Braintree Payment Settings

Prerequisite alert!

- Merchant account with Braintree.
- If offering third party options such as PayPal, Google Pay and Apple Pay, merchant accounts with each provider.
- Minimum website version 4.30 . Contact Commerce Vision to request a site version upgrade.

On this page:

- Overview
- Step by Step Guide
  - 1. Configure General Settings
  - 2. Configure payment options
    - Credit Card Settings
    - PayPal Settings
    - Google Pay Settings
    - Apple Pay Settings
  - 3. Fraud Protection Settings for Order Payment
- Additional Information
- Related help

Overview

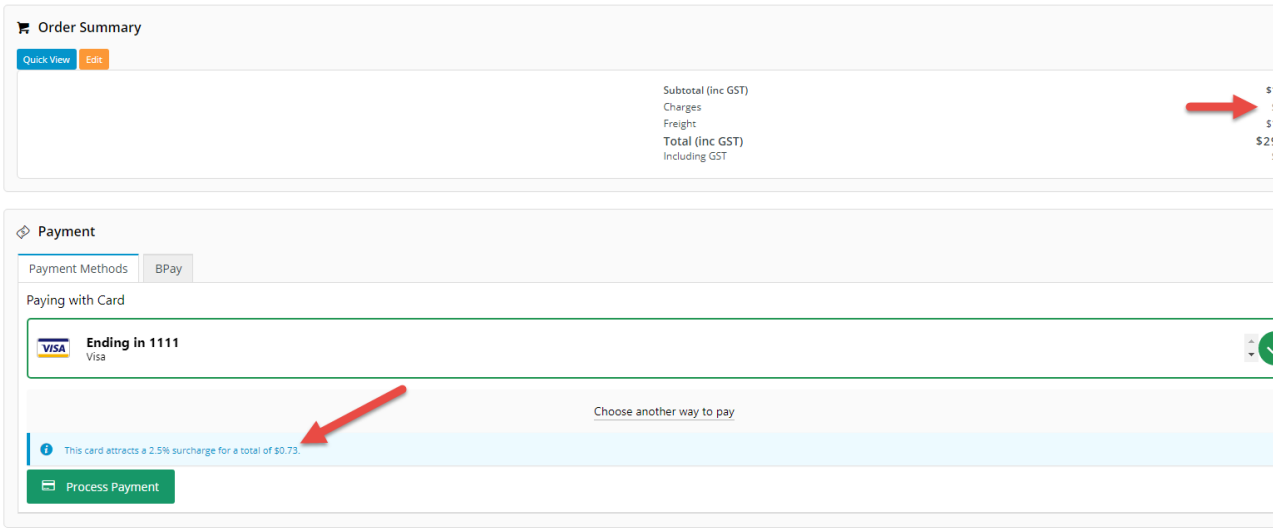
Once Braintree Payments has been implemented and switched on for your site by Commerce Vision, settings for the Braintree gateway including available payment options, vaulting (saving a payment for future use) and fraud protection, can be configured.

NOTE - When Braintree Payments is active, you can choose to use Braintree only for credit card and PayPal processing or include another credit card gateway and/or PayPal separately. These would be displayed under their own tabs on the checkout page.

Using surcharges or token management?

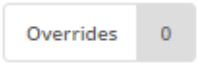
The Commerce Vision platform's credit card surcharge facility and token management feature have been integrated into Braintree Payments. If Braintree Payments is enabled, it will be used for saving a Customer credit card. This tokenised card can be used for future payment of account invoices.

- If any surcharge applies to an order, it will automatically be calculated, displayed and added to the total during checkout.



