

Authorize.Net

Advanced Integration Method

Miva Merchant Module

Documentation for module version 1.43

Last Updated: 5/07/03

Module and documentation created by 4TheBest.net

Authorize.Net Advanced Integration Method – Miva Merchant Module

This document describes the configuration and use of the module itself, and assumes the reader has a familiarity with the use of the Miva Merchant administration and runtime interfaces.

This documentation is for the `anaim.mv` and `anaim.mvc` modules that work for Miva Merchant versions 2.22+, 3.x, and 4.x

In versions of Miva Merchant below 4.14 the non-compiled `anaim.mv` file should be used, in versions of Miva Merchant 4.14 and above the compiled `anaim.mvc` file should be used.

Module Installation

This module is installed according to the normal method of module installation as outlined in Miva's documentation for the administrative interface.

The module requires no special additional files such as return scripts or commerce libraries, but it does require that the site is running **Miva Empresa version 3.94 or higher** and is configured properly to use SSL communications at the Miva script programming level.

It is recommended you consult with your host prior to installation to make sure they have the site configured properly. You can email your host's support department the information below and they should be able to understand it.

There are three Miva configuration directives that relate to ensuring that Miva Empresa 3.94 – 3.96 will work with SSL properly at the programming level. They are:

- 1. openssl**

The full path to where Miva Empresa can find the `libssl.so` file.

- 2. openssl_crypto**

The full path to where Miva Empresa can find the `libcrypto.so` file.

- 3. cadir**

The full path to the directory where Miva Empresa can find the SSL certificate files.

Here is an example of what the configurations might look like in the `miva.conf` configuration file:

```
cadir=/usr/local/miva/certs
openssl=/usr/lib/libssl.so
openssl_crypto=/usr/lib/libcrypto.so
```

In addition you need to make sure that the files that Miva Empresa is expecting actually exist in those locations. The `libssl.so` and `libcrypto.so` most likely already exist on the server and you just

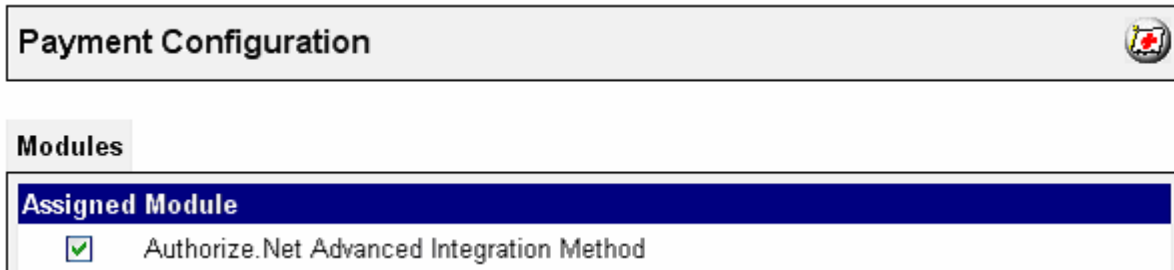
need to find where they are, or you can get them as part of the OepnSSL distribution from the OpenSSL Project website at <http://www.openssl.org/>.

For the “cadir” you need to take a copy of the "certs" directory that ships in the tar file for the Miva Empresa version 3.94 or higher distribution that is installed and put it in some sensible location such as parallel to the "lib" directory that contains the commerce libraries and then reference that directory as the "cadir".

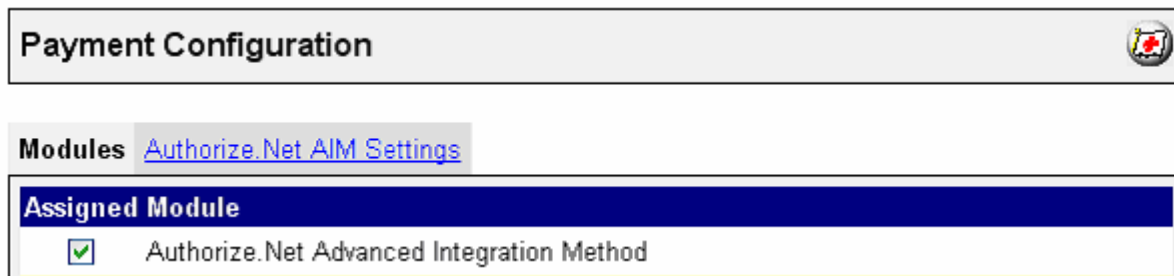
Special Note: Miva Empresa, 3.96, has several important fixes, see: <http://www.miva.com/docs/empresa/RelNote396.pdf> and even though the module runs fine under version 3.94 we recommend that you use version 3.96 for general performance and stability reasons.

