COLLECTING SOLUTION

Advanced risk assessment

Back Office user manual

Document version 1.7

Contents

1. HISTORY OF THE DOCUMENT

Version	Author	Date	Comment
1.7	Lyra Collect	22/04/2020	• Update of the “Enable 3D Secure” and “Disable 3D Secure” action description. • Addition of the equivalence between the Hosted Payment Page and REST API fields.
1.6	Lyra Collect	22/05/2019	Details on risk assessment methods via web services
1.4	Lyra Collect	19/02/2019	• Update of available criteria. • Removal of the “Setting up notification e-mails sent to the merchant” and “Creating a custom notification rule” chapters. • Addition of chapter “Creating notification rules specific to risk assessment”.
1.3	Lyra Collect	01/10/2018	Initial version

2. OBTAINING HELP

Looking for help? Check our FAQ on our website

https://lyra.com/doc/en/collect/faq/sitemap.html

If you have any technical questions or need assistance, our tech support is available

from Monday to Friday from 9 a.m. to 6 p.m.

by phone at: **0811900475** Service fee 0.06 € / min + call charge

by e-mail : *support-ecommerce@lyra-collect.com*

and via your Expert Back Office, **Help** > **Contact support**

To facilitate the processing of your demands, you will be asked to communicate your shop ID (an 8-digit number) .

3. ADVANCED RISK ASSESSMENT MODULE

The Lyra Collect payment gateway is a highly secure PCI-DSS certified payment solution. All payment attempts are systematically followed by an authorization request sent to the bank of the cardholder. If the merchant is enrolled for Visa, MasterCard or American Express, the payment process also involves 3D Secure authentication.

However, distance sales present a risk of outstanding payments detrimental for your business.

In order to **provide reinforced security to the merchant**, the **Advanced risk assessment** feature has been added to the payment gateway.

This feature allows to:

- minimize the risk of outstanding payments by rejecting transactions considered fraudulent,
- add controls in the event of suspected fraud.

The **Advanced risk assessment** feature provides a flexible custom service to help you fight against fraud. The provided filters enable you to define the preventive actions depending on the level of the risk and the specifics of your business without penalizing your sales. The advanced risk assessment may be configured based on the previously encountered risks or problems with fraud. You can adapt your rules depending on your buyers' profiles and the performed transactions.

3.1. Prerequisites

The merchant must enable the **Advanced risk assessment** feature via his or her payment gateway.

Once the feature is enabled, the merchant can:

- access its configuration via the merchant Back Office,
- use the service offered by the module to implement (customizable) protection during the payment process.

For more information, please contact the Middle Office.

3.2. Understanding how the module works

A shop has a set of profiles. Each profile consists of one or several rules. Each rule and each profile may be enabled or disabled.

A rule consists of:

- one or several criteria to be validated,
- one or several actions that will be triggered if all the criteria of the rule are validated.

Examples:

- A simple rule with one criterion and one action: if the amount is inferior to 100 EUR, disable 3D Secure.
- A more complex rule with two criteria and one action: if the buyer's country is different from the country where the merchant's shop is established and if the amount is superior to 100 EUR let the merchant manually validate the transaction.

Risk assessment and 3D Secure authentication

The 3D Secure service allows to reduce the risk of chargebacks, thanks to the liability shift from the Merchant to the cardholder's bank (see § 4.2 for more details).

The advanced risk assessment module allows to perform two specific actions when configuring the rules: "Enable 3D Secure" "Disable 3D Secure".

These actions allow the Merchant, depending on the protocols available for his/her MID:

- In 3DS1: to enable or disable 3D Secure authentication,
- In 3DS2: to express their desire to challenge the buyer with a strong authentication during the payment.

The **Selective 3DS** feature allows the Merchant, directly via his/her payment requests:

- In 3DS1: to enable or disable 3D Secure authentication,
- In 3DS2: to express their desire to challenge the buyer with a strong authentication during the payment.

For this, he/she uses the **strongAuthentification** field of the REST API or the **vads_threeds_mpi** field of the Hosted Payment Page.

This function can be used in addition to the risk module .

In this case, the parameter transmitted in the payment request has priority over the decisions of the risk assessment module.

Reminder:

In compliance with banking network rules, a transaction carried out without cardholder authentication does not benefit from liability shift.

Other rules may apply in priority to those defined by the Merchant (in his/her payment requests or via the risk assessment module):

- Some payment cards require cardholder authentication. This is the case of Maestro cards.
- In 3DS2, exceptional cases will be progressively introduced by the payment gateway.

  For example, for payments in euro lower than €30 and within the limit of 5 consecutive payments of less than €30, the Merchant preference transmitted to the issuer will be "No Challenge Requested". If the issuer accepts it, the authentication will be frictionless.
- American Express reserves the right to perform strong authentication according to its own rules, even if the Merchant has requested to disable 3D Secure for the transaction.

Managing the criteria

The merchant can decide to modify the payment process based on different criteria:

- Criteria related to the amount

  These include transaction details (amount, currency, shopping cart, buyer, etc.).
- Criteria related to card analysis

  These include the card type (Visa, Mastercard, etc.), the card product (personal, commercial, prepaid), the issuer country, etc.
- Criteria related to the 3D Secure result

  These include cardholder enrollment, authentication status.
- Criteria related to the country

  Verification of different countries: billing country, shipping country, card issuing bank country, etc.

- Criteria related to the risk assessment result

  These include data transmitted by a risk analyzer (e.g. CyberSource) to the payment gateway, such as the returned score.

- Velocity criteria

  These include the criteria that evolve depending on the activity of the card, of the e-mail, etc. in the merchant shop.

Managing actions

Several actions are available to the Merchant.

- **Disable 3D Secure**

This action is only available if the shop's default 3D Secure behavior is set to **3D Secure enabled by default**.

Depending on the 3D Secure protocol available for the MID (contract), this action allows:

- In 3DS1: to not perform cardholder authentication,
- In 3DS2: to not express a specific preference concerning the authentication ("No Preference").

  If the issuer decides to perform an authentication without interaction (frictionless), the payment will be guaranteed.

Note:

This option becomes available only after selecting the Selective 3D Secure option.

By default, the behavior of the shop is "3D Secure enabled".

- **Enable 3D Secure**

This action is only available if the shop's default 3D Secure behavior is set to **3D Secure disabled by default**.

Depending on the 3D Secure protocol available for the MID (contract), this action allows:

- In 3DS1: proceed to cardholder authentication,
- In 3DS2: request strong authentication of the buyer ("Challenge Requested").

- **Refuse** the payment

This action allows to refuse a payment.

Example: refuse a payment if the used card is a commercial card.

- **Raise an alert**

This action allows to warn the Merchant about an identified risk (see chapter ***Configuring notification e-mails addressed to the merchant***).

Examples: the amount of the transaction is greater than 1000 EUR, the transaction has been made with a card from a country considered as high-risk for online fraud, etc.

The alert allows the Merchant to trigger processing or verification for the transaction.

This action allows the Merchant to trigger actions such as put the shipping process on hold while the transaction is being verified. Technically, the module will generate a "Warning" notification for the transaction. To be informed, the Merchant must configure his/her notification center before triggering an IPN URL, an e-mail or an SMS based on the "Warning" status of the transaction. For more information on the notification configuration process, please see chapter *Creating notification rules specific to risk assessment* on page 38.

