Authorize.Net®

Getting Started Guide

Setting Up Your Payment Gateway Account

Table of Contents

Introduction

The purpose of this guide is to provide you with the information necessary to begin processing transactions using your Authorize.Net Payment Gateway account. Once you have activated your account, an Account Owner will need to log into the account to review the default settings and make any necessary changes.

This guide will introduce you to the different settings and features available with your payment gateway account. You should become familiar with these settings as they will help you submit and manage transactions, and otherwise maintain your payment gateway account.

Merchant Interface

The Merchant Interface is a secure website that allows you to access your payment gateway account, manage transactions, configure account settings, view account statements, generate reports and more. It is available from any computer with an Internet connection and web browser—you never need to download or install any software.

We highly recommend you bookmark the Merchant Interface login page at https://account.authorize.net. You can also access the Merchant Interface by visiting the Authorize.Net home page and clicking **SIGN IN,** then **Merchants**.

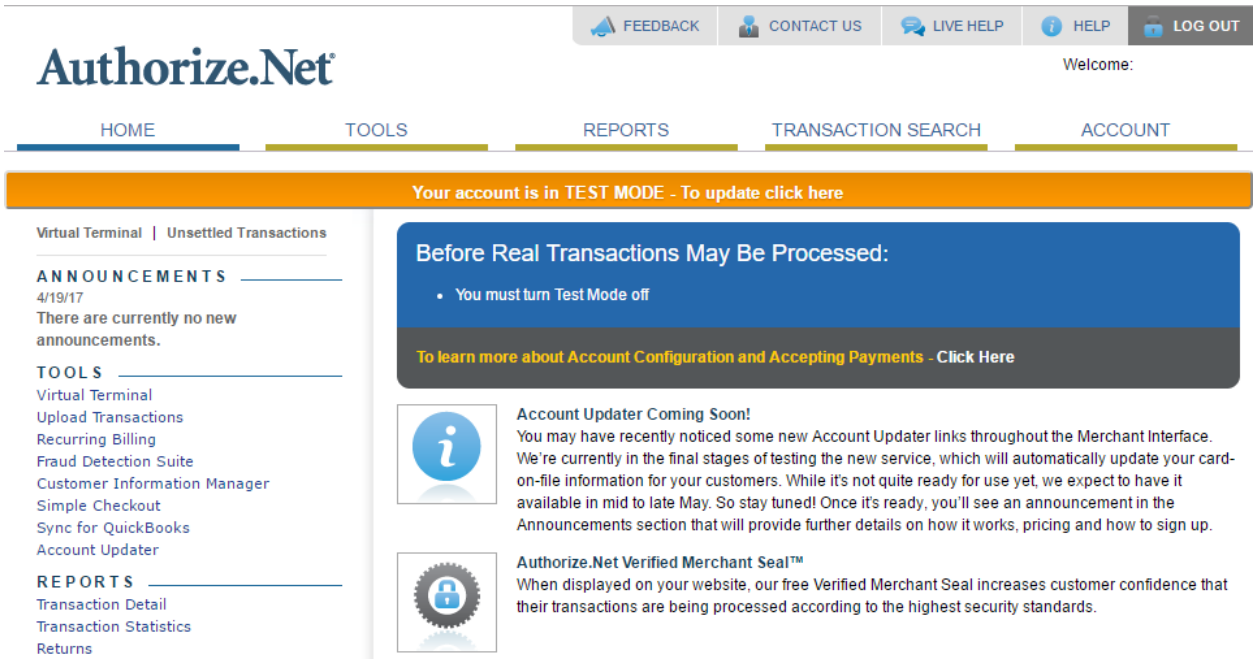
After you have activated your payment gateway account using the activation link from your welcome email, you will automatically be signed into the Merchant Interface.

Test Mode

Once activation is complete, your account is automatically placed in **Test Mode**, which is indicated by the orange banner at the top of every Merchant Interface page. Test Mode allows you to submit test transactions for testing your connection to the payment gateway without actually charging real transactions.

Please work with your web or payment solution developer to test your connection to the payment gateway. Once your connection is successfully tested, you may begin processing live transactions after switching Test Mode off. You can switch Test Mode off by clicking the orange banner.

Figure 1. Example of Merchant Interface in Test Mode



You can also switch Test Mode on at any time as a temporary safeguard in the event that you need to monitor suspicious activity on your account.

