New Connection Method and Payment Gateway Enhancements

Introduction

In an effort to continually improve the functionality and security of the Authorize.Net Payment Gateway for our merchants, Authorize.Net has released several enhancements that affect existing and new merchant accounts. This guide has been designed as a reference to help you understand how recent changes to the Payment Gateway and Merchant Interface may affect the new merchant setup process and the merchant experience with Authorize.Net.

On October 30, 2002, Authorize.Net released a new connection method named Simple Integration Method (SIM). Along with the release of SIM, some additional enhancements have been implemented to improve the merchant's experience with Authorize.Net. These enhancements, along with other recent changes, include:

All Merchants (Existing and New)

- The new connection method, Simple Integration Method (SIM)
- Renaming ADC Direct Response to Advanced Integration Method (AIM)
- Eventual discontinuation of WebLink
- Relocation of the Merchant Menu User's Guide (MMUG) and Developer's Guide from the Authorize.Net Corporate website to inside the Merchant Interface
- One-time survey pages at first login on or after October 30, 2002

New Merchants (Set up after October 30, 2002)

- New merchant account setup in the Reseller Interface
    - The merchant Login ID must comply to Authorize.Net lexical rules
    - Temporary Passwords assigned by Authorize.Net
- Default settings upon activation of Authorize.Net account
- Only SIM and AIM connection methods will be available to new merchants (set up after October 30, 2002)
    - Helping merchants choose a connection method
    - Shopping cart solutions
- Temporary Enable WebLink option for merchants that can't immediately integrate to SIM or AIM due to third-party configurations.

Existing Merchants (Set up before October 30, 2002)

- Disable WebLink option for existing ADC Direct Response merchants

Changes Affecting All Merchants

The New Connection Method, Simple Integration Method (SIM)

Authorize.Net has developed a new gateway connection method. This new method, referred to as Simple Integration Method (SIM), maximizes the security of transactions submitted to the gateway via non-secure sockets layer (SSL) connections while maintaining an intermediate level of web development.

SIM uses robust scripts to encrypt transaction information submitted to the Payment Gateway for processing. Using an encryption matching process, the Payment Gateway authenticates both the origin of the transaction and transaction information. Implementing SIM does not require the merchant to understand or program in scripting languages. However, the merchant must be able to host a script file on their web server. For more information regarding the use of scripts, please direct merchants to the Sample Simple Integration (SIM) Scripts in the Documentation and Reference Guides section of the Help Menu in the Merchant Interface.

ADC-Direct Response Renamed Advanced Integration Method (AIM)

With the release of SIM, and the eventual discontinuation of outdated connection methods, Authorize.Net has renamed ADC ***Direct*** Response (not to be confused with Relay Response) to match the naming methodology of SIM. Moving forward, the ADC Direct Response connection method will be renamed Advanced Integration Method (AIM). However, the integration process does not change with the renaming.

Eventual Discontinuation of WebLink

SIM provides merchants with a superior alternative to the WebLink and Relay Response connection methods. In time, WebLink and Relay Response will be discontinued and transactions will no longer be accepted using these connection methods. For this reason, Authorize.Net encourages all merchants currently using WebLink or Relay Response to plan and prepare for migration to either SIM or AIM (formerly known as ADC Direct Response).

Note: Relay Response is a term sometimes used to refer the transaction **submission** (or connection method) ADC Relay Response. (Transaction submission means how you submit transactions to the Payment Gateway.) Relay Response is also used to refer to a transaction **response** method by which the Payment Gateway relays a transaction response (like a receipt) from the merchant back to the customer.

These are two separate processes. Relay Response, the transaction **response** method, will NOT be discontinued.

Relocation of the Merchant Menu User's Guide and Developer's Guide

The Merchant Menu User's Guide (MMUG) and Developer's Guide have been removed from the Authorize.Net Corporate website and relocated to the Documentation and Reference Guides section of the Help Menu in the Merchant Interface. The MMUG has been replaced with the contextual Online Help Files located in the Merchant Interface. The Developer's Guide has been separated and individual Implementation Guides created for each connection method.