Module Setup

The module is enabled at the store level by checking the box next to Authorize.Net Advanced Integration Method and pressing the Update button.



Once the module has been enabled a new tab will appear called “Authorize.Net AIM Settings”.



This new tab is where you will find all the configuration options for the module.

Payment Configuration



[Modules](#) **Authorize.Net AIM Settings**

[Check for Updates](#) | [Buy Modules](#) | [Help](#)

Please enter the license you received when purchasing this product.

Note: you need a separate license for each store.

License Number:

END USER LICENSE AGREEMENT FOR 4THEBEST.NET SOFTWARE

IMPORTANT - READ CAREFULLY

This 4THEBEST.NET End-User License Agreement ("EULA") is a legal agreement between you (either an individual person or a single legal entity, who will be referred to in this EULA as "YOU") and K1 Enterprises, Inc. DBA 4THEBEST.NET ("4THEBEST.NET") for the software that accompanies this EULA, is the software for which the documentation that contains this EULA pertains, or is the software YOU were

By checking the preceding box I state that I have read and agree to the EULA above.

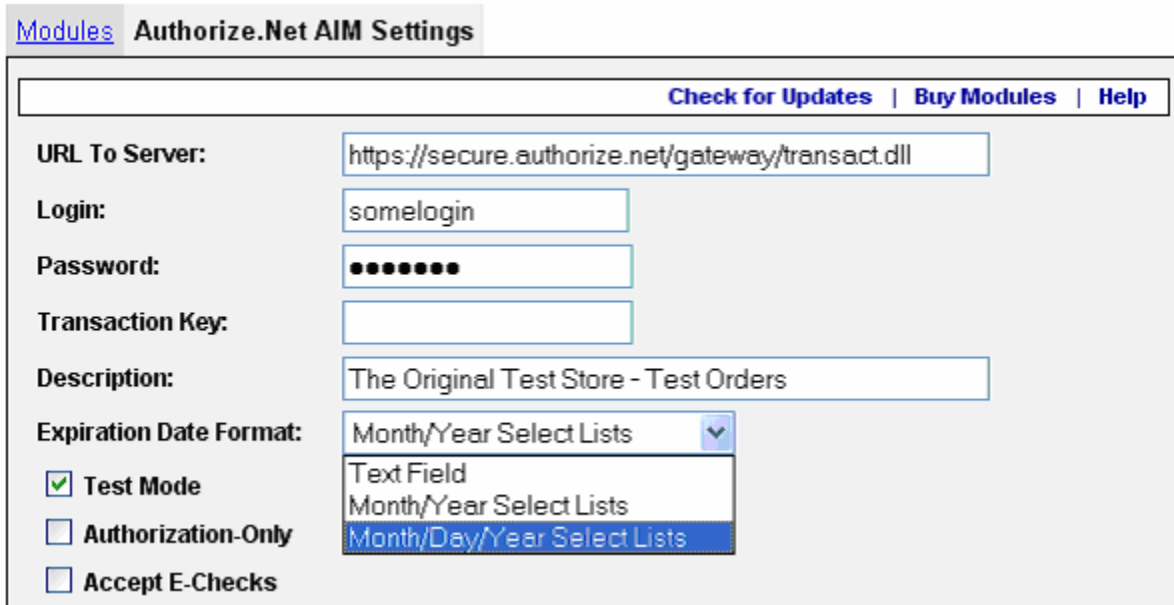
Update

Reset

When you first go to this tab, you will be required to enter a valid license number for the product that was issued to you, read and agree to the End User License Agreement, check the box confirming that you have done so, and then click the update button. Naturally if you don't agree to the EULA then you shouldn't check the box, and thus are not allowed to use the software.

