

Fraud Detection Manual

Welcome to Fraud Detection User Manual

The Fraud Detection extension prevents fraud based on a fraud risk score for every order. It is a backend-only extension, intended for staff use.

It applies a score-based algorithm to evaluate order risks from 1 to 100 using indicators and special rules. The higher the score, the riskier the order is, and the more reasons there are to cancel it.

Such a solution will greatly speed up your staff's ability to do work since it automates the most difficult task - checking the credibility of your customers.

Go ahead, dive in!

Firstly, please find our extension in the [My Downloadable Products](#) section of our store. Learn [how to install extension](#), and proceed with [Quick Start](#), which will guide you in setting up your Fraud Detection service.

How to install the extension

1. Back up your store's database and web directory.
2. Log in to the SSH console of your server and navigate to the root directory of the Magento 2 store.
3. Copy the installation instructions from the page [My Downloadable Products](#) to the SSH console and press ENTER.
4. Run the command `php -f bin/magento module:enable Mirasvit_Core Mirasvit_FraudCheck` to enable the extension.
5. Run the command `php -f bin/magento setup:upgrade` to install the extension.
6. Run the command `php -f bin/magento cache:clean` to clean the cache.
- 7.

Deploy static view files

```
rm -rf pub/static/*; rm -rf var/view_preprocessed/*; php -f bin/magento setup:static-content:deploy
```

If the extension was installed through direct files uploading, you also need to run the command `composer require geoip2/geoip2:~2.0` to install the required libraries.

Quick Start

Our Fraud Detection extension is a simple yet powerful extension that works out-of-box, and allows you to begin monitoring your orders from scratch.

However, there's more to adjust and tune-up to make your fraud detection more precise.

1. Start with [indicators](#) and their importance. [Monitor score of your orders](#) and decide which of them are actually important and which are not.
2. If the indicators are insufficiently effective, create your own [Fraud Detection Rules](#), which will analyze other order and customer properties, and mark the Fraud Levels of the orders.
3. Constantly check your fraud detection performance, adjust the indicators and rules, and your store will become a much safer place.

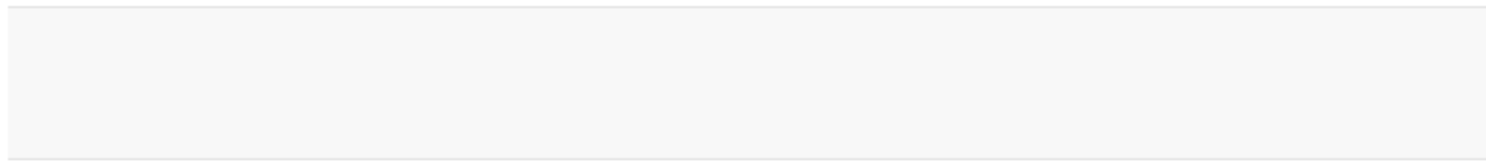
This is a good start. Refer to the corresponding sections of the manual to learn more.

Working with Fraud Risk Scores

A Fraud Detection extension checks all orders which come to your store, and rates them according to the **Risk Score** multi-factor check that is defined by **indicators** and **rules**.

It will be shown at the **Sales -> Orders** grid as a colored mark in the **Fraud Score** column, with a corresponding numerical rate value.

Orders



20 records found

<input type="checkbox"/>	ID	Fraud Score	Purchase Point	Purchase Date	Bill-to Name	Ship-to
<input type="checkbox"/>	000000020	69	Main Website Main Website Store Default Store View	Mar 21, 2018 5:13:14 AM	Romaguera Virgie	Romag
<input type="checkbox"/>	000000019	66	Main Website Main Website Store Default Store View	Mar 21, 2018 5:12:46 AM	Pacocha Danyka	Pacoch
<input type="checkbox"/>	000000018	69	Main Website Main Website Store Default Store View	Mar 21, 2018 5:12:37 AM	Dickinson Manuela	Dickins
<input type="checkbox"/>	000000017	69	Main Website Main Website Store Default Store View	Mar 21, 2018 5:12:10 AM	Romaguera Erich	Romag
<input type="checkbox"/>	000000016	65	Main Website Main Website Store Default Store View	Mar 21, 2018 5:11:54 AM	Waelchi Jamaal	Waelch
<input type="checkbox"/>	000000015	69	Main Website Main Website Store Default Store View	Mar 21, 2018 5:11:40 AM	Wunsch Tyler	Wunsch

