should sign all request fields with the exception of fields that contain data the customer is entering. To prevent malicious actors from impersonating Cybersource, do not allow unauthorized access to the signing function.

2. The customer enters and submits their payment details (the unsigned data fields). The transaction request message, the signature, and the signed and unsigned data fields are sent directly from your customer's browser to the Cybersource servers. The unsigned data fields do not pass through your network.

   Cybersource reviews and validates the transaction request data to confirm it has not been amended or tampered with and that it contains valid authentication credentials. Cybersource processes the transaction and creates and signs the response message. The response message is sent to the customer's browser as an automated HTTPS form POST.

   Warning:

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

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

3. The response HTTPS POST data contains the transaction result in addition to the masked payment data that was collected outside of your domain. Validate the response signature to confirm that the response data has not been amended or tampered with.

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

4. Cybersource recommends that you implement the merchant POST URL notification 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. See Merchant Notifications (on page 27).

Payment Tokens

Important: Contact Cybersource Customer Support to activate your merchant account for the Token Management Service (TMS). You cannot use payment tokens until your account is activated and you have enabled payment tokens for Secure Acceptance. See Creating a Secure Acceptance Profile (on page 18).

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 ACH 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.

Payment tokens represent the customer token in the Token Management Service (TMS). They are unique identifiers for sensitive customer and payment data that cannot be mathematically reversed. The payment token replaces the payment card, and optionally the associated billing and shipping information. No sensitive card information is stored on your servers, thereby reducing your PCI DSS obligations.

Secure Acceptance offers limited support for TMS, providing the ability to create and update a customer's default payment and shipping information. In the Secure Acceptance API, the **payment_token** field identifies the TMS customer token.

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.

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 Business Center. See Viewing Transactions in the Business CenterYour Merchant Services Account (on page 78).

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.

Subscription Types

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" (on page 63).
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

Subscription Types (continued)

Type of Subscription	Description
	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" (on page 65).

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 and corporate cards along with purchase and 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.

For detailed descriptions of each Level II field, see the Bank of America Integration Guide that also describes how to request sale and capture transactions.

Payouts Payment Tokens

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

Creating a Payment Token for Payouts

1. Create a Secure Acceptance Profile and define your checkout page. See Payment Acceptance Configuration (on page 18) or Portfolio Management for Resellers (on page 33).

2. For transaction processing, create a payment token. See "Payment Tokens" (on page 53).

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

See the Payouts Developer Guides.

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. Go-Live implementations do not occur on Fridays.

Payment Acceptance Configuration

Creating a Secure Acceptance Profile

Contact Cybersource Customer Support to enable your account for Secure Acceptance. You must activate a profile in order to use it. See Activating a Profile (on page 31).

1. Log in to the Business Center:
   - **Production**: https://businesscenter.cybersource.com
   - **Production in India**: https://businesscenter.in.cybersource.com
   - **Test**: https://businesscentertest.cybersource.com
2. Log in to **Merchant Services** inside Business Advantage 360.
3. In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
4. In the left navigation panel, choose **Payment Acceptance Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
5. Click **New Profile**. The Create Profile page appears.
6. Enter or verify these profile details.

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 IntegrationCheckout API**.
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 Payment Transactions (on page 48).

Profile Detail	Description
Decision ManagerFraud Management Essentials	Check **Decision ManagerFraud Management Essentials**. For more information, see Decision Manager (on page 75)refer to the guides in the Fraud Management section in your Merchant Services account.
Verbose Data	Check **Verbose Data**. For more information, see Decision Manager (on page 75)refer to the guides in the Fraud Management section in your Merchant Services account.
Generate Device Fingerprint	Check **Generate Device Fingerprint**. For more information, see Decision Manager (on page 75)refer to the guides in the Fraud Management section in your Merchant Services account.

7. Click **Submit**.

Payment Method Configuration

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 these 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 Click to Pay is the only enabled payment method for the profile. See Enabling the Payment Method for Visa Click to Pay (on page).

Important: Visa Click to Pay uses Visa Checkout services and API fields.

You can skip displaying the payment method selection page by specifying card or echeck as the only available payment method. See Enabling ACH Payments (on page 23).

Customers can change the payment method during the checkout process.

Adding 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.

1. In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
2. In the left navigation panel, choose **Payment Acceptance Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
3. Choose a profile. The General Settings page appears.
4. Find the profile, and click the more options ellipsis (...).
5. Select **Edit Profile**. The General Settings page appears.
6. Click **Payment Settings**. The Payment Settings page appears.
7. Click **Add Card Types**. The list of card types appear.
8. Check each card type that you want to offer to the customer as a payment method. Your payment processor must support the card types.
9. Click the settings icon for each card type. The card settings and currencies lists appear.
10. Check **CVN Display** to display the CVN field on Secure Acceptance. The customer decides whether to enter the CVN. Cybersource recommends that you display the CVN to reduce fraud.
11. 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 that you require the CVN to reduce fraud.
12. Check **Payer Authentication**.
13. 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.
14. Click **Submit**. The card types are added as an accepted payment type.
15. Click **Save**.

Payer Authentication3-D Secure Configuration

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

Before you can use Payer Authentication, you must contact Customer Support to configure your account. Your merchant ID must be enabled for payer authentication. For more information about payer authentication, see the Payer Authentication Developer Guides.

3-D Secure is the Cybersource implementation of Payer Authentication. It prevents unauthorized card use and provides added protection from fraudulent chargeback activity. 3-D Secure is not available to Bank of America merchants in production at this time. You will see a Payer Authentication section within the Payment Acceptance Configuration tab in the Demonstration and Certification Environment (DCE), if you choose to use the DCE.

Before you can use Bank of America 3-D Secure, you must contact Bank of America Technical Support to configure your account. Your merchant ID must be enabled for 3D Secure.

Secure Acceptance supports 3-D Secure 1.0 and 2.0.

For Secure Acceptance, Cybersource supports these kinds of payer authentication:

- American Express SafeKey
- China UnionPay (3-D Secure 2.0 only)
- Diners ProtectBuy
- J/Secure by JCB
- Mastercard Identity Check
- Visa Secure

For each transaction, you receive detailed information in the replies and in the transaction details page of the Business Centeryour Merchant Services account. 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 present again 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 (on page 77).

Configuring Payer Authentication

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

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

3. Choose a profile. The General Settings page appears.

4. Find the profile, and click the more options ellipsis (...).

5. Select **Edit Profile**. The General Settings page appears.

6. Click **Payment Settings**. The Payment Settings page appears.

7. Choose a 3-D Secure version. If you choose 3-D Secure 2.0 and the card issuer is not 3-D Secure 2.0 ready, some transactions might still authenticate over 3-D Secure 1.0. The **payer_authentication_specification_version** response field indicates which version was used.

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

    - American Express
    - Cartes Bancaires
    - China UnionPay
    - Diners Club
    - JCB
    - Mastercard
    - Maestro (UK Domestic or International)
    - Visa

Enabling Automatic Authorization Reversals

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

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

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

3. Choose a profile. The General Settings page appears.

4. Find the profile, and click the more options ellipsis (...).

5. Select **Edit Profile**. The General Settings page appears.

6. Click **Payment Settings**. The Payment Settings page appears.

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

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

9. Click **Save**.

> **Important:** 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 (on page)Types of Notifications (on page 215).

Enabling ACH Payments

An ACH payment 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 ACH transactions. 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 that you 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.

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

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

3. Click **Payment Settings**. The Payment Settings page appears.

4. Check **Enable Echeck Payments**. The list of account types appears.

5. Check the account type(s):

- Checking
- Savings
- Corporate Checking
- General Ledger

6. Click **Add Currencies**. The ACH settings page appears.
7. Check **Select All** or check each currency.
8. Click **Save**.

You must configure the ACH information fields. See Configuring ACH Information Fields (on page).

Enabling PayPal Express Checkout

PayPal Express Checkout is a form of Digital Payments, which are not available to Bank of America merchants at this time. You will see Digital Payments within the Demo and Certification Environment (DCE), if you choose to use the DCE.

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 the PayPal guide. *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 your checkout page and 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.

Add the PayPal Express Checkout payment method to the Hosted Checkout Integration 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.

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

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

3. Choose a profile. The General Settings page appears.

4. Find the profile, and click the more options ellipsis (...).

5. Select **Edit Profile**. The General Settings page appears.

6. Click **Payment Settings**. The Payment Settings page appears.

7. Check **Enable PayPal Express Checkout**.

8. 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.

9. When the transaction type is authorization, check one of these options:

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

     > **Important:** The customer funds are not captured using this option. You must request a PayPal capture; see the PayPal guide. If the transaction type is `sale`, Secure Acceptance authorizes and captures the customer funds.

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

     > **Important:** The customer funds are not authorized or captured using this option. You must request a PayPal authorization followed by a PayPal capture request; see the PayPal guide. If the transaction type is `sale`, Secure Acceptance authorizes and captures the customer funds.

10. Click **Save**.

Security Keys

Before you can activate a profile, you must create a security key to protect each transaction from data tampering. A security key expires in two years.

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

- **Test**: https://businesscentertest.cybersource.com
- **Production**: https://businesscenter.cybersource.com
- **Production in India**: https://businesscenter.in.cybersource.com

On the Profile Settings page, click **Security**. The Security Keys page appears. The security script signs the request fields using the secret key and the HMAC SHA256 algorithm. To verify data, the security script generates a signature to compare with the signature returned from the Secure Acceptance server.

Creating Security Keys

1. Log in to the Business Center.
2. In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
3. Log in to your Merchant Services account.
4. In the left navigation panel, choose **Payment Acceptance Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
5. Choose a profile. The General Settings page appears.
6. Find the profile, and click the more options ellipsis (...).
7. Select **Edit Profile**. The General Settings page appears.
8. Click **Security**. The security keys page appears.
9. Click the Create Key plus sign (+).
10. Click **Create Key**.
11. Enter a key name (required).
12. Choose signature version 1 (default).
13. Choose signature method **HMAC-SHA256** (default).
14. Click **Create**.
15. Click **Confirm**. The Create New Key window expands and displays the new access key and secret key. This panel closes after 30 seconds.
16. 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 Scripting Language Samples (on page 46).
- Secret key: signs the transaction data and is required for each transaction. Copy and paste this secret key into your security script. See Scripting Language Samples (on page 46).

> **Important:** When done pasting the secret keys into your script, 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.

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.

> **Important:** 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.

Configuring Merchant Notifications

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

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

3. Choose a profile. The General Settings page appears.

4. Find the profile, and click the more options ellipsis (...).

5. Select **Edit Profile**. The General Settings page appears.

6. Click **Notifications**. The Notifications page appears.

7. 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 Response Fields (on page 159). 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 Response Fields (on page 159).

8. 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

9. Click **Save**.

Customer Receipts

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).

Configuring Customer Notifications

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

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

3. Choose a profile. The General Settings page appears.

4. Find the profile, and click the more options ellipsis (...).

5. Select **Edit Profile**. The General Settings page appears.

6. Click **Notifications**. The Notifications page appears.

7. Check **Email Receipt to Customer**.

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

9. Enter the sender name of your business. It is displayed on the customer receipt.

10. Check **Send a copy to**. This setting is optional.

11. 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.

12. Check **Display Notification Logo**.

13. 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 (width) x 60 (height) pixels and must be GIF, JPEG, or PNG. The logo filename must not contain any special characters, such as a hyphen (-).

14. Check **Custom Email Receipt**.
    Cybersource recommends that you implement a DNS configuration to enable Cybersource to send email receipts on your behalf.

15. 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.

16. 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.

17. Click **Save**.

Customer 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.

You must choose to display a response page to the customer at the end of the checkout process. Enter a URL for your own customer response page. This page is displayed to the customer after the transaction is processed. 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.

Configuring a Transaction Response Page

1. In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
2. Choose a profile. The General Settings page appears.
3. Click **Customer Response**. The Customer Response page appears.
4. Enter the URL for your customer response page. Use port 80, 443, or 8080 in the URL.

Only port 443 should be used with an HTTPS URL.

A POST request with the transaction data is provided to this URL after the customer completes checkout.

The POST request contains the reason code value of the transaction, which helps you determine possible actions to take on the transaction.

See Reason Codes (on page 211).

5. Click **Save**.

Activating a Profile

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

- Payment Method Configuration (on page 19)
- Security Keys (on page 25)
- Customer Response Page (on page 30)

1. On the left navigation pane, click the **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
2. Perform one of these 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.
3. On the left navigation pane, click the **Payment Acceptance Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
4. Find the inactive profile and click the **Promote Profile** button.
5. 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.

Portfolio Management for Resellers

Creating a Hosted Checkout IntegrationCheckout API Profile

Contact Cybersource Customer Support to enable your account for Secure Acceptance. You must activate a profile in order to use it. See Reseller: Activating a Profile (on page 45).

1. Log in to the Business Center:
   - **Production**: https://businesscenter.cybersource.com
   - **Production in India**: https://businesscenter.in.cybersource.com
   - **Test**: https://businesscentertest.cybersource.com
2. In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
3. Click **New Profile**.
4. Enter or verify these profile details.

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 CheckoutCheckout API**.
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 Payment Transactions (on page 48).

Profile Detail	Description
Decision Manager	Check **Decision Manager**. For more information, see Decision Manager (on page 75).
Verbose Data	Check **Verbose Data**. For more information, see Decision Manager (on page 75).
Generate Device Fingerprint	Check **Generate Device Fingerprint**. For more information, see Decision Manager (on page 75).

5. Click **Submit**.

Payment Method Configuration

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

Important: Visa Click to Pay uses Visa Checkout services and API fields.

A payment method selection page is displayed as part of the checkout process for any of these 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 Click to Pay is the only enabled payment method for the profile. See Reseller: Configuring Visa Click to Pay (on page).

You can skip the payment method selection page by specifying card or echeck as the only available payment method. See Reseller: Enabling ACH Payments (on page 37).

Customers can change the payment method during the checkout process.

Reseller: Adding 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.

1. In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
2. Choose a profile. The General Settings page appears.
3. Click **Payment Settings**. The Payment Settings page appears.
4. Click **Add Card Types**. The list of card types appear.
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.
6. Click **Settings** for each card type. The card settings and currencies lists appear.
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.
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.
9. Check the currencies for each card.

   Important: By default, all currencies are listed as disabled. You must select at least one currency. Contact your merchant account provider for a list of supported currencies. If you select the Elo or Hipercard card type, only the Brazilian Real currency is supported.

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

Payer Authentication 3-D Secure Configuration

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

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 the Payer Authentication Developer Guides.

For Secure Acceptance, Cybersource supports these kinds of payer authentication:

- American Express SafeKey
- China UnionPay (3-D Secure 2.0 only)
- Diners ProtectBuy
- J/Secure by JCB
- Mastercard Identity Check
- Visa Secure

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 present again 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 (on page 77).

Reseller: Configuring Payer Authentication

1. In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
2. Choose a profile. The General Settings page appears.
3. Click **Payment Settings**. The Payment Settings page appears.
4. Choose the 3-D Secure version that you want to use. If you choose 3-D Secure 2.0 and the card issuer is not 3-D Secure 2.0 ready, some transactions might still authenticate over 3-D Secure 1.0. The **payer_authentication_specification_version** response field indicates which version was used.
5. Click **Save**. The card types that support payer authentication are:
    - American Express
    - Cartes Bancaires
    - China UnionPay
    - Diners Club
    - JCB

- Mastercard
- Maestro (UK Domestic or International)
- Visa

Reseller: Enabling Automatic Authorization Reversals

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

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

> **Important:** 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 (on page)Types of Notifications (on page 215).

Reseller: Enabling ACH Payments

An ACH payment 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 ACH transactions. 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.

1. In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
2. Choose a profile. The General Settings page appears.
3. Click **Payment Settings**. The Payment Settings page appears.
4. Check **Enable Echeck Payments**. The list of account types appears.
5. Check the account type(s):
    - Checking
    - Savings
    - Corporate Checking
    - General Ledger
6. Click **Add Currencies**. The ACH settings page appears.
7. Check **Select All** or select a currency.
8. Click **Save**.

You must configure the ACH information fields. See Reseller: Configuring ACH Information Fields (on page).

Reseller: Enabling 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 your checkout page and redirect the customer to their PayPal account login. the Secure Acceptance Hosted Checkout Integration 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.

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

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

3. Click **Payment Settings**. The Payment Settings page appears.

4. Check **Enable PayPal Express Checkout**.

5. Click **Save**.

Service Fees

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 ACH 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.

Reseller: Enabling Service Fees

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

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

3. Click **Payment Settings**. The Payment Settings page appears.

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.

