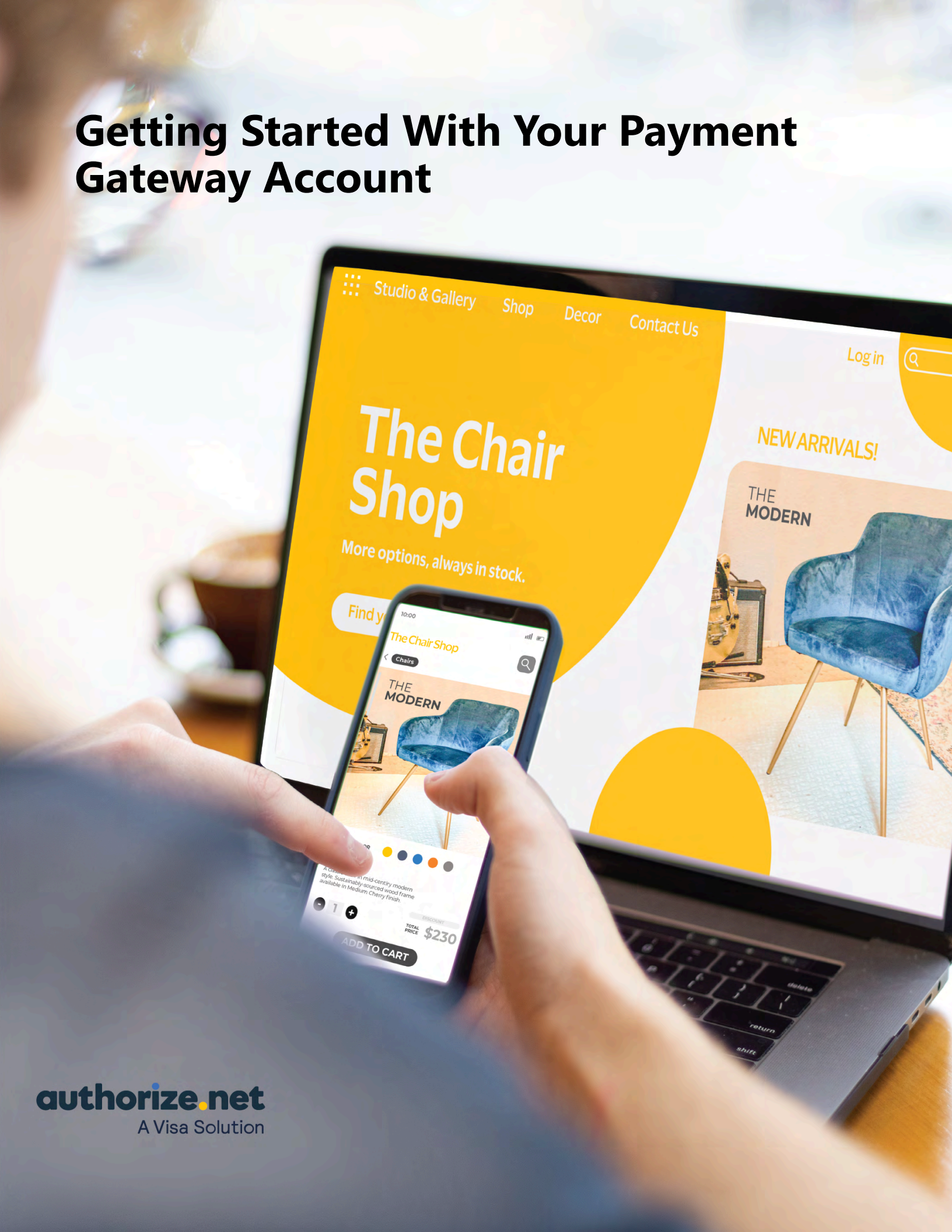
Getting Started With Your Payment Gateway Account



authorize.net
A Visa Solution

Version: 24.01

Contents

About This Guide

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

Audience and Purpose

This guide provides new merchants information about features and settings they should review when setting up their new Authorize.net account.

Conventions

The following 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:

https://support.authorize.net

Recent Revisions to This Document

24.01

Initial release of reformatted guide.

Introduction to The Merchant Interface

The Merchant Interface enables you to access your payment gateway account, manage transactions, configure account settings, view account statements, and generate reports. It is available from any computer with an internet connection and web browser.