The color of the mark corresponds with three possible Fraud Risk levels:

- **Green - Accept** level, which marks orders as safe to complete. By default, it corresponds to a score from 0 to 20.
- **Yellow - Review** level, which warns you about inconsistencies found in order's properties. By default, it corresponds to a score from 30 to 80.
- **Red** - is the highest level **Reject**, equals to 80 - 100 points, and marks the order as dangerous.

The minimum possible score is 0 (all indicators and rules are passed) - **not fraud**. The maximum score is 100 - **fraud** (e. q. all checks failed).

This numerical value is calculated from a set of built-in indicators, which are summed and compared to the level definition. You can [adjust](#) level bounds, if you need.

Each indicator is a separate check, and the result of them are shown on respective tab, added to the Order Edit page:

#000000020

← Back

ORDER VIEW

Information

Invoices

Credit Memos

Shipments

Comments History

Fraud Risk Score

69

Review

Facebook

<https://www.facebook.com/virgie.romaguera>

Twitter

<https://www.twitter.com/romaguera>

LinkedIn

<https://www.linkedin.com/in/virgie.romaguera>

Fraud Checklist

High-Risk Countries

-

Shipping and billing addresses



The shipping and billing addresses are the same



The shipping and billing addresses are different



The shipping and billing addresses are different



The shipping and billing addresses are different

Customer Location



Order placed from a high-risk country



Order placed from a high-risk country

Order amount



Order total outside of the United States

Phone number



The customer's phone number is not a valid phone number

Customer Email



The customer's email address is not a valid email address

Customer History



Customer has not placed an order in the last 90 days

IP History



IP has not placed an order in the last 90 days

Distance



Distance between shipping and billing addresses is greater than 100 miles



Distance between shipping and billing addresses is greater than 100 miles



Read more about these checks in the [Fraud Indicators](#) section.

How to adjust levels of Fraud Risk Score

To adjust the Fraud Risk Score levels, take the following steps:

- Go to **System -> Fraud Detection -> Fraud Risk Score** and press the **Configure** button.
- At the top part of the Configuration Page, under **Statuses** title, you will see a colored line, which defines Fraud Levels. Move the sliders to adjust bounds of levels.
- Save the configuration.
- After that, our extension will recalculate scores for the last 10 orders, which will be shown on the same page.

You can also adjust the indicator importance in the same Configuration page. Proceed to [Fraud Indicators](#) section to find out more.

Configuring Fraud Scores

Our extension calculates Fraud Scores using indicators and rules. Each one is a separate check, and results are displayed in the dedicated tab at the Order Edit Page.

#000000020

← Back

ORDER VIEW

Information

Invoices

Credit Memos

Shipments

Comments History

Fraud Risk Score

69

Review

Facebook

<https://www.facebook.com/virgie.romaguera>

Twitter

<https://www.twitter.com/romaguera>

LinkedIn

<https://www.linkedin.com/in/virgie.romaguera>

Fraud Checklist

High-Risk Countries

-

Shipping and billing addresses



The shipping and billing addresses are the same



The shipping and billing addresses are different



The shipping and billing addresses are different



The shipping and billing addresses are different

Customer Location



Order placed from a high-risk country



Order placed from a high-risk country

Order amount



Order total outside of the United States

Phone number



The customer's phone number is not a valid phone number

Customer Email



The customer's email address is not a valid email address

Customer History



Customer has not placed an order in the last 12 months

IP History



IP has not placed an order in the last 12 months

Distance



Distance between shipping and billing addresses is greater than 100 miles



Distance between shipping and billing addresses is greater than 100 miles



- **Social Network Check** - although untitled, this check is displayed first, above **Fraud Checklist** section. It included links to social media that **possibly** belong to the customer:
 - **Facebook** - a personal Facebook profile.
 - **Twitter** - a Twitter feed.
 - **Linkedin** - a Linkedin page.