One-Time Survey Pages at First Login

At first login to the Merchant Interface on or after October 30, 2002, the merchant is asked to complete a couple of survey pages about their use of shopping carts and web development tools.

The merchant will is also asked to select a secret question and provide the secret answer to the selected question. Please emphasize to the merchant the importance of remembering and safeguarding the secret answer, as it will be essential to granting them access to certain security features in the Merchant Interface, and is also used to verify the identity of the merchant when calling Customer Support. Also be sure to inform merchants that the secret answer is case sensitive.

Note: For new merchant first-time logins, the survey pages appear after the account setup pages have been verified and completed by the merchant, and after the Service Agreement has been accepted.

Changes Affecting New Merchants

New Merchant Account Setup in the Reseller Interface

When a new merchant is set up in the system, the Reseller-assigned Login ID must be alphanumeric. It should contain both upper and lower case letters and not contain any part of the merchant's business or principal owner information as part of the login. Once a new account setup has been completed in the Reseller Interface, Authorize.Net will assign a password to the new merchant's account. This password is temporary. The new merchant will be prompted to change the temporary password immediately after first login to the Merchant Interface.

Please refer new merchants to the What's New Guide for details regarding password selection and guidelines for password protection.

Default Settings for New Merchants

Newly setup Payment Gateway accounts have certain default settings. The merchant might need to modify these settings to match their business processes and transaction acceptance policies before processing live transactions.

Test Mode

All new Authorize.Net Payment Gateway accounts start out in Test Mode. Test mode secures the merchant's account while testing their integration to the Payment Gateway. Test transactions submitted while the account is in Test Mode are not live, and do not actually charge real credit cards. However, these test transactions will simulate approved and declined responses based on the merchant's configuration as opposed to transaction information, which is the case with live transactions.

Once the integration has been successfully tested, the merchant can turn Test Mode OFF in the Merchant Interface to begin processing live transactions.

Merchants can also use Test Mode as a safeguard from unauthorized account activity. Test Mode can be turned ON at any time to help merchants monitor suspicious activity on their account.

Password-Required Mode

All new Authorize.Net Payment Gateway accounts are configured to Password-Required Mode. When an account is designated as Password-Required, no transaction can be processed without initially providing the account password. This mode prevents transactions from being completed with only the Login ID to validate the merchant.

Password-Required Mode is highly recommended (and will eventually be required) for all Merchants who connect to Authorize.Net via the AIM or SIM connection method. **DO NOT use this feature with the WebLink or Relay Response connection methods.**

Note: To use Password-Required Mode with a shopping cart, merchants should contact their shopping cart provider and request that they enable the cart to pass the Authorize.Net password (or fingerprint for SIM) with every transaction.

Address Verification System (AVS)

Address Verification System (AVS) is a verification system that compares the billing address information provided by the customer online with the billing address on file at the customer's credit card issuing bank. Authorize.Net reports the AVS Response Code to the Merchant (match or no match). After screening for the AVS Response Codes that the Merchant has specified to allow through the address verification system, the transaction is accepted or rejected accordingly.

For newly created merchant accounts, 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.

Only SIM/AIM Available as Connection Methods for New Merchants

To streamline the effort to gradually discontinue the WebLink and Relay Response connection methods, new merchants set up after October 30, 2002 will only be able to integrate to SIM or AIM. The WebLink and Relay Response connection methods will not be available to new merchants for integration to the Payment Gateway.

Helping Merchants Choose a Connection Method

The first thing a new merchant will need to do in order to fully optimize the use of their Authorize.Net Payment Gateway account is choose and integrate to an accepted connection method. Connection methods define the technical requirements for submitting information via the Internet, or a website, to the Authorize.Net Payment Gateway. The current acceptable connection methods are:

1. Simple Integration Method (SIM). Released in part to accommodate for the eventual discontinuation of WebLink and Relay Response, SIM is an increased security option for merchants who cannot establish a secure sockets layer (SSL) connection.
2. Advanced Integration Method (AIM) (formerly known as ADC Direct Response). The preferred connection method, AIM facilitates high security for transactions submitted using a merchant-initiated, direct SSL connection to the gateway.