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

5. Enter the Consent Page URL.

Cybersource sends the order information and the service fee amount to the consent page URL by HTTPS POST. The customer is directed from your checkout page to the consent page URL to accept or decline the service fee amount. See the Secure Acceptance Checkout API Service Fee Guide for detailed information.

6. Click **Save**.

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

Security Keys

Before you can activate a profile, you must create a security key to protect each transaction from data tampering. A security key expires in two years.

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

- **Test**: https://businesscentertest.cybersource.com
- **Production**: https://businesscenter.cybersource.com
- **Production in India**: https://businesscenter.in.cybersource.com

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

Reseller: Creating Security Keys

1. In the left navigation panel, choose **Payment Configuration > Key Management.**
2. Click **Generate Key**.
3. Select a key type.
4. Click **Next Step**.
5. Select the key subtype **Secure Acceptance**.
6. Click **Next Step**.
7. Enter a key name (required).
8. Choose signature version **1**.

9. Choose signature method **HMAC-SHA256**.
10. Select a security profile.
11. Click **Submit**.
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.
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 Scripting Language Samples (on page 46).
    - Secret key: signs the transaction data and is required for each transaction. Copy and paste this secret key into your security script. See Scripting Language Samples (on page 46).

    Important: When done pasting the secret keys into your script, 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.
14. Click **Key Management**. The Key Management page appears.

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.

Important: 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.

Reseller: Configuring Merchant Notifications

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

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

3. Click Notifications. The Notifications page appears.

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 Response Fields (on page 159).

     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 Response Fields (on page 159).

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

6. Click **Save**.

Customer Receipts

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).

Reseller: Configuring Customer Notifications

1. In the left navigation panel, choose **Portfolio Management > Secure Acceptance Profiles**. The Secure Acceptance Profile page appears.
2. Choose a profile. The General Settings page appears.
3. Click **Notifications**. The Notifications page appears.
4. Check **Email Receipt to Customer**.
5. Enter the sender email address to be displayed on the customer receipt. The customer will reply to this email with any queries.
6. Enter the sender name of your business. It is displayed on the customer receipt.
7. Check **Send a copy to**. This setting is optional.
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.
9. Check **Display Notification Logo**.
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 (width) x 60 (height) pixels and must be GIF, JPEG, or PNG. The logo filename must not contain any special characters, such as a hyphen (-).
11. Check **Custom Email Receipt**.

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

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**.

14. Click **Save**.

Customer 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.

You must choose to display a response page to the customer at the end of the checkout process. Enter a URL for your own customer response page. This page is displayed to the customer after the transaction is processed. 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.

Reseller: Configuring a Transaction Response Page

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

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

3. Click **Customer Response**. The Customer Response page appears.

4. Enter the URL for your customer response page. Use port 80, 443, or 8080 in the URL. Only port 443 should be used with an HTTPS URL.

   A POST request with the transaction data is provided to this URL after the customer completes checkout.

The POST request contains the reason code value of the transaction, which helps you determine possible actions to take on the transaction.

See Reason Codes (on page 211).

5. Click **Save**.

Reseller: Activating a Profile

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

- Payment Method Configuration (on page 34)
- Security Keys (on page 40)
- Customer Response Page (on page 44)

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

Reseller: 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.

Scripting Language Samples

Secure Acceptance can support any dynamic scripting language that supports HMAC256 hashing algorithms.

Select the scripting language you use to download a sample script:

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

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

Sample Transaction Process Using JSP

1. ***payment_form.jsp*** file—represents the customer's product selection on a website. 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. ***signeddatafields.jsp*** file—paste your access key and profile ID into their respective fields. The customer enters billing, shipping, and other information. POST the fields to your server to sign and create the signature. The fields must be included in the **signed_field_names** field as a CSV list.

3. ***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 Security Keys (on page 25).

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

- Request authentication—the signature is generated on the merchant server by the keyed-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.

4. ***payment_confirmation.jsp*** file—represents the customer order review page on a website, before the customer makes a payment. POST transaction to the Secure Acceptance endpoint and render the Hosted Checkout Integration. See Payment Transactions (on page 48).

5. ***unsigneddatafields.jsp*** file—customer enters their payment information: card type, card number, and card expiry date. Include these fields in the **unsigned_field_names** field. POST the transaction to the Secure Acceptance endpoint.

Payment Transactions

This section provides endpoints and transaction use cases.

Endpoints and Transaction Types

Endpoints

Create Payment Token Endpoints See Creating a Payment Card Token (on page 53).	

Test	`https://testsecureacceptance.cybersource.com/token/create`
	`https://testsecureacceptance.cybersource.com/silent/token/create`
	`https://testsecureacceptance.merchant-services.bankofamerica.com/token/create`
	`https://testsecureacceptance.merchant-services.bankofamerica.com/silent/token/create`

Production	`https://secureacceptance.cybersource.com/token/create`
	`https://secureacceptance.cybersource.com/silent/token/create`
	`https://secureacceptance.merchant-services.bankofamerica.com/token/create`
	`https://secureacceptance.merchant-services.bankofamerica.com/silent/token/create`

Production in India	`https://secureacceptance.in.cybersource.com/token/create` `https://secureacceptance.in.cybersource.com/silent/token/create`
Supported transaction type	`create_payment_token`
Iframe Create Payment Token Endpoints See Iframe Implementation (on page 222).	

Test	`https://testsecureacceptance.cybersource.com/embedded/token/create`
	`https://testsecureacceptance.cybersource.com/silent/embedded/token/create`
	`https://testsecureacceptance.merchant-services.bankofamerica.com/embedded/token/create`
	`https://testsecureacceptance.merchant-services.bankofamerica.com/silent/embedded/token/create`

Production	`https://secureacceptance.cybersource.com/embedded/token/create`
	`https://secureacceptance.cybersource.com/silent/embedded/token/create`
	`https://secureacceptance.merchant-services.bankofamerica.com/embedded/tok`

Endpoints (continued)

	`en/create` `https://secureacceptance.merchant-services.bankofamerica.com/silent/embedded/token/create`
Production in India	`https://secureacceptance.in.cybersource.com/embedded/token/create` `https://secureacceptance.in.cybersource.com/silent/embedded/token/create`
Supported transaction type	`create_payment_token`
Iframe Transaction Endpoints See Iframe Implementation (on page 222).	

Test	`https://testsecureacceptance.cybersource.com/embedded/pay`
	`https://testsecureacceptance.cybersource.com/silent/embedded/pay`
	`https://testsecureacceptance.merchant-services.bankofamerica.com/embedded/pay`
	`https://testsecureacceptance.merchant-services.bankofamerica.com/silent/embedded/pay`

Production	`https://secureacceptance.cybersource.com/embedded/pay`
	`https://secureacceptance.cybersource.com/silent/embedded/pay`
	`https://secureacceptance.merchant-services.bankofamerica.com/embedded/pay`
	`https://secureacceptance.merchant-services.bankofamerica.com/silent/embedded/pay`

Production in India	`https://secureacceptance.in.cybersource.com/embedded/pay` `https://secureacceptance.in.cybersource.com/silent/embedded/pay`
Supported transaction type	• `authorization` • `authorization,create_payment_token` • `authorization,update_payment_token` • `sale` • `sale,create_payment_token` • `sale,update_payment_token` • `create_payment_token`
Iframe Update Payment Token Endpoints See Iframe Implementation (on page 222).	

Endpoints (continued)

Test	`https://testsecureacceptance.cybersource.com/embedded/token/update`
	`https://testsecureacceptance.cybersource.com/silent/embedded/token/update`
	`https://testsecureacceptance.merchant-services.bankofamerica.com/embedded/token/update`
	`https://testsecureacceptance.merchant-services.bankofamerica.com/silent/embedded/token/update`

Production	`https://secureacceptance.cybersource.com/embedded/token/update`
	`https://secureacceptance.cybersource.com/silent/embedded/token/update`
	`https://secureacceptance.merchant-services.bankofamerica.com/embedded/token/update`
	`https://secureacceptance.merchant-services.bankofamerica.com/silent/embedded/token/update`

Production in India	`https://secureacceptance.in.cybersource.com/embedded/token/update` `https://secureacceptance.in.cybersource.com/silent/embedded/token/update`
Supported transaction type	`update_payment_token`
One-Click Endpoints See One-Click Checkout (on page).	
Test	`https://testsecureacceptance.cybersource.com/oneclick/pay` `https://testsecureacceptance.merchant-services.bankofamerica.com/oneclick/pay`
Production	`https://secureacceptance.cybersource.com/oneclick/pay` `https://secureacceptance.merchant-services.bankofamerica.com/oneclick/pay`
Production in India	https://secureacceptance.in.cybersource.com/oneclick/pay
Supported transaction types	• `authorization` • `authorization,update_payment_token` • `sale` • `sale,update_payment_token`
Process Transaction Endpoints	

Endpoints (continued)

Test	`https://testsecureacceptance.cybersource.com/pay`
	`https://testsecureacceptance.cybersource.com/silent/pay`
	`https://testsecureacceptance.merchant-services.bankofamerica.com/pay`
	`https://testsecureacceptance.merchant-services.bankofamerica.com/silent/pay`

Production	`https://secureacceptance.cybersource.com/pay`
	`https://secureacceptance.cybersource.com/silent/pay`
	`https://secureacceptance.merchant-services.bankofamerica.com/pay`
	`https://secureacceptance.merchant-services.bankofamerica.com/silent/pay`

Production in India	`https://secureacceptance.in.cybersource.com/pay` `https://secureacceptance.in.cybersource.com/silent/pay`
Supported transaction types	• `authorization` • `authorization,create_payment_token` • `authorization,update_payment_token` • `sale` • `sale,create_payment_token` • `sale,update_payment_token`
Update Payment Token Endpoints See Payment Token Updates (on page 68).	

Test	`https://testsecureacceptance.cybersource.com/token/update`
	`https://testsecureacceptance.cybersource.com/silent/token/update`
	`https://testsecureacceptance.merchant-services.bankofamerica.com/token/update`
	`https://testsecureacceptance.merchant-services.bankofamerica.com/silent/token/update`

Production	`https://secureacceptance.cybersource.com/token/update`
	`https://secureacceptance.cybersource.com/silent/token/update`
	`https://secureacceptance.merchant-services.bankofamerica.com/token/update`
	`https://secureacceptance.merchant-services.bankofamerica.com/silent/token/update`

Endpoints (continued)

Production in India	`https://secureacceptance.in.cybersource.com/token/update` `https://secureacceptance.in.cybersource.com/silent/token/update`
Supported transaction type	`update_payment_token`
Visa Click to Pay Endpoints	
Test	`https://testsecureacceptance.cybersource.com/pay` `https://testsecureacceptance.merchant-services.bankofamerica.com/pay`
Production	`https://secureacceptance.cybersource.com/pay` `https://secureacceptance.merchant-services.bankofamerica.com/pay`
Production in India	`https://secureacceptance.in.cybersource.com/pay`
Supported transaction types	• `authorization` • `sale`

Required Signed Fields

Signing fields protects them from malicious actors adding or changing transaction data during transmission. To sign fields, include them in a comma-separated string in the **signed_field_names** field in your request.

> **Important:** To prevent data tampering, sign all request fields with the exception of fields that contain data the customer is entering.

These signed fields are required in all Secure Acceptance requests:

- **access_key**
- **amount**
- **currency**

- **locale**
- **payment_method**
- **profile_id**
- **reference_number**
- **signed_date_time**
- **signed_field_names**
- **transaction_type**
- **transaction_uuid**
- **unsigned_field_names**

For descriptions of these fields, see Request Fields (on page 80).

Payment Tokens

Creating a Payment Card Token

Important: Include the appropriate endpoint that supports the `create_payment_token` transaction type. See Endpoints and Transaction Types (on page 48). For descriptions of all request and response fields. See Hosted Checkout IntegrationCheckout API Fields (on page 79).

Include all request fields in the **signed_field_names** field with the exception of the **card_number**, **card_cvn**, and **signature** fields. 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: Creating a Standalone Payment Card Token

Request

```
reference_number=12x456789 // Replace X with 3
transaction_type=create_payment_token
currency=usd
amount=100.00
locale=en
```

```
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
transaction_uuid=02815b4f08e56882751a043839b7b481
signed_date_time=2020-07-11T15:16:54Z
signed_field_names=reference_number,transaction_type,currency,amount,locale,access
_key,profile_id,transaction_uuid,signed_date_time,signed_field_names,etc...
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
payment_method=card
card_type=001
card_number=411111111111xxxx // Replace x with 1
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
```

```
reference_number=12x456789 // Replace X with 3
transaction_type=create_payment_token
currency=usd
amount=100.00
locale=en
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
transaction_uuid=02815b4f08e56882751a043839b7b481
signed_date_time=2020-07-11T15:16:54Z
signed_field_names=reference_number,transaction_type,currency,amount,locale,paymen
t_method,access_key,profile_id,transaction_uuid,signed_date_time,signed_field_name
s,unsigned_field_names,etc...
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
payment_method=card
card_type=001
card_number=411111111111xxxx // Replace x with 1
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
```

Response

```
req_reference_number=12x456789 // Replace X with 3
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=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_transaction_uuid=02815b4f08e56882751a043839b7b481
signed_date_time=2020-07-11T15:16:54Z
signed_field_names=reference_number,transaction_type,currency,amount,locale,access
_key,profile_id,transaction_uuid,signed_date_time,signed_field_names,etc...
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
decision=ACCEPT
reason_code=100
transaction_id=3735553783662130706689
req_payment_token=CF2194C8A0F545CDE053AF598E0A20DA
```

```
req_reference_number=12x456789 // Replace X with 3
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=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_transaction_uuid=02815b4f08e56882751a043839b7b481
signed_date_time=2020-07-11T15:16:54Z
signed_field_names=reference_number,transaction_type,currency,amount,locale,paymen
t_method,access_key,profile_id,transaction_uuid,signed_date_time,signed_field_name
s,unsigned_field_names,etc...
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
decision=ACCEPT
reason_code=100
transaction_id=3735553783662130706689
req_payment_token=CF2194C8A0F545CDE053AF598E0A20DA
```

```
req_reference_number=12x456789 // Replace X with 3
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
payment_token_instrument_identifier_id=0000111122225555
req_access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
req_profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_transaction_uuid=02815b4f08e56882751a043839b7b481
signed_date_time=2020-07-11T15:16:54Z
signed_field_names=reference_number,transaction_type,currency,amount,locale,access
_key,profile_id,transaction_uuid,signed_date_time,signed_field_names,etc...
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
decision=ACCEPT
reason_code=100
transaction_id=3735553783662130706689
req_payment_token=CF2194C8A0F545CDE053AF598E0A20DA
```

Creating an ACH Token

Important: Include the appropriate endpoint that supports the `create_payment_token` transaction type. See Endpoints and Transaction Types (on page 48). For descriptions of all request and response fields, see Hosted Checkout IntegrationCheckout API Fields (on page 79).

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: Creating a Standalone ACH Payment Token

Request

```
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p1
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
transaction_type=create_payment_token
currency=USD
amount=100.00
locale=en
reference_number=1730560013735542024294683
transaction_uuid=02815b4f08e56882751a043839b7b481
signed_date_time=2022-07-11T15:16:54Z
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
signed_field_names=reference_number,transaction_type,currency,amount,locale,access
_key,profile_id,transaction_uuid,signed_date_time,signed_field_names,etc...
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=X4-782X9-X96 // Replace X with 3
date_of_birth=19901001
echeck_account_type=c
company_tax_id=12x456789 // Replace X with 3
echeck_sec_code=WEB
echeck_account_number=4528941xx // Replace x with 0
echeck_routing_number=6723x2882 // Replace x with 0
```

```
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p1
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
transaction_type=create_payment_token
currency=USD
amount=100.00
locale=en
reference_number=1730560013735542024294683
transaction_uuid=02815b4f08e56882751a043839b7b481
signed_date_time=2022-07-11T15:16:54Z
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
signed_field_names=reference_number,transaction_type,currency,amount,locale,paymen
t_method,access_key,profile_id,transaction_uuid,signed_date_time,signed_field_name
s,unsigned_field_names,etc...
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=X4-782X9-X96 // Replace X with 3
date_of_birth=19901001
echeck_account_type=c
company_tax_id=12x456789 // Replace X with 3
echeck_sec_code=WEB
echeck_account_number=4528941xx // Replace x with 0
echeck_routing_number=6723x2882 // Replace x with 0
```

Response

```
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=reference_number,transaction_type,currency,amount,locale,access
_key,profile_id,transaction_uuid,signed_date_time,signed_field_names,etc...
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=2022-07-11T15:11:41Z
req_currency=USD
req_reference_number=1730560013735542024294683
req_echeck_routing_number=xxxxx2882
transaction_id=3735553783662130706689
req_amount=100.00
req_profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_company_tax_id=12x456789 // Replace X with 3
req_transaction_uuid=38f2efe650ea699597d325ecd7432b1c
req_payment_token=CF2194C8A0F545CDE053AF598E0A20DA
req_bill_to_surname=Soap
req_bill_to_forename=Joe
req_bill_to_email=joesoap@yahoo.com
req_access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p1
```

Payment Token Transactions

To create a single-click checkout experience for returning customers, send the payment token instead of the payment data to the transaction endpoints. See Endpoints and Transaction Types (on page 48).

