



QwkGuard

**Fraud Protection and Auto-Lockout
System**

Miva Merchant Module

Documentation for module version 2.11

Last Updated: 1/9/2004

QwkGuard - Fraud Protection and Auto-Lockout System

QwkGuard helps to reduce your credit card processing fees by intercepting fraudulent orders before they are sent to your credit card processor for validation. QwkGuard offers three layers of protection:

Detecting excessive customer activity

Hackers can use online stores to determine if stolen credit card numbers are valid. When this is done in large batches, you the merchant can face significant credit card processing charges. QwkGuard can help you to detect and block this sort of activity.

Blocking orders from IP addresses

If you know hackers are attacking from a certain IP address or range of IP addresses, you can use QwkGuard to block all orders coming from those IP addresses.

Large Order Blocking

A million-dollar order would be a dream come true for most merchants. But if you're paying a 1% processing fee and that order turns out to be fraudulent, you could be stuck with a huge fee. QwkGuard can block these large orders.

Other Features

QwkGuard offers options for logging and email notification. It's also possible to bypass fraud checking for trusted users based on several criteria.

Using this document

This document describes the configuration and use of the QwkGuard module itself. It assumes that the reader is familiar with Miva Merchant administration and runtime interfaces.

Administrative settings are covered on a tab-by-tab and field-by-field basis. There is also a short how-to section at the end covering common tasks.

This documentation is for the qwkguard.mv and qwkguard.mvc modules for Miva Merchant versions 2.22+, 3.x, and 4.x

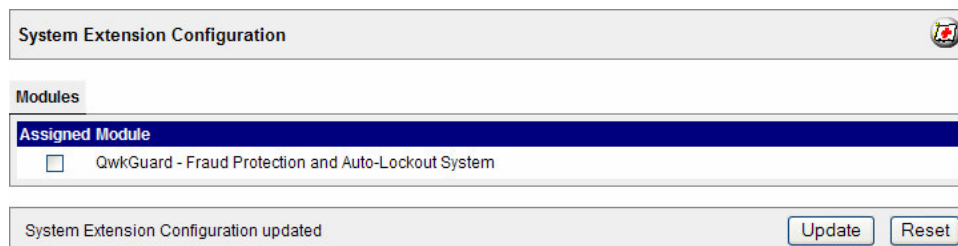
In versions of Miva Merchant below 4.14, the non-compiled qwkguard.mv file should be used; in versions of Miva Merchant 4.14 and above, the compiled qwkguard.mvc file should be used.

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

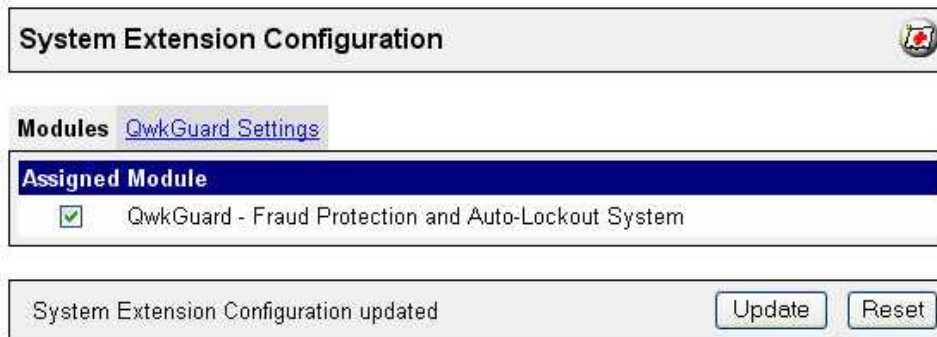
The module is enabled at the store level by checking the box next to "QwkGuard - Fraud Protection and Auto-Lockout System" and pressing the Update button.



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 entry: "QwkGuard - Fraud Protection and Auto-Lockout System", which has an unchecked checkbox next to it. At the bottom of the interface, there is a status bar that says "System Extension Configuration updated" and two buttons: "Update" and "Reset".