- **Validate manually**

This action allows to temporarily block the payment capture.

In the meantime, the Merchant can verify the transaction and decide if he or she wishes to validate or cancel it.

The transaction is then created via manual validation. It can be validated as long as the capture delay has not passed. Once the delay has passed, the payment takes the **Expired** status. This status is final.

Identifying priorities when it comes to actions

An order of priorities is defined among certain actions:

- The **Refuse** a transaction action has priority over the action **Manual validation**.
- The action **Enable 3D Secure** cancels such actions as **Disable 3D Secure**.

  Note:

  *The **Advanced risk assessment** feature allows:*

  - *to **Disable 3DS** when 3DS is enabled by default,*
  - *to **Enable 3DS** when 3DS is disabled by default.*

Other actions can be combined, for example: **Raise an alert**, **Enable 3D Secure** and **Validate manually**.

3.3. Understanding the control process

The **Advanced risk assessment** feature can be called several times when a payment is created.

- Maximum 3 times:
  - After data validation,
  - After performing 3D Secure authentication,
  - After authorization.

With each call, this feature potentially returns one or more actions that will impact the payment process. All types of payments (single payment, deferred payment, installment payment, split payment, etc.) are subject to the controls of the **Advanced risk assessment**.

Note:

In case of unavailability, incorrect configuration or malfunction, the payment is made as if the Merchant did not have the advanced risk assessment feature.

4. CONFIGURING THE ADVANCED RISK ASSESSMENT VIA THE EXPERT BACK OFFICE

The advanced risk assessment is accessible via the Back Office.

To access it:

1. Sign in to the Back Office: *https://secure.lyra.com/portal/*.
2. Click **Other actions** and sign in to your Expert Back Office.
3. Select **Settings** > **Advanced risk assessment**.

   Note:

   If you have multiple shops, select a shop.

   The controls are grouped by tabs.

   - Configuration
   - 3D Secure result
   - Amount
   - Payment method
   - Shopping cart
   - Country
   - Velocity
   - Media
   - Risk Analysis result
   - SafeKey result

IMPORTANT

In order to be properly taken into account, controls are configured as follows:

1. ***I define the rule in the corresponding tab.***
2. ***Then, I apply the rule in the Configuration tab.***

4.1. Configuration tab

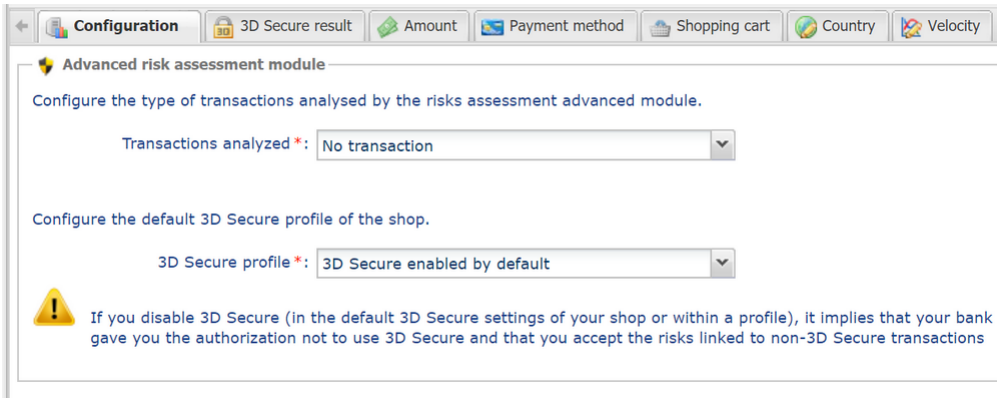

Figure 1: Configuration tab

When you have finished configuring your control types in the tabs, you must display the **Configuration** tab in order to:

- Specify the analyzed transactions.

  The possible values are:

  - No transaction (control is disabled)
  - Only TEST transactions

    The controls configured in the different tabs will be applied only in TEST mode transactions.
  - All transactions

    The controls configured in the different tabs will be applied to all transactions (TEST and PRODUCTION).
- Define the shop's 3D Secure (enabled or disabled) default behavior.

  The possible values are:

  - 3D Secure enabled by default

    The controls configured in the tab related to 3D Secure will be applied to the shop's transactions.
  - 3D Secure disabled by default

    None of the controls configured in the tab related to 3D Secure will be applied to the shop's transactions.

All changes must be saved by clicking the **Save** button.

4.2. 3D Secure result tab

3D Secure, also called "*Visa Secure*" by Visa, "*Mastercard Identity check*" by Mastercard and "*Safekey*" by American Express is an international protocol standard used to secure online transactions.

The principle of 3D Secure consists in asking the buyer, in addition to the usual bank details (bank card number, expiry month and year, CVV code - if the card has one), to provide additional information that is not linked to the card to make sure that the buyer is the owner of the payment method. In most cases it is a one-time confidential code communicated by e-mail or by SMS for each new transaction. If this information is not correctly filled in by the buyer, the transaction ends.

Its purpose is to:

- Reduce fraud for merchants,
- Secure payments for buyers.

3D Secure authentication consists of two phases:

- Verification of the cardholder's enrollment,
- Authentication of the cardholder.

Each phase includes several results.

The diagram below illustrates the principle of the 3D Secure authentication:

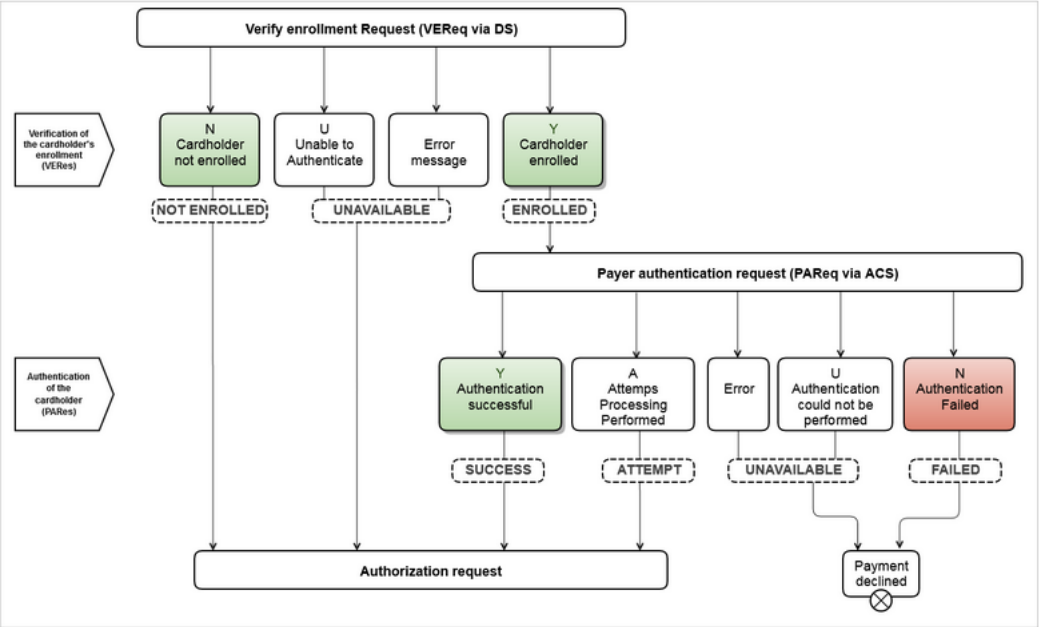

Figure 2: Illustration of the two phases

Thus, depending on the results returned during each of these two phases, the payment gateway provides several profiles to trigger actions.