Note

Our extension does not retrieve the social pages of the customer by email, or other contact information. It just tries to **guess** these links, using different combinations of a customer's first and last name. Usually, customers pick their social media nicknames in relation to their real names, so this guess is very likely to succeed.

The rest of the indicators are displayed in the **Fraud Checklist** section. All of these indicators have their own **importance** (e.g. whether they can be reliably used for fraud detection). Our extension comes with pretty good weights for each of them, but you can [adjust](#) to fit your specifics.

Here is a short description of each indicator:

- **Shipping and Billing Addresses** - this check compares shipping and billing addresses, and they need to match in order to pass this check.
- **Customer Location** - this check compares country included in addresses with the country, as defined by IP address, from which order was placed. They need to match to pass this check.
- **Order amount** - this check measures the average order total by the store, and compares it to the current order's total. If the amount is too small or too large, the check fails.

Note

This indicator is likely to fail when your store's community is only just forming, or in the case of a sales event. We recommend that you give this check low importance (by default, it is 3).

- **Phone number** - this check analyzes phone numbers and searches for combinations that can expose them as false - repetitive patterns, the same digits, unusual length, etc.

Note

This indicator is also likely to fail since phone numbers can be very different. By default, its importance is 1, e. q. very low.

- **Customer Email** - this check analyzes risky patterns in emails. To pass this check, the email **should not** contain sections of the customer name or blacklisted words, such as `example`.

Note

Our extension has a very restricted built-in blacklist, so we recommend having this indicator on a low-profile, and instead create a custom blacklist with a Rule. We have a good [example](#) of it to follow.

- **Customer History** - this check is merely informational. It contains short statistics of customer sales.
 - **Quantity of Completed Orders** - orders that were fully satisfied.
 - **Quantity of Refunded Orders** - refund numbers.
 - **Quantity of Cancelled Orders** - orders that were canceled.

Note

If the customer has not placed an order yet, there will be the following notification Customer has not placed orders before.

- **IP History** - it is basically the same check as above, but with IP filter. To pass this check, the customer needs to have most of the orders placed from the same IP.
- **Distance** - is a geo-based check that measures the distance between the actual customer location (calculated from IP) and the location of the billing and shipping address. To pass this check, they need to match.
- **Location** - this check is untitled since it acts as an addition to the previous one, and visually highlights the actual customer location.

You can also see the **High-Risk Countries** indicator at the top of the checklist. This indicator is added by the **Fraud Detection Rule**. It has a high priority and can even declare the order as **Fraud** just by matching said conditions. Read more in the [Fraud Detection Rules](#) sections.

How to adjust Importance of Indicators

To adjust the importance of Indicators, you need to visit the **System -> Fraud Detection -> Fraud Risk Score** section, and do the following:

- Press the **Configure**

button, and you will be brought to the Risk Configuration Page.

Fraud Risk Score Configuration ▾

Statuses



Checklist

Status	Importance	Rule
<input checked="" type="checkbox"/>	●●●●●●●●○○	Shipping and billing addresses
<input checked="" type="checkbox"/>	●●●●●●●●○○	Customer Location
<input checked="" type="checkbox"/>	●●●○○○○○○○○	Order amount
<input checked="" type="checkbox"/>	●○○○○○○○○○○	Phone number
<input checked="" type="checkbox"/>	●○○○○○○○○○○	Customer Email
<input checked="" type="checkbox"/>	●●●●●○○○○○○	Customer History
<input checked="" type="checkbox"/>	●●●●●●○○○○	IP History
<input checked="" type="checkbox"/>	●●●●●●●○○○	Distance

Importance

1 - not important indicator, 10 - very important indicator

- Edit properties of the indicators as you need, using the following columns:
 - **Status** - allows you to turn on/off this indicator.
 - **Importance** - displayed only when the **Status** is turned on. It allows you to set the weight of this indicator from 0 (unimportant) to 10 (definitive).
 - **Rule** - is the name of the indicator. It is all pre-defined and cannot be changed.
- When you change properties, fraud levels for the last 10 orders are recalculated and displayed on the

- right side of the pane. Use it to verify whether you have set the importance level correctly.
- Save configuration.

From that moment, our extension will check orders and rate them according to these indicators.