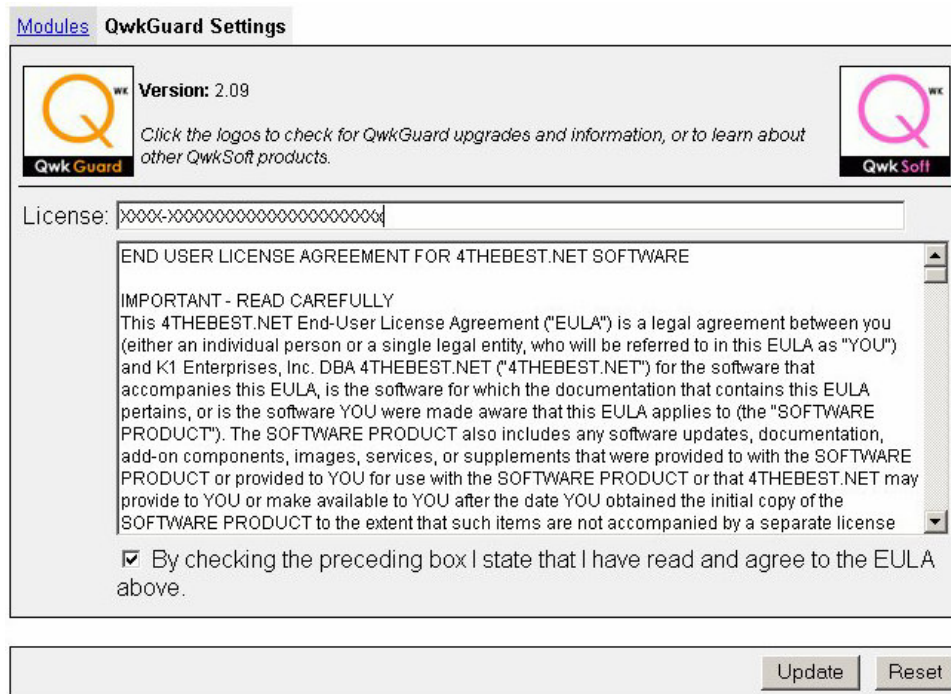
Assigned Module
<input type="checkbox"/> QwkGuard - Fraud Protection and Auto-Lockout System

Once the module has been enabled, a new tab will appear called “QwkGuard Settings”.



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. In addition, three more QwkGuard tabs will appear: “QwkGuard Permanent Blocks”, “QwkGuard Lockouts”, and “QwkGuard Logs”. Each of these tabs is described separately below.




QwkGuard Settings Tab

System Extension Configuration

[Modules](#) **QwkGuard Settings** [QwkGuard Permanent Blocks](#) [QwkGuard Lockouts](#) [QwkGuard Logs](#)



Version: 2.09
License: XXXXXXXXXXXXXXXXXXXX



QwkSoft

Click the logos to check for QwkGuard upgrades and information, or to learn about other QwkSoft products.

Log when:	<input type="checkbox"/> Activate QwkGuard <input type="checkbox"/> Always Trust Zero-Total Orders <input type="checkbox"/> Always Trust Logged-in Customers <input type="checkbox"/> Lockout activated <input type="checkbox"/> Order attempted by locked user <input type="checkbox"/> Order attempted from blocked ip <input type="checkbox"/> Always
Tries:	<input type="text" value="3"/>
Period:	<input type="text" value="60"/> seconds
Lockout:	<input type="checkbox"/> Permanent <input type="text" value="300"/> seconds <input checked="" type="checkbox"/> Check Session ID <input checked="" type="checkbox"/> Check IP Address <input checked="" type="checkbox"/> Reset Lock when order attempted by locked user
Lockout Orders Over:	<input type="text"/>
Lockout Message:	<div style="border: 1px solid gray; padding: 2px; min-height: 40px;">Account locked due to excessive activity.</div>
	<input checked="" type="checkbox"/> Send Email On Lockout
Send Email on Orders Over:	<input type="text"/>
Limit Email To:	<input type="text" value="1"/> Times Per <input type="text" value="Day"/>
Email From:	<input type="text" value="Tests@secureclicks.com"/>
Email To:	<input type="text" value="Tests@secureclicks.com"/>
Email CC:	<input type="text"/>
Email Subject:	<input type="text" value="QwkGuard Lockout Has Occurred"/>

System Extension Configuration updated

The fields on this tab control the overall behavior of QwkGuard.