3D Secure payment with a cardholder whose authentication cannot be verified

In order to trigger one or several actions when the cardholder's 3D Secure authentication status cannot be verified:

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.
2. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - Raise an alert
   - Validate manually
   - Refuse

   If you want to define one or more other actions:
3. Click the **Add** button.
4. Select another action that you wish to trigger when the profile appears.
5. Click **Save** at the bottom of the page.

Card not enrolled in the 3D Secure program

To trigger one or more actions when the transaction is made with a card that is not enrolled in the 3D Secure program:

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.
2. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - Raise an alert
   - Validate manually
   - Refuse

   If you want to define one or more other actions:
3. Click on the **Add** button.
4. Select another action that you wish to trigger when the profile appears.
5. Click **Save** at the bottom of the page.

3D Secure payment with a card whose enrollment cannot be verified

To trigger one or more actions when the transaction is made with a card whose enrollment in the 3D Secure program cannot be verified due to a malfunction of the 3D Secure environment:

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.
2. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - Raise an alert
   - Validate manually
   - Refuse

   If you want to define one or more other actions:
3. Click on the **Add** button.
4. Select another action that you wish to trigger when the profile appears.
5. Click **Save** at the bottom of the page.

Liability shift

This profile allows you to trigger one or more actions when the transaction does not benefit from the liability shift.

The transactions benefiting from the liability shift are transactions for which the cardholder cannot shift the liability for an outstanding payment to the merchant on the grounds of "Objection by the Cardholder".

Note:

AMEX transactions cannot benefit from liability shift.

To trigger one or more actions when the transaction does not benefit from liability shift:

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.
2. Specify a minimum amount and its currency.
3. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - Raise an alert
   - Validate manually
   - Refuse

   If you want to define one or more other actions:
4. Click the **Add** button.
5. Select another action that you wish to trigger when the profile appears.
6. Click **Save** at the bottom of the page.

4.3. Amount tab

The **Amount** tab allows you to trigger one or more actions depending on the transaction amount.

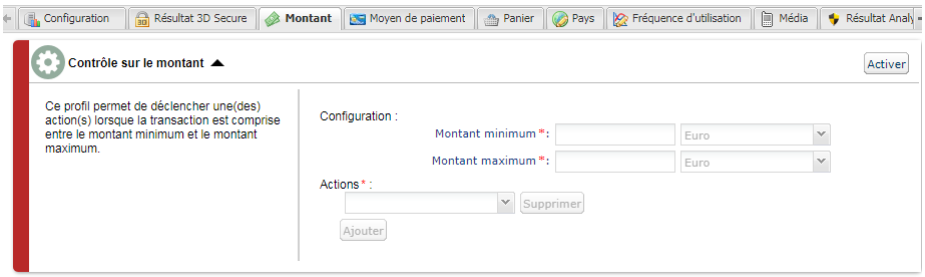

Figure 3: Amount tab

To do this:

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.
2. Specify a minimum and maximum amount that will allow to trigger an action.
3. Specify the currency that applies to the defined minimum and maximum amount.
   The applied currencies must be the same otherwise the **Save** button will not be active.
4. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - **Raise an alert**
   - **Validate manually**
   - **Enable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure disabled by default"
   - **Disable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure enabled by default"
   - **Refuse**

   If you want to define one or more other actions:
5. Click **Add**.
6. Select another action that you wish to trigger when the profile appears.
7. Click **Save** at the bottom of the page.

Minimum amount limit control

It is possible to enable only a minimum amount control.

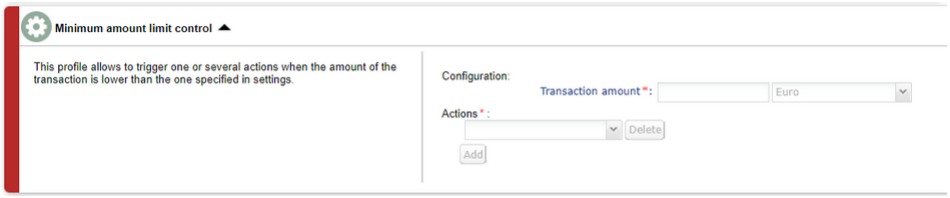

Figure 4: Minimum amount limit control

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.
2. Specify a transaction amount that will allow to trigger an action if the transaction amount is lower than the specified amount.
3. Specify the currency that applies to the defined minimum amount.
4. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - **Raise an alert**
   - **Validate manually**
   - **Enable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure disabled by default"
   - **Disable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure enabled by default"
   - **Refuse**

   If you want to define one or more other actions:
5. Click **Add**.
6. Select another action that you wish to trigger when the profile appears.
7. Click **Save** at the bottom of the page.

Maximum amount limit control

It is possible to enable only a maximum amount control.

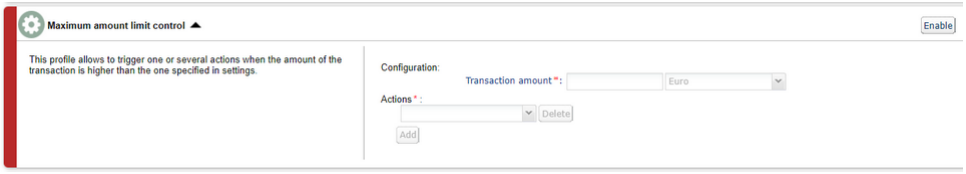

Figure 5: Maximum amount limit control

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.
2. Specify a transaction amount that will allow to trigger an action if the transaction amount is higher than the specified amount.
3. Specify the currency that applies to the defined maximum amount.
4. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - **Raise an alert**
   - **Validate manually**
   - **Enable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure disabled by default"
   - **Disable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure enabled by default"
   - **Refuse**

   If you want to define one or more other actions:
5. Click **Add**.
6. Select another action that you wish to trigger when the profile appears.
7. Click **Save** at the bottom of the page.

Control of the amount accumulated for a payment method over a week

It is possible to enable the control of the amount accumulated over a week.

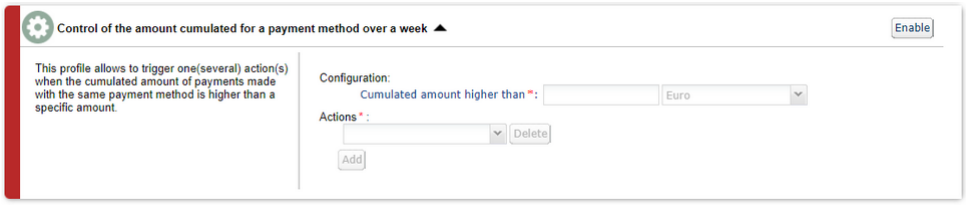

*Figure 6: Control of the accumulated **amount***

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.

2. Specify a transaction amount that will allow to trigger an action if the transaction amount reaches the specified limit.
3. Specify the currency that applies to the accumulated amount.
4. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - **Raise an alert**
   - **Validate manually**
   - **Enable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure disabled by default"
   - **Disable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure enabled by default"
   - **Refuse**

   If you want to define one or more other actions:
5. Click **Add**.
6. Select another action that you wish to trigger when the profile appears.
7. Click **Save** at the bottom of the page.

