
First Atlantic Commerce Kount Implementation Guide

Version 1.1, December 2021

Change Log

Document Version	Description	Release Date
V1.0	Initial version	15 Mar 2021
V1.1	Added TiloPay to list of compatible plug-ins	3 Dec 2021

Table of Contents

Introduction	4
What is Kount.....	4
Implementing Kount when using a pre-developed plugin or application.....	5
Implementing Kount when using Hosted Payment Page Integration.....	5
Creating a hosted payment page.....	6
Working with a hosted payment page template that contains Kount code	7
Working with a hosted payment page template that does not yet contain Kount code.....	7
Implementing Kount for a DIRECT API Integration	8
Fraud Control - Client-side Implementation Requirements for Kount Service	8
Kount Risk Assessment	10
Kount Risk Assessment Response.....	11
Accessing the Kount Portal	12
Verifying Kount support is working successfully	12
Reviewing transactions in the Kount Portal.....	13
Transaction Lookup.....	13
Kount Rules	14
Enabling a Rule.....	16
Rule Modification.....	18
Updating a Rule.....	18
Adding a New Rule.....	19
Persona Exclusions	20
VIP Lists.....	21
Adding Users for the Kount Portal Access.....	22
Appendix.....	23
Kount Training Videos.....	23
Kount Support Resource Website.....	23

Introduction

This document will guide a developer through the integration process required to add support for the Kount Fraud Service to transactions processing through First Atlantic Commerce's (FAC) Payment Gateway (PG)

What is Kount

FAC's Fraud Control service main component uses a highly rated fraud scoring engine/service called Kount™ (third-party solution & partner). The Kount service provides an additional layer of fraud prevention by using data from both the payment transaction and the device that initiates it to conduct real time analysis on the transaction, return a fraud response code, and a score that assesses the level of fraud risk for the transaction. This provides the merchant with one point of integration for sending an Authorization that includes a Fraud check, or indeed to send a separate "Fraud Check Only" Authorization message.

Adding support for Kount requires the following steps:

- 1) The merchant requests that the FAC business development team add the Kount service to the integration. A member of the business development team will order a merchant ID from Kount and provide any information on additional costs.
- 2) The Kount ID is added to the merchant's FAC account once it has been received.
- 3) Development work necessary to add KOUNT support to the website application should be undertaken. The amount of development involved will depend upon the type of Integration you are using. The level of additional development required will depend upon the integration approach used.
 - a. Pre-developed plugin or application integration (Lowest level of development required)
 - b. Hosted Payment Page Integration (Moderate development required)
 - c. DirectAPI Integration (Most development required)

NOTE: For all implementations, billing and/or address information should be passed in the authorization where possible. This information helps Kount provide a more accurate risk assessment.

Implementing Kount when using a pre-developed plugin or application

If you have purchased a plugin or pre-developed shopping cart application that is already integrated to FAC, entering the Kount ID into the configuration section should be sufficient if the FAC merchant account is also enabled for Kount.

Applications that support Kount

Vendor	Shopping Cart	URL
BizSpice	Magento	https://www.bizspice.com/fac-first-atlantic-commerce-magento-2-payment-gateway.html
Quoviz	WooCommerce	https://quoviz.com/product/3ds-first-atlantic-commerce-woocommerce-plugin/
TiloPay	WooCommerce, WIX, Shopify, Magento 2, Adobe Commerce Cloud, PrestaShop, Opencart	https://tilopay.com
WebGold	Shopify	A hosted payment page integration is required for this plugin. Kount support is easily added to the hosted page.
WebGold	WooCommerce	https://webgold.co/products/first-atlantic-commerce-woocommerce-plugin/

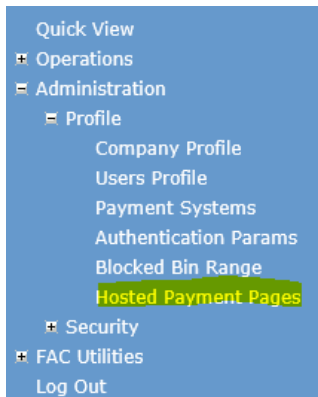
Implementing Kount when using Hosted Payment Page Integration

The Hosted Page integration includes support for the Fraud Control service, however a few additional lines of code are required to enable it.

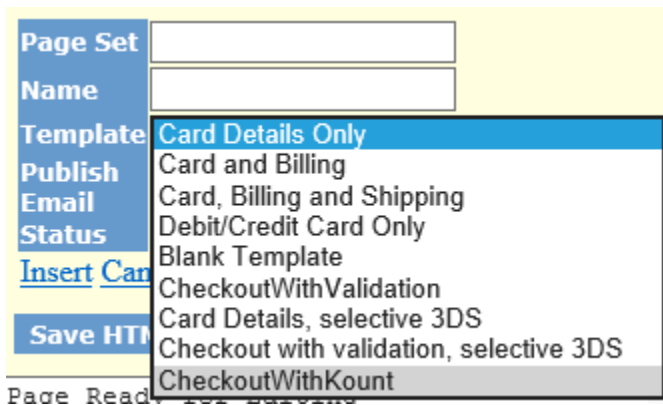
1. If you have not already done so, request a KOUNT ID from FAC Business Development.
2. Once the FAC support team has emailed your KOUNT ID to you, take one of the two following steps.