Activate QwkGuard

Check the box to enable QwkGuard. Uncheck it to temporarily disable the module. Unchecking leaves all of your settings and log files intact, but QwkGuard does not block orders or write logs.

Trust Settings

Configuring QwkGuard for the highest level of security can cause some legitimate shoppers to be blocked. Trust settings allow you to bypass normal QwkGuard processing for trusted customers. These checks occur before and bypass any of the other checks. Orders placed by trusted customers are logged if you have selected “Always” under logging options.

Always Trust Zero-Total Orders

Check this box to tell QwkGuard to always allow orders totaling \$0.00. This checks the product total only, and does not include tax or shipping.

Always Trust Logged-in Customers

Check this box to tell QwkGuard to always allow orders placed by customers who are logged in.

Trust Customers in Group

Select an availability group from the list to tell QwkGuard to always allow orders placed by customers who belong to that group.

Note: This field only appears if you have configured at least one availability group.

Log when

This tells QwkGuard which events to log. The more you log, the more complete information you have, but you also use more disk space for the log files.

Lockout activated

Check this to create a log record each time a shopper is locked out.

Order attempted by locked user

Check this to create a log record each time a locked-out shopper attempts to place an order.

Order attempted from blocked IP

Check this to create a log record each time an order is attempted from a blocked IP address.

Always

Check this to create a log for all events. When this is checked, the other three checkboxes are ignored, and all QwkGuard Events are logged.

Activity based lockout

QwkGuard detects shoppers who try to place an excessive number of orders in a short period of time and prevents them from making further attempts for a period of time. Here's where you specify what you think is excessive.

Tries

The number of order attempts the shopper can make before a lockout occurs.

Note: Each time the shopper submits payment information for validation is a try. This means that if you set Tries to 1, then shoppers must type all of their payment information exactly right the first time or they will be locked out.

Period

How close together the tries have to be to count. This is the total time from the first to the last try.

Lockout

This is how long shoppers will be locked out, in seconds, if they exceed the allowed number of tries.

Note: When the lockout period is changed, it applies to all existing lockouts. For example, if you have Lockout set to 3600 (one hour) then change it to 300 (5 minutes), a shopper locked out 10 minutes ago (when the lockout was still set to an hour) will now be able to place an order.

Check Session ID / Check IP Address

This tells QwkGuard how to tell if two orders come from the same shopper. Session ID is an internal identifier set by Miva Merchant and is more reliable for normal shoppers, but is easier for hackers to circumvent. IP Address is part of the Internet protocol. Under some circumstances two different shoppers can have the same IP address, or a shopper's IP address can change from screen to screen.

For the highest degree of security, select both. If this slows performance, select one or the other. Again, Session ID is slightly more reliable for normal users, but somewhat easier for hackers to bypass.

Reset Lock when order attempted by locked user

If this is checked, QwkGuard resets the lockout clock when the shopper attempts to place an order. For example, if a shopper halfway through a 30-minute lockout tries to place an order, and this option is selected, the lockout timer resets, and they will have to wait 30 minutes from the time of the new attempt.

Lockout Orders Over

If a value is selected here, a lockout will be triggered when a shopper attempts to place an order over the specified amount. This allows you to avoid excessive credit card processing fees for large fraudulent orders.

Lockout Message

This is the message that shoppers will see if they trigger a lockout. This message usually appears on the payment information screen in the store, but the exact format in which it is presented depends on the UI module in use. Here is an example of what the message might look like if you're using the Miva Merchant User Interface with the default settings:



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 the Miva Merchant User Interface 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:



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. Similarly, you could try using a fake message that matches one of those returned from your payment gateway to confuse the hacker.