This guide provides you with the information necessary to begin processing transactions using your Authorize.net account. When you have activated your account, an account owner must log into the account to review the default settings and make any necessary changes.

This guide is an introduction to the settings and features available with your Authorize.net account. You should become familiar with these settings.

Bookmark the Merchant Interface login page at https://login.authorize.net. You can also access the Merchant Interface by visiting the Authorize.net home page and choosing **Sign In > Merchants**.

After you activate your payment gateway account using the activation link from your welcome email, you are signed into the Merchant Interface.

Important: Follow the steps in this guide in the order they are presented to ensure that your account is set up to meet your business needs.

Warning: Your account defaults to Test Mode. It is important that you disable Test Mode before you start processing transactions. Failure to do so will result in no transactions being processed or recorded in your account. For more details, see Test Mode (on page 16)

.

Transaction Processing Settings

To connect your website or other payment application to the payment gateway, you must have your API login ID and transaction key or signature key. Both are unique to your payment gateway account and must be included with all transaction requests.

Depending on your connection method, either provide this information to your web developer, or enter it into your shopping cart or other software integration.

Important: Your API login ID and transaction key or signature key are not the same as your Merchant Interface login ID and password.

API Login ID

The API login ID is used by the payment gateway to identify you as an authorized merchant. This value is only generated once in the Merchant Interface by an account owner or account administrator with the correct permissions. As the API login ID is an essential credential for your connection to the payment gateway, contact Customer Support if you need to change it.

