

QwkGuard

Fraud Protection and Auto-Lockout System

Miva Merchant Module

Documentation for module version 1.00

Last Updated: 5/1/2003

QwkGuard - Fraud Protection and Auto-Lockout System

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 qwkguard.mv and qwkguard.mvc modules that work for Miva Merchant versions 2.22+, 3.x, and 4.x

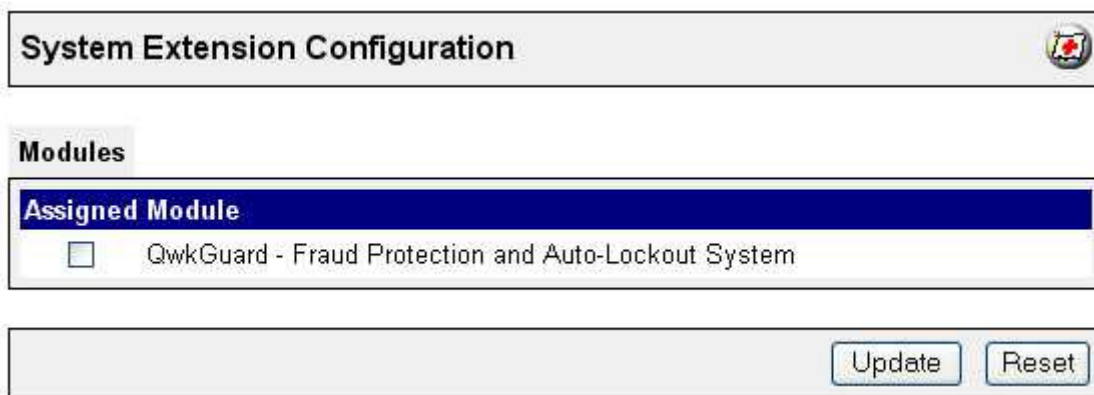
In versions of Miva Merchant below 4.14 the non-compiled qwkguard.mv file should be used, in versions of Miva Merchant 4.14 and above the compiled qwkguard.mvc file should be used.

Module Installation

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

Module Setup

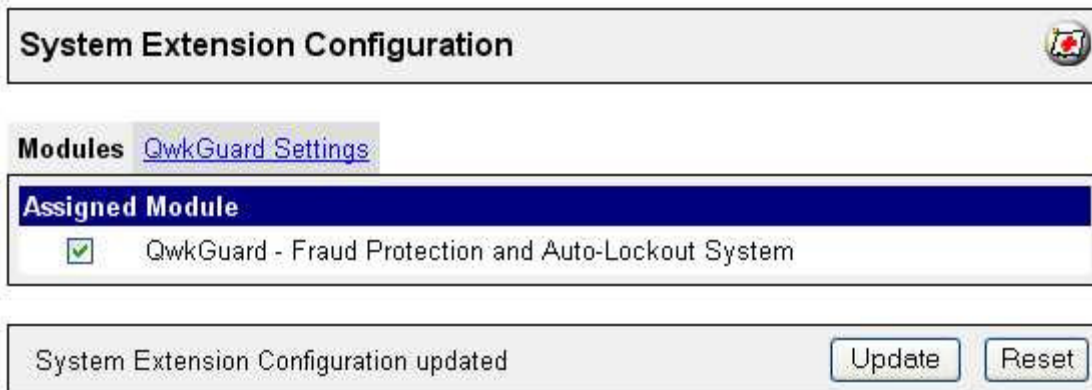
The module is enabled at the store level by checking the box next to "QwkGuard - Fraud Protection and Auto-Lockout System" and pressing the Update button.



The screenshot shows a web interface for "System Extension Configuration". It features a "Modules" section with a table of "Assigned Module". The table has one row with a checkbox and the text "QwkGuard - Fraud Protection and Auto-Lockout System". Below the table are "Update" and "Reset" buttons.

Assigned Module	
<input type="checkbox"/>	QwkGuard - Fraud Protection and Auto-Lockout System

Once the module has been enabled a new tab will appear called "QwkGuard Settings".



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




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.

System Extension Configuration

System Extension Configuration 

[Modules](#) **QwkGuard Settings**

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

Activate QwkGuard

Tries:

Period:

Lockout:

Check Session ID

Check IP Address

Reset Lock

Lockout Message:

Send Email On Lockout

Email Frequency:

Email From:

Email To:

Email CC:

Email Subject:

The settings are as follows.

Activate QwkGuard

Check the box to enable the module, or uncheck it to temporarily disable the module.

Tries

This is the number of times within a given period of time that a shopper can attempt or complete a transaction without being subject to a lockout.

Period

This is the period of time during which the number of tries must be exceeded to cause a lockout to occur.

Lockout

How long, in seconds, someone will be locked out if a lockout occurs.

Check Session ID

With this option selected the system will attempt to detect multiple transaction attempts by cross-referencing the Miva Merchant Session ID.

Check IP Address

With this option selected the system will attempt to detect multiple transaction attempts by cross-referencing the IP Address of the shopper.

NOTE: You can use both Session ID and IP Address to detect duplicate transaction attempts but you must use at least one, and the checks are done in order, first the session ID and then the IP address. This order is important because in theory the Session ID if available is more guaranteed to accurately tie multiple transaction attempts together whereas it is possible that two different shoppers could both get issued the same IP Address although it is unlikely. For this reason the Session ID will be checked first and only if no match is found will the system check the IP Address.