Requesting a Payment Card Transaction with a Token

Important: Include the appropriate endpoint that supports the authorization or sale transaction types. See Endpoints and Transaction Types (on page 48). For descriptions of all request and response fields, see Hosted Checkout IntegrationCheckout API Fields (on page 79).

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

Payment Card Transaction with a Token

Request

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
reference_number=1350029885978
payment_token=CF2194C8A0F545CDE053AF598E0A20DA
consumer_id=1239874561
transaction_type=authorization
amount=100.00
currency=USD
payment_method=card
locale=en
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2020-01-17T10:46:39Z
signed_field_names=reference_number,transaction_type,currency,amount,locale,paymen
t_method,access_key,profile_id,transaction_uuid,signed_date_time,signed_field_name
s,unsigned_field_names,etc...
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
```

Response

```
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
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==2022-08-14T134608Z
req_payment_token=CF2194C8A0F545CDE053AF598E0A20DA
signed_field_names=reference_number,transaction_type,currency,amount,locale,paymen
t_method,access_key,profile_id,transaction_uuid,signed_date_time,signed_field_name
s,unsigned_field_names,etc...
signed_date_time=2022-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
payment_token_latest_card_suffix=1717
payment_token_latest_card_expiry_date=11-2024
payment_solution=015
```

ACH Payment with a Token

The customer is directed to the Order Review page. Depending on the settings you configured for Secure Acceptance Hosted Checkout Integration, the customer can view or update billing, shipping, and payment details before confirming to pay. See Checkout Configuration (on page).

Important: Include the appropriate endpoint that supports the `authorization` or `sale` transaction types. See Endpoints and Transaction Types (on page 48). For descriptions of all request and response fields, see Hosted Checkout IntegrationCheckout API Fields (on page 79).

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

Example: Processing a Payment with an ACH Token

Request

```
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
reference_number=1845864013783060468573616
transaction_type=sale
currency=USD
amount=100.00
locale=en
payment_token=CF2194C8A0F545CDE053AF598E0A20DA
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2022-01-17T10:46:39Z
```

```
signed_field_names=reference_number,transaction_type,currency,amount,locale,access
_key,profile_id,transaction_uuid,signed_date_time,signed_field_names,etc...
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

```
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
reference_number=1845864013783060468573616
transaction_type=sale
currency=USD
amount=100.00
locale=en
payment_method=echeck
payment_token=CF2194C8A0F545CDE053AF598E0A20DA
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2022-01-17T10:46:39Z
signed_field_names=reference_number,transaction_type,currency,amount,locale,paymen
t_method,access_key,profile_id,transaction_uuid,signed_date_time,signed_field_name
s,unsigned_field_names,etc...
unsigned_field_names=comma separated list of unsigned fields
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

Response

```
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=reference_number,transaction_type,currency,amount,locale,access
_key,profile_id,transaction_uuid,signed_date_time,signed_field_names,etc...
req_payment_method=echeck
req_transaction_type=sale
req_echeck_account_type=c
signature=ZUk7d99c/yb+kidvVUbz10JtykmjOt8LMPgkllRaZR8=
req_locale=en
reason_code=100
req_echeck_account_number=xxxxx4100
req_bill_to_address_line1=1 My Apartment
req_echeck_sec_code=WEB
signed_date_time=2022-06-12T09:59:50Z
req_currency=USD
req_reference_number=7735300137103108077269 3
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=2022-03-25T104341Z
req_profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_company_tax_id=12x456789 // Replace X with 3
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

Your merchant ID must be enabled to process 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.

Important: Include the appropriate endpoint that supports the `authorization,create_payment_token` or `sale,create_payment_token` transaction types. See Endpoints and Transaction Types (on page 48). For descriptions of all request and response fields, see Hosted Checkout IntegrationCheckout API Fields (on page 79).

Important: The **amount** field is an optional field that indicates the setup fee for processing recurring payments.

Example: Creating a Recurring Billing Payment and Token

Request

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
transaction_type=authorization,create_payment_token
locale=en
amount=5.00
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2020-01-17T10:46:39Z
signed_field_names=reference_number,transaction_type,currency,amount,locale,access
_key,profile_id,transaction_uuid,signed_date_time,signed_field_names,etc...
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
consumer_id=x23987456x // Replace x with 1
```

```
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=411111111111xxxx // Replace x with 1
card_expiry_date=12-2022
card_cvn=005
transaction_reason=setup_recurring
recurring_frequency=monthly
recurring_amount=25.00
recurring_start_date=20200125
payment_method=card
```

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
transaction_type=authorization,create_payment_token
locale=en
amount=5.00
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2020-01-17T10:46:39Z
signed_field_names=reference_number,transaction_type,currency,amount,locale,paymen
t_method,access_key,profile_id,transaction_uuid,signed_date_time,signed_field_name
s,unsigned_field_names,etc...
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
consumer_id=x23987456x // Replace x with 1
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=411111111111xxxx // Replace x with 1
card_expiry_date=12-2022
card_cvn=005
transaction_reason=setup_recurring
recurring_frequency=monthly
recurring_amount=25.00
recurring_start_date=20200125
payment_method=card
```

Response

```
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,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=x23987456x // Replace x with 1
req_recurring_frequency=monthly
req_recurring_amount=25.00
req_recurring_start_date=20200125
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=2022-08-14T134608Z
req_payment_token=CF2194C8A0F545CDE053AF598E0A20DA
signed_field_names=reference_number,transaction_type,currency,amount,locale,access
_key,profile_id,transaction_uuid,signed_date_time,signed_field_names,etc...
signed_date_time=2022-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

Installment Payments

Your merchant ID must be enabled to process 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.

Important: Include the appropriate endpoint that supports the `authorization,create_payment_token` or `sale,create_payment_token` transaction types. See Endpoints and Transaction Types (on page 48). For descriptions of all request and response fields, see Hosted Checkout IntegrationCheckout API Fields (on page 79).

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

Example: Creating an Installment Payment and Token

Request

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
transaction_type=authorization,create_payment_token
amount=5.00
locale=en
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2020-01-17T10:46:39Z
signed_field_names=reference_number,transaction_type,currency,amount,locale,access
_key,profile_id,transaction_uuid,signed_date_time,signed_field_names,etc...
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
consumer_id=x23987456x // Replace x with 1
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=411111111111xxxx // Replace x with 1
card_expiry_date=12-2022
card_cvn=005
recurring_frequency=monthly
recurring_number_of_installments=6
recurring_amount=25.00
recurring_start_date=20200125
payment_method=card
```

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
transaction_type=authorization,create_payment_token
amount=5.00
locale=en
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2020-01-17T10:46:39Z
signed_field_names=reference_number,transaction_type,currency,amount,locale,paymen
t_method,access_key,profile_id,transaction_uuid,signed_date_time,signed_field_name
s,unsigned_field_names,etc...
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
consumer_id=x23987456x // Replace x with 1
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=411111111111xxxx // Replace x with 1
card_expiry_date=12-2022
card_cvn=005
recurring_frequency=monthly
recurring_number_of_installments=6
recurring_amount=25.00
recurring_start_date=20200125
payment_method=card
```

Response

```
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,create_payment_token
req_reference_number=1350029885978
req_amount=5.00
req_currency=USD
req_locale=en
req_payment_method=card
req_consumer_id=x23987456x // Replace x with 1
req_recurring_frequency=monthly
req_recurring_number_of_installments=6
req_recurring_amount=25.00
```

```
req_recurring_start_date=20200125
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==2022-08-14T134608Z
req_payment_token=CF2194C8A0F545CDE053AF598E0A20DA
signed_field_names=reference_number,transaction_type,currency,amount,locale,access
_key,profile_id,transaction_uuid,signed_date_time,signed_field_names,etc...
signed_date_time=2022-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

Payment Token Updates

Updating a Payment Card Token

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.

The **payment_token** field identifies the TMS customer token and its default payment instrument and shipping address. 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 Configuring Order Review Details (on page).

Important: 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 (on page 46). You must include the **allow_payment_token_update** field and set it to `true`.

Example: Updating a Payment Card Token

Request

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
transaction_type=update_payment_token
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
reference_number=1350029885978
payment_token=CF2194C8A0F545CDE053AF598E0A20DA
amount=100.00
currency=USD
payment_method=card
card_type=001
card_number=411111111111xxxx // Replace x with 1
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=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2020-01-17T10:46:39Z
consumer_id=x23987456x // Replace x with 1
signed_field_names=reference_number,transaction_type,currency,amount,locale,access
_key,profile_id,transaction_uuid,signed_date_time,signed_field_names,etc...
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
```

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
transaction_type=update_payment_token
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
reference_number=1350029885978
payment_token=CF2194C8A0F545CDE053AF598E0A20DA
amount=100.00
currency=USD
payment_method=card
card_type=001
```

```
card_number=411111111111xxxx // Replace x with 1
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=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2020-01-17T10:46:39Z
consumer_id=x23987456x // Replace x with 1
signed_field_names=reference_number,transaction_type,currency,amount,locale,paymen
t_method,access_key,profile_id,transaction_uuid,signed_date_time,signed_field_name
s,unsigned_field_names,etc...
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
```

Response

```
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=x23987456x // Replace x with 1
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=2022-08-14T134608Z
payment_token=CF2194C8A0F545CDE053AF598E0A20DA
signed_field_names=comma separated list of signed fields
signed_date_time=2022-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

```
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=x23987456x // Replace x with 1
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
payment_token_instrument_identifier_id=0000111122225555
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=2022-08-14T134608Z
payment_token=CF2194C8A0F545CDE053AF598E0A20DA
signed_field_names=comma separated list of signed fields
signed_date_time=2022-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

Updating an ACH Token

The **payment_token** field identifies the ACH 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 Configuring Order Review Details (on page).

> **Important:** 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: Updating an ACH Payment Token

Request

```
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
reference_number=1845864013783060468573616
currency=USD
amount=100.00
locale=en
payment_token=CF2194C8A0F545CDE053AF598E0A20DA
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2022-01-17T10:46:39Z
signed_field_names=reference_number,transaction_type,currency,amount,locale,access
_key,profile_id,transaction_uuid,signed_date_time,signed_field_names,etc...
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=X4-782X9-X96 // Replace X with 3
date_of_birth=19901001
echeck_account_type=c
company_tax_id=12x456789 // Replace X with 3
echeck_sec_code=WEB
echeck_account_number=4528941xx // Replace x with 0
echeck_routing_number=6723x2882 // Replace x with 0
```

```
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
reference_number=1845864013783060468573616
currency=USD
amount=100.00
locale=en
payment_token=CF2194C8A0F545CDE053AF598E0A20DA
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2022-01-17T10:46:39Z
signed_field_names=reference_number,transaction_type,currency,amount,locale,paymen
t_method,access_key,profile_id,transaction_uuid,signed_date_time,signed_field_name
s,unsigned_field_names,etc...
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=X4-782X9-X96 // Replace X with 3
date_of_birth=19901001
echeck_account_type=c
company_tax_id=12x456789 // Replace X with 3
echeck_sec_code=WEB
echeck_account_number=4528941xx //Replace x with 0
echeck_routing_number=6723x2882 //Replace x with 0
```

Response

```
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=2022-07-11T15:11:41Z
req_currency=USD
req_reference_number=1730560013735542024294683
req_echeck_routing_number=xxxxx2882
transaction_id=3735553783662130706689
req_amount=100.00
req_profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_company_tax_id=12x456789 // Replace X with 3
req_transaction_uuid=38f2efe650ea699597d325ecd7432b1c
payment_token=CF2194C8A0F545CDE053AF598E0A20DA
req_bill_to_surname=Soap
req_bill_to_forename=Joe
req_bill_to_email=joesoap@yahoo.com
req_access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p1
```

Decision Manager

Important: Contact 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.

These are the optional Decision Manager fields:

- **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 the platform overrides the merchant-generated device fingerprint ID.
- **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 Request Fields (on page 80). For detailed descriptions of all Decision Manager response fields, see the *Decision Manager Using the SCMP API Developer Guide* in the Business Center.

Test and View Transactions

> **Important:** 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.

To test China UnionPay cards, use the card number BIN01037 65273, in which BIN is 620009.

Testing Transactions

1. Log in to the Business Center test environment: https://businesscentertest.cybersource.com
2. Go to the Bank of America testing environment:
   - `https://sandbox.sbob.merchant-services.bankofamerica.com`
   - `https://sandbox.cashpro.merchant-services.bankofamerica.com`
   - `https://sandbox.associate.merchant-services.bankofamerica.com`

   `https://businesscentertest.cybersource.com/ebc2` `https://businesscentertest.visaacceptance.com/ebc2` `https://admin.smartpayfuse-test.barclaycard/ebc` `https://gateway-portal-test.nab.com.au/ebc2`
3. Create a Secure Acceptance profile. See Creating a Secure Acceptance Profile (on page 18).
4. Integrate with Secure Acceptance. See Scripting Language Samples (on page 46).

   > **Important:** Include the test transactions endpoint in your HTML form. See Sample Transaction Process Using JSP (on page 46).

5. You can use test payment card numbers for transactions. See Testing Credit Card Services for test payment card numbers. Remove spaces when sending the request to Cybersource.

Viewing Transactions in the Business CenterYour Merchant Services Account

Use the transaction request ID to search for transactions received from your customer's browser and see full transaction details, including the transaction response that was provided to your customer's browser. This is helpful for troubleshooting issues.

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

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

Hosted Checkout IntegrationCheckout API Fields

Data Type Definitions

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

Data Type Definitions

Data Type	Permitted Characters and Formats
Alpha	Any letter from any language
AlphaNumeric	Alpha with any numeric character in any script
AlphaNumericPunctuation	Alphanumeric including ! "#$%&'()*+,-./:;=?@^_~
Amount	012x456789 // Replace X with 3 including a decimal point (.)
ASCIIAlphaNumericPunctuation	Any ASCII alphanumeric character including !&'()+,-./:@
Date (a)	MM-yyyy
Date (b)	yyyyMMDD
Date (c)	yyyy-MM-DD hh:mm z yyyy-MM-DD hh:mm a z yyyy-MM-DD hh:mma z
Email	Valid email address.
Enumerated String	Comma-separated alphanumeric string

Data Type Definitions (continued)

Data Type	Permitted Characters and Formats
IP	Valid IP address
ISO 8601 Date	yyyy-MM-DDThh:mm:ssZ
Locale	[a-z] including a hyphen (-)
Numeric	012x456789 // Replace X with 3
Phone	( ),+-.*#xX12x456789 // Replace X with 30
URL	Valid URL (http or https)

Request Fields

Important: To prevent data tampering, sign all request fields except for fields that contain data the customer is entering.

Important:

When signing fields in the request, create a comma-separated list of the fields. The sequence of the fields in the string is critical to the signature generation process. For example:

```
bill_to_forename=john
bill_to_surname=doe
bill_to_email=jdoe@example.com
signed_field_names=bill_to_forename,bill_to_email,bill_to_surname
```

When generating the security signature, create a comma-separated name=value string of the POST fields that are included in the **signed_field_names** field. The sequence of the fields in the string is critical to the signature generation process. For example:

- `bill_to_forename=john`
- `bill_to_surname=doe`
- `bill_to_email=jdoe@example.com`

The string to sign is
`bill_to_forename=john,bill_to_email=jdoe@example.com,bill_to_surname=doe`

For information on the signature generation process, see the security script of the sample code for the scripting language you are using. See Scripting Language Samples (on page 46).

The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Visa Platform Connect 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.