Step by Step Guide

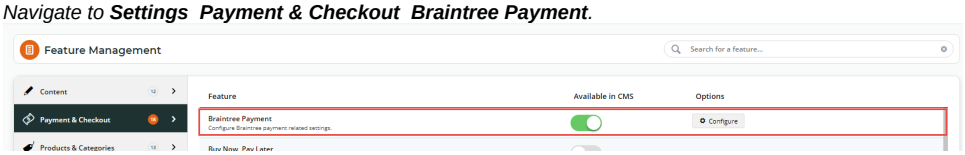
1. Configure General Settings

1. ***You will need your Sandbox or Production credentials (API keys and Merchant ID) for this step. You can retrieve these from your Braintree Sandbox or Production accounts.***
2. If the Overrides option 

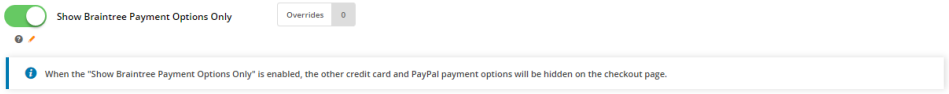
is displayed next to a setting, instead of being switched on and off for all users, it can be configured against specific Users, Roles or Customers.

To configure Braintree Payment Settings:

1. *Navigate to **Settings Payment & Checkout Braintree Payment**.*



2. *If the **Available in CMS** toggle is not enabled, toggle it ON.*
3. *Click **Configure**.*
4. *In **Braintree Payment Settings**, configure **General Settings**.*
    a. *To enable Braintree for all Users on your site, toggle ON **Enable Braintree Payment**. **TIP -** Leave this global toggle off and add Role Overrides to only offer Braintree to specific roles, e.g., B2C customers.*
    b. *If your site will use Braintree Payments only for credit card and/or PayPal transactions, toggle on **Show Braintree Payment Options Only**. This will disable other credit card gateways and turn off the separate PayPal feature.*

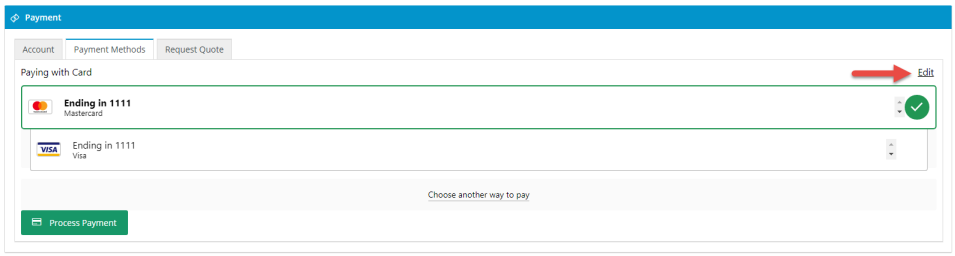


    c. *In **Mode**, select 'Sandbox' if testing the Stage site, or 'Production' if the live site.*

> *The sandbox is an entirely separate environment from your production account. Your sandbox login information, merchant ID, and API keys will be different. **Nothing created in the Sandbox (e.g. processing options, recurring billing settings) will transfer to Production.***

    d. *Enter credentials for either 'Sandbox' or 'Production'. You will need the following from your Braintree account:*
    *- **Merchant ID** - this is the default ID used to verify the account. If your business has several Merchant Account IDs and you want to specify one of them, enter it in the Merchant Account ID field instead of here.*
    *- **Public Key***
    *- **Private Key***
    *- **Merchant Account ID** - leave blank if the 'Merchant ID' is to be used.*

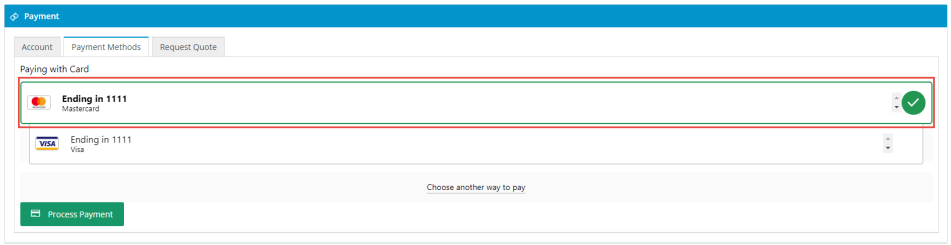
5. *To allow Users to delete a saved (vaulted) payment, toggle ON **Allow Vault Management**. When this setting is enabled, in the Payments panel during checkout, there is an **Edit** link on the top right side.*