Creating a hosted payment page

1. Access the Hosted Payment Pages Editor under Administration → Profile → Hosted Payment Pages in the FAC Merchant Administration Portal



2. Select New to create a new hosted page and enter a PageSet and PageName for your hosted page. Select one of the provided templates as a starting point. It is recommended that you select the CheckoutWithKount page since you will be supporting Kount.



Page Set
 Name
 Template **Card Details Only**
 Publish Card and Billing
 Email Card, Billing and Shipping
 Status Debit/Credit Card Only
 Insert Card Blank Template
 Save HTML CheckoutWithValidation
 Card Details, selective 3DS
 Checkout with validation, selective 3DS
 CheckoutWithKount

3. Select Insert and then Save to save the page before modification. Once saved ensure that the correct hosted page is displayed in the PageSet and Name fields. If not, select the blue 'Select' link in front of the page to ensure it is the active one you are working on.
4. Once you have completed the page editing, select publish to publish the page to the FAC Servers. This step must be taken before you can use the page from your website.

Working with a hosted payment page template that contains Kount code

Create a new hosted page using the CheckoutWithKount template.

Select HTML tab at the bottom of the editor page to bring up the hosted page HTML source code. Then scroll to the bottom of the page and replace [KOUNTID] with the Kount ID received from FAC.

```
</script>  
  <script src="/MerchantPages/scripts/kountdatacollector.min.js" defer="defer"  
type="text/javascript" data-merchantid="[KOUNTID]"></script>  
</body>  
</html>
```

 Design  HTML  Preview

Save and publish the hosted page.

Working with a hosted payment page template that does not yet contain Kount code

Create a hosted payment page using one of the templates provided in the FAC Merchant Administration Portal. If you are not using the CheckoutWithKount template, or if you are updating an existing hosted page that does not have Kount support, add the following items to your hosted page.

1. Include this script import in the <head> element of your page

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.4.1/jquery.min.js"></script>
```

2. Add the following script between the closing </form> tag and the closing </body> tag :

```
<script type="text/javascript" src="/MerchantPages/scripts/Kountdatacollector.min.js"  
data-merchantid="[KOUNTID]"></script>
```

Note: the script requires your Kount Merchant ID, not your FAC Merchant ID.

The added script code routes to the Kount site and back again while the customer is interacting with the hosted page. During this process, Kount is able to collect information about the cardholder's browser or device. This information is collected by a process on the Kount site called the "Data Collector".

Implementing Kount for a DIRECT API Integration

Fraud Control - Client-side Implementation Requirements for Kount Service

While some fraud services do not require any involvement from the client browser, the Kount fraud service, now integrated to FAC Payment Gateway, does require some work on the part of the Merchant, but this work is minimal. Kount calls this client-side integration the “Data Collector”.

Kount uses some proprietary java-script code to obtain detailed information about the browser and the client machines properties. This enables a more accurate fraud check as specific data is known about the Cardholders environment. The KOUNT Client Collector SDK data collection process is triggered by a load data event in the <body> tag.

To tie this data in with the Authorization data, a session id is required. This is something the Merchant must generate and pass to the Data Collection URL also added to the checkout page.

Practical Example

In this example we are using JQuery/JavaScript to implement the client side requirements. On the server-side, PHP is used. The server side code could just as easily be done in JSP or .NET code behind.

There are several terms you will need to understand the meaning of:

Name	Size	Description	Example
KOUNT_SERVER_URL	N/A	HTTPS URL Path to Kount servers	https://tst.kaptcha.com (Staging Platform) https://ssl.kaptcha.com (Production)
MERCHANT_ID	6	Six digit Merchant Identifier issued by Kount	240000
SESSION_ID	1-32	Unique Session ID created by Merchant.	BDB721BA17E4A4BB58B21A54
MERCHANT_URL	N/A	Merchant’s Website URL	https://somerchant.com/

Client Side:

In any page prior or on the payment page, you must create the session id, and pass this together with your merchant id to the DATA COLLECTOR URL used on the checkout page. The variable “MERCHANT_ID” is the KOUNT ID provided by FAC and the “SESSION_ID” is generated and supplied by the website application.

Creating a Session ID

Example Script that can be used to generate a session id:

```
<script>  
  var uuid = 'xxxxxxxxxxxx4xxxxyxxxxxxxxxxxxxxxxxxxx'.replace(/[xy]/g, function(c) {  
    var r = Math.random()*16|0, v = c == 'x' ? r : (r&0x3|0x8);  
    return v.toString(16);  
  });  
</script>
```

This has the advantage of not requiring you to pass in values to an already existing element. The element is created with the parameters in place.

You could also use PHP for creating the session id on the payment form. Here is an example that uses the built in `session_id()` function.