Request Fields

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
access_key	Required for authentication with Secure Acceptance. See Security Keys (on page 25). **Important:** To prevent data tampering, sign this field.	Required by the Secure Acceptance application.	Alphanumeric String (32)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
aggregator_id	Value that identifies you as a payment aggregator. Get this value from your processor. **Visa Platform Connect**—The value for this field corresponds to this data in the TC 33 capture file: • Record: CP01 TCR6 • Position: 95-105 • Field: Mastercard Payment Facilitator ID **FDC Compass**—This value must consist of uppercase characters. **Field Length** American Express Direct: 20 Visa Platform Connect: 11 FDC Compass: 20 FDC Nashville Global: 15 **Required/Optional** American Express Direct: R for all aggregator transactions. Visa Platform Connect: 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)

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: • `true`: Customer can update details. • `false`: 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. **Important:** To prevent data tampering, sign this field.	• 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)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
auth_indicator	Flag that specifies the purpose of the authorization. Possible values: • `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 customer support.	authorization (See description)	String (1)
auth_type	Authorization type. Possible values: • `AUTOCAPTURE`: Automatic capture. • `STANDARDCAPTURE`: Standard capture. • `verbal`: Forced capture. ***Asia, Middle East, and Africa Gateway; Cielo; Comercio Latino; and Cybersource Latin American Processing*** Set this field to `AUTOCAPTURE` 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 `STANDARDCAPTURE` and include it in a standard authorization or bundled request to indicate that you are overriding an automatic capture.	• authorization (See description.) • capture (Required for a verbal authorization; otherwise, not used.)	Cielo, Comercio Latino, and Cybersource Latin American Processing: String (15) All other processors: String (11)

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: • `true`: Bill payment or loan payment. • `false` (default): Not a bill payment or loan payment.	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 Configuring Billing Information Fields (on page).	• create_payment_token (R) • authorization or sale (R) • authorization,create_payment_token (R) • sale,create_payment_token (R) • update_payment_token (O)	AlphaNumericPunctuation Atos: String (32) All other processors: String (50)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
bill_to_address_country	Country code for the billing address. Use the two-character ISO country codes. 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 Configuring Billing Information Fields (on page).	• 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 Configuring Billing Information Fields (on page).	• create_payment_token (R) • authorization or sale (R) • authorization,create_payment_token (R) • sale,create_payment_token (R) • update_payment_token (O)	AlphaNumericPunctuation Atos: String (29) Visa Platform Connect: String (40) Moneris: String (50) Worldpay VAP: String (35) All other processors: String (60)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
bill_to_address_line2	Second line of 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 Configuring Billing Information Fields (on page).	Optional	AlphaNumericPunctuation Atos: String (29) Visa Platform Connect: String (40) Moneris: String (50) Worldpay VAP: String (35) All other processors: String (60)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
bill_to_address_postal_code	Postal code for the billing 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**: A1B2C3 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 Configuring Billing Information Fields (on page).	See description.	AlphaNumericPunctuation See description.

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
bill_to_address_state	State or province in the billing address. For the U.S. and Canada, use the standard state, province, and territory codes. This field is required if **bill_to_address_country** is U.S. or Canada. 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 Configuring Billing Information Fields (on page).	See description.	AlphaNumericPunctuation String (30)
bill_to_company_name	Name of the customer's company. 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 Configuring Billing Information Fields (on page).	Optional	AlphaNumericPunctuation String (40)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
bill_to_email	Customer email address, including the full domain name. 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 Configuring Billing Information Fields (on page).	• create_payment_token (R) • authorization or sale (R) • authorization,create_payment_token (R) • sale,create_payment_token (R) • update_payment_token (O)	Email String (255)
bill_to_forename	Customer first name. This name must be the same as the name on the card. 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 Configuring Billing Information Fields (on page).	• create_payment_token (R) • authorization or sale (R) • authorization,create_payment_token (R) • sale,create_payment_token (R) • update_payment_token (O)	AlphaNumericPunctuation String (60)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
bill_to_phone	Customer phone number. Cybersource recommends that you include the country code if the order is from outside the U.S. 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 Configuring Billing Information Fields (on page). This field is optional for card payments. For ACH payments this field is required if your processor is Cybersource ACH Service or TeleCheck.	See description.	Phone String (6 to 15) String (10) if using TeleCheck for ACH payments.
bill_to_surname	Customer last name. This name must be the same as the name on the card. 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 Configuring Billing Information Fields (on page).	• create_payment_token (R) • authorization or sale (R) • authorization,create_payment_token (R) • sale,create_payment_token (R) • update_payment_token (O)	AlphaNumericPunctuation String (60)
card_account_type	Flag that specifies the type of account associated with the card. The cardholder provides this information during the payment process. ***Cielo and Comercio Latino*** Possible values:	authorization (O)	String (2)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
	• `CR`: Credit card • `DB`: Debit card ***Visa Platform Connect*** Possible values: • `CH`: Checking account • `CR`: Credit card account • `SA`: Savings account This field is required for: • Debit transactions on Cielo and Comercio Latino. • Transactions with Brazilian-issued cards on Visa Platform Connect. Combo cards in Brazil contain credit and debit functionality in a single card. Visa systems use a credit 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. It is strongly recommended that you include this field for combo card transactions.		

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
card_cvn	Card verification number. For American Express card types, the CVN must be 4 digits. This field can be configured as required or optional. See Payment Method Configuration (on page 19).	See description.	Numeric String (4)
card_expiry_date	Card expiration date. Format: MM-yyyy	• create_payment_token (R) • authorization or sale (R) • authorization,create_payment_token (R) • sale,create_payment_token (R) • update_payment_token (O)	Date (a) String (7)
card_number	Card number. Use only numeric values. Be sure to include valid and well-formed data for this field.	• create_payment_token (R) • authorization or sale (R) • authorization,create_payment_token (R) • sale,create_payment_token (R) • update_payment_token (O)	Numeric String (20)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
card_type	Type of card to authorize. Possible values: • `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 • `062`: China UnionPay	• create_payment_token (R) • authorization or sale (R) • authorization,create_payment_token (R) • sale,create_payment_token (R) • update_payment_token (O)	Enumerated String (3)

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: • `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`.	authorization (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 Configuring ACH Information Fields (on page).	• sale (See description) • create_payment_token (See description) • sale,create_payment_token (See description) • update_payment_token (See description)	AlphaNumericPunctuation String (9)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
complete_route	Concatenation of individual travel legs in the format for example: SFO-JFK:JFK-LHR:LHR-CDG. For a complete list of airport codes, see IATA's City Code Directory. In your request, send either the complete route or the individual legs (**journey_leg#_orig** and **journey_leg#_dest**). If you send all the fields, the value of **complete_route** takes precedence over that of the **journey_leg#** fields.	Optional See Decision Manager (on page 75). For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	AlphaNumericPunctuation String (255)
conditions_accepted	Indicates whether the customer accepted the service fee amount. Possible values: • `false`: Customer did not accept. • `true`: Customer did accept.	Required when service fee is enabled for the profile. See Service Fees (on page 39).	Enumerated String (5)
consumer_id	Identifier for the customer's account. This field is defined when you create a subscription.	• create_payment_token (O) • authorization,create_payment_token (O) • sale,create_payment_token (O) • update_payment_token (O)	AlphaNumericPunctuation String (100)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
credential_stored_on_file	Indicates whether to associate the new network transaction ID with the payment token for future merchant-initiated transactions (MITs). Set this field to `true` when you use a payment token for a cardholder-initiated transaction (CIT) and you plan to set up a new schedule of MITs using an existing payment token. This will ensure that the new network transaction ID is associated with the token. Possible values: • `true` • `false` **Important:** In Europe, enable Payer Authentication on Secure Acceptance and set the **payer_authentication_challenge_code** field to `04` on the initial cardholder-initiated transaction (CIT) to ensure compliance with Strong Customer Authentication (SCA) rules.	Optional	String (5)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
cryptocurrency_purchase	Flag that specifies whether the payment is for the purchase of cryptocurrency. This field is supported only for Visa transactions on Visa Platform Connect. Possible values: • `true`: Payment is for the purchase of cryptocurrency. • `false` (default): Payment is not for the purchase of cryptocurrency.	Optional	String (5)
currency	Currency used for the order. For the possible values, see the ISO currency codes. **Important:** To prevent data tampering, sign this field.	• 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_browser_color_depth	Indicates the bit depth of the color palette for displaying images, in bits per pixel. Secure Acceptance automatically populates this field, but you can override it. For more information, see https://en.wikipedia.org/wiki/Color_depth.	Optional	String (2)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
customer_ browser_java_ enabled	Indicates the ability of the cardholder browser to execute Java. The value is returned from the **navigator.javaEnabled** property. Secure Acceptance automatically populates this field, but you can override it. Possible values: • `true` • `false`	Optional	String (5)
customer_ browser_ javascript_ enabled	Indicates the ability of the cardholder browser to execute JavaScript. This value is available from the fingerprint details of the cardholder's browser. Secure Acceptance automatically populates this field, but you can override it. Possible values: • `true` • `false`	Optional	String (5)
customer_ browser_ language	Indicates the browser language as defined in IETF BCP47. Secure Acceptance automatically populates this field, but you can override it. For more information, see https://en.wikipedia.org/wiki/IETF_language_tag.	Optional	String (8)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
customer_browser_screen_height	Total height of the customer's screen in pixels. Secure Acceptance automatically populates this field, but you can override it. **Example**: 864	Optional	String (6)
customer_browser_screen_width	Total width of the customer's screen in pixels. Secure Acceptance automatically populates this field, but you can override it.	Optional	String (6)
customer_browser_time_difference	Difference between UTC time and the cardholder browser local time, in minutes. Secure Acceptance automatically populates this field, but you can override it.	Optional	String (5)
customer_cookies_accepted	Indicates whether the customer's browser accepts cookies. Possible values: • `true`: Customer browser accepts cookies. • `false`: Customer browser does not accept cookies.	Optional See Decision Manager (on page 75). For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	Enumerated String (5)
customer_gift_wrap	Indicates whether the customer requested gift wrapping for this purchase. Possible values: • `true`: Customer requested gift wrapping. • `false`: Customer did not request gift wrapping.	Optional See Decision Manager (on page 75). For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	Enumerated String (5)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
customer_ip_address	Customer's IP address reported by your web server using socket information.	Optional See Decision Manager (on page 75). For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	IP IPv4: String (15) IPv6: String (39)
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 Configuring ACH Information Fields (on page).	Optional	Date (b) String (8)
debt_indicator	Flag that indicates a payment for an existing contractual loan under the VISA Debt Repayment program. Contact your processor for details and requirements. Possible formats: • `false` (default): Not a loan payment. • `true`: Loan payment.	Optional	Enumerated String (5)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
departure_time	Departure date and time of the first leg of the trip. Use one of these formats: • yyyy-MM-DD HH:mm z • yyyy-MM-DD hh:mm a z • yyyy-MM-DD hh:mma z • HH = 24-hour format • hh = 12-hour format • a = am or pm (case insensitive) • z = time zone of the departing flight. **Examples** • 2023-01-20 23:30 GMT • 2023-01-20 11:30 PM GMT • 2023-01-20 11:30pm GMT	Optional See Decision Manager (on page 75). For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	Date (c) DateTime (29)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
device_ fingerprint_id	Field that contains the session ID for the fingerprint. The string can contain uppercase and lowercase letters, digits, and these special characters: hyphen (-) and underscore (_) However, do not use the same uppercase and lowercase letters to indicate different session IDs. The session ID must be unique for each merchant ID. You can use any string that you are already generating, such as an order number or web session ID. **Important:** The Cybersource-generated device fingerprint ID overrides the merchant-generated device fingerprint ID.	Optional See Decision Manager (on page 75). For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	AlphaNumericPunctuation String (88)
driver_license_ number	Driver's license number of the customer. 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. 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 Configuring ACH Information Fields (on page).	• sale (See description) • create_payment_token (See description) • sale,create_payment_token (See description) • update_payment_token (See description)	AlphaNumeric String (30)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
driver_license_state	State or province where the customer's driver's license was issued. For the U.S. and Canada, use the standard state, province, and territory codes. 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 Configuring ACH Information Fields (on page).	• sale (See description) • create_payment_token (See description) • sale,create_payment_token (See description) • update_payment_token (See description)	Alpha String (2)
e_commerce_indicator	Commerce indicator for the transaction type. Value: `install` This field is required only for installment payments on Cybersource Latin American Processing.	authorization (See description)	String (20)
echeck_account_number	Account number. 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 Configuring ACH Information Fields (on page).	• sale (R) • create_payment_token (R) • sale,create_payment_token (R) • update_payment_token (O)	Numeric Non-negative integer (8 to 17)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
echeck_account_type	Account type. Possible values: • `C`: Checking • `S`: Savings (USD only) • `X`: Corporate checking (USD only) • `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 Configuring ACH Information Fields (on page).	• sale (R) • create_payment_token (R) • sale,create_payment_token (R) • update_payment_token (O)	Enumerated String (1)
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 Configuring ACH Information Fields (on page).	• sale (See description) • create_payment_token (See description) • sale,create_payment_token (See description) • update_payment_token (See description)	Numeric Integer (8)
echeck_effective_date	Effective date for the transaction. This date must be within 45 days of the current date. Format: MMDDyyyy	• sale (O) • sale,create_payment_token (O)	Date (b) String (8)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
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 Configuring ACH Information Fields (on page).	• sale (R) • create_payment_token (R) • sale,create_payment_token (R) • update_payment_token (O)	Numeric Non-negative integer (See description)
echeck_sec_code	Authorization method used for the transaction. See SEC Codes (on page 209). Bank of America ACH possible values: • `CCD` • `PPD` • `TEL` • `WEB` Chase Paymentech Solutions in Canada, use `WEB` for all ACH transactions. Chase Paymentech Solutions in the U.S. possible values:	• sale (O) • create_payment_token (O) • sale,create_payment_token (O) • update_payment_token (O)	Enumerated String (3)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
	• `CCD` • `PPD` • `TEL` • `WEB` TeleCheck possible values: • `PPD` • `TEL` • `WEB` Wells Fargo ACH possible values: • `CCD` • `PPD` • `TEL` • `WEB`		
health_care_#_amount	Amount of the healthcare payment. # can range from `0` to `4`. Send this field with a corresponding **health_care_#_amount_type** field.	authorization (O)	String (13)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
health_care_#_amount_type	Type of healthcare payment. # can range from `0` to `4`. Mastercard possible values: • `eligible-total`: total amount of healthcare. • `prescription` Visa possible values: • `clinic` • `dental` • `healthcare`: total amount of healthcare. • `healthcare-transit` • `prescription` • `vision` Send this field with a corresponding **health_care_#_amount** field.	authorization (O)	String (35)
ignore_avs	Ignore the results of AVS verification. Possible values: • `true` • `false` **Important:** To prevent data tampering, sign this field.	Optional	Enumerated String (5)