*When the User clicks on **Edit**, the delete icon displays next to each payment. The User can click on it to remove the saved payment.*

*If the toggle is OFF, the **Edit** link is not displayed. To delete a vaulted payment, Users will need to contact your customer service and have the saved payment deleted in your Braintree account.*

6. *If the vaulted payment is to be preselected during checkout, toggle ON **Preselect Vaulted Payment Method.** The preselected payment is foregrounded and has a tick next to it. If this toggle is OFF, the last entered payment will be preselected.*



7. *If the nominated default payment option (set in the Braintree account) is to be displayed at the top of the list, toggle ON **Show Default Payment Method First**.*

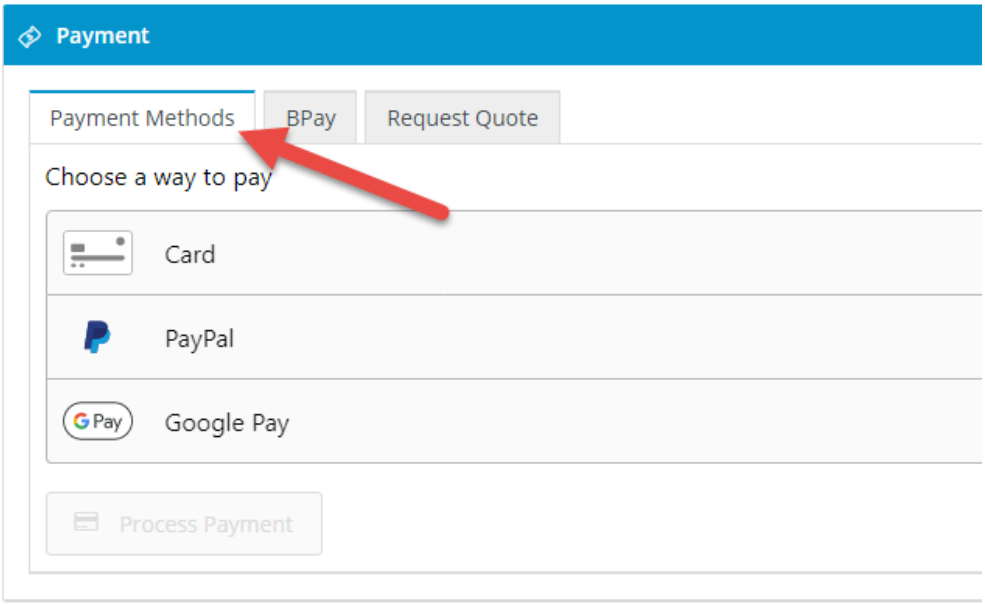
> ***To flag as default***
>
> *To make a payment option default, in your Braintree account, go to the **Vault** and find the User. Click on the payment option and click **Edit**. Tick the **Default Payment Method for Customer?** checkbox.*

2. Configure payment options

The next step is to configure the payment options your site offers. Each one can be enabled or disabled at any time. Note that options enabled here must also be turned on in your Braintree account.

> Your Braintree account will allow you to automatically offer credit card payments. To include PayPal, Google Pay or Apple Pay, your business must also have accounts with each respective provider.

All enabled Braintree payment methods will display under a common **Payment Methods** tab during checkout. **TIP -** You can change the tab name 'Payment Methods' in the Checkout Payments Options Widget. PayPal Express and Pay in 4 buttons can also be added to the product and cart pages.