```
<?php  
$sess = session_id();  
if ?>  
(!$sess) {  
  // If the session hasn't already been started, start it now and look up the id  
  session_start();  
  $sess = session_id();  
}  
// The session id is now available for use in the variable $sess  
// For more details and examples on working with sessions in PHP, see:  
// http://us2.php.net/manual/en/book.session.php  
// http://us2.php.net/session\_start  
// http://us2.php.net/session\_id
```

IMPORTANT: The same Session ID must be passed to the KOUNT Data Collection and the FAC Payment Gateway in the AuthorizeRequest.

This is required to match up the data retrieved from the cardholder by Kount with the data passed to Kount from the transaction processed through FAC.

IMPORTANT: All authorizations must be sent with a Session ID.

DATA Collection Code

The Kount Client Collector SDK data collection process is triggered by the load data event.

1. Add the following specified class and attribute to the BODY tag in your Checkout page

```
<body class="kaxsdc" data-event="load">
```

2. Include these scripts to the bottom of the <body></body> element in the Checkout page:

```
<script type='text/javascript'  
src='https://KOUNT_SERVER_URL/collect/sdk?m=merchantId&s=sessionId'></script>
```

Input parameters:

- **KOUNT_SERVER_URL** - tst.kaptcha.com (staging) or ssl.kaptcha.com (production)
- **merchantId** - Kount ClientId
- **sessionId** - Kount SessionId

Add script

```
<script type='text/javascript'  
  var client=new ka.ClientSDK();  
  client.autoLoadEvents();  
</script>
```

Once the Kount script is finished, it then does another re-direct back to the checkout page on the Merchant's Server.

Kount Risk Assessment

Kount supports two risk assessment approaches – the Persona Score and the newer Omniscore.

Persona Score

“A Persona is created from a combination of data elements received for a transaction or group of transactions. Each transaction is examined against Kount's entire customer base of transactional data in search of linked data elements, allowing for the creation of a Persona as a unique, identifiable entity.

A given Persona has a 14-day duration. During this interval, the transaction will be continuously reevaluated to identify additional risk.

<https://support.Kount.com/hc/en-us/articles/360045236312-FAQ-What-is-a-Persona-and-How-is-a-Persona-Score-Calculated->

Personal Score – 1 to 99. The higher the score the higher the risk.

Omniscore

Omniscore is a transaction safety rating that can be used in rule creation and during the manual review process to determine the disposition of an order (approve, decline, review). It is the output of Kount's next-generation AI model analyzing hundreds of millions of transactions—their outcomes (including approvals, declines, chargebacks, refunds, etc.) and their real-time linkages and patterns. The AI weighs the risk of fraud against the value of the customer and provides an evaluation (approximating an experienced human fraud analyst) in the form of a score which helps identify good customers, bad customers, and fraudsters.

<https://support.Kount.com/hc/en-us/articles/360045236732-Omniscore-FAQ>

Omniscore – 1 to 99. The higher the score the lower the risk.

Kount Risk Assessment Response

When the KOUNT Service is enabled transactions processed through the FAC Gateway will pass transaction information to KOUNT through the Authorize transaction and the Data Collection code on the checkout page. KOUNT then returns Risk Assessment Response Code and Reason Code, which FAC passes back to the website application in the AuthorizeResponse FraudControlResults section.

Example:

```
<FraudControlResults>  
<FraudControlId>31C407RGDVSR</FraudControlId>  
<FraudResponseCode>A</FraudResponseCode>  
<ResponseCode>1</ResponseCode>  
<Score>29</Score>  
</FraudControlResults>
```

Fraud Response Code: A – Approved, R – Review, D – Deny, E – Escalate
ResponseCode (Persona Score): On a scale of 1 – 99 where 99 is the highest risk score

IMPORTANT: An authorization will not proceed when a 'D' Decline fraud response is received from KOUNT. For these transactions a decline response code of '34' Suspected fraud' will be returned in the authorization response.

Accessing the Kount Portal

Here are the URL's for the KOUNT portal in the test environment and for the live production environment.

Staging Platform	https://portal.test.Kount.net
Production Platform	https://portal.Kount.net

When FAC provides your KOUNT ID they will also request that you provide an email address that can be configured to access the KOUNT portal for your account. Once the userid is created an automated email will be sent to you with the temporary password for first time login.

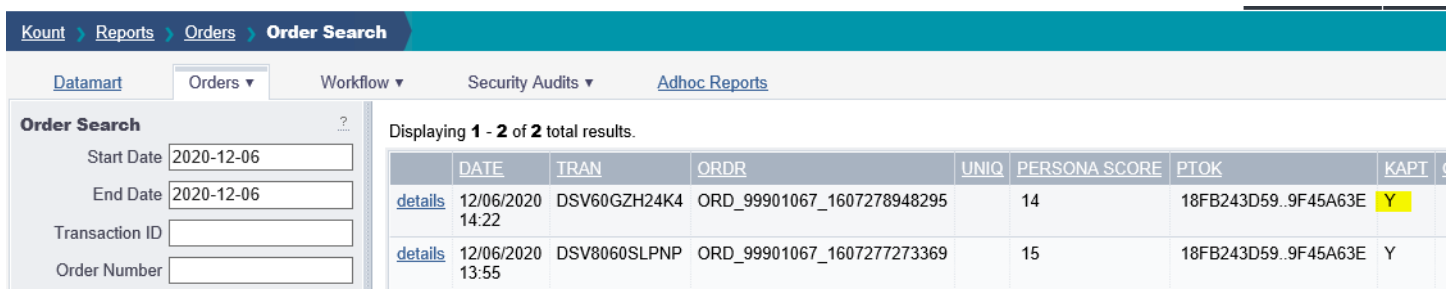
Verifying Kount support is working successfully

1. Verifying RIS (Risk Inquiry Service) support is working

Confirm FraudControlResults are returned in the Authorize or Authorize3DS Response

2. Verifying the Data Collection is working

- Log into the KOUNT Portal and run an Order search for the most recent transactions. Confirm that a 'Y' value appears in the KAPT column. This is the 8th column in the Transaction Record.



The screenshot shows the Kount Order Search interface. The breadcrumb navigation is Kount > Reports > Orders > Order Search. The main navigation includes Datamart, Orders (selected), Workflow, Security Audits, and Adhoc Reports. The Order Search section has input fields for Start Date (2020-12-06), End Date (2020-12-06), Transaction ID, and Order Number. Below the search fields, it says "Displaying 1 - 2 of 2 total results." and shows a table with the following data:

	DATE	TRAN	ORDR	UNIQ	PERSONA SCORE	PTOK	KAPT
details	12/06/2020 14:22	DSV60GZH24K4	ORD_99901067_1607278948295		14	18FB243D59..9F45A63E	Y
details	12/06/2020 13:55	DSV8060SLPNP	ORD_99901067_1607277273369		15	18FB243D59..9F45A63E	Y

- Open the Transaction details using the details link in the first column of the transaction record. Confirm 'Y' is present in the Collector field of the "Last Persona Risk Evaluation" section.

Kount > Workflow > Transaction Details Faith M

Suspect Orders Special Alerts Search Persona Orders Settings ▾ Auto Agent ▾ Queue Assigner ▾

Transaction Summary

Trans. ID: DSV60GZH24K4
 Type: Internet Order
 Website ID: DEFAULT
 Date: 12/06/2020 14:22
 Order Num: [ORD_999010_7278948295](#)
 Session ID: 51QKwZ1STE..NZxy2xg3w2
 Curr. Status: **Review**
 Agent: Unassigned

Persona™

Score: **14**
 No Persona Orders
 Exclusions: No exclusions detected

Omniscore™

Last Persona Risk Evaluation

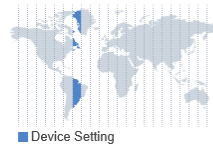
Evaluated On	Reply	Persona Score	Geox	Velo	Vmax	Network	Cards	Emails	Devices	Collector
12/06/2020 14:22	R	14	BM	0	0	N	1	1	1	Y

Rules Triggered

Review Rules

- Card on Network Chargeback List >0

Timezones