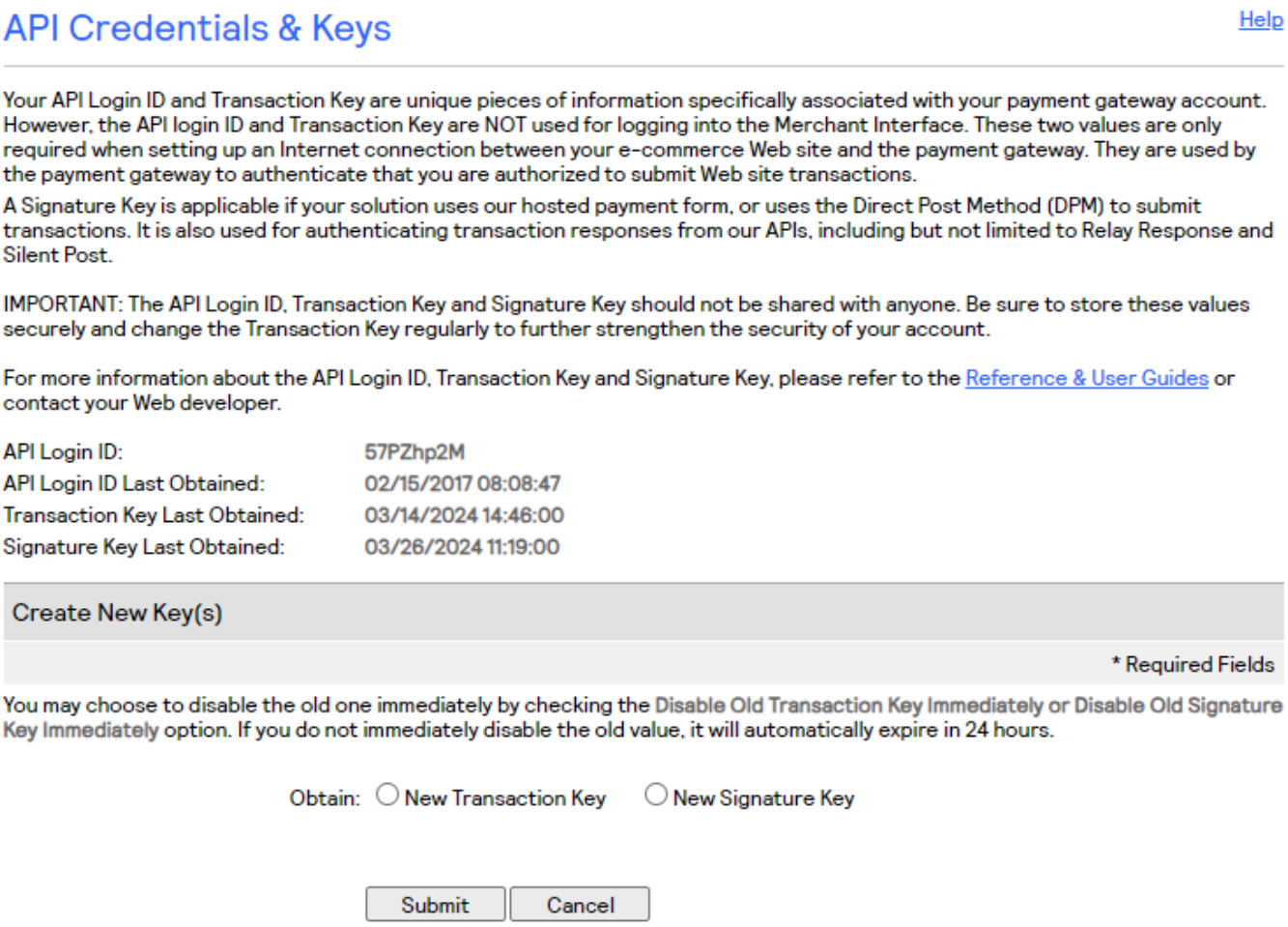
Transaction Key and Signature Key

Two types of keys are available for your account: the transaction key and the signature key. Both are used by the payment gateway to authenticate that transactions submitted for your account are actually being submitted by you. The transaction key is used along with the API login ID to authenticate API calls. The signature key is used to authenticate payment form requests and responses.

You can generate a new transaction key or signature key from within the Merchant Interface at any time.

> **Warning:** To avoid interruptions to your API or payment form transactions, you must notify your web developer or the person that manages your payment gateway connection each time the transaction key or signature key are updated. By default, the previous Transaction Key and Signature Key expire within 24 hours when a new transaction key or signature key is generated.

Example of API Credentials & Keys Page



Creating Your API Login ID and Transaction Key

Follow these steps to create your API login ID and transaction key:

1. Log in to the Merchant Interface at https://login.authorize.net.
2. Choose **Account > API Credentials & Keys**.
3. Choose **New Transaction Key**.
4. Click **Submit**.
5. Request and verify a PIN to confirm that this request is from an authorized user.

The API login ID and transaction key appear.

Important: Store the API login ID and transaction key in a secure location.

Creating a New Transaction Key or Signature Key

You must first create a transaction key before you can create a signature key.

Follow these steps to create a new transaction key or signature key:

1. Log in to the Merchant Interface at https://login.authorize.net.
2. Choose **Account > API Credentials & Keys**.
3. Choose the radio button for the credential you wish to create.
    - New Transaction Key
    - New Signature Key
4. Optionally, click **Disable Old Transaction Key Immediately** or **Disable Old Signature Key Immediately**. Use this option only if you must stop transaction processing immediately if, for example, you must stop fraudulent transactions from an unauthorized source.
5. Click **Submit**.
6. Request and verify a PIN to confirm that this request is from an authorized user.

A new transaction key or signature key appears. Provide these credentials to your software developer or software solution.

Important: Unless you checked **Disable Old Transaction Key Immediately** or **Disable Old Signature Key Immediately**, the previous transaction key or signature key will expire within 24 hours.

Important: Store the transaction key or signature key in a secure location.

Security Settings

The following settings are standard features of your payment gateway account and are designed to help prevent fraudulent transactions.

Address Verification Service (AVS) Settings

AVS is a payment card verification system that compares the billing address information provided by the customer in a transaction with the billing address on file at the customer's card issuing bank. AVS returns a response code that indicates the results of the comparison. Authorize.net then accepts or rejects the transactions according to the settings you have specified.

By default, your AVS settings are set to reject transactions that do not have a street address or ZIP code match. International cards are also rejected by default.

It is recommended that you review and configure your AVS settings according to your business model.

Reviewing and Editing Your AVS Settings

Follow these steps to review and edit your AVS settings:

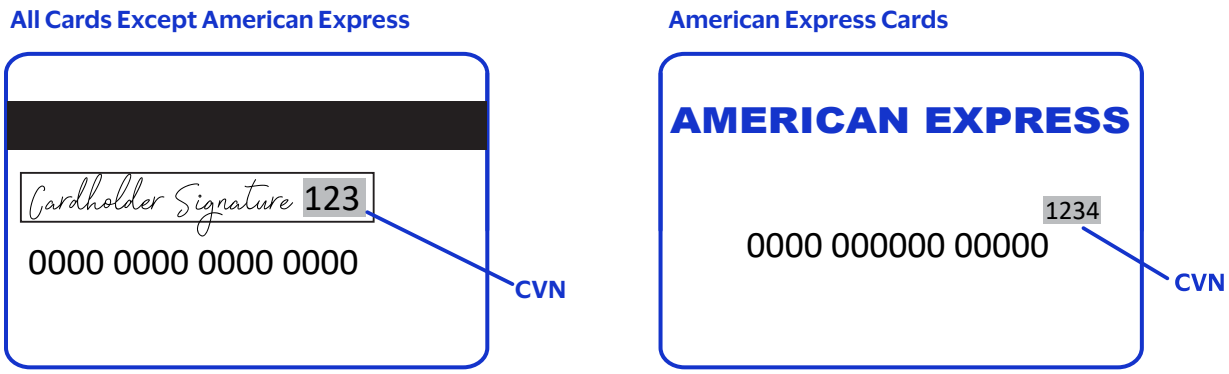
1. Log in to the Merchant Interface at https://login.authorize.net.
2. Choose **Account > Enhanced Address Verification Service**.
3. Optionally, for each AVS response code, Choose the option that represents how you would like to handle transactions that are returned with an AVS response code.
    - Allow
    - Allow, Report Triggered Filter(s)
    - Authorize and Hold For Review
    - Decline
4. If you have changed your AVS settings, click **Save**.

Your AVS settings are saved and will be applied to any new transactions submitted to your account.

Card Code Verification Settings

Card Code Verification (CCV) is a credit card verification system that compares the three- or four-digit card code on the customer's card with the value on file at the customer's card issuing bank. The card code appears to the right of the signature panel on the back of most cards. For American Express cards, the card code appears on the front of the card above the end of the credit card number.

Examples of Card Codes



CCV returns a response code indicating the results of the comparison. Authorize.net then accepts or rejects transactions according to the settings you have specified.

By default, your CCV settings are set to reject transactions where the card code submitted with the transaction does not match the value of the card code on file at the customer's card issuing bank, and they are set not to reject transactions when no card code is submitted.

It is recommended that you review your CCV settings and configure them according to your business model.

Reviewing and Editing Your CCV Settings

Follow these steps to review and edit your CCV settings:

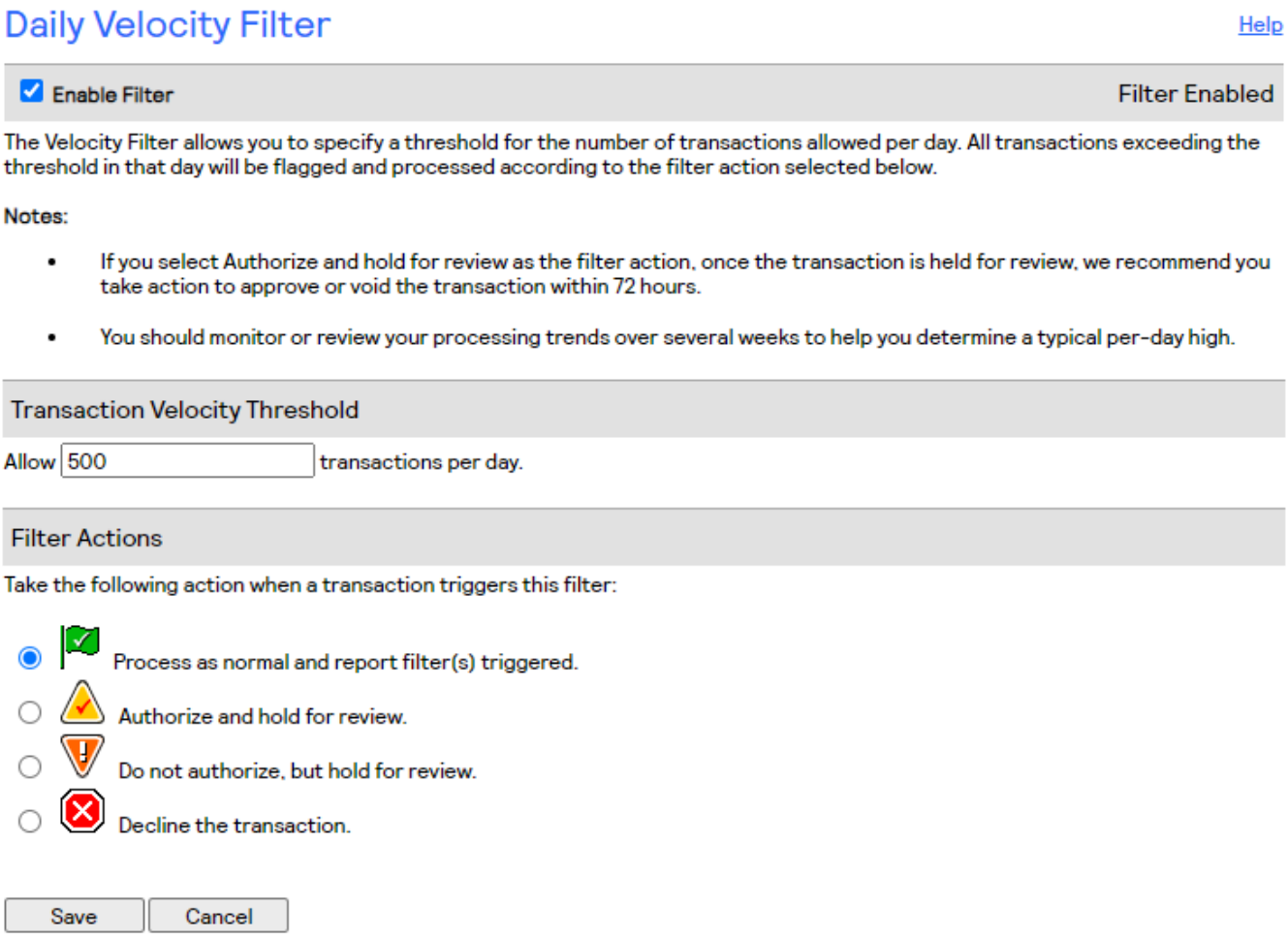
1. Log in to the Merchant Interface at https://login.authorize.net.
2. Choose **Account > Enhanced Card Code Verification**.
3. Optionally, for each CCV response code, choose the the option that represents how to handle transactions returned with that CCV response code.
    - Allow
    - Allow, Report Triggered Filter(s)
    - Authorize and Hold For Review
    - Decline
4. If you have changed your CCV settings, click **Save**.

