

Getting Started Guide

Table of Contents

Getting Started Guide	1
Table of Contents.....	2
Introduction	3
Help Using the Merchant Interface	5
Choosing a Connection Method	6
Maintaining Account Security	6
Customer Support	7

Introduction

The purpose of this guide is to introduce you to the different account settings and features available in the Merchant Interface. You should become familiar with these settings as they will help you log into your account, submit transactions and otherwise maintain your payment gateway account. Upon activation of your account, you should configure the account settings described in this guide.

Test Mode

Once activation is complete, your account is placed in Test Mode. 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 configure the following settings for your account and to test your connection to the payment gateway. Once your connection is successfully tested, you may begin processing live transactions after turning Test Mode off. (You can access Test Mode from the Merchant Interface Settings menu.)

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

Access Settings

The following settings are required in order to submit transactions to the payment gateway:

API Login ID

The Application Programming Interface (API) Login ID is unique to your payment gateway account and should be submitted with each transaction. It 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. (You can access the API Login ID setting from the Merchant Interface Settings menu.)

Transaction Key

The Transaction Key is also unique to your payment gateway account and can be generated at any time in the Merchant Interface. It is used by the payment gateway to authenticate that transactions submitted for your account are actually being submitted from you. As the Transaction Key is an essential key for your connection to the payment gateway, **you must notify your Web developer or the person that manages your payment gateway connection each time the Transaction Key is updated.** Otherwise your transaction processing might be interrupted. (You can access the Transaction Key setting from the Merchant Interface Settings menu.)

Security Settings

Please configure the following built-in security settings to increase the security of your transaction processing.

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. The payment gateway reports the AVS response code (match or no match). After screening for the AVS response codes that you have specified to allow through AVS, the transaction is accepted or rejected accordingly.

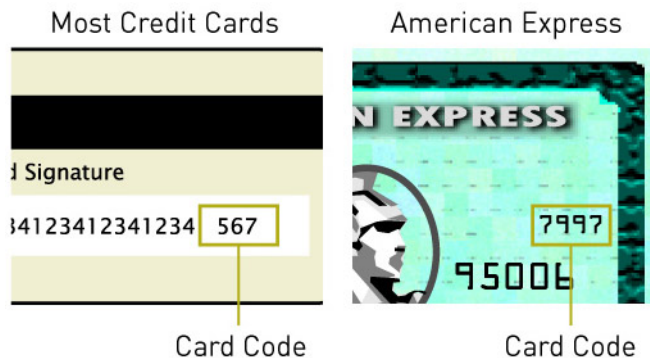
AVS settings are defaulted to reject any transaction that does not have a street address and/or ZIP code match. By default, all international cards are also rejected.

It is recommended that you review and configure these settings in accordance with your business practices. (You can access the AVS setting from the Merchant Interface Settings menu.)

Card Code Verification

The Card Code (CVV2/CVC2/CID) 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 on the front of the card just above the end of the credit card number.

Figure 1. 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 his or her possession in order 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 the Card Code filter, you are able to make a more informed decision about whether to accept or reject credit card transactions. (You can access CCV setting from the Merchant Interface Settings menu.)

Additionally, we strongly recommend that you employ advanced fraud prevention tools and best practices to achieve a maximum level of protection for your account and your transaction processing. You can learn more about recommended security measures in our *Security Best Practices White Paper* at <http://www.authorize.net/files/securitybestpractices.pdf>.

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. (You can access the Time Zone setting from the Merchant Interface Settings menu.)

Transaction Cut-Off Time

This setting allows you to specify the daily cut-off time for batched transactions to be picked up and submitted for processing and settlement. Transactions submitted after the specified cut-off time will be submitted for settlement with the next day's batch. (You can access the Transaction Cut-Off Time setting from the Merchant Interface Settings menu.)