To switch Test Mode on or off:

1. Log into the Merchant Interface at https://account.authorize.net.
2. Click **Account** from the main toolbar.
3. Click **Test Mode** under General Security Settings.
4. Drag the slider to **Test** or **Live**.

Remember, you must switch Test Mode off before you can begin processing live transactions.

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, you will need to either provide this information to your web developer, or enter it into your shopping cart or other software integration.

Note:	Your API Login ID and Transaction Key/Signature Key are **not** the same as your Merchant Interface Login ID and password.

API Login ID

The Application Programming Interface (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. As the API Login ID is an essential key for your connection to the payment gateway, you will need to contact Customer Support if you ever need to have it reset.

Transaction Key and Signature Key

There are two types of keys 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 XML and delimited requests. The Signature Key is used to authenticate payment form requests and responses.

You can generate a new Transaction or Signature Key from within the Merchant Interface at any time. As the Transaction and Signature Keys are essential keys for your connection to the payment gateway, **you must notify your web developer or the person that manages your payment gateway connection each time they are updated**. Otherwise your transaction processing might be interrupted.

Creating Your API Login ID and Transaction Key

1. Log into the Merchant Interface at https://account.authorize.net.
2. Click **Account** from the main toolbar.
3. Click **API Credentials & Keys** under General Security Settings.
4. Enter your **Secret Answer** to your Secret Question in the field provided. You should have configured a Secret Question and Secret Answer during account activation.
5. Click the radio button next to **New Transaction Key**.
6. Click **Submit**. The API Login ID and Transaction Key generated for your payment gateway account will appear.

Once you have initially created your API Login ID, you may not change it in the Merchant Interface. To reset your API Login ID, please contact Customer Support.

Note:	You cannot generate a Signature Key for your account until you have generated a Transaction Key using the instructions above.

Generating a New Transaction Key or a Signature Key

1. Log into the Merchant Interface at https://account.authorize.net.
2. Click **Account** from the main toolbar.
3. Click **API Credentials & Keys** under General Security Settings.
4. Enter your **Secret Answer** to your Secret Question in the field provided.

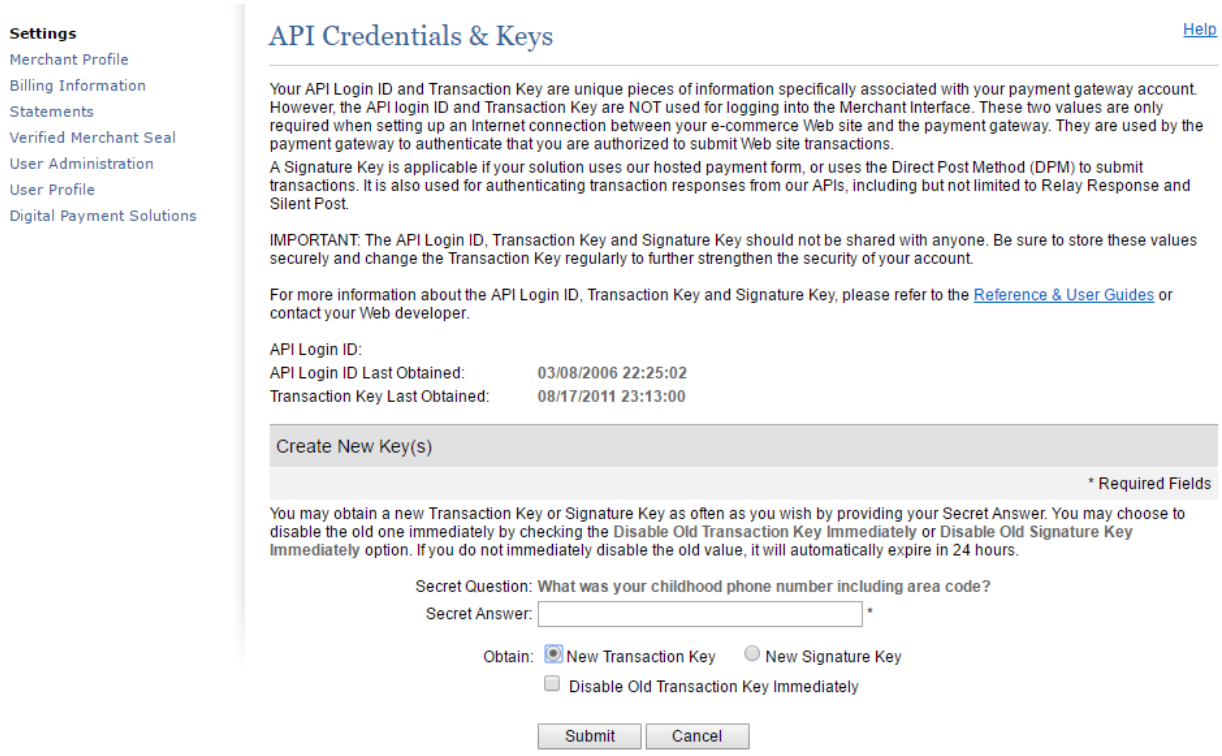
5. Click the radio button next to **New Transaction Key** or **New Signature Key**.