■ Device Setting

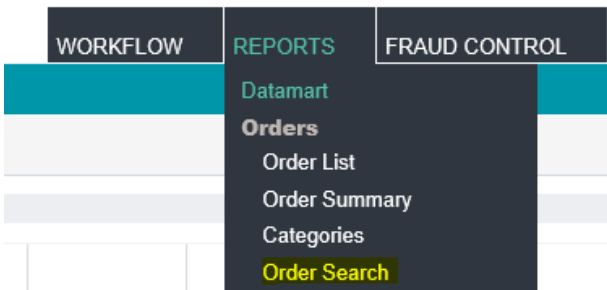
Maps

1. [Device](#)

Reviewing transactions in the Kount Portal.

Transaction Lookup

1. Log into the Kount portal select the REPORTS → Order Search menu option



WORKFLOW **REPORTS** FRAUD CONTROL

Datamart

Orders

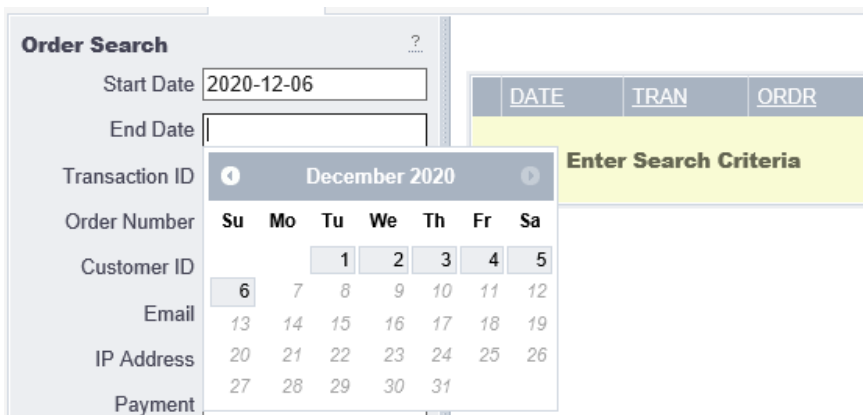
Order List

Order Summary

Categories

Order Search

2. Enter a date range that includes the transactions you wish to view.



Order Search ?

Start Date: 2020-12-06

End Date:

Transaction ID

Order Number

Customer ID

Email

IP Address

Payment

December 2020

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

DATE TRAN ORDR

Enter Search Criteria

3. Use the Search button at the bottom left of the page to pull up the list of transactions.

DATE	TRAN	ORDR	UNIQ	PERSONA SCORE	PTOK	KAPT	GEOX	DVCC	DVID	VELO	EMAL	IPAD
details 12/06/2020 14:22	DSV60GZH24K4	ORD_99901067_1607278948295		14	18FB243D59.9F45A63E	Y	BM	BM	67E198B62F.1BB50FD0	0		199.172.239.242
details 12/06/2020 13:55	DSV8060SLPNP	ORD_99901067_1607277273369		15	18FB243D59.9F45A63E	Y	BM	BM	1828EBC7EA.7714E24F	0		199.172.239.242

The 'details' link in the first column of the transaction can be used to open up the Transaction Details for the specific transaction.

Transaction Summary

Trans. ID: DSV60GZH24K4
 Type: Internet Order
 Website ID: DEFAULT
 Date: 12/06/2020 14:22
 Order Num: [ORD_999010_7278948295](#)
 Session ID: 51QKwZ1STE.NZxy2xg3w2
 Curr. Status: **Review**
 Agent: Unassigned

Persona™
 Score: **14**
 No Persona Orders
 Exclusions: No exclusions detected

Omniscore™
 Safety Rating: **65.6**

Customer
 Created: 12/06/2020
 Name:
 Email: noemail@kount.com
 Cust. ID:

Payment
 Total: 5.00 USD
 Type: Visa Credit Card
 BIN Country: GB
 Flags: ✓MACK ✓AUTH -AVSZ -AVST -CVVR
[Add refund or chargeback](#)

Device
 Location: Hamilton, 03, BM (Collector)
 IP Address: 199.172.239.242


VIP Summary
 No fields are being reviewed
 No fields are being declined

User Defined Fields

Last Persona Risk Evaluation

Evaluated On	Reply	Persona Score	Geox	Velo	Vmax	Network	Cards	Emails	Devices	Collector
12/06/2020 14:22	R	14	BM	0	0	N	1	1	1	Y

Rules Triggered
Review Rules
 • Card on Network Chargeback List >0

Timezones

 1. [Device](#)
[Show All](#)

Addresses
 No addresses

Phone Numbers
 No phone numbers

External Services
 No external services enabled

Shopping Cart
 1 item totaling \$0.00 USD
 Default -- DEFAULT
 Default

Bank Information

Card	Bin+4	BIN Country	Indicator
Visa Classic	424242-4242	GB	Credit

Stripe Payments Uk Limited
[+ more data](#)

Distances - km

kilometers	BA	BP	SA	SP	DV	PX
Bill Addr	-	n/a	n/a	n/a	n/a	n/a
Bill Phn	n/a	-	n/a	n/a	n/a	n/a
Ship Addr	n/a	n/a	-	n/a	n/a	n/a
Ship Phn	n/a	n/a	n/a	-	n/a	n/a
Device	n/a	n/a	n/a	n/a	-	n/a
Proxy	n/a	n/a	n/a	n/a	n/a	-

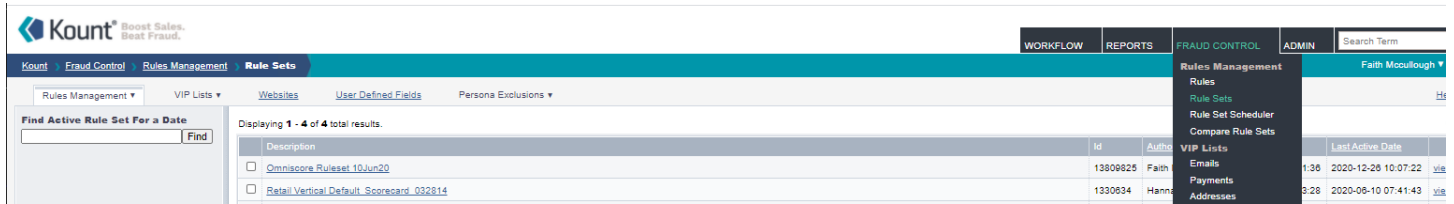
Persona Risk Evaluation History

Evaluated On	Reply	Persona Score	Geox	Velo	Vmax	Network	Cards	Emails	Devices
12/06/2020 14:22	R	14	BM	0	0	N	1	1	1

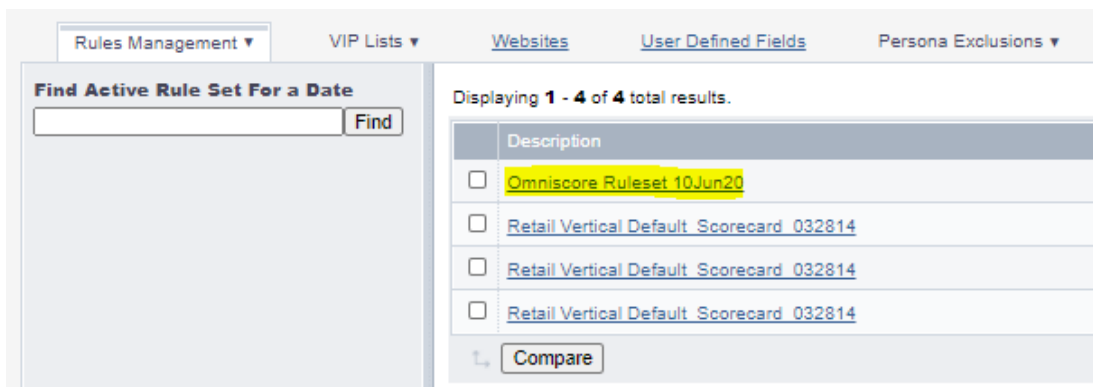
Kount Rules

The KOUNT ruleset is located under the FRAUD CONTROL → Rules Management → Rules menu option