Confusing the hacker may not do you much good, but it could cause them to discard a credit card that they could otherwise use, saving someone somewhere from credit card fraud.

Email Notification settings

QwkGuard can send you email when a shopper is locked out and/or when a large order is placed:

Send Email on Lockout

Check this to tell QwkGuard to send you an email when a lockout occurs.

Send Email on Orders Over

If you enter a value here, QwkGuard will send email when an order with a total product value over this amount is placed. QwkGuard does not include tax or shipping in the total.

Limit Email To

An automated hacking attempt could easily generate many hundreds of lockouts. To prevent this from clogging your email box and degrading the performance of your server, QwkGuard allows you limit the number of email messages QwkGuard sends. The emails are spread evenly over the specified time, so 5 emails an hour really means no more than 1 every 12 minutes. One email an hour and 24 emails a day are the same thing. If you leave this blank, emails will not be limited.

Email From

This specifies where the email will appear to have been sent from: that is, where the reply will go if you reply to the email.

Email To

This specifies where the email is sent.

Email CC


A copy of the email will be sent to this address, if given.

Email Subject

The email will be sent with this subject. If you have set QwkGuard to send email on large orders, you might want to change the text of the subject to avoid confusion.

The email that gets sent contains the subject you configured, the domain and store name plus the following data about the shopper: Order Total, 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.

QwkGuard Permanent Blocks Tab

System Extension Configuration 

[Modules](#) [QwkGuard Settings](#) **QwkGuard Permanent Blocks** [QwkGuard Lockouts](#) [QwkGuard Logs](#)

Block / Clear Range: Start
End
 Block Range Clear Range

Set Filter Data:

Begin IP:
Display Limit:

Click update to view records matching these filter criteria.

QwkGuard allows you to specify IP addresses that are always blocked. For example, if you get repeated lockouts on IP 1.2.3.4, you can set a permanent block on that IP address. Or if you get repeated lockouts on IP addresses starting with 1.2.3, then you could block the entire range of address from 1.2.3.0 to 1.2.3.255.

Block / Clear Range

This is the range of addresses you want to block or clear. You can enter a Start and End IP to block a range, or a Start IP address to block just that IP, or a partial Start IP to block a range. For example, to block 1.2.3.0 to 1.2.3.255 you can either enter 1.2.3.0 for the Start and 1.2.3.255 for the End or you can just enter 1.2.3 for the start

Block Range / Clear Range (radio buttons)

If you select "Block Range", QwkGuard will add the IPs to the block list. If you specify "Clear Range" the QwkGuard will remove the IPs from the Block list. The Clear Range feature is useful when you find that legitimate customers use a portion of a previously blocked range. For example, if you had blocked 1.2.3.0 to 1.2.3.255, then later found that IPs 1.2.3.127 to 1.2.3.132 were being used by legitimate customers, you could clear that range, while leaving the rest of the range blocked. Note that when you clear a range, it splits the blocked range. In the above example, you will not see a listing saying 1.2.3.127 to 1.2.3.132 is clear; you will see two listings saying 1.2.3.0 to 1.2.3.126 and 1.2.3.133 to 1.2.3.255 are blocked.

Filters

These filters allow you to display just a portion of the blocked IP address list. This can be useful if you have a very long list of blocked IP address ranges.

Begin IP:


This is the IP address where you would like the list to start. It can be partial, and it does not have to actually exist in the list. For example, if you are blocking 1.2.3.4 and 10.20.30.40 and set Begin IP to 5, you will see only the entry for 10.20.30.40. If the Begin IP falls inside of a blocked range, you will see the entire blocked

range. For example, if you are blocking 10.0.0.0 to 20.0.0.0 and begin at 15, the display will start at the 10.0.0.0 to 20.0.0.0 block.

Display Limit:

This is the maximum number of blocks that will display. You can leave it blank to specify no limit. If there are more records than can be displayed within the limit, a message to that effect will display.