After clicking on the Update button, and assuming there were no errors, such as a warning that you didn't confirm your reading and agreement to the EULA or a warning that you entered an invalid license number, you will then see the configuration options appear as described below. This will be the screen you will see when clicking on the settings tab from then on.

Administrative Interface Payment Configuration



Modules Authorize.Net AIM Settings

Check for Updates | Buy Modules | Help

URL To Server:

Login:

Password:

Transaction Key:

Description:

Expiration Date Format:

Test Mode

Authorization-Only

Accept E-Checks

The first portion of the configurations is as follows.

URL To Server

This is the secure URL to the Authorize.Net transaction server. The default should not need to be changed.

Login

This is the login name for your Authorize.Net account.

Password

This is the password for your Authorize.Net account. IT will be sent for all transactions unless a Transaction Key has been set.

Transaction Key

The transaction key will be sent instead of the password if it is present. You should only use this option if your account is configured to use Transaction Key.

Description

This is an option field that can contain a description that will be sent to Authorize.Net during transactions and can be useful for quickly determining which transactions were placed via the Miva Merchant software and which ones were placed directly through your Authorize.Net virtual terminal. A good example would be something like “Your Store Name Miva Merchant Transactions”

Expiration Date Format

This is where you choose the format you want to use to gather the expiration date from the shopper. There are three options.

Text Field

Use this if you want a single “Expiration Date:” field that the shopper could type the date in using any of the following valid formats: MMY, MM/YY, MM-YY, MMYYY, MM/YYYY, MM-YYYY, YYYY-MM-DD, or YYYY/MM/DD. The advantage to this is it is more compact, and allows for easy entering of any of the valid formats. The disadvantage is that a shopper can easily make a mistake.

Month/Year Select Lists

Use this format to provide two drop select lists labeled “Expiration Month” and “Expiration Year”. The advantage to this is that it is easy to use and less likely for a customer to make a mistake. The disadvantage is that for cases where a card has an expiration date that includes a day, as in “11/18/04”, the shopper might be confused and possibly the validation on the back-end might have a problem.

Month/Day/Year Select Lists

Use this method to display three select lists labeled “Expiration Month”, “Expiration Day”, and “Expiration Year”. The month and the year are required but the “Day” allows the shopper to choose an option of “None”. If the day is selected then the expiration date is sent to the transaction server in the form “YYYY/MM/DD” otherwise it is sent as “MM/YYYY”

Test Mode

This box should be checked only when you want to place a test transaction via Miva Merchant. Test transactions do not actually charge the credit card, and in fact you can even use certain special fake credit card numbers such as a the fake Visa card number 4111111111111111.

Authorization-Only

When this option is checked the transaction placed during the Miva Merchant checkout procedure will be an Authorize-Only transaction. Such transactions do not actually get captured and no funds are transferred unless you later process the order via the Miva Merchant order processing system, or directly via the virtual terminal.

This is useful when you want to make sure the customer has a legitimate card and sufficient funds, but you may need or want to wait to finalize the transaction later. This would commonly be used if you accept orders online for items that make days or weeks to prepare for shipping. If you don't capture the transaction within 30 days it will expire.

NOTE: The AIM module sends the all the vital information to Authorize.Net in real time, such as the credit card number, card code, and expiration date, and does not store it on your website. It gets back a special transaction Id from Authorize.Net that is used later when processing which allows you to process the order later without the need for storing the card number, card code, etc.

This provides you and your customers with a higher level of security without limiting functionality.

Accept E-Checks

With this option checked the system will offer your customers the option to pay with electronic checks. This will only work if your Authorize.Net and Merchant accounts are setup to accept the E-Check ACH transactions.

Credit Card Settings

The next section of configuration options are related to what types of credit cards you want to accept and whether you want to request Card Code (CVV2) numbers during checkout.