Reset Lock

If this options is enabled then every additional transaction attempt after a lockout resets the lockout time. Thus if the lockout time were only 60 seconds but the hacker was using a program to resubmit the requests over and over, they lockout would keep them locked out the entire time as long as their transaction requests came as frequently as the lockout time. If the option were turned off then after the lockout time elapsed the system would let the next transaction attempt to go through even though the hacker had been attempting to put through new transactions during the lockout period.

Lockout Message

This is the message that will appear when someone is locked out. The error appears on payment information screen in the store. Here is an example of what this would look like.

Unable to authorize payment: Account locked due to excessive activity.

Ship To:		Bill To:	
Name:	Test Tester	Name:	Test Tester

NOTE: the text entered into the “Lockout Message” in the settings is what appears after the colon above. It is also possible to have no error message entered. When no error message is entered then Miva Merchant by default will display no colon and no additional error information beyond the “Unable to authorize payment.” Here is what it would look like if you left the “Lockout Message” blank:

Unable to authorize payment.

Ship To:		Bill To:	
Name:	Test Tester	Name:	Test Tester

The main reason why you might want to do this is to give as little information as possible to a hacker. If they saw a message like the above they would not know why the transaction failed. In a similar vein you could try using a fake message that matches one of those returned from your payment gateway to confuse the hacker.

Send Email On Lockout

Check the box to have the module send emails when lockouts occur.

Email Frequency

The number of seconds you want between the sending of lockout emails. If you set this to 0 then every lockout will trigger an email. If you set it to 3600 you would be limited to one email an hour about the given lockout that triggered the email. If you set it to 86400 you would be limited to one email a day about the given lockout that triggered the email.

Email From:

Check the box to have the module send emails when lockouts occur.

Email To:

Check the box to have the module send emails when lockouts occur.

Email CC:

Check the box to have the module send emails when lockouts occur.

Email Subject:

Check the box to have the module send emails when lockouts occur.

The email that gets sent contains the subject you configured, the domain and store name plus the following data about the shopper: Session ID, IP Address, Shipping First Name, Shipping Last Name, Shipping Email, Shipping Company, Shipping Phone, Shipping Fax, Shipping Address, Shipping City, Shipping State, Shipping Zip, Shipping Country, Billing First Name, Billing Last Name, Billing Email, Billing Comp, Billing Phone, Billing Fax, Billing Address, Billing City, Billing State, Billing Zip, Billing Country.

Unlocking The Locked Out

If for some reason somebody trips your lockout settings and gets locked out and you want to unlock the site you can do it in several ways:

- Temporarily uncheck the “Activate QwkGuard” setting, for example while you were on the phone with the customer, and activate it again after the conversation.
- Uncheck the “active” checkbox for the module under the main module settings for Miva Merchant (Assuming your version of Miva Merchant supports that feature).
- Uninstall the module from the store and then reinstall it. This would only take a moment and wipes out all records of blocked transactions and starts things over again from scratch.
- Set the period and lockout to 0, place a test order (Even if you put in fake data and the payment validation fails) and then reset the settings back to normal.

Provisioning

For sites running Miva Merchant 4.x the module supports Miva's provisioning system with the following data format:

Position	Setting	Format
1	Activate QwkGuard	Y/N
2	Tries	Number
3	Period	Number
4	Lockout	Number
5	Check Session ID	Y/N
6	Check IP Address	Y/N
7	Reset Lock	Y/N
8	Lockout Message	Text
9	Send Email On Lockout	Y/N
10	Email Frequency	Number
11	Email From	Text
12	Email To	Text
13	Email CC	Text
14	Email Subject	Text
15	Accept EULA	Y/N
16	License Number	Text

Settings 8, 11, 12, 13, and 14 accept the value #NONE# to indicate that you want to set the value in the database to nothing.

Below is an example provisioning line for the module that assumes a store with a store code of “test”.

NOTE: this is a single line of text in the provisioning file.

```
MERCHANT||test|MODULE|qwkguard|,|Y,2,60,600,Y,Y,Y,Account locked  
out.,Y,3600,from@4thebest.net,to@4thebest.net,cc@4thebest.net,QwkGuard Lockout Has  
Occurred,Y,4THEBEST-QWKGUARD-00000000000000000000
```

Below is an example of the provisioning line used with other basic provisioning commands to install the module at the domain level, install it in the store (still assuming a store code of test) and configuring the module settings.

NOTE: these are seven lines of text in the provisioning file.

```
MERCHANT|||COMMAND|INSERT_MESSAGE||Begin provisioning for QwkGuard  
MERCHANT|||ACTION|DOMAIN_INSTALL_MODULE|,|modules/system/qwkguard.mvc  
MERCHANT|||COMMAND|INSERT_MESSAGE||QwkGuard module installed  
MERCHANT||test|ACTION|STORE_INSTALL_MODULE|,|qwkguard  
MERCHANT|||COMMAND|INSERT_MESSAGE||QwkGuard module installed in store  
MERCHANT||test|MODULE|qwkguard|,|Y,2,60,600,Y,Y,Y,Account locked  
out.,Y,3600,from@4thebest.net,to@4thebest.net,cc@4thebest.net,QwkGuard Lockout Has  
Occurred,Y,4THEBEST-QWKGUARD-00000000000000000000  
MERCHANT|||COMMAND|INSERT_MESSAGE||QwkGuard module configured
```