For detailed information about acceptable connection methods, please direct merchants to the AIM/SIM Conversion Guide or the Implementation Guides for AIM or SIM in the Documentation and Reference Guides section of the Help Menu in the Merchant Interface.

Alternative Hosting Solutions for Merchants

Shopping Cart Solutions

In association with choosing a connection method, shopping carts can be a very viable solution for merchants. Shopping carts are Internet companies that host payment forms for merchant websites. For merchants that cannot easily comply with the highest web development and security requirements of SIM or AIM, shopping carts allow them to submit transactions securely without actually having to upgrade their web systems and security. For more information about shopping carts, view the list of Authorize.Net-certified shopping carts at http://www.authorize.net/alliances/carts.php.

HyperMart QuickCharge

For merchants that cannot easily integrate to SIM or AIM, HyperMart and Authorize.Net have partnered to provide an alternative web-hosting package. QuickCharge allows Authorize.Net merchants to use a HyperMart-hosted payment form for collecting payment information, and submits transaction information securely and directly to the Payment Gateway. For more information about QuickCharge, please see HyperMart's QuickCharge FAQ at http://www.hypermart.net/t/quickcharge/faq.

Enable WebLink Option for Merchants

For those new merchants unable to integrate immediately to SIM or AIM, the option to enable WebLink will be available through the Merchant Interface. This option is to be used as a temporary integration solution for new merchants actively working to integrate to SIM or AIM, and will not be available once WebLink and Relay Response are discontinued.

Authorize.Net strongly discourages Merchants to rely on WebLink. The temporary option to enable WebLink is offered only in an effort to avoid interrupting transaction processing for merchants during the holiday season. Merchants should only use this option if they are using a third-party solution that does not integrate to Authorize.Net via SIM or AIM.

Changes Affecting Existing Merchants

Disable WebLink Option for Merchants using AIM or SIM

For merchants that have completed integration to SIM or AIM, the option to disable WebLink will be available through the Merchant Interface. Disabling WebLink allows the merchant to fully convert to their new SIM or AIM connection method and provides additional security for their account. It is strongly recommended that the merchant disable WebLink as soon as they are successfully processing transactions using SIM or AIM.

WebLink and Relay Response will eventually be discontinued as acceptable Payment Gateway connection methods. Please encourage your merchants to plan and prepare for full integration to AIM or SIM to avoid any possible future inability to process transactions on their Payment Gateway account.

Maintaining Account Security

Maintaining security for the Authorize.Net Payment Gateway account is the most important way merchants can safeguard themselves and their customers from unauthorized transactions or account activity.

Each connection method has several different options for increasing the security of transactions submitted to the Payment Gateway, including Password-Required Mode, Address Verification System (AVS), and Card Code Verification. These options can be selected and configured for a merchant's account through the Merchant Interface.

Optimal security, in some cases, can be as simple as storing a password safely, or changing it on a regular basis. To learn more about how merchants can enhance and maximize security for their account, read the Security "Best Practices" White Paper.

Shopping Cart Certification Program

In conjunction with recent changes, Authorize.Net also announced a Shopping Cart Certification Program (SCC), created to certify shopping carts that integrate to strict Payment Gateway and

transaction security standards. For merchants that cannot easily comply with the highest web development and security requirements of the AIM connection method, Authorize.Net-certified shopping carts allow them to submit transactions securely without actually having to upgrade their web systems and security.

The goal of the SCC Program is to help merchants using shopping carts gain confidence that their shopping cart meets high integration and security standards. Authorize.Net anticipates that the SCC Program will also encourage other existing and new merchants that do not use a shopping cart to integrate to the Payment Gateway using an Authorize.Net-certified shopping cart.

Reseller Support

For questions about Payment Gateway enhancements, or if you have any problems setting up new merchant accounts, please contact Reseller Customer Support at resellersupport@authorize.net. You can also access Support through the Reseller Interface:

1. In the Reseller Interface, click **Support** in the main menu.
2. Enter your question or message in the provided form.
3. Click **Send**. A Customer Support representative will contact you.