Credit Card Settings		
Card Type	Accept Card	Request CVV2
Visa	<input type="checkbox"/>	<input type="checkbox"/>
Mastercard	<input type="checkbox"/>	<input type="checkbox"/>
American Express	<input type="checkbox"/>	<input type="checkbox"/>
Discover	<input type="checkbox"/>	<input type="checkbox"/>
Diner's Club	<input type="checkbox"/>	<input type="checkbox"/>

In the left hand column are listed the available card types. Which cards you can accept depends on your Authorize.Net and merchant account settings. The check boxes in the next two columns determine whether you will display the card as an option for payment during checkout and whether you want the system to request a CVV2 card code.

If you enable a card type but don't request CVV2 then the customer will only be given the option to enter their card number and expiration date. If you request CVV2 then a card code field will be displayed that the shopper can enter their card code into. Even if you request CVV2 it won't mean that the customer has to supply it. Depending on your Authorize.Net settings, and the card the shopper is using, the transaction server may allow a transaction even without a CVV2 card code. This is a good thing, because then you don't stop people from purchasing if they have cards that really don't have a CVV2 card code, and yet you have the control via your Authorize.Net settings to reject transactions from those cards that should have a CVV2 card code assigned to them, but that the shopper hasn't given you.

Payment Information Screen Messages

The last three configuration options are related to messages displayed during the checkout process.

Payment Screen Message



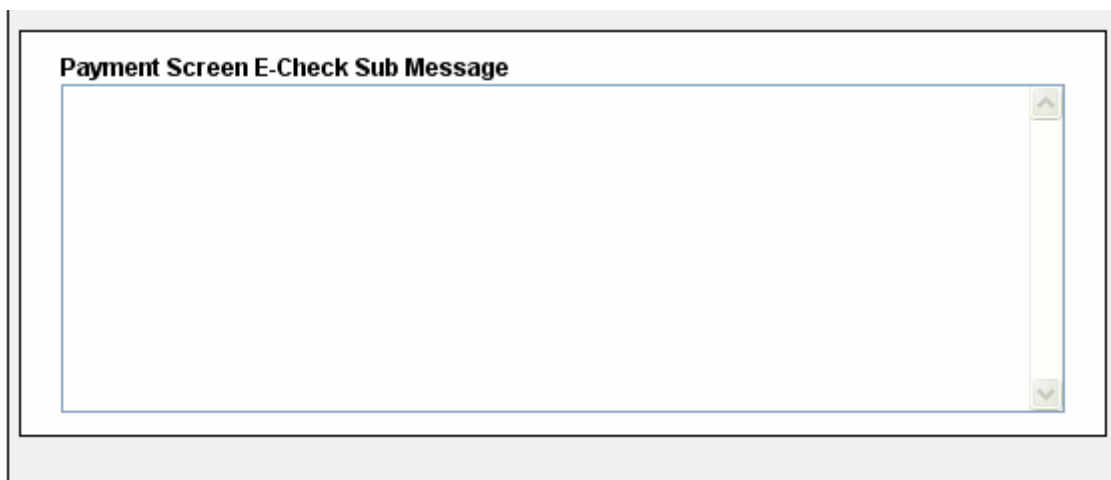
The first configuration is the Payment Screen Message. This is intended contain the basic text or html code for the message to be displayed when a shopper is about to enter the payment information. So if you simply wanted to tell shoppers that you don't charge the card right away, but will charge it later when you ship the product you could enter that here. Also if you are requesting CVV2 card codes you might want to give the customer some instructions on where to find the card codes on their credit cards.

Because it is reasonable for some merchants to want to give different information about what to do depending on whether the customer has chosen a credit card for purchase or the E-Check option, the message can contain a special token called `%submessage%` which will be replaced automatically with the text/html configured in the next two options.

NOTE: All the messages also accept a token called `%paytype%` which will be replaced with the payment type that the shopper chose. The possible types are Visa, MasterCard, American Express, Discover, Diner's Club, or Check

This is the same value that will appear on the payment information screen if no payment message is configured.