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: • `true` • `false` **Important:** To prevent data tampering, sign this field.	Optional	Enumerated String (5)
industry_datatype	Indicates whether the transaction includes industry data. For certain industries, you must set this field to an industry data value to be sent to the processor. When this field is not set to an industry value or is not included in the request, industry data does not go to the processor. Possible values: • `healthcare_medical` • `healthcare_transit`	authorization (O)	String (20)
installment_amount	Amount for the current installment payment. This field is required only for installment payments on Cybersource Latin American Processing or Visa Platform Connect.	authorization (See description)	Amount (12)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
installment_frequency	Frequency of the installment payments. Possible values: • `B`: Biweekly • `M`: Monthly • `W`: Weekly This field is supported only on Visa Platform Connect.	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: • `1`: Merchant-funded installment plan • `2`: Issuer-funded installment plan If you do not include this field in the request, the value in your account is used. To change this value, contact customer support. **Visa Platform Connect** American Express-defined code that indicates the type of installment plan for this transaction. Contact American Express for: • Information about the types of installment plans that American Express provides. • Values for this field.	authorization (See description)	Cybersource Latin American Processing: String (1) Visa Platform Connect: String (2)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
installment_sequence	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 as **installment_sequence** = 2 and **installment_total_count** = 5. This field is required only for installment payments on Visa Platform Connect.	authorization (See description)	Integer (2)
installment_total_amount	Total amount of the loan that is being paid in installments. This field is required only for installment payments on Cybersource Latin American Processing and Visa Platform Connect.	authorization (see description)	Amount (12)
installment_total_count	Total number of installment payments as part of an authorization. Possible values: `1` to `99` This field is required only for installment payments on Cybersource Latin American Processing and Visa Platform Connect.	authorization (See description)	Numeric String (2)
issuer_additional_data	Data defined by the issuer. See the "Discretionary Data" section in *Credit Card Services Optional Features SCMP API Supplement* or *Credit Card Services Optional Features Simple Order API Supplement*.	authorization (O)	Alphanumeric String (256)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
item_#_code	Type of product. # can range from `0` to `199`.	Optional If you include this field, you must also include the **line_item_count** field.	AlphaNumericPunctuation String (255)
item_#_name	Name of the item. # can range from `0` to `199`. This field is required when the **item_#_code** value is not default nor related to shipping or handling.	See description. If you include this field, you must also include the **line_item_count** field.	AlphaNumericPunctuation String (255)
item_#_passenger_email	Passenger's email address.	Optional See Decision Manager (on page 75). For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	String (255)
item_#_passenger_forename	Passenger's first name.	Optional See Decision Manager (on page 75). For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	String (60)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
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.	Optional See Decision Manager (on page 75). For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	String (32)
item_#_passenger_phone	Passenger's phone number. If the order is from outside the U.S., include the country code.	Optional See Decision Manager (on page 75). For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	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.	Optional See Decision Manager (on page 75). For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	String (32)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
item_#_passenger_surname	Passenger's last name.	Optional See Decision Manager (on page 75). For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	String (60)
item_#_passenger_type	Passenger classification associated with the price of the ticket. Possible values: • `ADT`: Adult • `CNN`: Child • `INF`: Infant • `YTH`: Youth • `STU`: Student • `SCR`: Senior Citizen • `MIL`: Military	Optional See Decision Manager (on page 75). For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	String (32)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
item_#_quantity	Quantity of line items. The default value is `1`. Required field when one of these product codes is used: • adult_content • coupon • electronic_good • electronic_software • gift_certificate • service • subscription # can range from `1` to `199`. This field is required when the **item_#_code** value is not default nor related to shipping or handling.	See description. If you include this field, you must also include the **line_item_count** field.	Numeric String (10)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
item_#_sku	Identification code for the product. Required field when one of these product codes is used: • adult_content • coupon • electronic_good • electronic_software • gift_certificate • service • subscription # can range from `0` to `199`.	See description. If you include this field, you must also include the **line_item_count** field.	AlphaNumericPunctuation String (255)
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.	Optional If you include this field, you must also include the **line_item_count** field.	Amount String (15)
item_#_unit_price	Price of the line item. # can range from `0` to `199`. This value cannot be negative. **Important:** You must include either this field or the amount field in the request.	See description. If you include this field, you must also include the **line_item_count** field.	Amount String (15)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
journey_leg#_dest	Airport code for the destination leg of the trip, designated by the pound (#) symbol in the field name. A maximum of 30 legs can be included in the request. This code is usually three digits long, for example: SFO = San Francisco. Do not use the colon (:) or the hyphen (-). For a complete list of airport codes, see IATA's City Code Directory. In your request, send either the **complete_route** field or the individual legs (**journey_leg#_orig** and **journey_leg#_dest**). If you send all the fields, the complete route takes precedence over the individual legs.	Optional See Decision Manager (on page 75). For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	Alpha String (3)
journey_leg#_orig	Airport code for the origin leg of the trip, designated by the pound (#) symbol in the field name. A maximum of 30 legs can be included in the request. This code is usually three digits long, for example: SFO = San Francisco. Do not use the colon (:) or the hyphen (-). For a complete list of airport codes, see IATA's City Code Directory. In your request, send either the **complete_route** field or the individual legs (**journey_leg#_orig** and **journey_leg#_dest**). If you send all the fields, the complete route takes precedence over the individual legs.	Optional See Decision Manager (on page 75). For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	Alpha String (3)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
journey_type	Type of travel, such as one way or round trip.	Optional See Decision Manager (on page 75). For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	AlphaNumericPunctuation String (32)
jpo_installments	Total number of Japanese installment payments. Possible values: • `2` • `3` • `5` • `6` • `10` • `12` • `15` • `18` • `20` • `24`	Required when the jpo_payment_method value is `4` and the currency type is `JPY`.	Numeric String (2)
jpo_payment_method	Japanese payment method. Possible values:	Required when the currency type is `JPY`.	Numeric String (1)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
	• `1`: Single payment • `2`: Bonus payment • `4`: Installment payment • `5`: Revolving repayment		
line_item_count	Total number of line items. Maximum number is 200.	This field is required when you include any item fields in the request.	Numeric String (2)
locale	Indicates the language to use for customer-facing content. Possible value: `en-us`. See "Activating a Profile" (on page 31). **Important:** To prevent data tampering, sign this field.	Required by the Secure Acceptance application.	Locale String (5)
merchant_defined_data#	Optional fields that you can use to store information (see Configuring Customer Notifications (on page 29)). # can range from `1` to `100`. Merchant-defined data fields `1` to `4` are associated with the payment token and are used for subsequent token based transactions. Merchant defined data fields `5` to `100` are passed trough to Decision ManagerFraud Management Essentials as part of the initial payment request and are not associated with the payment token.	Optional See Decision Manager (on page 75). For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	AlphaNumericPunctuation String (100)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
	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). If it is discovered that a merchant is capturing and/or transmitting personally identifying information via the merchant-defined data fields, whether or not intentionally, the merchant's account WILL immediately be suspended, which will result in a rejection of any and all transaction		

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
	requests submitted by the merchant after the point of suspension.		
merchant_ descriptor merchant_ descriptor_ alternate merchant_ descriptor_city merchant_ descriptor_ contact merchant_ descriptor_ country merchant_ descriptor_post al_ code merchant_ descriptor_state merchant_ descriptor_street	For the descriptions, used-by information, data types, and lengths for these fields, see the Merchant Descriptors Developer Guides.	authorization (See description)	

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
merchant_ descriptor	Your business name. This name appears on the cardholder's statement. When you include more than one consecutive space, extra spaces are removed. **Important:** This value must consist of English characters.	authorization (O)	String (23)
merchant_ descriptor_ alternate	Alternate contact information for your business, such as an email address or URL. This value might appear on the cardholder's statement. When you do not include this value in your request, the merchant URL in your account is sent. **Important:** This value must consist of English characters.	authorization (O)	String (13)
merchant_ descriptor_city	City for your business location. This value might appear on the cardholder's statement. When you do not include this value in your request, the merchant city in your account is sent. **Important:** This value must consist of English characters.	authorization (O)	String (13)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
merchant_ descriptor_ contact	Telephone number for your business. This value might appear on the cardholder's statement. When you include more than one consecutive space, extra spaces are removed. When you do not include this value in your request, the merchant phone number in your account is sent. **Important:** This value must consist of English characters.	authorization (O)	String (14)
merchant_ descriptor_ country	Country code for your business location. Use the standard ISO Standard Country Codes. This value might appear on the cardholder's statement. When you do not include this value in your request, the merchant country in your account is sent. **Important:** This value must consist of English characters.	authorization (O)	String (2)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
merchant_ descriptor_post al_ code	Postal code for your business location. This value might appear on the cardholder's statement. If your business is domiciled in the U.S., you can use a 5-digit or 9-digit postal code. A 9-digit postal code must follow this format: [5 digits][dash][4 digits] **Example**: 12345-6789 If your business is domiciled in Canada, you can use a 6-digit or 9-digit postal code. A 6-digit postal code must follow this format: [alpha][numeric][alpha][space] [numeric][alpha][numeric] **Example**: A1B 2C3 When you do not include this value in your request, the merchant postal code in your account is sent. **Important:** This value must consist of English characters. **Important:** Mastercard requires a postal code for any country that uses postal codes. You can provide the postal code in your account or you can include this field in your request.	authorization (O)	String (14)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
merchant_descriptor_state	State code or region code for your business location. This value might appear on the cardholder's statement. For the U.S. and Canada, use the standard state, province, and territory codes. When you do not include this value in your request, the merchant state in your account is sent. **Important:** This value must consist of English characters.	authorization (O)	String (3)
merchant_descriptor_street	Street address for your business location. This value might appear on the cardholder's statement. When you do not include this value in your request, the merchant street in your account is sent. **Important:** This value must consist of English characters.	authorization (O)	String (60)
merchant_secure_data1 merchant_secure_data2 merchant_secure_data3	Optional fields that you can use to store information. The data is encrypted before it is stored in the payment repository.	Optional	AlphaNumericPunctuation String (100)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
merchant_secure_data4	Optional field that you can use to store information. The data is encrypted before it is stored in the payment repository.	Optional	AlphaNumericPunctuation String (2000)
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.	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.	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.	Optional	URL String (255)
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`.	Optional	Integer (5)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
override_paypal_order_setup	Overrides the PayPal order setup profile setting. Possible values: • `include_authorization`: The PayPal order is created and authorized. • `exclude_authorization`: The PayPal order is created but not authorized.	Optional See Enabling PayPal Express Checkout (on page 24).	String (21)
payer_authentication_acquirer_country	Send this to tell issuers that the acquirer's country differs from the merchant country, and the acquirer is in the European Economic Area (EEA) and UK and Gibraltar.	Optional	String (2)
payer_authentication_acs_window_size	Sets the challenge window size that displays to the cardholder. The Access Control Server (ACS) replies with content that is formatted appropriately for this window size. The sizes are width x height in pixels. Secure Acceptance calculates this value based on the size of the window in which Secure Acceptance is displayed, but you can override it. Possible values: • `01`: 250 x 400 • `02`: 390 x 400 • `03`: 500 x 600 • `04`: 600 x 400 • `05`: Full page	Optional	Integer (2)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
payer_ authentication_ challenge_code	Possible values: • `01`: No preference • `02`: No challenge request • `03`: Challenge requested (3-D Secure requestor preference) • `04`: Challenge requested (mandate) • `05`: No challenge requested (transactional risk analysis is already performed) • `06`: No challenge requested (data share only) • `07`: No challenge requested (strong consumer authentication is already performed) • `08`: No challenge requested (use whitelist exemption if no challenge required) • `09`: Challenge requested (whitelist prompt requested if challenge required) This field will default to `01` on merchant configuration and can be overridden by the merchant. EMV 3-D Secure 2.1.0 supports values `01`-`04`. Version 2.2.0 supports values `01`-`09`.	Optional	Integer (2)
payer_ authentication_ customer_annual_ transaction_ count	Number of transactions (successful and abandoned) for this cardholder account within the past year.	Optional	Integer (3)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
payer_ authentication_ customer_daily_ transaction_ count	Number of transaction (successful or abandoned) for this cardholder account within the past 24 hours.	Optional	Integer (3)
payer_ authentication_ indicator	Indicates the type of authentication request. Secure Acceptance automatically populates this field, but you can override it. Possible values: • `01`: Payment transaction • `02`: Recurring transaction • `03`: Installment transaction • `04`: Add card • `05`: Maintain card • `06`: Cardholder verification as part of EMV token identity and verification (ID&V)	Optional	Integer (2)
payer_ authentication_ marketing_source	Indicates origin of the marketing offer.	Optional	String (40)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
payer_ authentication_ merchant_fraud_ rate	Calculated by merchants according to Payment Service Directive 2 (PSD2) and Regulatory Technical Standards (RTS). European Economic Area (EEA) and UK and Gibraltar card fraud divided by all EEA and UK and Gibraltar card volumes. Possible values: • 1: Represents fraud rate ≤1 • 2: Represents fraud rate >1 and ≤6 • 3: Represents fraud rate >6 and ≤13 • 4: Represents fraud rate >13 and ≤25 • 5: Represents fraud rate >25	Optional	Integer (2)
payer_ authentication_ merchant_name	Your company's name as you want it to appear to the customer in the issuing bank's authentication form. This value overrides the value specified by your merchant bank.	Optional	String (25)
payer_ authentication_ merchant_score	Risk score provided by merchants. Used for Cartes Bancaires transactions.	Optional	String (20)
payer_ authentication_ message_category	Identifies the category of the message for a specific use case 3-D Secure Server. Possible values:	Optional	String (2)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
	• `01`: PA (payment authentication). • `02`: NPA (non-payment authentication). • `03-71`: Reserved for EMVCo future use (values invalid until defined by EMVCo). • `80-99`: Reserved for directory server use.		
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.	Optional	Integer (25)
payer_ authentication_ new_customer	Indicates whether the customer is a new or existing customer with the merchant. Possible values: • `true` • `false`	Optional	String (5)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
payer_ authentication_ pre_order	Indicates whether cardholder is placing an order with a future availability or release date. Possible values: • `01`: Merchandise available • `02`: Future availability	Optional	Integer (2)
payer_ authentication_ pre_order_date	Expected date that a pre-ordered purchase will be available. Format: yyyyMMDD	Optional	Integer (8)
payer_ authentication_ prior_ authentication_ data	Data that the ACS can use to verify the authentication process.	Optional	String (2048)
payer_ authentication_ prior_ authentication_ method	Method that the cardholder used previously to authenticate to the 3-D Secure requester. Possible values: • `01`: Frictionless authentication through the ACS • `02`: Cardholder challenge through the ACS • `03`: AVS verified • `04`: Other issuer methods • `05-79`: Reserved for EMVCo future use (values invalid until defined by EMVCo) • `80-99`: Reserved for directory server use	Optional	Integer (2)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
payer_authentication_prior_authentication_reference_id	This field contains the ACS transaction ID for an authenticated transaction. For example, the first recurring transaction that was authenticated with the cardholder.	Optional	String (36)
payer_authentication_prior_authentication_time	Date and time in UTC of the previous cardholder authentication. Format: yyyyMMDDhhmm	Optional	Integer (12)
payer_authentication_product_code	Specifies the product code, which designates the type of transaction. Possible values: • `AIR`: Airline purchase **Important:** Required for American Express SafeKey (U.S.). • `ACC`: Accommodation Rental • `ACF`: Account funding • `CHA`: Check acceptance • `DIG`: Digital Goods • `DSP`: Cash Dispensing • `GAS`: Fuel • `GEN`: General Retail • `LUX`: Luxury Retail • `PAL`: Prepaid activation and load • `PHY`: Goods or services purchase	Optional	String (3)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
	• `QCT`: Quasi-cash transaction • `REN`: Car Rental • `RES`: Restaurant • `SVC`: Services • `TBD`: Other • `TRA`: Travel **Important:** Required for Visa Secure transactions in Brazil. Do not use this request field for any other types of transactions.		
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.	Optional	Integer (8)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
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.	Optional	Integer (3)
payer_ authentication_ reorder	Indicates whether the cardholder is reordering previously purchased merchandise. Possible values: • `01`: First time ordered • `02`: Reordered	Optional	Integer (2)
payer_ authentication_ secure_corporate_ payment	Indicates that dedicated payment processes and procedures were used. Potential secure corporate payment exemption applies. Possible values: • `0` • `1`	Optional	String (1)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
payer_ authentication_ ship_to_address_ first_used	Date on which this shipping address was first used. Possible values: • `-1`: Guest account • `0`: First used during this transaction If neither value applies, enter the date in yyyyMMDD format.	Optional	Integer (8)
payer_ authentication_ transaction_ mode	Transaction mode identifier. Identifies the channel from which the transaction originates. Possible values: • `M`: MOTO (Mail Order Telephone Order) • `R`: Retail • `S`: E-commerce • `P`: Mobile Device • `T`: Tablet	Required by the Secure Acceptance application.	String (1)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
payer_ authentication_ whitelisted	Enables the communication of trusted beneficiary and whitelist status among the ACS, the directory server, and the 3-D Secure requester. Possible values: • `true`: 3-D Secure requester is whitelisted by cardholder • `false`: 3-D Secure requester is not whitelisted by cardholder	Optional	String (5)
payment_method	Method of payment. Possible values: • `card` • `echeck` • `paypal` • `visacheckout`	OptionalRequired by the Secure Acceptance application.	Enumerated String (30)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
payment_token	Identifier for the payment details. The payment token retrieves the card data, billing information, and shipping information from the payment repository. When this field is included in the request, the card data and billing and shipping information are optional. You must be using Token Management Services. Populate this field with the customer token. This field is required for token-based transactions. Identifier for the TMS customer token or the instrument identifier token. Populates the request with the information associated with the token.	• authorization or sale (R) • authorization,update_payment_token (R) • sale,update_payment_token (R) • update_payment_token (R)	Numeric String (32)
payment_token_comments	Optional comments you can add for the customer token.	Optional	AlphaNumericPunctuation String (255)
payment_token_title	Name or title for the customer token.	Optional	AlphaNumericPunctuation String (60)
profile_id	Identifies the profile to use with each transaction.	Assigned by the Secure Acceptance application.	ASCIIAlphaNumericPunctuation String (36)
promotion_code	Promotion code for a transaction.	Optional	String (100)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
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)	Numeric String (10)
recipient_ date_of_birth	Recipient's date of birth. Format: yyyyMMDD.	authorization (R for recipient transactions, otherwise not used)	Date (b) String (8)
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.	authorization (R for recipient transactions, otherwise not used)	Alphanume ric String (6)
recipient_ surname	Recipient's last name.	authorization (R for recipient transactions, otherwise not used)	Alpha String (6)
recurring_amount	Payment amount for each installment or recurring subscription payment.	• create_payment_t oken (R) • authorization,cre ate_payment_to ken (R) • sale,create_paym ent_token (R) • update_payment_ token (O)	Amount String (15)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
recurring_automatic_renew	Indicates whether to automatically renew the payment schedule for an installment subscription. Possible values: • `true` (default): Automatically renew. • `false`: Do not automatically renew.	• create_payment_token (O) • authorization,create_payment_token (O) • sale,create_payment_token (O) • update_payment_token (O)	Enumerated String (5)
recurring_frequency	Frequency of payments for an installment or recurring subscription. Possible values: • `weekly`: Every 7 days. • `bi-weekly`: Every 2 weeks. • `quad-weekly`: Every 4 weeks. • `monthly` • `semi-monthly`: Twice every month (1st and 15th). • `quarterly` • `semi-annually`: Twice every year. • `annually`	• create_payment_token (R) • authorization,create_payment_token (R) • sale,create_payment_token (R) • update_payment_token (O)	Enumerated String (20)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
recurring_number_of_installments	Total number of payments set up for an installment subscription. Maximum values: • `261`: Weekly • `130`: Bi-weekly • `65`: Quad-weekly • `60`: Monthly • `120`: Semi-monthly • `20`: Quarterly • `10`: Semi-annually • `5`: Annually	• create_payment_token (R) • authorization,create_payment_token (R) • sale,create_payment_token (R) • update_payment_token (O)	Numeric String (3)
recurring_start_date	First payment date for an installment or recurring subscription payment. Date must use the format yyyyMMDD. If a date in the past is supplied, the start date defaults to the day after the date was entered.	• create_payment_token (O) • authorization,create_payment_token (O) • sale,create_payment_token (O) • update_payment_token (O)	Date (b) String (8)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
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.	AlphaNumericPunctuation 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 these values: • `true` • `false`	Optional See Decision Manager (on page 75). For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	Enumerated String (5)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
sales_ organization_id	Company ID assigned to an independent sales organization. Obtain this value from Mastercard. Visa Platform Connect The value for this field corresponds to this data in the TC 33 capture file: Record: CP01 TCR6 Position: 106-116 Field: Mastercard Independent Sales Organization ID	authorization (Required for Mastercard aggregator transactions on Visa Platform Connect)	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 Configuring Shipping Information Fields (on page).	Optional	AlphaNumer icPunctuat ion String (50)
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 Configuring Shipping Information Fields (on page).	Optional	Alpha String (2)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
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 Configuring Shipping Information Fields (on page).	Optional	AlphaNumericPunctuation 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 Configuring Shipping Information Fields (on page).	Optional	AlphaNumericPunctuation String (60)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
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 Configuring Shipping Information Fields (on page).	Optional	AlphaNumericPunctuation See description.