See the step-by-step guide for each payment method:

Credit Card Settings

Configure Braintree Credit Card Settings

PayPal Settings

Configure Braintree PayPal Settings

Google Pay Settings

Configure Braintree Google Pay Settings

Apple Pay Settings

Configure Apple Pay Settings

3. Fraud Protection Settings for Order Payment

Braintree Payments has three fraud protection modes, and one must be selected. Information provided here is limited to setting up an option for your website. Details about fraud protection options are available from the Braintree website. (**NOTE -** Advanced and Kount are options that incur additional fees.) In addition, 3D Secure, which provides an extra layer of security by prompting a User to authenticate card ownership by entering a PIN, can be enabled.

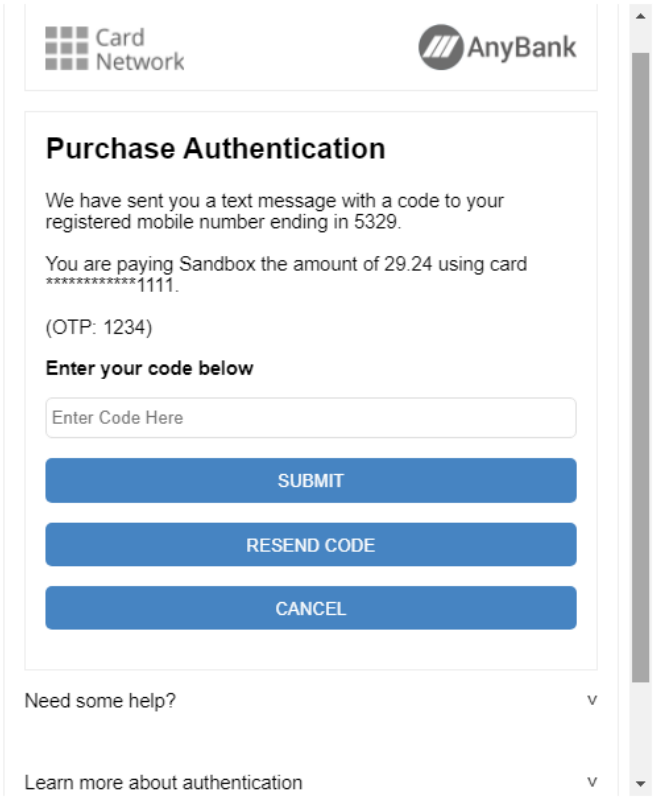
1. *In **Braintree Payment Settings**, scroll down to the **Fraud Protection Settings for Order Payment** section.*
2. *In **Fraud Protection Mode**, select Basic, Advanced or Kount. **NOTE -** The mode enabled her must be the same as the mode enabled in your Braintree account.*
   ***Basic** - all fraud protection is handled by Braintree and no further configuration is required here.*
3. **(For 'Advanced' or 'Knout' only.)** *In **Treat Decision 'Not Evaluated' As**, select 'Review' or 'Approve'.*
   ***Review:** the transaction with this status is treated as suspicious and put on hold subject to further verification*
   ***Approve:** the transaction with this status is treated as a successful one and the order is released.*
4. **(For 'Knout' only.)** *In **Treat Decision 'Escalate' As**, select 'Review' or 'Approve'.*
   ***Review:** the transaction with this status is treated as suspicious and put on hold subject to further verification*
   ***Approve:** the transaction with this status is treated as a successful one and the order is released*
5. *To use 3D Secure, toggle ON **Enable 3D Secure**. **NOTE -** This feature adds another layer of security for payments that use credit cards, including Google Pay. It is applicable only to cardholders who have enrolled in 3D Secure with their issuer.*

During the checkout process, if the cardholder is enrolled in 3D Secure, the issuing bank will decide whether the cardholder's identity can be verified using data supplied regarding the cardholder and their device, or if an additional authentication process is necessary. If additional authentication is necessary, Braintree will begin a process provided by the issuing bank to verify the cardholder's identity via SMS one-time passcode, the issuing bank's mobile app, biometric methods, or other means.