Your CCV settings are saved and will be applied to new transactions submitted to your account.

Daily Velocity Filter

The Daily Velocity Filter enables you to set a Transaction Velocity Threshold to control the maximum number of transactions processed in a given day. All transactions exceeding the Transaction Velocity Threshold are filtered depending on the filter actions that you set. The default filter action is to process as normal but report that the filter has been triggered.

Example of Daily Velocity Filter Screen



Configuring the Daily Velocity Filter

Follow these stepd to configure the daily velocity filter:

1. Log in to the Merchant Interface at https://login.authorize.net.
2. Choose **Account > Daily Velocity**.
3. Check **Enable Filter**.

4. Enter your **Transaction Velocity Threshold**. Use the maximum number of transactions that you expect to process on a given day, with padding to account for high-volume transaction days.
5. Choose the filter action. This action will occur when the Transaction Velocity Threshold is exceeded.
    - Process as normal and report filter(s) triggered.
    - Authorize and hold for review.
    - Do not authorize, but hold for review.
    - Decline the transaction.
6. Choose **Save**.

Your daily velocity filter settings are saved and will be applied to new transactions submitted to your account.

Advanced Fraud Detection Suite Settings

In addition to the standard payment gateway features above, Authorize.net provides the Advanced Fraud Detection Suite (AFDS). AFDS is a powerful set of customizable, rules-based filters and tools that identify, manage, and prevent suspicious and potentially costly fraudulent transactions.

For more information on AFDS, choose **Tools > Fraud Detection Suite**.

General Settings

These basic settings can be used to customize your payment gateway account to your business.

Transaction Cut-Off Time

This setting enables you to specify the daily cut-off time for batched transactions to be submitted to your processor for settlement. The default transaction cut-off time is 4:00 p.m. Pacific time.

Reviewing and Editing Your Transaction Cut-Off Time

Follow these steps to review and edit your transaction cut-off time:

1. Log in to the Merchant Interface at https://login.authorize.net.
2. Choose **Account > Transaction Cut-Off Time**.
3. Optionally, select the time from the drop-down menus.
4. If you have changed your tranaction cut-off time, click **Submit**.

Your transaction cut-off time is set.

Important: Any transactions entered or successfully authorized after the cut-off time will not be sent to the processor for settlement until the following day's cut-off time. Changing the cut-off time will not cause settlement to occur sooner.