Payment Screen E-Check Sub Message



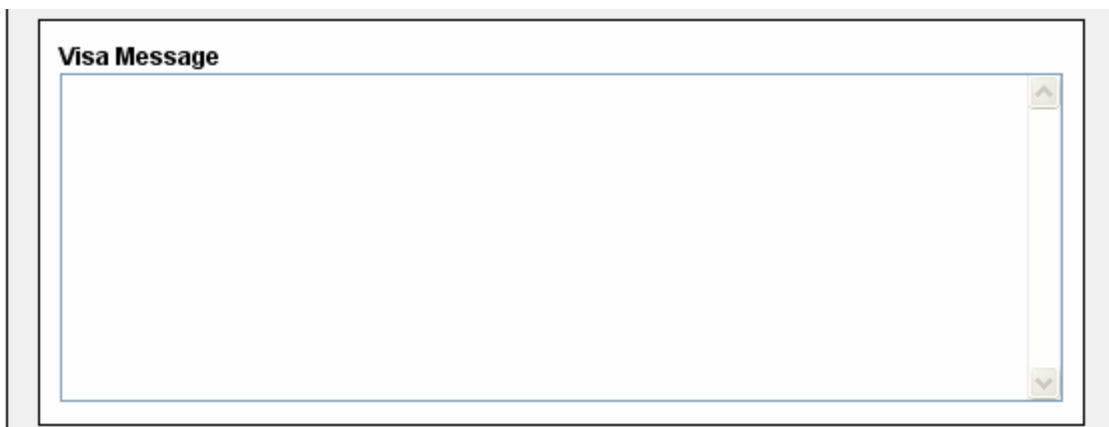
This is where you would place text or html related to the use of the E-Check option. For example you could explain where someone would be likely to find the account number and routing number on a physical check so they would know what numbers to enter when they are requested. You could even include the html code to display an image of a check with the routing and account numbers circled in red. Obviously you would need to create such an image and it would be advisable to use a fake check with phony routing and account numbers.

Payment Screen Credit Cards Sub Message



The image shows a rectangular text area with a light gray border. At the top left, the text "Payment Screen Credit Cards Sub Message" is displayed in bold. Below it, in a smaller font, is the placeholder text "(Accepts Card Type Message Token %typemessage%)". The rest of the area is empty, with a vertical scrollbar on the right side.

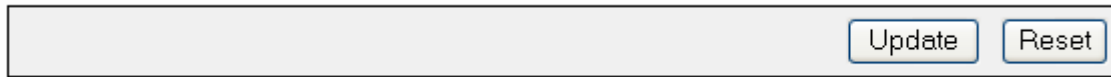
This sub message would be used to describe your credit card specific instructions or information for the shopper. Here is where you might want to explain about CVV2 Card Codes, or your policy on refunds, or whatever you want related to credit card processing. This screen also accepts a token of %typemessage% which will be replaced with the Credit Card specific message for the card the shopper selected.



The image shows a rectangular text area with a light gray border. At the top left, the text "Visa Message" is displayed in bold. The rest of the area is empty, with a vertical scrollbar on the right side.

The above is an image of the "Visa Message" field. The software has a field to contain a "Type Message" for each of the five supported cards.

Updating Changes To The Settings

A horizontal rectangular box containing two buttons: "Update" and "Reset".

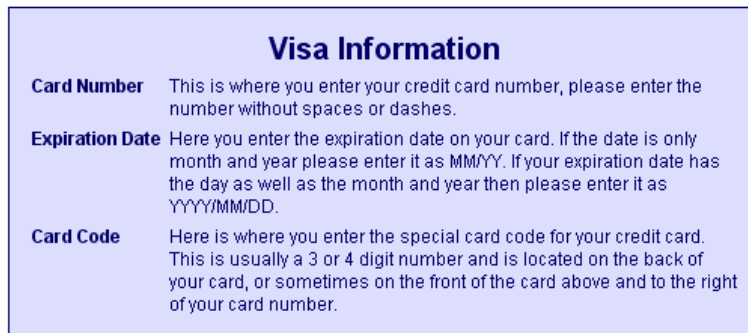
When the settings are as you wish them click the update button and the settings will be saved to the Miva Merchant databases.

Store Front Payment Information Fields

The following is information on fields displayed in the storefront that are seen by the shopper. The exact manner in which the fields are displayed depends on the user interface module being used. Our examples here are using the standard Miva Merchant Look & Feel module that ships with Miva Merchant.