QwkGuard Lockouts Tab

System Extension Configuration 

[Modules](#) [QwkGuard Settings](#) [QwkGuard Permanent Blocks](#) **QwkGuard Lockouts** [QwkGuard Logs](#)

Set Filter Data:

Date Range: : : to
 : :

IP:

Session:

Display Limit:

Click update to view records matching these filter criteria.

The Lockout tab displays the currently active lockouts. The list is not displayed when you first access this tab. This is done so that you have a chance to specify a filter without first having to wait for the entire lockout list to display.

Filters

Filters let you display just a subset of the lockout database.

Date Range

This is the starting and ending date and time you would like to view. Date and time represent when the lockout was set or reset, not when it expires.

IP

Specify an IP address to view only the lockout records for that IP address. You may specify a partial IP address. For example, enter 1.2 to view lockouts for IP addresses from 1.2.0.0 to 1.2.255.255.

Session

Specify a session to view only the lockout records for that session. QwkGuard will search for any portion of the string specified in the Session ID. Case is ignored.

Display Limit

Limits the number of lockout records that will be displayed. Leave blank to view all lockout records matching the other filter criteria. If there are more records than can be displayed, a message will display saying so.

Lockout Records

This displays all currently active lockouts that match the filter criteria.

Date / Time

This is the date and time that the lockout was set or reset, not when it expires.

IP

This is the shopper's IP address.

Session


This is the shopper's session ID.

Clear

Check this box and hit update to clear this lockout. This clears all the lockouts for this IP address and session ID. Usually there will only be one, but under certain very rare circumstances there could be more.

Note: When you clear the lockout, QwkGuard also resets the number of tries made for this IP address and session ID. This means that that if you allow 5 tries before lockout occurs and reset the lock, the shopper gets 5 more tries.

QwkGuard Logs Tab

System Extension Configuration 

[Modules](#) [QwkGuard Settings](#) [QwkGuard Permanent Blocks](#) [QwkGuard Lockouts](#) **QwkGuard Logs**

Select Fields to Display: ▶

Set Filter Data: ▶

Action: Display Export Purge

Click update to view records matching these filter criteria.

The Logs contain a record of actions taken by QwkGuard. You can select what gets logged on the QwkGuard Settings tab. The Log tab allows you view the logs.

Note: When you first click over to the Log tab, none of the log records are displayed. This allows you to set filters without having to wait for a large log database to load.

Select Fields to Display

Each log record contains a large amount of data, far more than can be displayed conveniently in a row. By default only the Date / Time, Event, Reason, IP Address, Session, Bill First, Name Bill Last Name and Bill Email are shown. Clicking on words "Select Fields to Display" or on the triangle next to those words will open a panel that lets you select log fields to display.

Select Fields to Display: ▼

<input checked="" type="checkbox"/> Date / Time	<input checked="" type="checkbox"/> Event	<input checked="" type="checkbox"/> Reason
<input checked="" type="checkbox"/> IP Address	<input checked="" type="checkbox"/> Session	<input type="checkbox"/> Ship First Name
<input type="checkbox"/> Ship Last Name	<input type="checkbox"/> Ship Email	<input type="checkbox"/> Ship Company
<input type="checkbox"/> Ship Phone	<input type="checkbox"/> Ship Fax	<input type="checkbox"/> Ship Address
<input type="checkbox"/> Ship City	<input type="checkbox"/> Ship State	<input type="checkbox"/> Ship Zip
<input type="checkbox"/> Ship Country	<input checked="" type="checkbox"/> Bill First Name	<input checked="" type="checkbox"/> Bill Last Name
<input checked="" type="checkbox"/> Bill Email	<input type="checkbox"/> Bill Company	<input type="checkbox"/> Bill Phone
<input type="checkbox"/> Bill Fax	<input type="checkbox"/> Bill Address	<input type="checkbox"/> Bill City
<input type="checkbox"/> Bill State	<input type="checkbox"/> Bill Zip	<input type="checkbox"/> Bill Country

Filter Data

Filters allow you display a subset of the log records, making it easier for you to find the information you’re really interested in. Clicking on the words “Set Filter Data” or on the triangle next to those words opens a panel that lets you set filter criteria.