4.4. Payment method tab

The **Payment method** tab allows you to define different profiles to trigger one or more actions based on the category of the card used by the buyer.

Control of commercial cards

A commercial card is a business card. It can be issued to an employee for work purposes, for example.

To trigger one or more actions when a buyer uses a commercial card to make a payment:

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.
2. Select one or more card brand to control.
   It is possible to select several cards.
   Controlled cards are:
   - CB,
   - VISA,
   - MASTERCARD,
   - MAESTRO,
   - ELECTRON,
   - VPAY.
3. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - **Raise an alert**
   - **Validate manually**
   - **Enable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure disabled by default"
   - **Disable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure enabled by default"
   - **Refuse**

   If you want to define one or more other actions:
4. Click **Add**.
5. Select another action that you wish to trigger when the profile appears.
6. Click **Save** at the bottom of the page.

Control of commercial cards depending on their origin

A commercial card is a business card. It can be issued to an employee for work purposes, for example.

To trigger one or more actions when a buyer makes a payment by using a commercial card issued by a country from the list:

1. Click the **Enable** button.

   The green bar indicates that the profile is activated.

2. Select one or several countries by clicking on the **Add** button.

   The country(ies) that allow(s) you to trigger an action appear(s) in the column **Selected countries**.

   This list is not static. You can remove one of the countries at any time by selecting it and clicking the **Remove** button.

3. Select one or more card brand to control.

   It is possible to select several cards.

   Controlled cards are:

   - CB,
   - VISA,
   - MASTERCARD,
   - MAESTRO,
   - ELECTRON,
   - VPAY.

4. Select the action that you wish to trigger when the profile appears.

   The possible values are:

   - **Raise an alert**
   - **Validate manually**
   - **Enable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure disabled by default"
   - **Disable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure enabled by default"
   - **Refuse**

   If you want to define one or more other actions:

5. Click **Add**.

6. Select another action that you wish to trigger when the profile appears.

7. Click **Save** at the bottom of the page.

Control of prepaid cards

A prepaid card is a payment method that is similar to an electronic wallet. Only the recharged amounts can be spent (no risk of overdraft, hacked bank account, etc.).

To trigger one or more actions when a buyer uses a prepaid card (Visa or MasterCard) to make a payment:

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.
2. Select one or more card brand to control.
   It is possible to select several cards.
   Controlled cards are:
   - CB,
   - VISA,
   - MASTERCARD,
   - MAESTRO,
   - ELECTRON,
   - VPAY.
3. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - **Raise an alert**
   - **Validate manually**
   - **Enable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure disabled by default"
   - **Disable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure enabled by default"
   - **Refuse**

   If you want to define one or more other actions:
4. Click **Add**.
5. Select another action that you wish to trigger when the profile appears.
6. Click **Save** at the bottom of the page.

Control of cards with unconditional authorization

A card with unconditional authorization is a payment card. Every time the card is used, the account balance is checked. The operation is not authorized if the provision is insufficient.

To trigger one or more actions when a buyer is using a Visa or a MasterCard card with unconditional authorization to make a payment:

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.
2. Select **MAESTRO** or **VISA_ELECTRON** from the list of card types that will trigger one or more actions.
3. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - **Raise an alert**
   - **Validate manually**
   - **Enable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure disabled by default"
   - **Disable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure enabled by default"
   - **Refuse**

   If you want to define one or more other actions:

   Note:

   *With a card of type **MAESTRO**, it is not possible to select the action **Disable 3D Secure**. A Maestro card is a MasterCard debit card and for this card type, MasterCard **requires 3D Secure**. If this data is missing from the authorization, the payment is rejected.*
4. Click **Add**.
5. Select another action that you wish to trigger when the profile appears.
6. If you wish to select another card type, repeat the steps 2 and 3 and, if needed, the steps 4 and 5.
7. Click **Save** at the bottom of the page.

Control of e-Carte Bleue

An e-Carte Bleue is a virtual card that provides an ephemeral card number for each transaction made on the Internet. Thus, the "real" credit card number does not appear on the Internet.

To trigger one or more actions when a buyer uses an e-Carte Bleue to make a payment:

1. Click the **Enable** button.

   The green bar indicates that the profile is activated.

2. Select the action that you wish to trigger when the profile appears.

   The possible values are:

   - **Raise an alert**
   - **Validate manually**
   - **Enable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure disabled by default"
   - **Disable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure enabled by default"
   - **Refuse**

   If you want to define one or more other actions:

3. Click **Add**.

4. Select another action that you wish to trigger when the profile appears.

5. Click **Save** at the bottom of the page.

Control of personal credit cards

A personal credit card is a payment card. A deferred debit is made on the account for all the purchases made over a specified period.

To trigger one or more actions when a buyer uses a personal card to make a payment:

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.
2. Select one or more card brand to control.
   It is possible to select several cards.
   Controlled cards are:
   - CB,
   - VISA,
   - MASTERCARD,
   - MAESTRO,
   - ELECTRON,
   - VPAY.
3. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - Raise an alert
   - Validate manually
   - Disable 3D Secure
   - Refuse

   If you want to define one or more other actions:
4. Click the **Add** button.
5. Select another action that you wish to trigger when the profile appears.
6. Click **Save** at the bottom of the page.

Control of personal debit cards

A personal debit card is a payment card. The account is debited progressively as the transactions are transmitted by the beneficiary merchants.

To trigger one or more actions when a buyer uses a personal debit card to make a payment:

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.
2. Select one or more card brand to control.
   It is possible to select several cards.
   Controlled cards are:
   - CB,
   - VISA,
   - MASTERCARD,
   - MAESTRO,
   - ELECTRON,
   - VPAY.
3. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - Raise an alert
   - Validate manually
   - Disable 3D Secure
   - Refuse

   If you want to define one or more other actions:
4. Click the **Add** button.
5. Select another action that you wish to trigger when the profile appears.
6. Click **Save** at the bottom of the page.

4.5. Shopping cart tab

The **Shopping cart** tab allows you to define different profiles to trigger one or more actions based on the contents of the buyer's shopping cart.

Control of the number of items in the cart

To trigger one or several actions when a buyer has a certain amount of items in the shopping cart when making a payment:

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.
2. Specify the number of items that will allow to trigger one or more actions.
3. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - **Raise an alert**
   - **Validate manually**
   - **Enable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure disabled by default"
   - **Disable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure enabled by default"
   - **Refuse**

   If you want to define one or more other actions:
4. Click **Add**.
5. Select another action that you wish to trigger when the profile appears.
6. Click **Save** at the bottom of the page.

Shopping cart items control

To trigger one or more actions when a buyer has one or more specific product codes in the shopping cart:

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.
2. Specify a product code for which you wish to trigger one or more actions.
3. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - **Raise an alert**
   - **Validate manually**
   - **Enable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure disabled by default"
   - **Disable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure enabled by default"
   - **Refuse**

   If you want to define one or more other actions:
4. Click **Add**.
5. Select another action that you wish to trigger when the profile appears.
6. If you wish to add another product code, repeat step 2 by separating the product codes by a "**;**".
7. Click **Save** at the bottom of the page.

