PaperCut | Payment Gateway Module Authorize.Net Quick Start Guide

This guide is designed to supplement the *Payment Gateway Module* documentation and provides a guide to installing, setting up, and testing the *Payment Gateway* module for use with Authorize.Net's Server Integration Method (SIM). The main *Payment Gateway Module* documentation may be downloaded from:

http://www.papercut.com/files/pcng/ext/payment-gateway/PaymentGatewayModule.pdf

Authorize.Net is a popular credit card processing gateway solution.

IMPORTANT: *You should have a registered and active Authorize.Net account before installing the payment gateway. The login information will be required during setup.*

Setup and testing time should take around 30 minutes. No system level restart is required; however the PaperCut application server will be restarted during the install process. If other administrators are using the PaperCut administration interface at this time, it may be advisable to warn them of the pending restart.

This document is written assuming the reader has good server administration skills and is experienced with general PaperCut administration.

Contents

Stage 1: Authorize.Net Merchant Interface Configuration 2
Stage 2: Installing the Payment Gateway Module 3
Stage 3: Firewall Configuration 5
Stage 4: Testing 6
Stage 5: Security 7
Stage 6: Go-Live 8
Troubleshooting 9

Stage 1: Authorize.Net Merchant Interface Configuration

1. Ensure that you have a valid and active *Authorize.Net SIM Merchant Account*.
2. Log into the merchant interface at: https://secure.authorize.net
3. Select *Settings* under *Account* in the main menu on the left.
4. Click *Relay Response* in the *Transaction Format Settings* section.
5. Enter a *URL:* of:

   `http://<externalservername>/rpc/gateway/authorize-net`

   Where `externalservername` is the public server name.
6. Click **Submit**.
7. If using *MD5-Hash:*

   a. Navigate to: *Account* > *Security Settings*

   b. Click *MD5-Hash*.

   Enter the secret word/string previously defined under `authorize-net.md5-hash-value` in the `payment-gateway-authorize-net.properties` file.

   c. Click **Submit**.
   Note: The MD5 Hash value is not displayed.
8. If using *SHA-2:*

   a. Navigate to: *Account* > *Security Settings* > *General Security Setting* > *API Credentials & Keys*

   b. In the **Create New Keys** section's **Obtain** field, select **New Signature Key**.

   c. Click **Submit**.
   Note:
   - A security question requiring an answer could be displayed.
   - The new "Signature Key" is displayed. Take note of this and use it when configuring the payment-gateway-authorize-net.properties file.

   d. Navigate to *Account* > *Transaction Format Settings* > *Transaction Response Settings* > *Response/ Receipt URLs*

   e. In **URL,** click the Default Relay Response URL's **Edit**.

   f. In the **Relay Response's Default Relay Response URL** field, enter:
   `http://<PaperCut+MF+Application+Server+IP+address>/rpc/gateway/authorize-net`

g. Click **Submit**.

9. PaperCut Software also recommends that you change other SIM settings such as the page display options include the titles, colors, and styles – The default scheme may be OK, however it may be useful to add some style and branding to the page so it looks like it's an official approved payment page for your organization.

   It is also recommended to disable/turn off the billing and shipping sections of the payment form as these are not relevant for a service that is not invoiced or shipped.

   These settings are changed under *Settings -> Payment Form*, and can be updated any time without affecting the system. Because of this we generally recommend changing these settings after initial testing (see below).

Stage 2: Installing the Payment Gateway Module

1. The Payment Gateway Module will function during the PaperCut NG 40 day trial period. After this, the module must be licensed. If you have been supplied with a new license, take the time to install this now. The license install procedure is documented in the PaperCut user manual chapter 'Licensing and Support'.

2. Download the Payment Gateway module from the PaperCut website at

   http://www.papercut.com/files/pcng/ext/payment-gateway/pcng-payment-gateway-module.exe

3. Install the module into the same directory as PaperCut NG. This is normally

   `C:\Program Files\PaperCut NG`

4. Open the file:

   `[app-path]\server\lib-ext\ext-payment-gateway-authorize-net.properties`

   in a text editor such as Notepad.

5. Locate the line `authorize-net.enabled=N` and change the `N` to `Y`. This will enable the Authorize.Net module.

6. Locate the following lines:

   `authorize-net.login`
   `authorize-net.public-relay-response-hostname`

   `authorize-net.login` is the Authorize.Net "API Login ID" associated with your merchant login account.

   `authorize-net.public-relay-response-hostname` is the hostname that Authorize.Net will connect to, on port 80, when sending its 'Relay Response' with the user's transaction details. Therefore this hostname must be publicly accessible and resolvable from the internet. See the next section for more information about firewall configuration.

7. If using *MD5-Hash*, locate the following lines:

authorize-net.transaction-key is the Authorize.Net “Transaction Key” associated with your merchant login account. It is a token that is known only to PaperCut and the Authorize.Net server and allows Authorize.Net to validate PaperCut’s transaction requests.

authorize-net.md5-hash-value is the Authorize.Net “MD5 Hash Value”, which may be configured in the Authorize.Net merchant interface. It is a token that is known only to PaperCut and the Authorize.Net server and allows PaperCut to validate Authorize.Net’s responses. This secret should be a random word/string of at least 6 characters.
Note: If this is used, ensure to delete the line authorize-net.sha2-hash-value.

8. If using *SHA-2*, locate the following line:

   authorize-net.sha2-hash-value

   authorize-net.sha2-hash-value is the Authorize.Net “Signature Key”, which can be obtained from the Authorize.Net merchant interface. It is a token that is known only to PaperCut and the Authorize.Net server. It allows Authorize.Net to validate PaperCut’s request and allows PaperCut to validate Authorize.Net’s responses. This key should be a random word/string of at least 128 characters.
   Note: If this is used, ensure to delete the line authorize-net.md5-hash-value.