Note:	If the **Disable Old Transaction Key** or **Disable Old Signature Key** check boxes are not selected, the old keys will automatically expire in 24 hours. Disabling them immediately is helpful if you suspect your previous Keys are being used fraudulently.

6. Click **Submit**. Your new key will be displayed.

Be sure to store the Transaction or Signature Key in a safe place and do not share it with anyone, as it is a sensitive piece of information.

Figure 2. Example of API Credentials & Keys Page



Security Settings

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

Address Verification Service

The Address Verification Service (AVS) is a credit 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 credit card issuing bank. AVS then returns a response code indicating the results of the comparison. The payment gateway then accepts or rejects the transactions according to the settings you have specified.

By default, your AVS settings are set to reject any transaction that does not have a street address and/or ZIP code match. All international cards are also rejected by default.

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

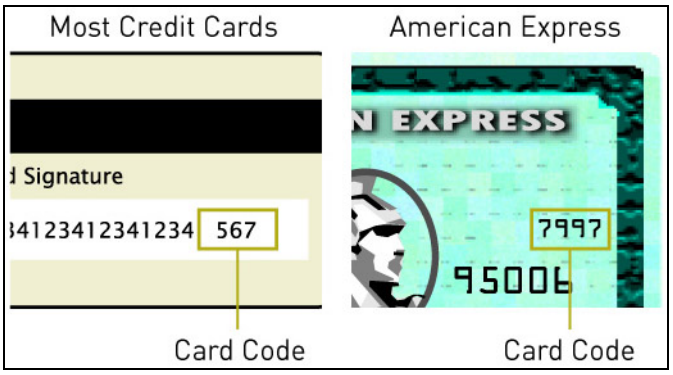
To review and edit your AVS settings:

1. Log into the Merchant Interface at https://account.authorize.net.
2. Click **Account** from the main toolbar.
3. Click **Address Verification Service** under Basic Fraud Settings.
4. Check or uncheck the box next to each AVS response code depending on whether you want to reject or accept those transactions. If you have questions regarding the response codes, please click **Help** at the top right of the page to review the help files, or review the helpful tips at the bottom of the page.

Card Code Verification

Card Code Verification (CCV) is a three- or four-digit security code that is printed on credit cards. The value appears in reverse italic at the top of the signature panel on the back of the card, or for American Express cards, on the front of the card just above the end of the credit card number.

Figure 3. Credit Card Codes



These additional numbers provide an extra measure of security against unauthorized credit card transactions. The customer would need to have the credit card in their possession to know the Card Code number, as it is not stored on any system outside of the credit card issuer. The payment gateway allows you to customize your account so that the system rejects transactions where the Card Code provided by the cardholder is invalid. By using CCV, you are able to make a more informed decision about whether to accept or reject credit card transactions.

To review and edit your CCV settings:

1. Log into the Merchant Interface at https://account.authorize.net.

2. Click **Account** from the main toolbar.
3. Click **Card Code Verification** under Basic Fraud Settings.
4. Check or uncheck the box next to each CCV response code depending on whether you want to reject or accept those transactions. If you have questions regarding the response codes, please click **Help** at the top right of the page to review the help files.