4.6. Country tab

The **Country** tab allows you to define different profiles to trigger one or more actions based on the country(ies) associated with the transaction.

Customer country control (billing address)

All the countries are accepted by default. The expression "Buyer's country" indicates the country of the billing address.

To trigger one or more actions to protect the merchant website from specific risks associated with one or several countries:

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.
2. Select one or several countries by clicking on the **Add** button.
   The country(ies) that allow(s) you to trigger an action appear(s) in the column **Selected countries**.
   This list is not static. You can remove one of the countries at any time by selecting it and clicking the **Remove** button.
3. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - **Raise an alert**
   - **Validate manually**
   - **Enable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure disabled by default"
   - **Disable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure enabled by default"
   - **Refuse**

   If you want to define one or more other actions:
4. Click **Add**.
5. Select another action that you wish to trigger when the profile appears.
6. Click **Save** at the bottom of the page.

Control of the shipping country

All the countries are accepted by default.

To trigger one or more actions to protect the merchant website from specific risks associated with one or several countries:

1. Click the **Enable** button.

   The green bar indicates that the profile is activated.

2. Select one or several countries by clicking on the **Add** button.

   The country(ies) that allow(s) you to trigger an action appear(s) in the column **Selected countries**.

   This list is not static. You can remove one of the countries at any time by selecting it and clicking the **Remove** button.

3. Select the action that you wish to trigger when the profile appears.

   The possible values are:

   - **Raise an alert**
   - **Validate manually**
   - **Enable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure disabled by default"
   - **Disable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure enabled by default"
   - **Refuse**

   If you want to define one or more other actions:

4. Click **Add**.

5. Select another action that you wish to trigger when the profile appears.

6. Click **Save** at the bottom of the page.

Control of diversity of countries

One or more actions can be triggered when the number of countries involved in the transaction exceeds a certain threshold and the amount of the transaction is between a minimum and maximum amount.

When this scenario occurs, a control is made on the basis of the following criteria:

- The country of the customer address
- The country of the shipping address
- The country of the IP address used during the payment
- The payment method country

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.
2. Set the threshold for countries (1, 2, 3 or 4) which will trigger one or more actions.
3. Specify a minimum and maximum amount that will allow to trigger an action.
4. Specify the currency that applies to the defined minimum and maximum amount.
   The applied currencies must be the same otherwise the **Save** button will not be active.
5. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - **Raise an alert**
   - **Validate manually**
   - **Enable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure disabled by default"
   - **Disable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure enabled by default"
   - **Refuse**

   If you want to define one or more other actions:
6. Click **Add**.
7. Select another action that you wish to trigger when the profile appears.
8. Click **Save** at the bottom of the page.

Control of card types issued by certain countries

This profile allows to trigger one or more actions when:

- the card type is one of the selected card types (prepaid card, commercial card, personal card)

  and
- the country of the card is on the list of selected countries.

To trigger one or more actions:

1. Click the **Enable** button.

   The green bar indicates that the profile is activated.
2. Select one or more card type(s) from the list.

   The possible values are:

   - **Prepaid card**
   - **Commercial card**
   - **Personal card**

     A personal card is a bank card delivered to an individual for personal use.
3. Select one or several countries by clicking on the **Add** button.

   The country(ies) that allow(s) you to trigger an action appear(s) in the column **Selected countries**.

   This list is not static. You can remove one of the countries at any time by selecting it and clicking the **Remove** button.
4. Select the action that you wish to trigger when the profile appears.

   The possible values are:

   - **Raise an alert**
   - **Validate manually**
   - **Enable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure disabled by default"
   - **Disable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure enabled by default"
   - **Refuse**

   If you want to define one or more other actions:
5. Click **Add**.
6. Select another action that you wish to trigger when the profile appears.
7. Click **Save** at the bottom of the page.

4.7. Velocity tab

The **Velocity** tab allows you to define different profiles to trigger one or more actions based on the velocity of the same payment method within a week.

Velocity of an e-mail address within a week

To trigger one or more actions when multiple payment attempts have been detected with the same e-mail address within a week:

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.
2. Determine the number of payment attempts made with the same e-mail address to trigger one or more actions.
3. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - **Raise an alert**
   - **Validate manually**
   - **Enable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure disabled by default"
   - **Disable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure enabled by default"
   - **Refuse**

   If you want to define one or more other actions:
4. Click **Add**.
5. Select another action that you wish to trigger when the profile appears.
6. Click **Save** at the bottom of the page.

Velocity of an IP address within a week

To trigger one or more actions when multiple payment attempts have been detected with the same IP address within a week:

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.
2. Determine the number of payment attempts made with the same IP address to trigger one or more actions.
3. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - **Raise an alert**
   - **Validate manually**
   - **Enable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure disabled by default"
   - **Disable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure enabled by default"
   - **Refuse**

   If you want to define one or more other actions:
4. Click **Add**.
5. Select another action that you wish to trigger when the profile appears.
6. Click **Save** at the bottom of the page.

Velocity of a payment method over a week

Note

The performed control applies to payment card numbers as well as to bank account numbers that were used for the wire transfer.

To trigger one or more actions when multiple payment attempts have been detected with the same card number within a week:

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.
2. Determine the number of payment attempts made with the same card number to trigger one or more actions.
3. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - **Raise an alert**
   - **Validate manually**
   - **Enable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure disabled by default"
   - **Disable 3D Secure** if the shop's default 3D Secure behavior is set to "3D Secure enabled by default"
   - **Refuse**

   If you want to define one or more other actions:

4. Click **Add**.

5. Select another action that you wish to trigger when the profile appears.

6. Click **Save** at the bottom of the page.

4.8. Media tab

The **Media** tab allows to define one or several actions to perform depending on the type of the device used for the payment.

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.

2. Select one or more equipment type(s) from the list: “Computer, Tablet, Mobile Phone”.

3. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - **Raise an alert**
   - **Validate manually**
   - **Enable 3D Secure** if the shop’s default 3D Secure behavior is set to “3D Secure disabled by default”
   - **Disable 3D Secure** if the shop’s default 3D Secure behavior is set to “3D Secure enabled by default”
   - **Refuse**

   If you want to define one or more other actions:

4. Click **Add**.

5. Select another action that you wish to trigger when the profile appears.

6. Click **Save** at the bottom of the page.

4.9. SafeKey result tab

American Express SafeKey is a 3D Secure authentication tool that aims to reduce online fraud by authenticating American Express cardholders via an authentication code.

Card not enrolled in SafeKey program

To trigger one or more actions when the transaction is made with a card that is not enrolled in the Safekey program:

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.
2. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - Raise an alert
   - Validate manually
   - Refuse

   If you want to define one or more other actions:
3. Click **Add**.
4. Select another action that you wish to trigger when the profile appears.
5. Click **Save** at the bottom of the page.

Payment with a card for which it is impossible to verify the enrollment into SafeKey program

To trigger one or more actions when the transaction is made with a card whose enrollment in the American Express Safekey program cannot be verified due to a malfunction of their Directory Server:

1. Click the **Enable** button.
   The green bar indicates that the profile is activated.
2. Select the action that you wish to trigger when the profile appears.
   The possible values are:
   - Raise an alert
   - Validate manually
   - Refuse

   If you want to define one or more other actions:
3. Click **Add**.
4. Select another action that you wish to trigger when the profile appears.
5. Click **Save** at the bottom of the page.