Set Filter Data: ▼

Date Range: January 1 2004 00 : 00 : 00 to
 January 1 2004 23 : 59 : 59

Event: All Events ▼

IP:

Session:

Email:

Display Limit: 25

Date / Time

This allows you to set the period of time you want to look at.

Event

“Lock” is a lockout event. “Retry” is when a locked-out shopper tries to place an order. “Block” is when a shopper tries to place an order from a blocked IP address. “Pass” is when the order was allowed: that is, when QwkGuard did not stop the order from being processed. Orders that were passed may or may not have actually gone through; the payment module may still have generated some kind of error.

IP

Specify an IP address to view only the log records for that IP address. You may specify a partial IP address. For example, enter 1.2 to view logs for IP addresses from 1.2.0.0 to 1.2.255.255.

Session

Specify a session to view only the log records for that session. QwkGuard will search for any portion of the string specified in the Session ID. Case is ignored.

Email:

This is the shopper’s email address. The string entered here does not have to be a complete email address, and case is ignored. If the string is found in either the shipping or billing email address, the record will be shown

(assuming other filter criteria are met). For example, if you enter “Smith” in the Email filter, you might see records for “smith@foo.com,” “bobsmith@bar.com” and “webmaster@smithsonian.org.”

Display Limit:

Limits the number of log records that will be displayed. Leave this blank to view all log records matching the other filter criteria. If there are more records than can be displayed, a message will display saying so.

Action

This allows you to tell QwkGuard what you want to do with the log records specified by the filter criteria.

Display – Display the records on the screen in table format.

Export – Show the records in tab delimited format in a text area, suitable to cut and paste to a text file for import to other programs.

Purge – Delete the indicated records.

Note: The display limit *does* apply to purge. For example, if the display limit is set to 25, only the first 25 records matching the criteria will be purged.

Log Field Descriptions

Date / Time – When the event occurred.

Event – What event occurred: “Lock” is a lockout event. “Retry” is when a locked-out shopper tries to place an order. “Block” is when a shopper tries to place an order from a blocked IP address. “Pass” is when the order was allowed: that is, when QwkGuard did not stop the order from being processed. Orders that were passed may or may not have actually gone through; the payment module may still have generated some kind of error.

Reason – Additional information about the event. For example, whether the lock was triggered by a session match, IP address match, or large order. Pass events show a reason of ## which should be read as “Try x of y.” That is to say “2/4” indicates that this was the second order of the four allowed.

IP Address – The shopper’s IP address.

Session – The shopper’s Session ID.

Total – The product total for the order.

The remaining fields are standard order fields, and should need no explanation.

How-tos

Finding and Clearing a Shopper Lockout

If you have QwkGuard configured for high degree of security, you may find it necessary to clear a lockout for a legitimate customer. The lockouts only contain the IP Address and Session ID, which can make finding the correct lockout a bit of a challenge. The easiest way to do this is to filter the logs using an event of “Lock” and the customer’s email address. You can then copy the IP Address or Session ID from the Logs and use it to filter the Lockouts.

Setting Up Trusted Customer Groups

Another way to ensure that legitimate customers are not locked out is to set up a trust group. This is simply a standard Miva Merchant availability group. See the Miva Merchant documentation for your version of the software for instructions on how to do create an availability group and assign customers to the group. Select the availability group from the dropdown list labeled “Trust Customers in Group” on the QwkGuard Settings tab.

Exporting Log Records

Rather than exporting log files to a file, QwkGuard exports the data to a text area. This provides the greatest accessibility to the largest number of users. On the tab screen, set the filter criteria appropriately, then select the “Export” action and press update. The log data will display in tab-delimited format in a text area. Simply cut and paste this into a text editor and save the file to your local system.