Time Zone

You can configure your payment gateway account to use the time zone of your business. This will enable you to properly configure your transaction cut-off time and view accurate statements and reports information.

Reviewing and Editing Your Time Zone

Follow these steps to review and edit your time zone setting:

1. Log in to the Merchant Interface at https://login.authorize.net.
2. Choose **Account > Time Zone**.
3. Optionally, select the appropriate time zone from the drop-down menu.
4. If you have changed your time zone setting setting, click **Submit**.

Your time zone setting is saved and will be applied to the timestamps of transactions in your account, as well as to your transaction cut-off time.

User Administration

The User Administration feature enables an account owner to create unique user accounts with distinct login IDs and passwords for employees who need access to the Merchant Interface. You can also customize permissions for each user account to match each employee's individual job responsibilities, which helps you keep transaction and account management activities in the Merchant Interface separate so that you can streamline your transaction management processes.

By default, the person who activates your payment gateway accountis an account owner. This account is the only user account until you create additional accounts.

Creating User Accounts

Follow these steps to create a user account:

1. Log in to the Merchant Interface at https://login.authorize.net.
2. Choose **Account > User Administration**.
3. Choose **+ Add User**.
4. From the **User Role** drop-down menu, select the type of user you would like to add .
    - Account Owner
    - Account Administrator
    - Transaction Manager
    - Account Analyst
    - Account Contact

    The default permissions associated with the selected role are displayed.
5. Optionally, you can customize the permissions by unchecking any boxes next to permissions you do not want enabled for the user.
6. Click **Next >**.
7. Unless the new user is an Account Contact, enter a login ID for the new user. The login ID must be at least six (6) characters long and should contain letters and numbers.
8. Enter the user's first name, last name, title, phone number and email address.
9. Choose the email notifications that you would like the user to receive.
10. If you want this user's email address to be used in the reply-to field in customer email receipts, check **Use this email address as reply-to**.
11. Click **Submit**.
12. Request and verify a PIN to confirm that this request is from a legitimate user.

The new user is created, and their login ID is displayed. An activation email is sent to the new user.

Important: The new user must activate their account before they can log in. The activation email expires within 24 hours.

Choosing a Connection Method

A connection method is a set of implementation requirements that enables you to connect a website or other application to the payment gateway for submitting transactions. If you have not yet decided on a connection method, here are a few options to consider:

- Use the Authorize.net Partner Directory to locate certified solution providers, developers, and hardware and business solution providers.
- If you or someone you know has web programming skills or in-house resources, use our flexible and customizable APIs for programming your own connection. Please visit the Authorize.net Developer Center for integration guides, sample code, and more.
- For detailed information and help deciding which connection method you should use, contact your Reseller, web developer, or Merchant Service Provider for assistance.
- Users of Windows PCs with Google Chrome can use the Virtual Point of Sale (VPOS) feature with a USB card reader for taking payments. For more information, see the VPOS FAQ.
- The Authorize.net mPOS mobile application enables you to securely accept payments anywhere you want using an Apple iOS or Android device with your Authorize.net Payment Gateway account. For more information, visit:

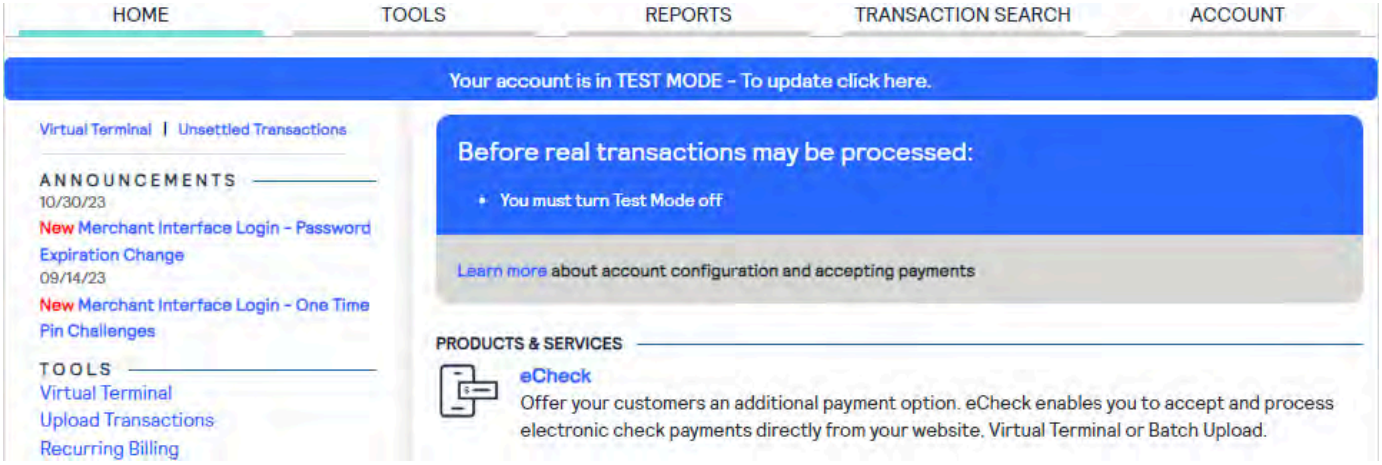
  https://www.authorize.net/resources/blog/2020/accept-payments-through-your-computer.html