9. Configure other options in this file as discussed in General Configuration Options in the Payment Gateway Module documentation. Options include limits on the amount to transfer, access groups and custom error messages.

10. Save the file and exit Notepad.

11. Restart the PaperCut Application Server service via Control Panel -> Administrative Tools -> Services and wait 30 seconds.

12. Check the end of the file [app-path]\server\logs\server.log for any obvious error messages.

Stage 3: Firewall Configuration

The Authorize.Net server communicates with the PaperCut server via HTTP on port 80. You will need to ensure that the Authorize.Net servers are able to contact the PaperCut server (the hostname configured under `authorize-net.public-relay-response-hostname` in Stage 1) via the internet. This will usually involve the following network changes:

1. Set up a public DNS entry to ensure the PaperCut server is publicly accessible via a friendly name (e.g. papercut.myorganization.org). This will be the same name used for `authorize-net.public-relay-response-hostname` in Stage 1.

2. Ensure no other application is using port 80 on the PaperCut server (e.g. IIS or another web server). To verify this, open the command-prompt (cmd.exe) and type:

   ```
   netstat –na | more
   ```

   Ensure that port 80 is not in a listening state. That is, the following line should not be displayed:

   ```
   TCP  0.0.0.0:80  0.0.0.0:0  LISTENING
   ```

3. Ensure your firewall allows traffic to port 80 on this server. Methods include adding “TCP Open” entry to your firewall and/or using port forwarding.

4. Test and ensure that the following URL is accessible via the public internet:

   http://publicservername/rpc/gateway/authorize-net

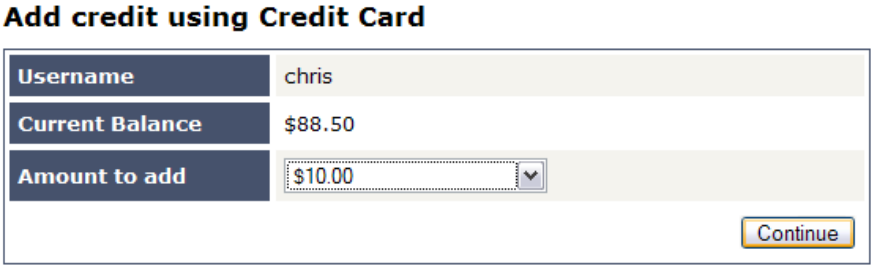
   where `publicservername` is the DNS name set up in step 1. Accessing this URL with a web browser should result in the browser displaying a simple confirmation page.

Stage 4: Testing

The first step is to enable test mode in Authorize.Net. This allows you to test the connection to the payment gateway without actually processing live transactions. **Important:** You *must* remember to turn this off after initial testing!

Log into the merchant interface at: https://secure.authorize.net

1. Select *Settings* under *Account* in the main menu on the left.
2. Click **Test Mode** in the *Security Settings* section.
3. Click *Turn Test ON* to place your account in Test Mode.
4. Log into PaperCut's end-user interface as a standard user (e.g. a test user account, or maybe your personal network account) via the URL: http://internalservername:9191/user
5. A new link called Add Credit should appear on the left. Click this link.
6. Select and amount to add and press Continue.



7. Enter a valid Credit Card number and associated details as requested. Note: Because the account is in Test Mode, your card will not really be charged.
8. Continue and confirm that the value is placed on the user's PaperCut account and the transaction is listed in their transaction history. See the Troubleshooting section if you have any problems.

Stage 5: Security

A confidential security token will provide a high level of security. Administrators may however wish to take further steps to prevent forged postbacks by filtering request by IP address. This can be done either at the application level inside PaperCut or at your firewall or both, and will prevent selected types of brute force attacks by limiting access to the Authorize.Net server only.

In a normal environment, PaperCut developers regard this level of security as overkill; however it's implemented in line with security best practice. You may choose to skips these steps depending on your security priorities.

To apply an IP addressed based filter:

1. Determine the postback IP address used by Authorize.Net by inspecting the log file located at:

   `[app-path]\server\logs\payment-gateway\event.log`

2. Open the file:

   `[app-path]\server\lib-ext\payment-gateway-authorize-net.properties`

   In your preferred text editor (e.g. Notepad).

3. Change the value `authorize-net.allowed-ip=` to the IP address discovered in step 1.

Note: The Authorize.Net IP address may change. It is recommended that you expand the IP range a little further by entering a mask similar to the following:

```
authorize-net.allowed-ip=64.94.118.33/255.255.255.0
```


Stage 6: Go-Live

1. Log into the merchant interface at: https://secure.authorize.net
2. Select *Settings* under *Account* in the main menu on the left.
3. Click **Test Mode** in the *Security Settings* section.
4. Click *Turn Test OFF* to place your account in production mode.

Your system is now live and will accept and charge real Credit Cards.

Troubleshooting

Administrators may find information in the following log files useful when trying to troubleshoot setup/configuration problems or issues reported by end-users.

Payment Gateway Event Log:
`[app-path]\server\logs\payment-gateway\event.log`
This log contains gateway specific error messages and events.

Application Log:
`[app-path]\server\logs\server.log`
This log contains general application specific error messages and events.

Transaction Log:

`[app-path]\server\logs\payment-gateway\transaction.log`

This log contains a list of successful transactions in a tab-delimited form.

Contact your reseller or Authorized Solution Center for assistance. You can find their contact information in your PaperCut Admin interface on the **About** page.