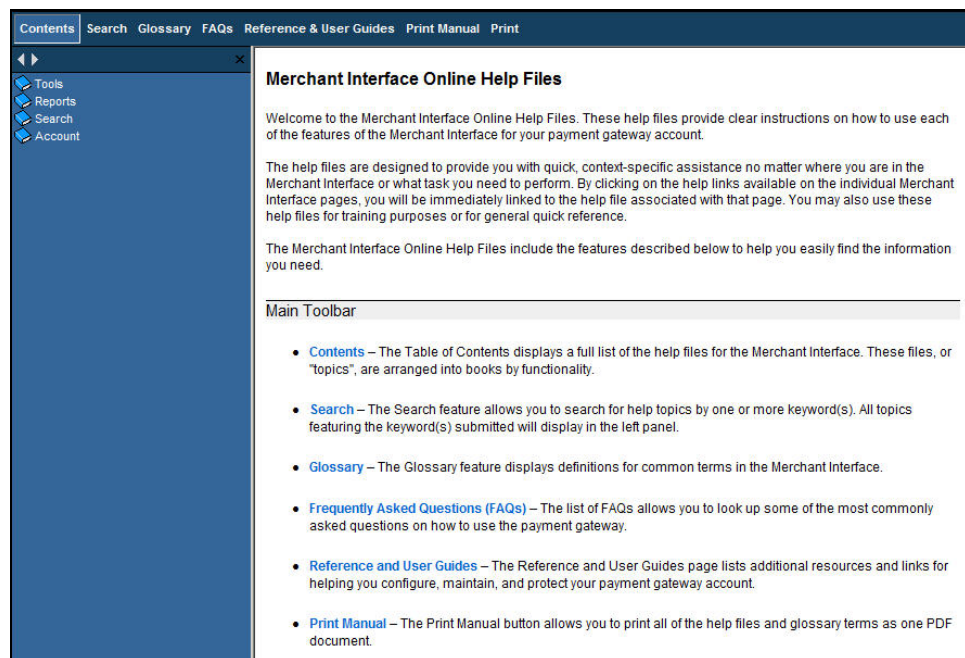
User Administration

The User Administration feature, or Multiple User Accounts, 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 customize permissions for user accounts 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. (You can add, edit, and manage account users in the Merchant Interface User Administration menu. This menu only appears for Account Owners or Account Administrators with user management permissions.)

Help Using the Merchant Interface

To get help 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 task-oriented screen in the Merchant Interface.

Figure 2. Merchant Interface Online Help Files



Choosing a Connection Method

A connection method is a set of implementation requirements that allows you to connect a Web site or other application to the payment gateway for submitting direct transactions.

Depending on your business model, there are several different ways to connect to the payment gateway.

- + Submit transactions manually at any time using the standard Virtual Terminal and Batch Upload features of the Merchant Interface.
- + If you have Web programming skills or in-house resources, use our flexible and customizable application programming interfaces (APIs) for programming your own connection. You can access several Implementation Guides in the Merchant Interface Online Help Files by clicking **Reference & User Guides** in the toolbar.
- + For professional assistance with programming a connection to the payment gateway, see our list of certified developers and solutions providers at <http://www.authorize.net/cdd>.
- + 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 at <http://www.authorize.net/posdir>.

For detailed information and help deciding which connection method you should use, contact your Web developer or merchant service provider for assistance.

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, read the *Security Best Practices White Paper* at <http://www.authorize.net/files/securitybestpractices.pdf>.

Customer Support

For assistance with your payment gateway account or the Merchant Interface, please visit the Authorize.Net Knowledge Base at <http://www.authorize.net/help>. Here you'll find useful information, including:

- + Comprehensive answers to the most common support questions.
- + [Merchant Interface Demos](#) - Tutorials about managing your account.
- + [Help Files](#) - Comprehensive, searchable information.

If you still need assistance, our support representatives are available to assist you via e-mail, online chat or phone at 877-447-3938.

Support Hours: Monday through Friday, 6 AM to 6 PM Pacific time (Closed on New Year's Day, Thanksgiving Day and Christmas Day)