4.10. Example

Disabling 3DS1 below a certain amount

1. Select the **Configuration** tab.
2. Define the shop's **3D Secure enabled by default** behavior.
3. Select the **Amount** tab.
4. Select **Minimum amount limit control**.
5. Click the **Enable** button.
   The green bar indicates that the profile is activated.
6. Enter the minimum transaction amount. AN action will be triggered if the transaction amount is lower than the specified amount.
7. Specify the currency that applies to the transaction amount.
8. Select the action **Disable 3D Secure**.
   This action will allow:
   - In 3DS1: to not perform cardholder authentication,
   - In 3DS2: to not express a specific preference concerning the authentication ("No Preference").

     If the issuer decides to perform an authentication without interaction (frictionless), the payment will be guaranteed.
9. Click **Save** at the bottom of the page.

5. CREATING NOTIFICATION RULES SPECIFIC TO RISK ASSESSMENT

Use case: The risk assessment action is configured in order to **Raise an alert**. The merchant wishes to receive an e-mail as soon as a verification process detects risk of fraud.

In order to create the associated notification rule:

1. In your Expert Back Office, go to the following menu: **Settings** > **Notification rules**.
2. Click the **Create a rule** button in the bottom left corner of the screen.
3. Select **Advanced notification**.

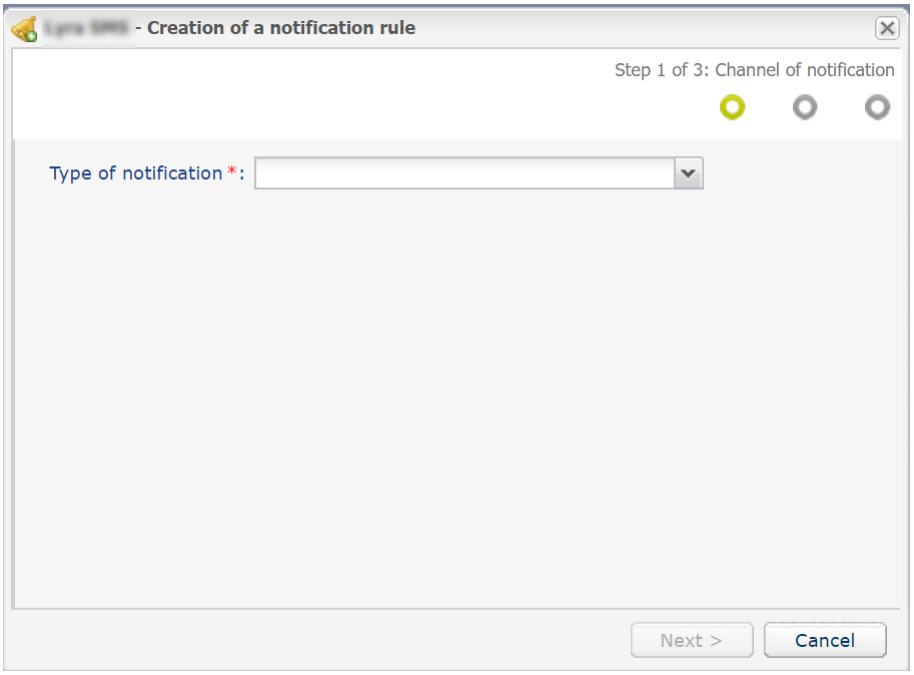

Figure 7: Creation of a notification rule wizard - step 1

4. Select the notification type (**E-mail sent to the merchant** in our use case).
5. Click **Next**.

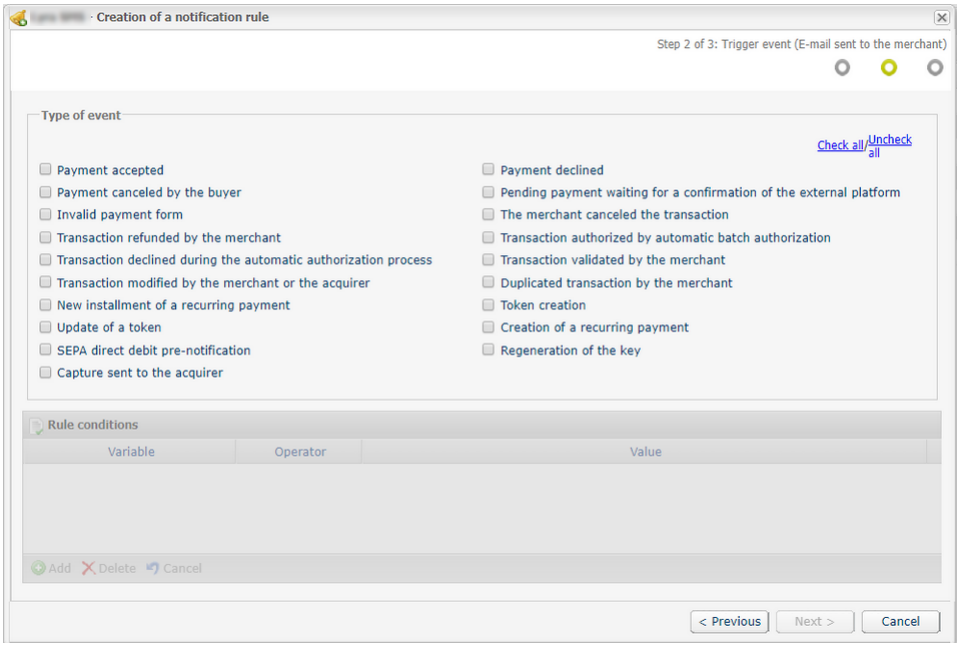

Figure 8: Creation of a notification rule wizard - step 2

6. Check the triggering events depending on your needs.
   Example: **Payment declined**, **Payment accepted** and **Token creation**.
7. In the **Rule Conditions** section, click **Add**.
8. In the **Variable** column, select **Informative risk assessment**.
9. Select the **equal to** operator.
10. Select the **Failed** value.
11. Click **Next**.
12. Enter the **Rule reference**.
13. Enter the e-mail address to notify.
14. By default, the risk controls details are included in the e-mails sent to the merchant.
15. If you want to change the content message, please click **Customize default text values** in the **E-mail Settings** section.
16. Once you have completed the configuration, click **Create**.

6. TRANSMITTING USEFUL DATA TO THE ADVANCED RISK ASSESSMENT

In order to perform the verification processes enabled and configured in the Expert Back Office, the payment request must contain the data to be analyzed.

For this reason, the Merchant must:

- Transmit the order details to know the shopping cart details,
- Transmit the buyer details to know the billing country (vads_cust_country),
- Transmit the shipping details to know the shipping country (vads_ship_to_country).

6.1. Transmitting order details

The Merchant can transmit the order details (order reference, description, shopping cart content, etc.). **To trigger one or several actions depending on the contents of the buyer's shopping cart, the shopping cart data must imperatively be transmitted in the payment request.**

This information can be found in the transaction details in the Expert Back Office.