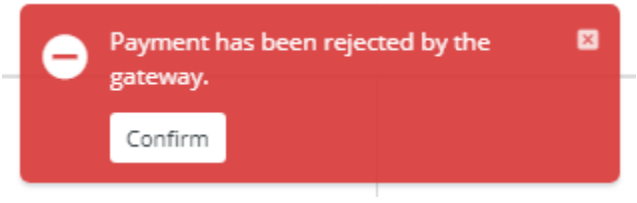
3D Secure can shift liability for fraud-related chargebacks from the merchant to the card issuer. For example, if the issuer ***does not*** *participate in 3D Secure but the card brand supports this extra protection (i.e. Visa or Mastercard), the liability for fraud-related chargebacks will shift to the issuer.*

NOTE - *3D Secure does not shift liability for all fraudulent chargebacks. You can determine whether or not liability shift occurred by the 3D Secure status code returned for the authentication.*

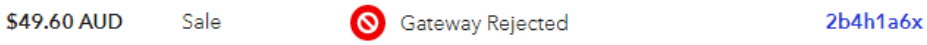
Example of 3D Secure popup:



If the credit card payment passes 3D Secure, the order will be completed. If the payment is rejected by 3D Secure, the User will see a 'Rejected by Gateway' popup error message on your site:

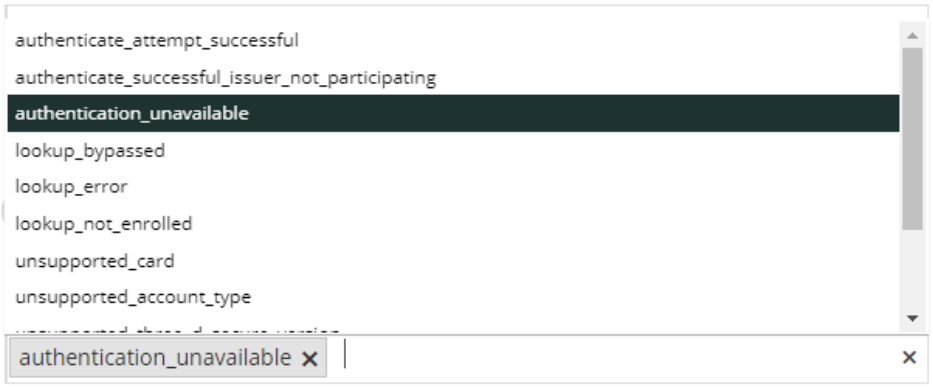


This status is also recorded in the Braintree account.

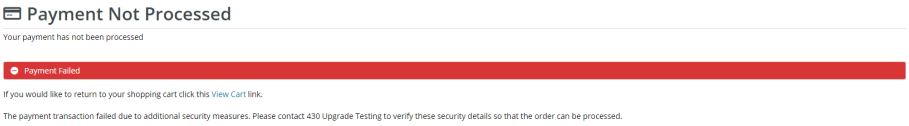


6. **(For use with 3D Secure only).** *The* ***3D Secure Review Status List*** *provides all 3D Secure statuses that will not reject the order if 3D is not required. it allows you to put such orders on hold for further verification. For instance, 'authenticate_attempt_successful' means that the card brand passed the attempt because the issuer's authentication server was unavailable. You can add one or more such statuses.* ***NOTE -*** *For a list of what each of the statuses mean, refer to the Braintree website.*

   Click on the list, then click to select all required statuses. These statuses will populate the field.



For cards that cannot be authenticated and the status is on this list, payment will not be processed and the User will see this message:



Additional Information

Minimum Version Requirements	4.31
Prerequisites	Braintree Account, third party payment accounts
Self Configurable	Yes
Business Function	Payment Types
BPD Only?	Yes
B2B/B2C/Both	Both
Third Party Costs	Fees may apply

Related help

- Braintree Payments
- Braintree Vaulting
- Braintree PayPal Settings
- Braintree Google Pay Settings
- Braintree Apple Pay Settings
- Braintree Credit Card Settings
- Braintree Payments - Credit Card Data Flow
- Braintree Test Credit Card Numbers