However, this rate can be overridden by [Fraud Score Rules](#), which gives you a more flexible way to check orders for fraud.

Fraud Detection Rules

Custom rules allow you to configure your indicator to check orders for fraud. These rules have higher priority than pre-defined indicators and provide you with increased possibilities.

All of them are located in their dedicated grid at **System -> Fraud Detection -> Custom Rules**.

Please, check the [examples](#) before creating your own rules.

How to create a new Fraud Score Rule.

Visit **System -> Fraud Detection -> Custom Rules** and press the **Add Rule** button. You will be brought to the Rule creation page, which consists of two subsections:

- **General Information** - defines properties and the action that should be assigned to order on conditions match:
 - **Name** - a logical name of the Rule. It will be displayed as an indicator at **Fraud Risk Score** of the order.
 - **Is Active** - indicates whether the rule is active and applies to order.
 - **Set Status to** - allows you to assign a Risk level to order bypassing pre-defined indicators.
- **Conditions** - defines conditions whose match will trigger the rule.

Each rule has four possible global modes of applying conditions in the respective **Conditions** tab, shown in a special header `If *[apply mode]* of these conditions are *[validation mode]*:`

Applying modes define when a rule will be triggered:

- **ALL** - implies that the rule will be executed only when strictly all conditions are met;
- **ANY** - implies that the rule will be executed only when one or more (but not all) of the conditions are met;

Validation modes define which result can produce each condition to be counted as "met":

- **TRUE** - implies that the conditions should be valid.
- **FALSE** - implies that the conditions should be invalid.

These modes allow for creating flexible condition sets to satisfy the policy of any complexity.

Each mode defines a block where the following conditions can be set:

- **Order Properties**

- **Discount Amount** - discount that is used in the current order.
- **Grand Total** - actually paid money amount of the current order.
- **Items Quantity** - the total quantity of all items in the order
- **Placed from IP** - an IP, from which order was placed.
- **Shipping Amount** - shipping fees, paid in the current order.
- **Subtotal** - subtotal of the current order (e.g. without fees and taxes).
- **Tax Amount** - tax paid in the current order.

- **Customer Properties**

- **Group** - the group that the customer belongs to.
- **Lifetime Sales** - total paid amount for all completed orders placed by the current customer.
- **Number of Orders** - the total quantity of orders placed by the customer
- **Is subscriber** - verifies whether the customer has subscribed to the store's newsletter
- **Number of Reviews** - the number of product reviews created by the current customer
- **Is Confirmed** - verifies whether the current customer has confirmed the account.
- **Created At** - date of customer registration
- **Associate to Website** - website on which the customer was registered

Note

You need to use a numerical Website ID here.

- **Create In** - name of the storeview where customer was registered
- **Personal Info Properties** - such as **Name Prefix, First Name, Last Name, Email, Date of Birth, Gender**, etc.
- **Tax/VAT Number** - Tax number of the current customer.
- **First Failure Date** - date on which the login of the customer was rejected (due to incorrect login/password or CAPTCHA).
- **Failures Number** - is the number of login failures that took place during the last session.

- **Billing Address Properties**

- **Payment Method** - payment method used for billing.
- **Billing Person Properties** - such as **Name Prefix, First Name, Last Name, Name Suffix**, etc.
- **Company** - company to which the billing belongs
- **Address Properties** - such as **Street, City, Country, State/Province, Zip Code**, etc.
- **VAT Number** - Tax/VAT number that is used for billing
- **VAT Number validity** - verifies whether the Tax/VAT number is valid.
- **VAT Number validation request ID** - ID of VAT validation request.
- **VAT Number validation request date** - ID of VAT validation request date.

- **VAT Number validation request success** - verifies whether the VAT was successfully validated.

- **Shipping Address Properties**

- **Shipping Method** - shipping method, used for the current order.
- **Same properties as in Billing Address**

You can also define sub-blocks, which will also contain the mode of applying conditions, as described above. This allows you to create complex conditions and detect nearly any possible fraud.

Examples of Fraud Score Rules

- **Set Fraud Level as Review, when order placed through proxy server**

Fraud Orders are often placed through proxy servers to hide the identity of the customer. This rule allows you to catch when the customer hides behind a proxy.