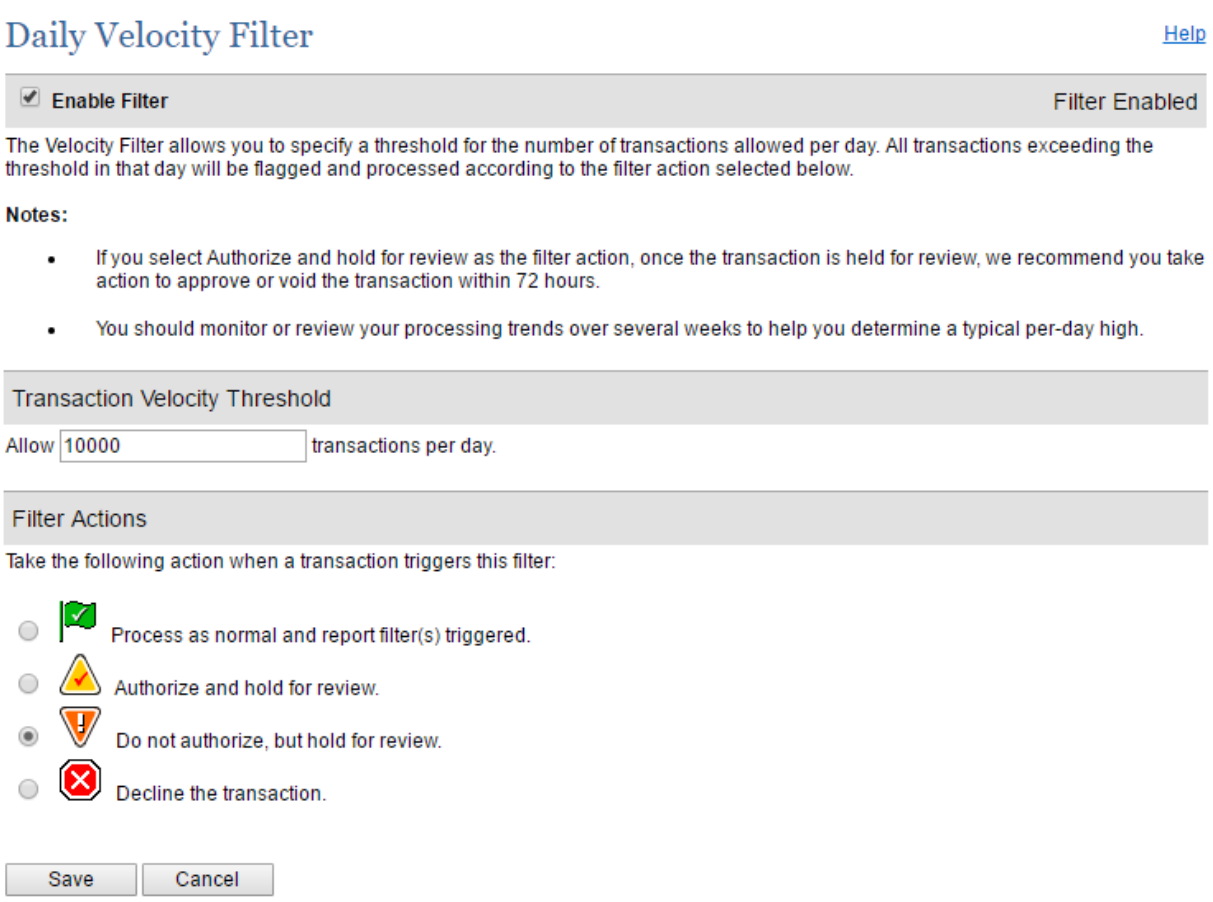
Daily Velocity Filter

The Daily Velocity Filter is a tool that allows you to specify a threshold for the number of transactions allowed per day. All transactions exceeding the threshold in that day will be flagged and processed according to the actions you specify. This is a useful tool for preventing high-volume attacks that are common with fraudulent transactions.

To configure the Daily Velocity Filter:

1. Log into the Merchant Interface at https://account.authorize.net.
2. Click **Account** from the main toolbar.
3. Click **Daily Velocity** under Basic Fraud Settings.
4. Check the **Enable Filter** checkbox.
5. Enter the amount of transactions you want to allow per day in the field provided.
6. Click the radio button next to the action you want to take on any transactions that exceed that amount. If you have questions regarding the actions, please click **Help** at the top right of the page to review the help files.
7. Click **Save**.