Kount uses Rule Sets to define the rules that will handle the risk assessment. Rule Sets are accessed under the FRAUD CONTROL → Rules Management → Rule Sets menu option.



To view Rules within a Rule Set select the blue Rule Set link from the list.



KOUNT provides a default set of rules based upon the merchant's business. It is anticipated that these will be reviewed and adjusted to suit the merchant's business model.

By default, the VIP and Chargeback rules are enabled and the remaining rules are disabled and should be reviewed and enabled where appropriate.

Omniscore_Shipping

Displaying 1 - 14 of 14 total results.

<input type="checkbox"/>	Action	Condition	Description
<input type="checkbox"/>	Approve	01: {{{vip.approve} in {email}}}	VIP Approve / Email Whitelist
<input type="checkbox"/>	Decline	02: {{{vip.decline} in {email} card ...}}	VIP Decline
<input type="checkbox"/>	Review	03: {{{vip.review} in {email} card g...}}	VIP Review
<input type="checkbox"/>	Decline	04: {{{xtv.country} in {CU EG GH...}}	Device Location = High Risk Country
<input type="checkbox"/>	Decline	05: {{{persona.geox} in {CU EG ...}}	GEOX = High Risk Country
<input type="checkbox"/>	Review	06: {{{persona.score} > {95}}}	Persona Score > 95
<input type="checkbox"/>	Review	07: {{{distance.device to billing}...}}	Device to Billing > 1000km (621mi) [US]
<input type="checkbox"/>	Decline	08: {{{negative.order.merc.charg...}}	Merchant Chargebacks >0
<input type="checkbox"/>	Review	09: {{{negative.order.all.chargeb...}}	Network Chargebacks >0
<input type="checkbox"/>	Review	10: {{{persona.velo} > {3}}}	> 4 Orders in 14 Days
<input type="checkbox"/>	Decline	11: {{{omniscore.safety.rating} <...}}	Omniscore < 15
<input type="checkbox"/>	Review	12: {{{omniscore.safety.rating} >...}}	Omniscore 15-59
<input type="checkbox"/>	Review	13: {{{order.ptok.country} != {xtv...}}	BIN Country <> Device Country (Visa/MC)
<input type="checkbox"/>	Review	14: {{{order.ptok.country} != {ord...}}	BIN Country <> Billing Country (Visa/MC)

Enabling a Rule



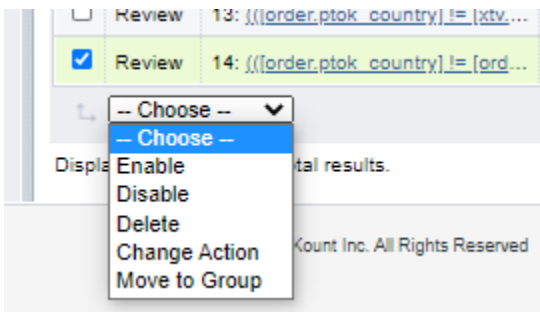
- + New Rules
- * Changed Rules
- o Disabled Rules
- ! Important rules

The default Ruleset provided by KOUNT will have most of the rules disabled.

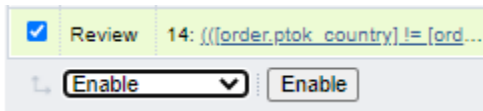
Rule Id	Group	+	*	o	!
14388049	VIP				
14388051	VIP				
14388053	VIP				
14388055	Country			o	
14388057	Country			o	
14388059	Persona			o	

Disabled Rule

To enable a rule, select the checkbox in the first column beside the rule and use the pull down menu in the lower left hand corner to display the menu. Select 'Enable' and an Enable button will be visible.



Select the Enable button to enable the rule.



Rule Modification

Once opened the Rule Set lists the rules that are contained within the set. The Action column indicates the action – Approve, Decline, Review or Escalate taken when the rule is triggered.

Omniscore_Shipping

Displaying 1 - 14 of 14 total results.

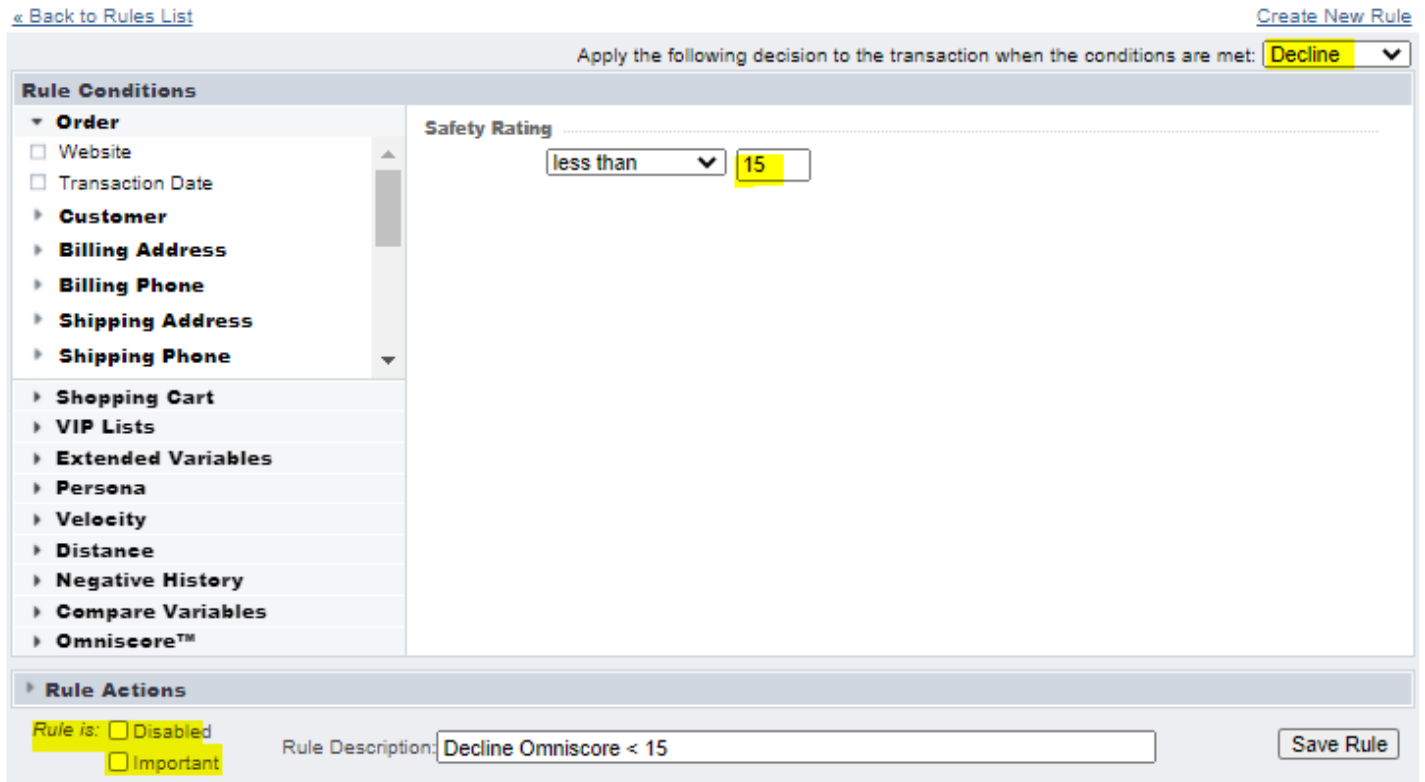
<input type="checkbox"/>	Action	Condition	Description
<input type="checkbox"/>	Approve	01: {{(vip.approve) in [email]}}	VIP Approve / Email Whitelist
<input type="checkbox"/>	Decline	02: {{(vip.decline) in [email card]}}	VIP Decline