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
ship_to_address_state	State or province of shipping address. For the U.S. and Canada, use the standard state, province, and territory codes. This field is required if shipping address is U.S. or Canada. 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 Configuring Shipping Information Fields (on page).	Optional	AlphaNumericPunctuation String (2)
ship_to_company_name	Name of the company receiving the product. 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 Configuring Shipping Information Fields (on page).	Optional	AlphaNumericPunctuation String (40)
ship_to_forename	First name of the person receiving the product. 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 Configuring Shipping Information Fields (on page).	Optional	AlphaNumericPunctuation String (60)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
ship_to_phone	Phone number of the 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 Configuring Shipping Information Fields (on page).	Optional	Phone String (6 to 15)
ship_to_surname	Last name of the person receiving the product. This can be entered by your customer during the checkout process, or you can include this in your request to Secure Acceptance. See Configuring Shipping Information Fields (on page).	Optional	AlphaNumericPunctuation String (60)
ship_to_type	Shipping destination. **Example**: Commercial, residential, store	Optional	String (25)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
shipping_method	Shipping method for the product. Possible values: • `sameday`: Courier or same-day service • `oneday`: Next day or overnight service • `twoday`: Two-day service • `threeday`: Three-day service • `lowcost`: Lowest-cost service • `pickup`: Store pickup • `other`: Other shipping method • `none`: No shipping method	Optional	Enumerated String String (10)
signature	Merchant-generated Base64 signature. This is generated using the signing method for the **access_key** field supplied.	Required by the Secure Acceptance application.	AlphaNumericPunctuation

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
signed_date_time	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. Format: yyyy-MM-DDThh:mm:ssZ **Example**: 2020-08-11T22:47:57Z equals August 11, 2020, at 22:47:57 (10:47:57 p.m.). The T separates the date and the time. The Z indicates UTC. Your system time must be accurate to avoid payment processing errors related to the **signed_date_time** field. **Important:** To prevent data tampering, sign this field.	Required by the Secure Acceptance application.	ISO 8601 Date String (20)
signed_field_ names	A comma-separated list of request fields that are signed. This field is used to generate a signature that is used to verify the content of the transaction to protect it from tampering. **Important:** All request fields should be signed to prevent data tampering, with the exception of the **card_number**, **card_cvn**, and **signature** fields.	Required by the Secure Acceptance application.	AlphaNumer icPunctuat ion Variable

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: • `true` (skip the preauthorization check) • `false` (perform the preauthorization check)	Optional	Enumerated String (5)
skip_decision_manager	Indicates whether to skip Decision ManagerFraud Management Essentials. This field can contain one of these values: • `true`: Decision ManagerFraud Management Essentials is not enabled for this transaction, and the device fingerprint ID will not be displayed. • `false`	Optional See Decision Manager (on page 75). For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	Enumerated 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. Visa Platform Connect: 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)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
submerchant_country	Sub-merchant's country. Use the two-character ISO country code. ***FDC Compass*** This value must consist of uppercase characters.	authorization American Express Direct: R for all aggregator transactions. Visa Platform Connect: not used. FDC Compass: O for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	String (3)
submerchant_email	Sub-merchant's email address. Visa Platform Connect With American Express, the value for this field corresponds to this data in the TC 33 capture file: • Record: CP01 TCRB • Position: 25-64 • Field: American Express Seller E-mail Address	authorization American Express Direct: R for all aggregator transactions. Visa Platform Connect: O for all aggregator transactions with American Express; otherwise, not used. FDC Compass: O for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	American Express Direct: String (40) Visa Platform Connect: String (40) FDC Compass: String (40) FDC Nashville Global: String (19)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
submerchant_id	The ID you assigned to your sub-merchant. ***FDC Compass*** This value must consist of uppercase characters. ***Visa Platform Connect*** With American Express, the value for this field corresponds to this data in the TC 33 capture file: • Record: CP01 TCRB • Position: 65-84 • Field: American Express Seller ID With Mastercard, the value for this field corresponds to this data in the TC 33 capture file: • Record: CP01 TCR6 • Position: 117-131 • Field: Sub-Merchant ID	authorization American Express Direct: R for all aggregator transactions. Visa Platform Connect: • O for all American Express aggregator transactions; • R for all Mastercard aggregator authorizations; • otherwise, not used. FDC Compass: R for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	American Express Direct: String (20) Visa Platform Connect with American Express: String (20) Visa Platform Connect with Mastercard: String (15) FDC Compass: String (20) FDC Nashville Global: String (14)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
submerchant_name	Sub-merchant's business name. ***FDC Compass*** This value must consist of uppercase characters.	authorization American Express Direct: R for all aggregator transactions. Visa Platform Connect: not used. FDC Compass: R for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	American Express Direct: String (37) FDC Compass with American Express: String (19) FDC Compass with Mastercard: String (37) FDC Nashville Global: String (12)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
submerchant_phone	Sub-merchant's telephone number. ***Visa Platform Connect*** With American Express, the value for this field corresponds to this data in the TC 33 capture file: • Record: CP01 TCRB • Position: 5-24 • Field: American Express Seller Telephone Number ***FDC Compass*** This value must consist of uppercase characters. Use one of these recommended formats: NNN-NNN-NNNN NNN-AAAAAAA	authorization American Express Direct: R for all aggregator transactions. Visa Platform Connect: O for all aggregator transactions with American Express; otherwise, not used. FDC Compass: R for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	American Express Direct: String (20) Visa Platform Connect: String (20) FDC Compass: String (13) FDC Nashville Global: String (10)
submerchant_postal_code	Partial postal code for the sub-merchant's address. ***FDC Compass*** This value must consist of uppercase characters.	authorization American Express Direct: R for all aggregator transactions. Visa Platform Connect: not used. FDC Compass: O for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	American Express Direct: String (9) FDC Compass: String (15) FDC Nashville Global: String (9)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
submerchant_state	Sub-merchant's state or province. For the U.S. and Canada, use the standard state, province, and territory codes. ***FDC Compass*** This value must consist of uppercase characters.	authorization American Express Direct: R for all aggregator transactions. Visa Platform Connect: not used. FDC Compass: O for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	String (2)
submerchant_street	First line of the sub-merchant's street address. ***FDC Compass*** This value must consist of uppercase characters.	authorization American Express Direct: R for all aggregator transactions. Visa Platform Connect: not used. FDC Compass: O for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	American Express Direct: String (30) FDC Compass: String (38) FDC Nashville Global: String (25)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
tax_amount	Total tax amount to apply to the order. This value cannot be negative. **Important:** To prevent data tampering, sign this field.	Optional	Amount String (15)
transaction_agreement_id	Unique ID generated by the merchant for recurring and unscheduled card-on-file transactions, and shared in subsequent transactions. The merchant generates an agreement ID for each card holder or payment agreement. This field can contain foreign/Arabic characters. This value is forwarded to the Saudi Arabian payment processor.	Required when transaction_reason is provided by Saudi Arabia merchants.	String (140)
transaction_reason	Reason for the transaction. Set this field to one of these values when you create a payment token. Possible values:	• create_payment_token (O) • authorization,create_payment_token (O) • sale,create_payment_token (O)	Enumerated String (26)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
	• `setup_recurring`: Set to this value when you plan to use the payment_token for a fixed amount on a fixed schedule. • `setup_standing_order`: Set to this value when you plan to use the payment_token for a variable amount on a fixed schedule. • `setup_installments`: Set to this value when you plan to use the payment_token for a regular payment with a specified recurring_number_of_installments. • `setup_unscheduled_payments`: Set to this value when you plan to use the payment_token for unscheduled payments (merchant or customer initiated).	• Required when you plan to use a payment token or establish a new agreement for scheduled or unscheduled payments using credentials-on-file in Saudi Arabia.	

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
transaction_type	The type of transaction. Possible values: • `authorization` • `authorization,create_payment_token` • `authorization,update_payment_token` • `sale` • `sale,create_payment_token` • `sale,update_payment_token` • `create_payment_token` • `update_payment_token` Only authorization and sale are supported for Visa Click to Pay transactions. **Important:** To prevent data tampering, sign this field.	Required by the Secure Acceptance application.	Enumerated String (60)
transaction_uuid	Unique merchant-generated identifier. Include with the **access_key** field for each transaction. This identifier must be unique for each transaction. This field is used to check for duplicate transaction attempts. **Important:** To prevent data tampering, sign this field.	Required by the Secure Acceptance application.	ASCIIAlpha NumericPunctuation String (50)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
unsigned_field_names	A comma-separated list of request fields that are not signed.	Required by the Secure Acceptance application.	AlphaNumericPunctuation Variable

Response Fields

Response fields are sent using these notification methods:

- Merchant POST URL. See "Merchant Notifications" (on page 27).
- Merchant POST Email. See "Merchant Notifications" (on page 27).
- POST to the URL specified in the Transaction or Custom Cancel Response page. See "Customer Response Page" (on page 30).

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

To ensure the integrity of the response 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 response fields have not been tampered with, create a signature using the fields listed in the **signed_field_names** response 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" (on page 46).

Important: Because response fields and reason codes can be added at any time, proceed as follows:

- Parse the response data according to the names of the fields instead of their order in the response. For more information on parsing response 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 response fields are sent back to your Merchant POST URL or email. See "Merchant Notifications" (on page 27). Your error handler should use the **decision** field to obtain the transaction result if it receives a reason code that it does not recognize.

The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Visa Platform Connect 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.

Response Fields

Field	Description	Data Type & Length
auth_affluence_indicator	***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. This field is supported for Visa, Mastercard, Discover, and Diners Club. Possible values: • `Y`: Yes • `N`: No • `X`: Does not apply/unknown ***Worldpay VAP*** Flag that indicates that a Visa cardholder or Mastercard cardholder is in one of the affluent categories. Possible values: • `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).	Chase Paymentech Solution: String (1) Worldpay VAP: String (13)
auth_amount	Amount that was authorized.	String (15)
auth_avs_code	AVS result code. See "AVS Codes" (on page 217).	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)

Response Fields (continued)

Field	Description	Data Type & Length
auth_card_commercial	Indicates whether the card is a commercial card, which enables you to include Level II data in your transaction requests. Possible values: • Y: Yes • N: No • X: Does not apply/unknown This field is supported for Visa and Mastercard on Chase Paymentech Solutions.	String (1)
auth_card_healthcare	Indicates whether the card is a healthcare card. Possible values: • Y: Yes • N: No • X: Does not apply/unknown This field is supported for Visa and Mastercard on Chase Paymentech Solutions.	String (1)
auth_card_issuer_country	Country in which the card was issued. This information enables you to determine whether the card was issued domestically or internationally. This field is supported for Visa, Mastercard, Discover, Diners Club, JCB, and Maestro (International) on Chase Paymentech Solutions.	String (3)

Response Fields (continued)

Field	Description	Data Type & Length
auth_card_level_3_eligible	Indicates whether the card is eligible for Level III interchange fees, which enables you to include Level III data in your transaction requests. Possible values: • `Y`: Yes • `N`: No • `X`: Does not apply/unknown This field is supported for Visa and Mastercard on Chase Paymentech Solutions.	String (1)
auth_card_payroll	Indicates whether the card is a payroll card. Possible values: • `Y`: Yes • `N`: No • `X`: Does not apply/unknown This field is supported for Visa, Discover, Diners Club, and JCB on Chase Paymentech Solutions.	String (1)

Response Fields (continued)

Field	Description	Data Type & Length
auth_card_prepaid	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. Possible values: • `Y`: Yes • `N`: No • `X`: Does not apply/unknown This field is supported for Visa, Mastercard, Discover, Diners Club, and JCB on Chase Paymentech Solutions.	String (1)
auth_card_regulated	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. Possible values: • `Y`: Yes (assets greater than $10B) • `N`: No (assets less than $10B) • `X`: Does not apply/unknown This field is supported for Visa, Mastercard, Discover, Diners Club, and JCB on Chase Paymentech Solutions.	String (1)

Response Fields (continued)

Field	Description	Data Type & Length
auth_card_signature_debit	Indicates whether the card is a signature debit card. This information enables you to alter the way an order is processed. Possible values: • Y: Yes • N: No • X: Does not apply/unknown This field is supported for Visa, Mastercard, and Maestro (International) on Chase Paymentech Solutions.	String (1)
auth_cavv_result	Mapped response code for the Visa Secure and American Express SafeKey: • See Visa Secure Response Codes (on page 224). • See American Express SafeKey Response Codes (on page 221).	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" (on page 220).	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_reconciliation_reference_number	Unique number that Cybersource generates to identify the transaction. **Ingenico ePayments**	String (20)

Response Fields (continued)

Field	Description	Data Type & Length
	You can use this value to identify transactions in the Ingenico ePayments Collections Report, which provides settlement information. Contact customer support for information about the report.	
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 transaction reports with your processor reports. For authorization requests, the transaction reference number is returned only for these processors: • American Express Direct • Asia, Middle East, and Africa Gateway • Atos • BML Direct • Chase Paymentech Solutions • Cielo • FDC Compass • FDC Nashville Global • Moneris • Visa Platform Connect • Worldpay VAP	AlphaNumeric (60)

Response Fields (continued)

Field	Description	Data Type & Length
bill_trans_ref_no	Reference number that you use to reconcile your transaction reports with your processor reports. This field is not supported on Visa Platform Connect.	AlphaNumeric (60)
card_type_name	Name of the card type. For security reasons, this field is returned only in the merchant POST URL and email notifications (not in the receipt POST through the browser).	String (50)
decision	The result of your request. Possible values: • `ACCEPT` • `DECLINE` • `REVIEW` • `ERROR` • `CANCEL` See "Types of Notifications" (on page).	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	Exchange rate if a currency conversion occurred. The 17 characters include the decimal point.	Decimal (17)
invalid_fields	Indicates which request fields were invalid.	Variable
message	Response message from the payment gateway.	String (255)