Figure 4. Example of Daily Velocity Filter Page



Advanced Security

In addition to the standard payment gateway features above, Authorize.Net also provides the Advanced Fraud Detection Suite™ (AFDS) at no additional cost. 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, click **Tools** from the main toolbar, then click **Fraud Detection Suite.**

General Settings

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

Time Zone

You may configure your payment gateway account to use the time zone in which your business is located. This will allow you to properly configure your Transaction Cut-Off Time (see below) and view accurate statements and reports information.

To review and update the Time Zone:

1. Log into the Merchant Interface at https://account.authorize.net.
2. Click **Account** from the main toolbar.
3. Click **Time Zone** under General Information Settings.
4. Select the appropriate time zone from the drop-down menu.
5. Click **Submit**.

Transaction Cut-Off Time

This setting allows you to specify the daily cut-off time for batched transactions to be picked up and submitted to your processor for settlement. Any transactions entered or successfully authorized after the cut-off time will not be sent to the processor for settlement until the cut-off time the following day. The default Transaction Cut-Off Time is 3:00 PM Pacific time.

To review and update the Transaction Cut-Off Time:

1. Log into the Merchant Interface at https://account.authorize.net.
2. Click **Account** from the main toolbar.
3. Click **Transaction Cut-Off Time** under General Information Settings.
4. Select the desired cut-off time using the Hour, Minute and AM/PM drop-down menus.
5. Click **Submit.**

Changes may not take effect immediately. If transactions have already been settled for the day, then the new Transaction Cut-Off Time will not take effect until the next day.

User Administration

The User Administration feature allows 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—helping you to keep transaction and account management activities in the Merchant Interface separate and streamlining your transaction management processes.

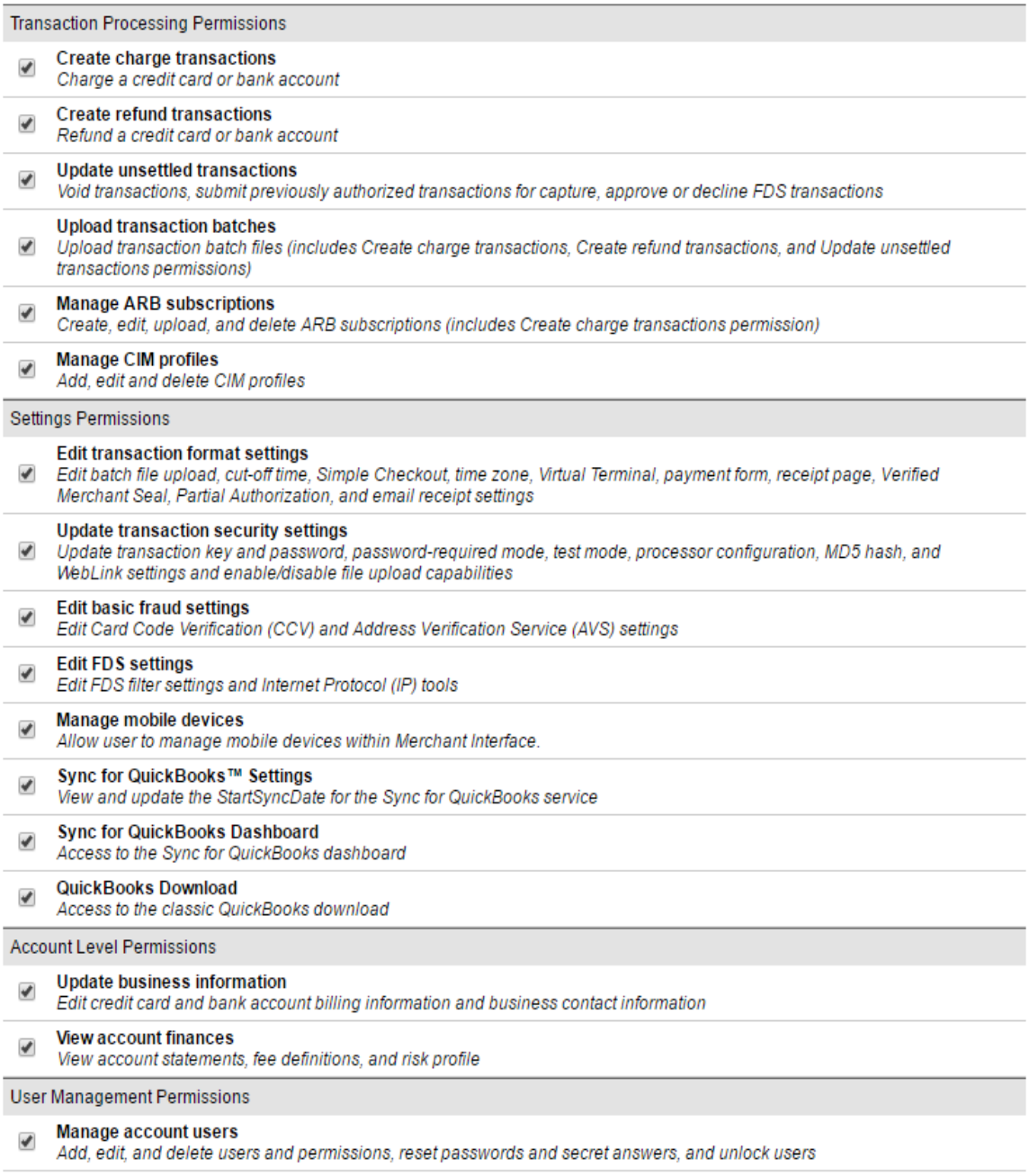
By default, the person who activated your payment gateway account will be an Account Owner. This will also be the only user account until you create additional accounts.