<input type="checkbox"/>	Review	03: {{(vip.review) in [email card]}}	VIP Review
<input type="checkbox"/>	Decline	04: {{(xtv.country) in [CUEG GH]}}	Device Location = High Risk Country
<input type="checkbox"/>	Decline	05: {{(persona.geox) in [CUEG]}}	GEOX = High Risk Country
<input type="checkbox"/>	Review	06: {{(persona.score) > [95]}}	Persona Score > 95
<input type="checkbox"/>	Review	07: {{(distance.device_to_billing) > [1000]}}	Device to Billing > 1000km (621mi) [US]
<input type="checkbox"/>	Decline	08: {{(negative.order.merc.charg) > [0]}}	Merchant Chargebacks >0
<input type="checkbox"/>	Review	09: {{(negative.order.all.chargeb) > [0]}}	Network Chargebacks >0
<input type="checkbox"/>	Review	10: {{(persona.velo) > [3]}}	> 4 Orders in 14 Days
<input type="checkbox"/>	Decline	11: {{(omniscore.safety.rating) < [15]}}	Omniscore < 15
<input type="checkbox"/>	Review	12: {{(omniscore.safety.rating) > [15]}}	Omniscore 15-59
<input type="checkbox"/>	Review	13: {{(order.ptok.country) != [xtv.country]}}	BIN Country <> Device Country (Visa/MC)
<input type="checkbox"/>	Review	14: {{(order.ptok.country) != [ord.country]}}	BIN Country <> Billing Country (Visa/MC)

Updating a Rule

To adjust a rule select the underlined Condition link for the rule you wish to adjust.

<input type="checkbox"/>	Decline	8: {{(omniscore.safety.rating) < [15]}}	Decline Omniscore < 15
--------------------------	---------	--	------------------------

Make the adjustment desired then Save the adjusted Rule using the button in the lower right corner of the screen.



The screenshot shows a web interface for configuring a rule. At the top left is a link "Back to Rules List" and at the top right is "Create New Rule". Below these is a header bar with the text "Apply the following decision to the transaction when the conditions are met:" followed by a dropdown menu currently set to "Decline".

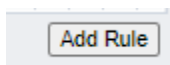
The main area is divided into two sections: "Rule Conditions" and "Rule Actions".

Rule Conditions: A left-hand menu lists various categories: Order (with sub-items Website and Transaction Date), Customer (with sub-items Billing Address, Billing Phone, Shipping Address, and Shipping Phone), Shopping Cart, VIP Lists, Extended Variables, Persona, Velocity, Distance, Negative History, Compare Variables, and Omniscore™. The "Omniscore™" category is currently selected. To the right of this menu, the "Safety Rating" is configured with a dropdown set to "less than" and a text input field containing the number "15".

Rule Actions: At the bottom left, there are checkboxes for "Rule is:" with options "Disabled" and "Important". To the right is a "Rule Description:" field containing the text "Decline Omniscore < 15". A "Save Rule" button is located at the bottom right of the configuration area.

Adding a New Rule

From the Rules List page, select the 'Add Rule' button in the lower right corner of the screen.



Select the desired Rule Condition from the left hand menu list and the action to take in the upper left pull down menu. This sets the Response Action to be returned when the rule is triggered.

[« Back to Rules List](#) [Create New Rule](#)

Apply the following decision to the transaction when the conditions are met: Review ▼