Field name	Description	Value
Hosted Payment Page: **vads_order_id** REST API: **orderId**	Order ID	E.g.: 2-XQ001
Hosted Payment Page: **vads_order_info** REST API: **metadata.info1**	Complementary order details	E.g.: Door phone code 3125
Hosted Payment Page: **vads_order_info2** REST API: **metadata.info2**	Complementary order details	E.g.: No elevator
Hosted Payment Page: **vads_order_info3** REST API: **metadata.info3**	Complementary order details	E.g.: Express
Hosted Payment Page: **vads_nb_products** REST API: N/A	Number of items in the cart	E.g.: 2
Hosted Payment Page: **vads_product_ext_idN** REST API: N/A	Product bar code on the merchant website. N corresponds to the index of the item (0 for the first one, 1 for the second one, etc.).	E.g.: 0123654789123654789
Hosted Payment Page: **vads_product_labelN** REST API: **cartItemInfo.productLabel**	Item name. N corresponds to the index of the item (0 for the first one, 1 for the second one, etc.).	E.g.: 3 day stay with dates
Hosted Payment Page: **vads_product_amountN** REST API: **cartItemInfo.productLabel**	Item amount expressed in the smallest currency unit. N corresponds to the index of the item (0 for the first one, 1 for the second one, etc.).	E.g.: 32150
Hosted Payment Page: **vads_product_typeN** REST API: **cartItemInfo.productType**	Item type. N corresponds to the index of the item (0 for the first one, 1 for the second one, etc.). See the table with values below.	E.g.: TRAVEL
Hosted Payment Page: **vads_product_refN** REST API: **cartItemInfo.productRef**	Item reference. N corresponds to the index of the item (0 for the first one, 1 for the second one, etc.).	E.g.: 1002127784

Field name	Description	Value
Hosted Payment Page: **vads_product_qtyN** REST API: **cartItemInfo.productQty**	Quantity of items. N corresponds to the index of the item (0 for the first one, 1 for the second one, etc.).	E.g.: 1
Hosted Payment Page: **vads_product_vatN** REST API: **cartItemInfo.productVat**	Item tax. N corresponds to the index of the item (0 for the first one, 1 for the second one, etc.).	
Hosted Payment Page: **vads_shipping_amount** REST API: **shoppingCart.shippingAmount**	Shipping fee amount expressed in the smallest currency unit.	
Hosted Payment Page: **vads_tax_amount** REST API: **shoppingCart.taxAmount**	Tax amount for the entire order expressed in the smallest currency unit.	

Item type (vads_product_type / productType).

Value	Description
FOOD_AND_GROCERY	Food and grocery
AUTOMOTIVE	Cars / Moto
ENTERTAINMENT	Entertainment / Culture
HOME_AND_GARDEN	Home and gardening
HOME_APPLIANCE	Household appliances
AUCTION_AND_GROUP_BUYING	Auctions and group purchasing
FLOWERS_AND_GIFTS	Flowers and presents
COMPUTER_AND_SOFTWARE	Computers and software
HEALTH_AND_BEAUTY	Health and beauty
SERVICE_FOR_INDIVIDUAL	Services for individuals
SERVICE_FOR_BUSINESS	Services for companies
SPORTS	Sports
CLOTHING_AND_ACCESSORIES	Clothes and accessories
TRAVEL	Travel
HOME_AUDIO_PHOTO_VIDEO	Sound, image and video
TELEPHONY	Telephony

6.2. Transmitting buyer details

The Merchant can specify the buyer's billing details (e-mail address, title, phone number, etc.). This information will be used to create the invoice.

All the data transmitted via the payment form can be viewed in the transaction details in the Expert Back Office (**Buyer** tab).

Field name	Description	Value
Hosted Payment Page: **vads_cust_email** REST API: **customer.email**	Buyer's e-mail address	E.g.: abc@example.com
Hosted Payment Page: **vads_cust_id** REST API: **customer.reference**	Buyer reference on the merchant website	E.g.: C2383333540
Hosted Payment Page: **vads_cust_title** REST API: **customer.billingDetails.title**	Buyer's title	E.g.: Mister
Hosted Payment Page: **vads_cust_status** REST API: **customer.billingDetails.category**	Status	**PRIVATE**: for private clients **COMPANY**: for companies
Hosted Payment Page: **vads_cust_first_name** REST API: **customer.billingDetails.firstName**	First name	E.g.: John
Hosted Payment Page: **vads_cust_last_name** REST API: **customer.billingDetails.lastName**	Name	E.g.: Smith
Hosted Payment Page: **vads_cust_legal_name** REST API: **N/A**	Buyer's legal name	E.g.: D. & Cie
Hosted Payment Page: **vads_cust_cell_phone** REST API: **customer.billingDetails.cellPhoneNumb**	Cell phone number	E.g.: 06 12 34 56 78
Hosted Payment Page: **vads_cust_address_number** REST API: **customer.billingDetails.streetNumber**	Street number	E.g.: 109
Hosted Payment Page: **vads_cust_address** REST API: **customer.billingDetails.address**	Postal address	E.g.: Rue de l'innovation
Hosted Payment Page: **vads_cust_address2** REST API: **customer.billingDetails.address2**	Second line of the address	E.g.:
Hosted Payment Page: **vads_cust_district** REST API: **customer.billingDetails.district**	District	E.g.: Downtown
Hosted Payment Page: **vads_cust_zip** REST API: **customer.billingDetails.zipcode**	Zip code	E.g.: 31670
Hosted Payment Page: **vads_cust_city** REST API: **customer.billingDetails.city**	City	E.g.: Labège
Hosted Payment Page: **vads_cust_state**	State / Region	E.g.: Occitanie

Field name	Description	Value
REST API: **customer.billingDetails.state**		
Hosted Payment Page: **vads_cust_country** REST API: **customer.billingDetails.country**	Country code in compliance with the ISO 3166 alpha-2 standard. **Must be transmitted in order to trigger one or several actions depending on the buyer's country**.	E.g.: "FR" for France, "PF" for French Polynesia, "NC" for New Caledonia, "US" for the United States

Note

vads_cust_phone and **vads_cust_cell_phone** fields accept all formats:

Examples:

- 0123456789
- +33123456789
- 0033123456789
- (00.571) 638.14.00
- 40 41 42 42

6.3. Transmitting shipping details

The Merchant can transmit the buyer's shipping details (e-mail address, phone number etc.).

This information can be found in the transaction details in the Expert Back Office (**Delivery** tab).

