Bambora Checkout

> The Bambora Checkout Hosted Payment configuration allows administrators to process secure online transactions through a fully integrated Bambora (Wordline) merchant account. Its primary purpose is to enable reliable payment processing and tokenized profiles directly within the OperationsCommander (OPSCOM) checkout flow by utilizing secure authorization headers. This article is intended for OPSCOM administrators.

Setup and Configuration

To properly configure your Bambora payment type in OPSCOM, you require two separate encoded authorization headers: the Payment Authorization Header and the Profile Authorization Header. Both require your Bambora Merchant ID (MID) and a specific API access passcode to generate.

Generating the Payment Authorization Header

1. Log in to your Bambora account.
2. Select **Administration**, click **Account Settings**, and then select **Order Settings** from the left navigation menu.
3. Scroll down to the API access passcode section.
4. Click the **Generate New Code** button if the field is empty.
5. Click the **Update** button at the bottom of the page to save your changes.

6. Locate and copy your Merchant ID from the top right of your Bambora account.
7. Navigate to the Bambora encoding tool URL provided by your implementation specialist.
8. Paste your Merchant ID and the new API access passcode into the appropriate fields.
9. Click the **Encode** button.
10. Copy the generated Payment Authorization Header. Ensure you only copy the string starting with the word Passcode (e.g., Passcode MzAw...). Do not copy the Authorization: prefix or the quotation marks.

Generating the Profile Authorization Header

1. Select **Configuration** and click **Payment Profile Configuration** from the left navigation menu in Bambora.
2. Ensure the **API access passcode** option is selected under the Security Settings section.
3. Click the **Generate New Code** button if the field is empty.
4. Click the **Update** button at the bottom of the page to save your changes.
5. Navigate back to the Bambora encoding tool.
6. Paste your Merchant ID and this specific Profile API access passcode into the appropriate fields.
7. Click the **Encode** button.
8. Copy the generated Profile Authorization Header, again ensuring you only copy the string starting with the word Passcode.

> **Use a Text Editor: Temporarily paste your generated headers into a program like Notepad** while switching between Bambora and OPSCOM. This ensures you do not lose the copied strings during the multi-step configuration process.

Adding the Payment Type in OPSCOM

1. Hover over **System Configuration** and click **Payments** then **Setup Payment Types**.
2. Click the **Add Type** button.
3. Select **Bambora - Checkout** from the Provider list.
4. Click the **Next Step** button.
5. Enter a clear, descriptive name into the **Type Name** field (e.g., Online Credit Card Payment).
6. Select the specific user groups who should have access to this method from the **Enabled for User Types** list.
7. Enable or disable the checkboxes for **Enable for Text2ParkMe**, **Enable for Permit Renewal Payments**, and **Enable for Guest Payments** based on your operational needs.
8. Select **Billing Details** from the **Prompt Information** drop-down menu if you are enforcing AVS in your Bambora account, or select **Email Address** if AVS is not required.
9. Paste your copied headers into the **Profile Authorization Header** and **Payment Authorization Header** fields under the Production Credentials section.
10. Enable the **Validate Card when adding subscriptions** checkbox if you want the card validated immediately by the payment provider

when it is first added as a subscription method in a user's profile.

11. Leave the **Phone Number Field** set to hidden unless specifically required by your fraud detection settings.
12. Click the **Update Payment Type** button at the bottom of the page to save your configuration.

> **AVS and Prompt Settings Match: You must align your OPSCOM prompt information with your Bambora AVS settings.** If Address Verification Service (AVS) is enabled in Bambora, you must set OPSCOM to prompt for Billing Details. If you only prompt for Email Address while AVS is active, transactions will fail to process.

Using this Feature

Because this is a backend payment gateway configuration, administrators do not manually interact with this feature on a daily basis. Once fully configured, the Bambora Checkout integration automatically handles electronic routing and card tokenization when users process transactions on the user portal or when administrators process manual credit card payments via the administrative portal.

Best Practices and Considerations

- **AVS Configuration:** If using AVS, **Bambora recommends enabling only the AVS Postal/Zip Code Mismatch option**. The Street Mismatch option is extremely sensitive and may result in a high rate of declined payments due to minor formatting typos.
- **User-Friendly Naming:** The text you enter into the **Type Name** field is exactly what your users will see when selecting a payment method

during checkout. Choose a generic and recognizable name, such as "Credit Card", to avoid confusion during the checkout process.

Revision #48
Created 14 May 2024 07:43:15
Updated 12 August 2026 12:01:26