Rule Conditions

- ▼ **Order**
- Match
- Billing and Shipping Postal Codes Match
- Order Shipping Type
- ▼ **Payment Amounts**
- Order Currency
- Order Total Amount
- Order Fencible Value

Order Currency

is ▼ [UZS] Uzbekistan som ▼

Select the appropriate checkbox on the left if you wish the rule to be disabled or marked as important. Add a label for the Rule in the Rule Descriptor and select the 'Create Rule' button to save the rule.

Rule Actions

Rule is: Disabled Important

Rule Description: Review if currency is UZS Create Rule

Once new rule is added or a rule is updated, the Rule Set must be saved.

!

This rule set has been modified. Don't forget to save your changes.

Omniscore_Shipping
Save

The Rule Set must be activated after it has been saved.

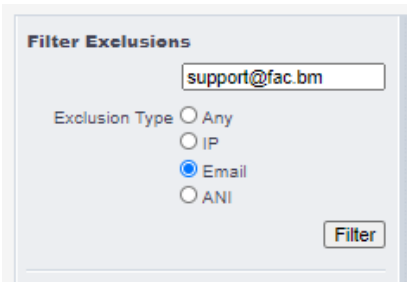
Rule Set Actions

- [Activate Rule Set](#)

Persona Exclusions

Persona Exclusions tab under Fraud Control → Link Exclusions excludes an IP or Email address from the Persona risk assessment.

Once the Filter Exclusions pop-up window is displayed enter the Exclusion type and the value to be excluded from risk assessment.



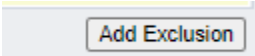
Filter Exclusions

support@fac.bm

Exclusion Type Any
 IP
 Email
 ANI

Filter

Once exclusion entry is created select 'Add Exclusion' to complete the process.



Add Exclusion

VIP Lists

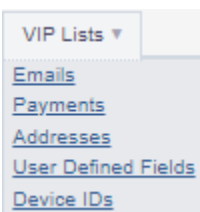
VIP Lists can be used to whitelist or blacklist using transaction specific information e.g. email addresses or device IDs.



Kount > Fraud Control > Vip Lists > **Emails**

Rules Management ▾ **VIP Lists ▾** Websites User Defined Fields Persona Exclusions ▾

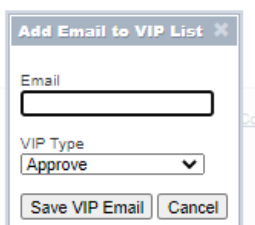
Select appropriate information to be used to filter on.



VIP Lists ▾

- [Emails](#)
- [Payments](#)
- [Addresses](#)
- [User Defined Fields](#)
- [Device IDs](#)

Enter information value and action to be taken when identified.



Add Email to VIP List ✕

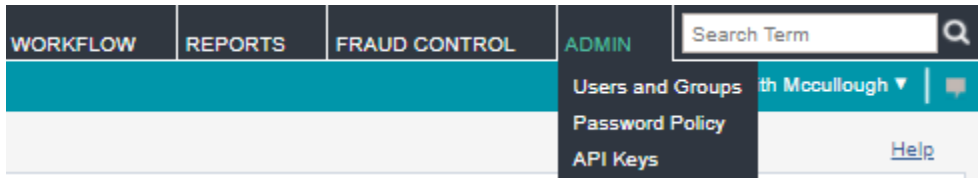
Email
[Text Input]

VIP Type
Approve ▾

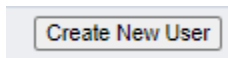
Save VIP Email **Cancel**

Adding Users for the Kount Portal Access

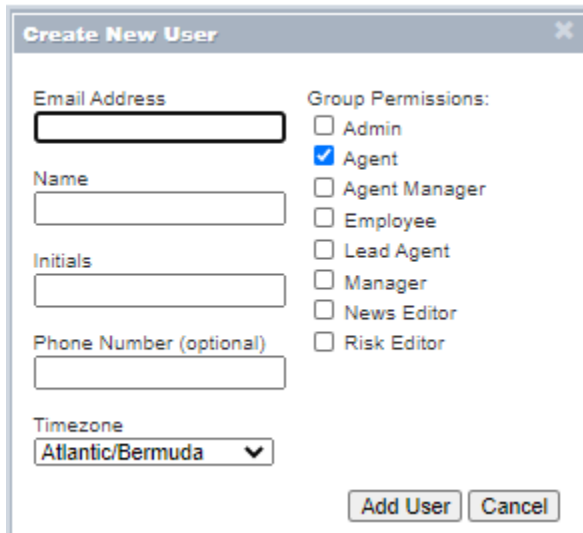
Add users under the ADMIN → Users and Groups menu option.



Select the 'Create New User' button to bring up the New User pop-up window.



Enter the new user's valid email address, Name and Initials and select the 'Add User' button.



The 'Create New User' pop-up window contains the following fields and options:

- Email Address:
- Name:
- Initials:
- Phone Number (optional):
- Timezone:
- Group Permissions:
 - Admin
 - Agent
 - Agent Manager
 - Employee
 - Lead Agent
 - Manager
 - News Editor
 - Risk Editor

Buttons:

Appendix

Kount Training Videos

The following training videos provide an overview of the KOUNT Portal use.

<https://support.kount.com/hc/en-us/articles/360046018491-Video-Tutorial-Library>

<https://support.kount.com/hc/en-us/articles/360045574312-Overview-of-Kount-Command-Agent-Web-Console>

<https://support.kount.com/hc/en-us/sections/360008910292-Rules>

Kount Support Resource Website

<https://support.kount.com/hc/en-us>