To create additional user accounts:

1. Log into the Merchant Interface at https://account.authorize.net.
2. Click **Account** from the main toolbar.
3. Click **User Administration** from the left side menu.

4. Click **Add User** from the User Administration page toolbar.
5. Select the type of user you would like to add from the **User Role** drop-down menu. Once you select a role, the default permissions associated with that role will be displayed.
6. You can further customize the permissions by un-checking any boxes next to permissions you do not want enabled for the user.

Figure 5. Example of User Permissions



Note: By default, Account Owners have all permissions enabled for their account and may not be customized.

7. Enter the **Secret Answer** to your Secret Question in the field provided at the bottom of the screen.
8. Click **Next** to continue**.**
9. Create a Login ID for the new user. The Login ID must be at least six (6) characters long and should contain a combination of letters and numbers.

Note: Account Contacts cannot access the Merchant Interface so no Login ID is necessary.

10. Enter the user's First Name, Last Name, Title, Phone and Email Address.
11. Check the checkboxes next to each type of email notice you would like the user to receive.
12. Click **Submit**.

Once submitted, a confirmation message will appear which displays the new user's Login ID and temporary password. You are responsible for securely providing the user with their temporary password. When the user logs in for the first time they will be required to change their password.

Virtual Terminal

The Virtual Terminal allows you to submit credit card or eCheck.Net® 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.

To submit a charge transaction using the Virtual Terminal:

1. Log into the Merchant Interface at https://account.authorize.net.
2. Click **Tools** from the main toolbar.
3. Select either **Charge a Credit Card** or **Charge a Bank Account**.
4. Select **Authorize and Capture**.
5. Enter customer's payment information in the fields provided.
6. Enter the amount of the transaction and enter any other customer information in the fields provided.
7. Click **Submit**.

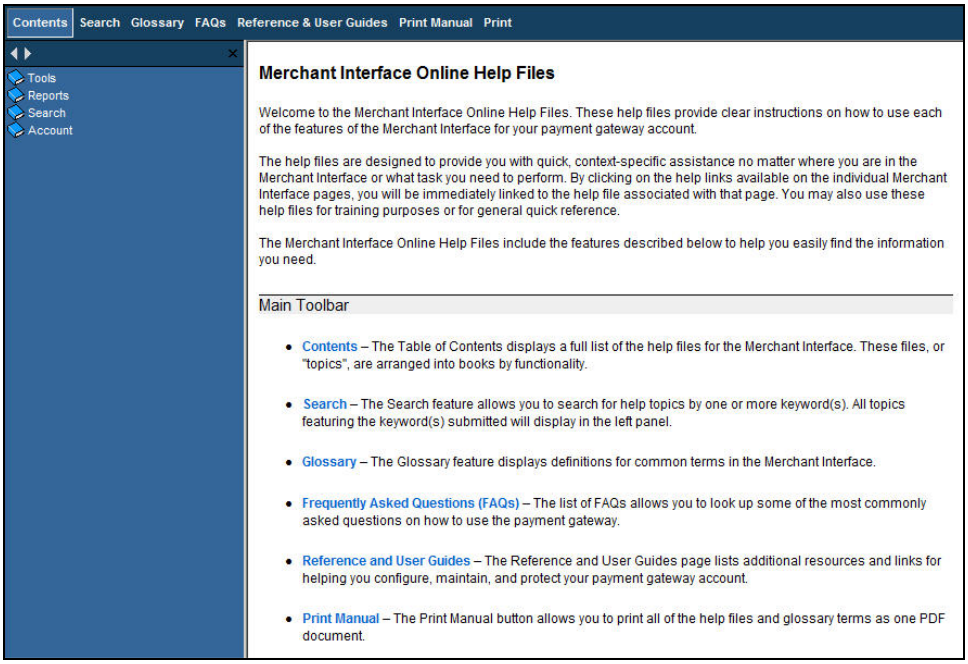
While a billing address is not required to process a transaction, the default AVS settings of the account will likely decline the transaction unless a billing address is provided, or the AVS settings have been updated.