Response Fields (continued)

Field	Description	Data Type & Length
payer_authentication_acs_transaction_id	Unique transaction identifier assigned by the ACS to identify a single transaction.	String (36)
payer_authentication_cavv	Cardholder authentication verification value (CAVV). Transaction identifier generated by the issuing bank or Visa Click to Pay. This field is used by the payer authentication validation service.	String (50)
payer_authentication_challenge_type	The type of 3-D Secure transaction flow that occurred. Possible values: • CH: Challenge • FR: Frictionless • FD: Frictionless with delegation (challenge not generated by the issuer but by the scheme on behalf of the issuer). Used for Cartes Bancaires transactions.	String (2)

Response Fields (continued)

Field	Description	Data Type & Length
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: • `05`: Successful authentication. • `06`: Authentication attempted. • `07`: Failed authentication. Possible values for China UnionPay: • `up3ds`: China UnionPay authentication verified successfully. • `up3ds_attempted`: China UnionPay card not enrolled, but the attempt to authenticate is recorded. • `up3ds_failure`: China UnionPay authentication unavailable. Possible values for Mastercard: • `00`: Failed authentication. • `01`: Authentication attempted. • `02`: Successful authentication.	String (15)

Response Fields (continued)

Field	Description	Data Type & Length
payer_authentication_enroll_e_commerce_indicator	Commerce indicator for cards not enrolled. Possible values: • `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)

Response Fields (continued)

Field	Description	Data Type & Length
payer_authentication_enroll_veres_enrolled	Result of the enrollment check. Possible values: • 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. 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. This value can be returned if you are using rules-based payer authentication: • B: Indicates that authentication was bypassed. For rules-based payer authentication information, see the Payer Authentication Guides.	String (255)
payer_authentication_network_score	The global score calculated by the Cartes Bancaires scoring platform and returned to the merchant.	Integer (2)

Response Fields (continued)

Field	Description	Data Type & Length
payer_authentication_pares_status	Raw result of the authentication check. Possible values: • 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_status_reason	Provides additional information about the PARes status value.	Integer (2)
payer_authentication_pares_timestamp	Decrypted time stamp for the payer authentication result. Visa Click to Pay generates this value. Format: Unix time, which is also called *epoch time*.	String
payer_authentication_proof_xml	XML element containing proof of enrollment verification. For cards not issued in the U.S. or Canada, your bank can require this data as proof of enrollment verification for any payer authentication transaction that you re-submit because of a chargeback. For cards issued in the U.S. or Canada, Visa can require this data for specific merchant category codes. This field is HTML encoded. This field is not returned for 3-D Secure 2.0 transactions.	String (1024)
payer_authentication_reason_code	Numeric value corresponding to the result of the payer authentication request. See "Reason Codes" (on page 211).	String (5)

Response Fields (continued)

Field	Description	Data Type & Length
payer_authentication_specification_version	This field contains the 3-D 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_type	Indicates the type of authentication that is used to challenge the card holder. Possible values: • `01`: Static • `02`: Dynamic • `03`: OOB (Out of Band)	Integer (2)
payer_authentication_uad	Mastercard Identity Check UCAF authentication data. Returned only for Mastercard Identity Check transactions.	String (32)
payer_authentication_uci	Mastercard Identity Check UCAF collection indicator. This field indicates whether authentication data is collected at your website. Possible values: • `0`: Authentication data was not collected and customer authentication not completed. • `1`: Authentication data was not collected because customer authentication not completed. • `2`: Authentication data was collected. Customer completed authentication.	String (1)

Response Fields (continued)

Field	Description	Data Type & Length
payer_authentication_validate_e_commerce_indicator	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 `vbv_failure` instead of internet when **payer_authentication_eci** is not present. The value of this field is passed automatically to the authorization service if you request the services together. Possible values: • `aesk`: American Express SafeKey authentication verified successfully. • `aesk_attempted`: Card not enrolled in American Express SafeKey, but the attempt to authenticate was recorded. • `internet`: Authentication was not verified successfully. • `js`: J/Secure authentication verified successfully. • `js_attempted`: JCB card not enrolled in J/Secure, but the attempt to authenticate was recorded. • `spa`: Mastercard Identity Check authentication verified successfully. • `spa_failure`: Mastercard Identity Check failed authentication. • `vbv`: Visa Secure authentication verified successfully. • `vbv_attempted`: Card not enrolled in Visa Secure, but the attempt to authenticate was recorded. • `vbv_failure`: Visa Secure authentication unavailable.	String (255)

Response 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. Possible values: • `-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 Click to Pay generates this value. Format: Unix time, which is also called epoch time.	String
payer_authentication_white_list_status	Enables the communication of trusted beneficiary and whitelist status among the ACS, the directory server, and the 3-D Secure requester. Possible Values: • `Y`: 3-D Secure requester is whitelisted by cardholder • `N`: 3-D Secure requester is not whitelisted by cardholder	String (1)

Response Fields (continued)

Field	Description	Data Type & Length
payer_authentication_white_list_status_source	This field is populated by the system setting whitelist status. Possible Values: • `01`: 3-D Secure Server • `02`: Directory server • `03`: ACS	Integer (2)
payer_authentication_xid	Transaction identifier generated by payer authentication. Used to match an outgoing payer authentication request with an incoming payer authentication response.	String (28)
payment_account_reference	Reference number serves as a link to the cardholder account and to all transactions for that account. The same value is returned whether the account is represented by a PAN or a network token.	String (32)
payment_solution	Type of credential-on-file (COF) payment network token. Returned in authorizations that use a payment network token associated with a TMS token. Possible values: • `014`: Mastercard • `015`: Visa • `016`: American Express	String (3)

Response Fields (continued)

Field	Description	Data Type & Length
payment_token	Identifier for the payment details. The payment token retrieves the card data, billing information, and shipping information from the payment repository. This payment token supersedes the previous payment token and is returned if: • The merchant is configured for a 16-digit payment token that displays the last four digits of the primary account number (PAN) and passes Luhn mod-10 check. See "Payment Tokens" (on page 14). • The customer 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 using Token Management Services.	String (32)
payment_token_latest_card_expiry_date	Card expiration date of the latest card issued to the cardholder. Returned when Network Tokenization is enabled, and a **payment_token** with an associated Network Token is used in a transaction. Network Tokens can continue to be used even if the original card has expired. Format: MM-yyyy	Date (a) (7)

Response Fields (continued)

Field	Description	Data Type & Length
payment_token_latest_card_suffix	Last four digits of the latest card issued to the cardholder. Returned when Network Tokenization is enabled, and a **payment_token** with an associated Network Token is used in a transaction. Network Tokens can continue to be used even if the original card number has changed due to a new card being issued. Use the last four digits in payment confirmation messages to cardholders, for example: "Thank you for your payment using your Visa card ending [payment_token_latest_card_suffix]".	String (4)
paypal_address_status	Status of the street address on file with PayPal. Possible values: • `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)
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)

Response Fields (continued)

Field	Description	Data Type & Length
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: • `verified` • `unverified`	String (10)

Response Fields (continued)

Field	Description	Data Type & Length
paypal_pending_reason	Indicates the reason that payment is pending. Possible values: • `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. • `electronic check`: 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	String (14)

Response Fields (continued)

Field	Description	Data Type & Length
paypal_pending_status	Status of the transaction. Possible values: • `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)

Response Fields (continued)

Field	Description	Data Type & Length
paypal_protection_eligibility	Seller protection in force for the transaction. Possible values: • `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)
paypal_protection_ eligibility_type	Seller protection in force for the transaction. Possible values: • `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. To enable the **paypal_protection_eligibility_type** field, contact customer support to have your account configured for this feature.	String (32)

Response Fields (continued)

Field	Description	Data Type & Length
paypal_request_id	Identifier for the request generated by the client.	String (26)
paypal_token	Timestamped PayPal token that identifies that PayPal Express Checkout is processing the transaction. Save this value to send in future request messages.	String (20)
paypal_transaction_type	Indicates the PayPal transaction type. Possible value: `expresscheckout`	String (16)
reason_code	Numeric value corresponding to the result of the payment card transaction request. See Reason Codes (on page 211).	String (5)
req_access_key	Authenticates the merchant with the application.	String (32)

Response Fields (continued)

Field	Description	Data Type & Length
req_aggregator_id	Value that identifies you as a payment aggregator. Obtain this value for the processor. **Visa Platform Connect**—The value for this field corresponds to this data in the TC 33 capture file: • Record: CP01 TCR6 • Position: 95-105 • Field: Mastercard Payment Facilitator ID **Field Length** American Express Direct: 20 **FDC Compass**—This value must consist of uppercase characters. Visa Platform Connect: 11 FDC Compass: 20 FDC Nashville Global: 15 **Required/Optional** American Express Direct: R for all aggregator transactions. Visa Platform Connect: R for Mastercard aggregator authorizations; otherwise, not used. FDC Compass: R for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	String (See description)

Response Fields (continued)

Field	Description	Data Type & Length
req_allow_payment_token_update	Indicates whether the customer can update the billing, shipping, and payment information on the order review page. Possible values: • `true`: Customer can update details. • `false`: Customer cannot update details.	String (5)
req_amount	Total amount for the order. Must be greater than or equal to zero.	String (15)
req_auth_indicator	Flag that specifies the purpose of the authorization. Possible values: • `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 customer support.	String (1)

Response Fields (continued)

Field	Description	Data Type & Length
req_auth_type	Authorization type. Possible values: • `AUTOCAPTURE`: Automatic capture. • `STANDARDCAPTURE`: Standard capture. • `verbal`: Forced capture. ***Asia, Middle East, and Africa Gateway; Cielo; Comercio Latino; and Cybersource Latin American Processing*** Set this field to `AUTOCAPTURE` 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 `STANDARDCAPTURE` and include it in a standard authorization or bundled request to indicate that you are overriding an automatic capture. ***Forced Capture*** Set this field to `verbal` and include it in the authorization request to indicate that you are performing a forced capture; therefore, you receive the authorization code outside the transaction processing system. ***Verbal Authorization*** Set this field to `verbal` and include it in the capture request to indicate that the request is for a verbal authorization.	Cielo, Comercio Latino, and Cybersource Latin American Processing: String (15) All other processors: String (11)

Response Fields (continued)

Field	Description	Data Type & Length
req_bill_payment	Flag that indicates a payment for a bill or for an existing contractual loan. Visa provides a Bill Payment program that enables customers to use their Visa cards to pay their bills. Possible values: • `true`: Bill payment or loan payment. • `false` (default): Not a bill payment or loan payment.	String (1)
req_bill_to_address_city	City in the billing address.	String (50) Visa Click to Pay: String (100)
req_bill_to_address_country	ISO country code for the billing address.	String (2)
req_bill_to_address_line1	First line of the street address in the billing address.	String (60) Visa Click to Pay: String (100)
req_bill_to_address_line2	Second line of the street address in the billing address.	String (60) Visa Click to Pay: 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 Click to Pay: String (100)
req_bill_to_address_state	The state or province for the bill-to address. For the United States and Canada, the two-character ISO state and province code is returned. See State, Province, and Territory Codes for the United States and Canada.	String (30)
req_bill_to_company_name	Name of the customer's company.	String (40)

Response Fields (continued)

Field	Description	Data Type & Length
req_bill_to_email	Customer email address.	String (255) Visa Click to Pay: String (256)
req_bill_to_forename	Customer first name.	String (60) Visa Click to Pay: String (256)
req_bill_to_phone	Customer phone number.	String (15) Visa Click to Pay: String (30)
req_bill_to_surname	Customer last name.	String (60) Visa Click to Pay: String (265)

Response Fields (continued)

Field	Description	Data Type & Length
req_card_account_type	Flag that specifies the type of account associated with the card. The cardholder provides this information during the payment process. ***Cielo and Comercio Latino*** Possible values: • CR: Credit card • DB: Debit card ***Visa Platform Connect*** Possible values: • CH: Checking account • CR: Credit card account • SA: Savings account This field is returned for: • Debit transactions on Cielo and Comercio Latino. • Transactions with Brazilian-issued cards on Visa Platform Connect. 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. It is strongly recommended that you include this field for combo card transactions.	String (2)
req_card_expiry_date	Card expiration date.	String (7)
req_card_number	Card number.	String (20)

Response Fields (continued)

Field	Description	Data Type & Length
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)
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 token.	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. Possible values: • `true`: Customer browser accepts cookies. • `false`: Customer browser does not accept cookies.	String (5)
req_customer_gift_wrap	Indicates whether the customer requested gift wrapping for this purchase. Possible values: • `true`: Customer requested gift wrapping. • `false`: Customer did not request gift wrapping.	String (5)

Response Fields (continued)

Field	Description	Data Type & Length
req_customer_ip_address	Customer 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: • `false` (default): Not a loan payment • `true`: Loan payment	String (5)
req_departure_time	Departure date and time of the first leg of the trip. Use one of these formats: • yyyy-MM-DD HH:mm z • yyyy-MM-DD hh:mm a z • yyyy-MM-DD hh:mma z • HH = 24-hour format • hh = 12-hour format • a = am or pm (case insensitive) • z = time zone of the departing flight.	String (29)

Response Fields (continued)

Field	Description	Data Type & Length
req_device_fingerprint_id	Field that contains the session ID for the fingerprint. The string can contain uppercase and lowercase letters, digits, and these special characters: hyphen (-) and underscore (_). However, do not use the same uppercase and lowercase letters to indicate different sessions IDs. The session ID must be unique for each merchant ID. You can use any string that you are already generating, such as an order number or web session ID.	String (88)
req_driver_license_number	Driver's license number of the customer. The 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.	String (2)
req_e_commerce_indicator	The commerce indicator for the transaction type. Value: `install` This field is returned only for installment payments on Cybersource Latin American Processing.	String (13)
req_echeck_account_number	Account number. This number is masked.	Non-negative integer (17)
req_echeck_account_type	Account type. Possible values: • `C`: Checking • `S`: Savings (USD only) • `X`: Corporate checking (USD only)	String (1)
req_echeck_check_number	Check number.	Integer (8)

Response 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 transit number.	Non-negative integer (9)
req_echeck_sec_code	The authorization method for the transaction. Possible values: • `CCD` • `PPD` • `TEL` • `WEB`	String (3)
req_ignore_avs	Ignore the results of AVS verification. Possible values: • `true` • `false`	String (5)
req_ignore_cvn	Ignore the results of CVN verification. Possible values: • `true` • `false`	String (5)
req_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 Visa Platform Connect.	Amount (12)

Response Fields (continued)

Field	Description	Data Type & Length
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 "Discretionary Data" section in *Credit Card Services Optional Features SCMP API Supplement* or *Credit Card Services Optional Features Simple Order API Supplement*.	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., it is recommended that you include the country code.	String (15)
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)

Response Fields (continued)

Field	Description	Data Type & Length
req_item_#_passenger_type	Passenger classification associated with the price of the ticket. Possible values: • `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. For a complete list of airport codes, see IATA's City Code Directory.	String (3)
req_journey_leg#_orig	Airport code for the origin of the leg of the trip, designated by the pound (#) symbol in the field name. This code is usually three digits long; for example: SFO = San Francisco. For a complete list of airport codes, see IATA's City Code Directory.	String (3)
req_journey_type	Type of travel, such as one way or round trip.	String (32)
req_jpo_installments	Total number of Japanese installment payments.	String (2)

Response Fields (continued)

Field	Description	Data Type & Length
req_jpo_payment_method	Japanese payment method.	String (1)
req_line_item_count	Total number of line items. Maximum amount is 200.	String (3)
req_locale	Indicates the language to use for customer content. See "Activating a Profile" (on page 31).	String (5)

Response Fields (continued)

Field	Description	Data Type & Length
req_merchant_defined_data#	Optional fields that you can use to store information. # can range from `1` to `100`. Merchant-defined data fields `1` to `4` are associated with the payment token and are used for subsequent token-based transactions. Merchant-defined data fields `5` to `100` are passed through to Decision ManagerFraud Management Essentials as part of the initial payment request and are not associated with the payment token. **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. 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). If it is discovered that a merchant is capturing and/or transmitting personally identifying information via the merchant-defined data fields, whether or not intentionally, the merchant's account WILL immediately be suspended, which will result in a rejection of any and all transaction requests submitted by the merchant after the point of suspension.	String (100)

Response Fields (continued)