Credit Card Fields

Payment Information:

A light blue rectangular box with the title "Visa Information" centered at the top. Below the title, there are three rows of text, each starting with a bold label followed by a description:

- Card Number** This is where you enter your credit card number, please enter the number without spaces or dashes.
- Expiration Date** Here you enter the expiration date on your card. If the date is only month and year please enter it as MM/YY. If your expiration date has the day as well as the month and year then please enter it as YYYY/MM/DD.
- Card Code** Here is where you enter the special card code for your credit card. This is usually a 3 or 4 digit number and is located on the back of your card, or sometimes on the front of the card above and to the right of your card number.

Three input fields are shown, each with a label to its left:

- Card Number:** followed by a long, empty text input field.
- Expiration Date:** followed by a short, empty text input field.
- Card Code:** followed by a short, empty text input field.

The portion of the above screen shot with the light blue background comes from the configured payment screen message and credit card sub message as configured in the admin interface. The word "Visa" appears where it does because the %paytype% token was used. The fields that appear in the screen shot, and the text of the message itself, only appear if the shopper chose a credit card. The fields here are a follows.

Card Number

This is the credit card number for the account.

Expiration date

This is the expiration date for the account. In our example payment message we told the shopper to use an expiration date format of either MM/YY or YYYY/MM/DD, but this was merely our attempt to make it easy for the customer to choose a valid formatted date. The AIM system actually supports all the following expiration date formats: MMY, MM/YY, MM-YY, MMYYYY, MM/YYYY, MM-YYYY, YYYY-MM-DD, YYYY/MM/DD But making all those options known to the shopper might simply confuse them.

Card Code

The Card Code, or CVV2 code, will only appear as an option if you have configured it to appear in the admin interface. As our example indicates to the customer this is the extra validation number that is found on the back of many credit cards or on the front for some cards like American Express.

Check Payment Fields

If the shopper chose the “Check” option they would see a very different set of payment information.

Payment Information:

Please fill out the fields below. For more information on what each field means please refer to our [Electronic Check Payment Information](#) page.

Bank Account Type:

Bank ABA Code:

Account Number:

Customer Type:

SSN/FTID:

Drivers License Number:

State Of Issue:

Date Of Birth:

The first big difference is that the message is basically a one liner with a link to a separate html page with more information. This different message appears because the E-Check Sub Message was configured differently than the check message.

The fields that appear are:

Bank Account Type

This is a choice of either Checking or Savings.

Bank ABA Code

This is the routing number for the bank. This is normally a 9-digit number that appears on the bottom of a physical check.

Account Number

This is the account number for the shopper's bank account.

Customer Type

This is either Individual or Business

SSN/FTID

This is the field for either the shopper's social Security Number or the company's Federal Tax ID Number. If the Customer type is Individual then they enter a SSN, if the type is Business, then they enter the FTID. The shopper must enter all the fields previous to this field, but if they fill out this field then they don't need to fill out the remaining fields. If they don't want to give out their SSN then they must enter all the following fields instead.

Drivers License Number

This is the Drivers License Number for the account holder.

State Of Issue

This needs to be the state that issued the license.

Date Of Birth

This needs to be the date of birth on the license.

Order Processing

If a transaction was sent using the Authorize-Only option then it is possible to capture that authorization via the Miva Merchant order processing system. You simply create a batch as normal, and then on the Process Orders screen for the batch you click the "Process" button and if that order was placed using the Authorize-Only option then a new communication is sent to the transaction server to capture the order. If the Authorize-Only option wasn't set then the "Process" button simply marks the order as processed in the same manner as the "Mark As Processed" button does.

Note that no credit card number is stored locally after an Authorize-Only transaction and yet the capture of that order still captures funds on the same card. This is because the module uses the transaction id from the Authorize-Only transaction and sends that back to the transaction server so that the transaction server knows what credit card authorization to capture.

Under no circumstances does the module store complete credit card numbers or Card Codes. For cross reference purposes the module does store the last four digits of a credit card number with the rest of the numbers replaced with "X" characters.