- **General Information**
 - **Set Status to:** Review
- **Conditions**
 - Placed from IP is one of 117.6.161.118, 40.76.17.123, 181.49.24.126, 78.36.39.220, 5.189.133.231

Note: the Free Proxy List used in this example can be obtained [here](#).

- **Set Fraud Level as Review, when Email contains words from blacklist**

Since our built-in blacklist is highly restrictive, you may need a more extensive blacklist check.

- **General Information**
 - **Set Status to:** Review
- **Conditions**
 - If ANY of these conditions are TRUE:
 - Email contains abuse (selected in the **Customer** condition drop-down section)
 - Email contains anticaptcha
 - Email contains blackhole
 - Email contains cymru
 - [any other expression]

Note: This way, you can also black-list unwanted persons, sites and services, and create custom blacklists for any other customer property.

- **Mark as Fraud orders, placed by unconfirmed customers with failures during login**

If you use the auto-registration feature while placing an order, you might also check whether such an order was placed by a robot.

- **General Information**

- **Set Status to:** Reject

- **Conditions**

- Is Confirmed is 0 (this and other conditions are selected from **Customer** drop-down section)
- Number of Orders equals or less than 1
- Failures Number equals or greater than 5

Note: Order from the unconfirmed customer is not a fraud, but when a newly registered customer fails 5 times - they most likely did not pass a CAPTCHA or other auto-login prevention tool.

- **Mark orders placed by the customer with an invalid Tax/VAT number as Fraud orders**

- **General Information**

- **Set Status to:** Reject

- **Conditions**

- If ANY of these conditions are TRUE:
 - Billing: VAT number validity is 0
 - Shipping: VAT number validity is 0

How to upgrade extension

To upgrade the extension, take the following steps:

1. Back up your store's database and web directory.
2. Log in to the SSH console of your server and navigate to the root directory of the Magento 2 store.
3. Run the command `composer require mirasvit/module-fraud-check:* --update-with-dependencies` to update the current extension with all dependencies.

Note

In some cases, the command above is not applicable, or you are unable to update just the current module, and need to upgrade all Mirasvit modules in a bundle. In this case, the command above will have no effect.

Instead, run the `composer update mirasvit/*` command. It will update all Mirasvit modules installed in your store.

4. Run the command `php -f bin/magento module:enable Mirasvit_Core Mirasvit_FraudCheck` to re-enable extension.

5. Run the command `php -f bin/magento setup:upgrade` to install the updates.
6. Run the command `php -f bin/magento cache:clean` to clean the cache.
- 7.

Deploy static view files

```
rm -rf pub/static/*; rm -rf var/view_preprocessed/*; php -f bin/magento setup:static-content:deploy
```

Disabling the Extension

Temporarily Disable

To temporarily disable the extension, please take the following steps:

1. Log in to the SSH console of your server and navigate to the root directory of the Magento 2 store.
2. Run the command `php -f bin/magento module:disable Mirasvit_FraudCheck` to disabled the extension.
3. Log in to the Magento backend and refresh the store cache (if enabled).

Extension Removal

To uninstall the extension, please take the following steps:

1. Log in to the SSH console of your server and navigate to the root directory of the Magento 2 store.
2. Run the command `composer remove mirasvit/module-fraud-check` to remove the extension.
3. Log in to the Magento backend and refresh the store cache (if enabled).

Change Log

1.1.3

(2021-04-29)

Fixed

- Score calculation
-

1.1.2

(2021-04-23)

Fixed

- Customer ip adress detection
-

1.1.1

(2020-12-30)

Fixed

- Fixed the issue with argument type error during the score calculation [#48]()
-

1.1.0

(2020-12-21)

Fixed

- Fixed the issue with the error during score calculation [#46]()
-

1.0.48

(2020-12-07)

Improvements

- Score calculation for orders from the admin panel [#44]()

Fixed

- Magento 2.4.* compatibility [#43]()
-

1.0.47

(2020-11-25)

Improvements

- Not display inactive rules on the order page [#41]()
-

1.0.46

(2020-09-15)

Fixed

- Fixed possible order data rewrite by customer data ([#38]())
-

1.0.45

(2020-07-30)

Improvements

- Support of Magento 2.4
-

1.0.44

(2020-06-03)