Additionally, if you are using CCV and need to enter the customer's card code, you may 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.

Help Using the Merchant Interface

For help with using the Merchant Interface, and for more information about settings and features, please refer to the Merchant Interface Online Help Files. You can access task-specific help files from any page in the Merchant Interface by clicking the **Help** link located in the top right of the page.

Figure 6. Merchant Interface Online Help Files



Choosing a Connection Method

A connection method is a set of implementation requirements that allows 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 an Authorize.Net Certified Shopping Cart or other certified solution.
- Contact an Authorize.Net Certified Web Developer to handle the integration for you.
- If you or your someone you know have web programming skills or in-house resources, use our flexible and customizable Application Programming Interfaces (APIs) for programming your own connection. Please visit the Authorize.Net Developer Center for integration guides, sample code and more.

- For more information about point-of-sale and mobile payments systems that are already integrated to the payment gateway, see our list of Certified POS Solutions.
- For detailed information and help deciding which connection method you should use, contact your Reseller, web developer or Merchant Service Provider for assistance.
- The free Authorize.Net mPOS mobile application allows 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 http://www.authorize.net/mobile

Maintaining Account Security

Maintaining security for your payment gateway account is the most important way to safeguard yourself and your customers from unauthorized transaction activity. Optimal security, in some cases, can be as simple as using complex system and user passwords, storing them safely, and changing them on a regular basis.

To learn more about how you can enhance and maximize security for your account, please read the *Security Best Practices White Paper* at http://www.authorize.net/files/securitybestpractices.pdf.

Card Present (CP) Merchants

If you are a Card Present (CP) merchant, you can use your existing payment gateway account to accept credit cards using our free, mobile application or the Authorize.Net Virtual Point of Sale (VPOS).

VPOS

VPOS turns any Internet-connected computer into a point-of-sale (POS) terminal with the simple addition of a USB HID MagTek® swipe card reader. VPOS uses your existing Internet connection, eliminating the need for additional phone lines.

For more information on VPOS, including system requirements and available readers, please visit http://www.authorize.net/vpos.

To access the VPOS interface, go to https://anet.vpos.authorize.net and enter your payment gateway Login ID and password. After entering your login information, the system will prompt you to install the ActiveX Control. Every time you use a new computer to access VPOS, you will be prompted to download the ActiveX control.

The ActiveX control is safe and secure, and is designed to ensure that no one will be able to retrieve credit card data from your computer while submitting a transaction. Additionally, the ActiveX control will automatically check for VPOS updates that have been released, ensuring that you are using the most current VPOS version.

Customer Support

Authorize.Net offers several methods for helping you with any questions you may have about your payment gateway account, transaction processing, the Merchant Interface and more.

Authorize.Net Support Center

The Support Center, located at http://support.authorize.net/, is an extensive database of answers to the most common support-related questions. The Support Center also includes a glossary and a form for submitting questions to customer support. We highly recommend using the Support Center for any questions you may have.

Contacting Customer Support

If you still need assistance, you can contact our Customer Support department by logging into the Merchant Interface and clicking **Contact Us** at the top of the page. From there you can click **Live Help** to chat with a support representative, or you can click **Create a New eTicket** to submit a question.

Customer Support representatives can also be reached by phone 24 hours a day, 7 days a week at 877-447-3938. Customer Support is closed on major holidays.