Test Mode

Your account defaults to test M=mode, which is indicated by the blue banner at the top of every Merchant Interface page. Test mode enables you to submit test transactions for testing your connection to the payment gateway without submitting a transaction for an actual payment method.

Contact your web or payment solution developer to test your connection to your Authorize.net account. After your connection is successfully tested, turn test mode off to begin processing live transactions. You can switch test mode off by clicking the blue banner.

Example of Merchant Interface in Test Mode



Email receipts for transactions will have a banner at the top of the email body to indicate that the transaction was submitted while your account was in Test Mode.

You can enable Test Mode at any time as a temporary safeguard if you need to stop suspicious activity on your account temporarily.

Warning: Transactions submitted to your Authorize.net account while Test Mode is enabled will not be processed for payment, and they will not appear in your account. Disable Test Mode before you process live transactions.

Changing the Test Mode Setting

Follow these steps to change the test mode setting:

1. Log in to the Merchant Interface at https://login.authorize.net.
2. Choose **Account > Test Mode**.
3. Drag the slider to **Test** or **Live**.

The blue Test Mode banner appears when the slider is set to Test. The banner disappears when the slider is set to Live.

Virtual Terminal

The Virtual Terminal enables you to submit credit card or eCheck transactions to the payment gateway manually through the Merchant Interface. This feature is especially useful if you accept payments for mail order/telephone order (MOTO) sales.

Even though a billing address is not required in order to process a transaction, the default AVS settings of the account will likely decline the transaction unless a billing address is provided or unless the AVS settings have been updated.

If you are using CCV and need to enter the customer's card code, you might need to configure your Virtual Terminal settings to display the card code field. You can configure your Virtual Terminal settings by clicking **Virtual Terminal Settings** at the bottom of the Virtual Terminal page.

Charging a Payment Card

Follow these steps to charge a payment card using the Virtual Terminal:

1. Log in to the Merchant Interface at https://login.authorize.net.
2. Click **Tools**. The Virtual Terminal appears by default.
3. Select **Charge a Credit Card**.
4. Select **Authorize and Capture**.
5. Click **Next**.
6. Enter the customer's payment information in the fields provided.
7. Enter the amount of the transaction.
8. Enter any other customer information in the fields provided.
9. Click **Submit**.

The Transaction Confirmation page shows a Transaction ID that identifies the transaction in your account.

Next Steps

Consider using the following Authorize.net products and services in order to better manage your business:

- Automated Recurring Billing (ARB) enables you to charge customers on a recurring basis. For more details, see the Support Center article, What is Automated Recurring Billing (ARB) and how to use and configure it?
- Customer Information Manager (CIM) enables you to store customer billing information, including payment methods and addresses, securely. For more details, see the Support Center article, What is Customer Information Manager (CIM) and how to use and configure it?
- Invoicing enables you to request payments from customers through a link provided by email. For more details, see the Support Center article, How do I use Invoicing?
- If you process retail transactions where the customer's card is presented in person for payment, you can use Virtual Point of Sale (VPOS) to turn your PC into a point-of-sale terminal. You can also use Mobile Point of Sale (mPOS) to turn your smartphone into a point-of-sale terminal. For more details, see the Support Center articles, Virtual Point of Sale (VPOS) FAQ and Mobile Point of Sale (mPOS) FAQ.
- The eCheck service enables you to process checking information electronically, avoiding the need for paper checks. For more details, see the Support Center article, What is eCheck and how do you apply for it?