Fixed

- Issue with incorrect coordinates detection for some IPs

Improvements

- Minor improvements
-

1.0.43

(2020-03-18)

- Code improvements
-

1.0.42

(2020-01-13)

Fixed

- Issue with actions in admin Custom Rules

1.0.41

(2019-12-13)

Fixed

- An extra output in cronjob
-

1.0.40

(2019-11-06)

Improvements

- Added notice (message) about wrong API keys

Fixed

- Badge display issue
-

1.0.39

(2019-07-18)

Improvements

- Shipping method rules
-

1.0.38

(2019-03-26)

- Temporary revert to 1.0.36

Fixed

- Payment Method validation

1.0.37

(2019-03-18)

Improvements

- UI

Fixed

- Payment Method validation
-

1.0.36

(2019-03-14)

Fixed

- Issue with Grand Total rule validation
 - Wrong shipping address points on map
 - Issue with counting refunded orders
 - Error if payment method was removed
-

1.0.35

(2018-12-26)

Improvements

- Added new condition to rules "Is new IP"
-

1.0.34

(2018-12-13)

Fixed

- Issue with google key
-

1.0.33

(2018-11-29)

Fixed

- Compatibility with Magento 2.3

1.0.32

(2018-08-28)

Fixed

- Issue with hold order by cronjob
-

1.0.31

(2018-08-16)

Improvements

- Added ability to change Google Maps API key
-

1.0.30

(2018-07-16)

Fixed

- Issue with shipping address
-

1.0.29

(2018-06-05)

Fixed

- Issue with map initialization
-

1.0.28

(2018-06-04)

Fixed

- initMap error
-

1.0.27

(2017-10-23)

Fixed

- Issue with shipping/billing address validate message
-

1.0.26

(2017-09-27)

Fixed

- M2.2
-

1.0.25

(2017-09-18)

Improvements

- Performance
-

1.0.24

(2017-08-30)

Fixed

- Subscriber load logic
-

1.0.23

(2017-08-22)

Fixed

- Score status calculations
-

1.0.22

(2017-07-19)

Fixed

- Css styles
-

1.0.21

(2017-07-17)

Improvements

- Performance on orders list page
-

1.0.20

(2017-07-10)

Fixed

- Move qty/count from quote to order
-

1.0.19

(2017-06-20)

Improvements

- Added rule for validate by IP
-

1.0.18

(2017-05-05)

Improvements

- Ability to create rule for payment method
-

1.0.17

(2017-05-05)

Fixed

- Issue with shipping and billing postcodes comparison
 - Fixed an issue with saving score
-

1.0.16

(2017-03-14)

Improvements

- Added ability to use count/qty in custom rules
-

1.0.15

(2017-03-13)

Fixed

- Fixed an issue with performance
-

1.0.14

(2017-03-10)

Fixed

- Disabled ability to filter by fraud score
-

1.0.13

(2017-02-23)

Improvements

- Social profiles
-

1.0.12

(2017-01-12)

Fixed

- Fixed an issue with "Ambiguous class resolution"
-

1.0.11

(2016-11-30)

Improvements

- Changed GeoIP database to GeoLite2-City.mmdb
-

1.0.10

(2016-11-29)

Fixed

- Fixed an issue with updating fraud score
-

1.0.9

(2016-10-17)

Fixed

- Fixed an issue with IP
-

1.0.6

(2016-10-11)

Fixed

- Fixed an issue with updating orders
-

1.0.5

(2016-09-30)

Features

- Ability to hold order review or reject status
-

1.0.4

(2016-09-28)

Fixed

- Fixed an issue with empty score
- Fixed an issue with infinity loop

Documentation

- Updated welcome section
-

1.0.3

(2016-09-14)

Improvements

- Hold order if fraud score is too high (review or reject)

Fixed

- Fixed an issue with fraud status calculations
-

1.0.2

(2016-08-15)

Fixed

- Fixed an issue with menu
-

1.0.1

(2016-06-24)

Fixed

- Compatibility with Magento 2.1
-

1.0.0

(2016-05-19)

Fixed

- Fixed an issue with orders grid
- Link to user manual
- Removed font-awesome

Improvements

- Added images to google map
-