Field	Description	Data Type & Length
req_merchant_descriptor req_merchant_descriptor_alternate req_merchant_descriptor_city req_merchant_descriptor_contact req_merchant_descriptor_country req_merchant_descriptor_postal_code req_merchant_descriptor_state req_merchant_descriptor_street	For the descriptions, used-by information, data types, and lengths for these fields, see the Merchant Descriptors Developers Guides.	
req_merchant_descriptor	Your business name. This name appears on the cardholder's statement.	String (23)
req_merchant_descriptor_alternate	Alternate contact information for your business, such as an email address or URL. This value might appear on the cardholder's statement.	String (13)
req_merchant_descriptor_city	City for your business location. This value might appear on the cardholder's statement.	String (13)
req_merchant_descriptor_contact	Telephone number for your business. This value might appear on the cardholder's statement.	String (14)
req_merchant_descriptor_country	Country code for your business location. This value might appear on the cardholder's statement.	String (2)

Response Fields (continued)

Field	Description	Data Type & Length
req_merchant_descriptor_postal_code	Postal code for your business location. This value might appear on the cardholder's statement.	String (14)
req_merchant_descriptor_state	State code or region code for your business location. This value might appear on the cardholder's statement.	String (3)
req_merchant_descriptor_street	Street address for your business location. This value might appear on the cardholder's statement.	String (60)
req_merchant_secure_data1 req_merchant_secure_data2 req_merchant_secure_data3	Optional fields that you can use to store information. The data is encrypted before it is stored in the payment repository.	String (100)
req_merchant_secure_data4	Optional field that you can use to store information. The data is encrypted before it is stored in the payment repository.	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: • `card` • `echeck` • `paypal` • `visacheckout`	String (30)

Response Fields (continued)

Field	Description	Data Type & Length
req_payment_token	Identifier for the payment details. The payment token retrieves the card data, billing information, and shipping information from the payment repository. 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.	String (32)
req_payment_token_ comments	Optional comments about the customer token.	String (255)
req_payment_token_title	Name of the customer token.	String (60)
req_profile_id	Identifies the profile to use with each transaction.	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)
req_recipient_postal_code	Partial postal code for the recipient's address.	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)

Response Fields (continued)

Field	Description	Data Type & Length
req_recurring_automatic_renew	Indicates whether to automatically renew the payment schedule for an installment subscription. Possible values: • `true` (default): Automatically renew. • `false`: 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. Possible values: • `true` • `false`	String (5)
req_sales_organization_id	Company ID assigned to an independent sales organization. Obtain this value from Mastercard. Visa Platform Connect The value for this field corresponds to this data in the TC 33 capture file: • Record: CP01 TCR6 • Position: 106-116 • Field: Mastercard Independent Sales Organization ID	Nonnegative integer (11)

Response Fields (continued)

Field	Description	Data Type & Length
req_ship_to_address_city	City of shipping address.	String (50) Visa Click to Pay: String (100)
req_ship_to_address_country	The two-character ISO country code.	String (2)
req_ship_to_address_line1	First line of shipping address.	String (60) Visa Click to Pay: String (100)
req_ship_to_address_line2	Second line of shipping address.	String (60) Visa Click to Pay: String (100)
req_ship_to_address_postal_code	Postal code for the shipping address.	String (10) Visa Click to Pay: String (100)
req_ship_to_address_state	The two-character State, Province, and Territory Codes for the United States and Canada.	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 Click to Pay: String (256)
req_ship_to_phone	Phone number for the shipping address.	String (15) Visa Click to Pay: String (30)

Response Fields (continued)

Field	Description	Data Type & Length
req_ship_to_surname	Last name of person receiving the product.	String (60) Visa Click to Pay: String (256)
req_shipping_method	Shipping method for the product. Possible values: • `sameday`: Courier or same-day service • `oneday`: Next day or overnight service • `twoday`: Two-day service • `threeday`: Three-day service • `lowcost`: Lowest-cost service • `pickup`: Store pick-up • `other`: Other shipping method • `none`: No shipping method	String (10)
req_skip_decision_manager	Indicates whether to skip Decision ManagerFraud Management Essentials. See Decision Manager (on page 75). Possible values: • `true` • `false` For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	String (5)

Response Fields (continued)

Field	Description	Data Type & Length
req_submerchant_city	Sub-merchant's city.	American Express Direct: String (15) FDC Compass: String (21) FDC Nashville Global: String (11)
req_submerchant_country	Sub-merchant's country.	String (3)
req_submerchant_email	Sub-merchant's email address. Visa Platform Connect With American Express, the value for this field corresponds to this data in the TC 33 capture file: • Record: CP01 TCRB • Position: 25-64 • Field: American Express Seller E-mail Address	American Express Direct: String (40) FDC Compass: String (40) FDC Nashville Global: String (19) Visa Platform Connect: String (40)

Response Fields (continued)

Field	Description	Data Type & Length
req_submerchant_id	The ID you assigned to your sub-merchant. ***Visa Platform Connect*** With American Express, the value for this field corresponds to this data in the TC 33 capture file: • Record: CP01 TCRB • Position: 65-84 • Field: American Express Seller ID With Mastercard, the value for this field corresponds to this data in the TC 33 capture file: • Record: CP01 TCR6 • Position: 117-131 • Field: Mastercard Sub-Merchant ID	American Express Direct: String (20) FDC Compass: String (20) FDC Nashville Global: String (14) Visa Platform Connect with American Express: String (20) Visa Platform Connect with Mastercard: String (15)
req_submerchant_name	Sub-merchant's business name.	American Express Direct: String (37) FDC Compass with American Express: String (19) FDC Compass with Mastercard: String (37) FDC Nashville Global: String (12)

Response Fields (continued)

Field	Description	Data Type & Length
req_submerchant_phone	Sub-merchant's telephone number. ***Visa Platform Connect*** With American Express, the value for this field corresponds to this data in the TC 33 capture file: • Record: CP01 TCRB • Position: 5-24 • Field: American Express Seller Telephone Number	American Express Direct: String (20) FDC Compass: String (13) FDC Nashville Global: String (10) Visa Platform Connect: String (20)
req_submerchant_postal_code	Partial postal code for the sub-merchant's address.	American Express Direct: String (9) FDC Compass: String (15) FDC Nashville Global: String (9)
req_submerchant_state	Sub-merchant's state or province.	String (2)
req_submerchant_street	First line of the sub-merchant's street address.	American Express Direct: String (30) FDC Compass: String (38) FDC Nashville Global: String (25)
req_tax_amount	Total tax to apply to the product.	String (15)
req_transaction_type	The type of transaction requested.	String (60)

Response Fields (continued)

Field	Description	Data Type & Length
req_transaction_uuid	Unique merchant-generated identifier. Include with the **access_key** field for each transaction.	String (50) Visa Click to Pay: String (100)
request_token	Request token data created for each response. 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)
service_fee_return_url	URL to POST the **conditions_accepted** field value to. See Service Fees (on page 39).	
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 2020-08-11T22:47:57Z equals August 11, 2020, 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)

Response Fields (continued)

Field	Description	Data Type & Length
utf8	Indicates whether the unicode characters are encoded. Possible value: ✓	String (3)
vc_avs_code_raw	Decrypted raw (unmapped) AVS code provided by Visa Click to Pay.	String (10)
vc_risk_score	Decrypted risk score used with your fraud model. See Configuring Visa Click to Pay (on page).	Positive Integer (2)
vc_wallet_reference_id	Decrypted order identifier generated by Visa Click to Pay.	String (100)

SEC Codes

The **echeck_sec_code** field specifies the authorization method for the transaction. Possible values:

- `ARC:` account receivable conversion—supports the conversion of checks received through U.S. mail into a merchant's unattended lock box. This value is used only by Chase Paymentech Solutions for U.S. dollar transactions. Contact your Chase Paymentech Solutions representative to ensure that your address city field has been set up.

- `CCD:` corporate cash disbursement—a 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. For Cybersource ACH Service, `CCD` is the default value for a credit when no value is set and when the **ecp_account_type check_accountTypeecheck_account_type** field is set to `X` or `G`.

- `POP:` point of purchase conversion—supports single entry debits used at the point of purchase. This value is used only by Chase Paymentech Solutions for U.S. dollar transactions. Contact your Chase Paymentech Solutions representative to ensure that your address city field has been set up. If you submit the **check_secCodeecp_sec_code** field with a value of `POP`, we strongly recommend that you also submit the **check_terminalCityecp_terminal_city** and **checkTerminal_Stateecp_terminal_state** fields. If you submit the **check_terminalCityecp_terminal_city** and **checkTerminal_Stateecp_terminal_state** fields in a transaction and you wish to perform a follow-on transaction, you must resubmit them with the follow-on transaction.

- `PPD:` prearranged payment and deposit entry—a 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 pre-arranged. A written authorization from the customer is required for one-time transactions, and a written standing authorization is required for recurring transactions. For Cybersource ACH Service, `PPD` is the default value for a debit when no value is set and when the **ecp_account_type check_accountTypeecheck_account_type** field is set to `C` or `S`.

- `TEL:` telephone-initiated entry—a 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 a payment authorization from the customer over the telephone. Only the Cybersource ACH processor supports recurring telephone-initiated debits and credits. For Cybersource ACH Service, if the e-commerce indicator (ECI) for the Virtual Terminal is `MOTO`, the value of the **check_secCodeecp_sec_codeecheck_sec_code** field defaults to `TEL`.

- `WEB:` internet-initiated entry—a 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. For a `WEB` entry, you must obtain payment authorization from the customer over the internet. For Cybersource ACH Service, if the ECI for the Virtual Terminal is not set to `MOTO`, the value of the **check_secCodeecp_sec_codeecheck_sec_code** field defaults to `WEB`. Use `WEB` as the SEC code for all Canadian dollar transactions on the Chase Paymentech Solutions connection.

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 default receipt page or your receipt page is displayed to the customer. Both you and your customer can also receive an email receipt. See "Merchant Notifications" (on page 27).

Reason Codes

Reason Code	Description
100	Successful transaction.
101	Request is missing one or more required fields. Examine the response fields **missingField_0** through **missingField_N** to identify which fields are missing. Resend the request with all the required fields.
102	One or more fields in the request contain invalid data. Possible action: see the response 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 Centeryour Merchant Services account to confirm that the transaction has not yet been processed. See Viewing Transactions in the Business CenterYour Merchant Services Account (on page 78).
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 Centeryour Merchant Services account or programmatically through the single transaction querysingle transaction query.

Reason Codes (continued)

Reason Code	Description
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 Centeryour Merchant Services account or programmatically through the single transaction querysingle 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 Centeryour Merchant Services account or programmatically through the single transaction querysingle transaction query.
200	The authorization request was approved by the issuing bank but declined because it did not pass the Address Verification System (AVS) check. Possible action: you can capture the authorization, but consider reviewing the order for fraud.
201	The issuing bank has questions about the request. You do not receive an authorization code programmatically, but you might receive one verbally by calling the processor. Possible action: call your processor to possibly receive a verbal authorization. For contact phone numbers, refer to your merchant bank information.
202	Expired card. You might also receive this value if the expiration date you provided does not match the date the issuing bank has on file. Possible action: request a different card or other form of payment.
203	General decline of the card. No other information was provided by the issuing bank. Possible action: request a different card or other form of payment.
204	Insufficient funds in the account. Possible action: request a different card or other form of payment.

Reason Codes (continued)

Reason Code	Description
205	Stolen or lost card. Possible action: review this transaction manually to ensure that you submitted the correct information.
207	Issuing bank unavailable. Possible action: To avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status either directly in the Business Centeryour Merchant Services account or programmatically through the single transaction querysingle transaction query.
208	Inactive card or card not authorized for card-not-present transactions. Possible action: request a different card or other form of payment.
210	The card has reached the credit limit. Possible action: request a different card or other form of payment.
211	Invalid CVN. Possible action: request a different card or other form of payment.
221	The customer matched an entry on the processor's negative file. Possible action: review the order and contact the payment processor.
222	Account frozen.
230	The authorization request was approved by the issuing bank but declined because it did not pass the CVN check. Possible action: you can capture the authorization, but consider reviewing the order for the possibility of fraud.
231	Invalid account number. Possible action: request a different card or other form of payment.
232	The card type is not accepted by the payment processor. Possible action: contact your merchant bank to confirm that your account is set up to receive the card in question.

Reason Codes (continued)

Reason Code	Description
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 account. Possible action: do not resend the request. Contact 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 Centeryour Merchant Services account or programmatically through the single transaction querysingle 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.
478	Strong customer authentication (SCA) is required for this transaction.
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 based on your Decision Manager settings. Possible action: review the authorization request.

Types of Notifications

Types of Notifications

Decision	Description	Type of Notification
ACCEPT	Successful transaction. See reason codes 100 and 110.	• Custom receipt page • Customer receipt email • Merchant POST URL • Merchant receipt email
REVIEW	Authorization was declined; however, a capture might still be possible. Review payment details. See reason codes 200, 201, 230, and 520.	• Custom receipt page • Customer receipt email • Merchant POST URL • Merchant receipt email
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, 478, and 481. If the retry limit is set to `0`, the customer receives the decline message, *Your order was declined. Please verify your information.* 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 3-D Secure credentials incorrectly.	• Custom receipt page • Merchant POST URL • Merchant receipt email
ERROR	Access denied, page not found, or internal server error. See reason codes 102, 104, 150, 151 and 152.	• Custom receipt page • Merchant POST URL

Types of Notifications (continued)

Decision	Description	Type of Notification
CANCEL	The customer did not accept the service fee conditions. The customer cancelled the transaction.	• Custom receipt page • Merchant POST URL

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 information, 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** response field. See Response Fields (on page 159).

Important: When you populate billing street address 1 and billing street address 2, Visa Platform ConnectCybersource concatenates the two values. If the concatenated value exceeds 40 characters, Visa Platform ConnectCybersource 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.

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

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.

U.S. Domestic AVS Codes (continued)

Code	Response	Description
C	No match	Street address and postal code do not match.
D	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.
G		Not supported.
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 these descriptions: • 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 registered to use AAV+ with the American Express Phoenix processor.

U.S. Domestic AVS Codes (continued)

Code	Response	Description
R	System unavailable	System unavailable.
S	Not supported	U.S.-issuing bank does not support AVS.
T	Partial match	Card member's name does not match, but street address matches. Returned only for the American Express card type.
U	System unavailable	Address information unavailable for one of these reasons: • The U.S. bank does not support non-U.S. AVS. • The AVS in a U.S. bank is not functioning properly.
V	Match	Card member's name, billing address, and billing postal code match. Returned only for the American Express card type.
W	Partial match	Street address does not match, but 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 5-digit postal code matches.
1	Not supported	AVS is not supported for this processor or card type.
2	Unrecognized	The processor returned an unrecognized value for the AVS response.
3	Match	Address is confirmed. Returned only for PayPal Express Checkout.
4	No match	Address is not confirmed. Returned only for PayPal Express Checkout.

CVN Codes

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 the **auth_cavv_result** field in the response message for an authorization request.

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 3-D Secure data was not used.
99	An unknown value was returned from the processor.

Iframe Implementation

Important: If you plan to embed Secure Acceptance in an iframe, ensure that you follow the guidelines in this section. PayPal Express Checkout is not supported on a Secure Acceptance iframe integration.

Important: For the Payer Authentication 3-D 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 the Payer Authentication guide.

You must select the single page checkout option for the hosted checkoutHosted Payments Page iframe implementation. See Checkout Configuration (on page).

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 Custom Checkout Appearance (on page).

Cybersource recommends that you manage the total amount value on your website containing the inline frame. You must also provide customers a cancel order functionality on your website containing the inline frame.

Refer to PCI DSS v4 section 6.4.3 for more information on how to secure iframes.

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 website within an iframe.

While no security remediation can prevent every clickjacking, developers must implement in accordance with relevant industry standards and guidelines, such as PCI DSS and Open Worldwide Application Security Project (OWASP) when using and securing iframes.

You are required to implement the recommended prevention techniques in your website. For more information on PCI DSS and OWASP, see these websites:

- PCI DSS v4
- OWASP website
- OWASP Clickjacking Defense Cheat Sheet
- OWASP Cross Site Scripting Prevention Cheat Sheet

Your developers must not use double framing on the same page where the hosted checkout iframe implementation is used.

Web application protections for Cross-Site Scripting (XSS) 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.

Iframe Transaction Endpoints

For iframe transaction endpoints and supported transaction types for each endpoint, see Endpoints and Transaction Types (on page 48).

Visa Secure Response Codes

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

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 3-D Secure data was not used.
99	An unknown value was returned from the processor.