Field name	Description	Value
Hosted Payment Page: **vads_ship_to_city** REST API: **customer.shippingDetails.city**	City	E.g.: Bordeaux
Hosted Payment Page: **vads_ship_to_country** REST API: **customer.shippingDetails.country**	Country code in compliance with the ISO 3166 standard. **Must imperatively be transmitted for triggering one or more actions if the Shipping country control profile is enabled**.	E.g.: FR
Hosted Payment Page: **vads_ship_to_district** REST API: **customer.shippingDetails.district**	District	E.g.: La Bastide
Hosted Payment Page: **vads_ship_to_first_name** REST API: **customer.shippingDetails.firstName**	First name	E.g.: John
Hosted Payment Page: **vads_ship_to_last_name** REST API: **customer.shippingDetails.lastName**	Name	E.g.: Smith
Hosted Payment Page: **vads_ship_to_legal_name** REST API: **customer.shippingDetails.legalName**	Legal name	E.g.: D. & Cie
Hosted Payment Page: **vads_ship_to_phone_num** REST API: **customer.shippingDetails.phoneNumbe**	Phone number	E.g.: 0460030288
Hosted Payment Page: **vads_ship_to_state** REST API: **customer.shippingDetails.state**	State / Region	E.g.: Nouvelle Aquitaine
Hosted Payment Page: **vads_ship_to_status** REST API: **customer.shippingDetails.status**	Allows to specify the type of the shipping address.	**PRIVATE**: for shipping to a private individual **COMPANY**: for shipping to a company
Hosted Payment Page: **vads_ship_to_street_number** REST API: **customer.shippingDetails.streetNumbe**	Street number	E.g.: 2
Hosted Payment Page: **vads_ship_to_street** REST API: **customer.shippingDetails.address**	Postal address	E.g.: Rue Sainte Catherine

Field name	Description	Value
Hosted Payment Page: **vads_ship_to_street2** REST API: **customer.shippingDetails.address2**	Second line of the address	
Hosted Payment Page: **vads_ship_to_zip** REST API: **customer.shippingDetails.zipCode**	Zip code	E.g.: 33000

Note

The **vads_ship_to_phone_num** field supports all formats:

Examples:

- 0123456789
- +33123456789
- 0033123456789
- (00.571) 638.14.00
- 40 41 42 42

7. VIEWING TRANSACTION DETAILS FROM THE EXPERT BACK OFFICE

Transactions can be viewed via the **Management** > **Transactions** menu.

To view the details of a transaction:

1. Select a transaction.

2. Rick click and select **Display transaction details**.
   The **Details of a transaction** dialog box appears.
   The content of the **Details** tab is displayed by default.
   Transaction lifecycle contains the transaction status.

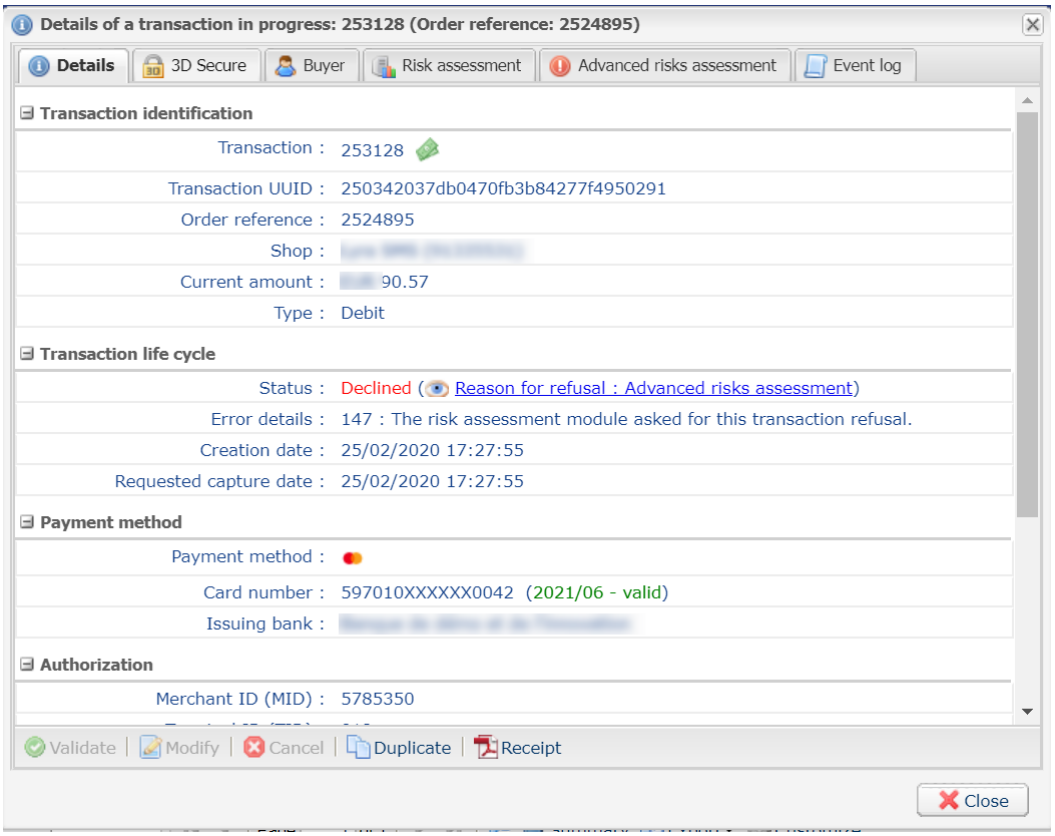

Figure 9: Details tab

3. Click the **Advanced risk assessment** tab to identify the applied rule and the executed action.

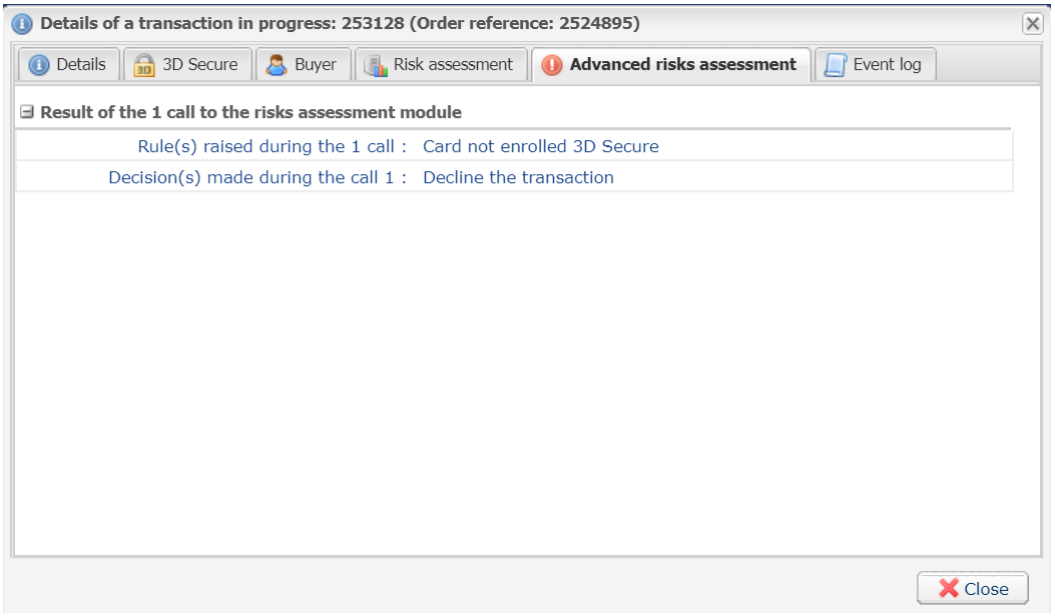

Figure 10: Advanced risks assessment tab

8. MANUAL VALIDATION OF A TRANSACTION

If the merchant has opted for manual validation of the transaction during profile configuration, he/she will have to subsequently validate the payment in the Back Office.

To do this:

1. Right-click on the transaction with the **To be validated** status.
2. Select **Validate**.
3. Confirm that you really wish to validate the selected transaction.

9. IDENTIFYING AND ANALYZING THE DIFFERENT ACTIONS RETURNED BY THE ADVANCED RISK ASSESSMENT MODULE

The actions returned by the advanced risk assessment module are returned in the IPN via the fields:

- **vads_risk_assessment_result** for the hosted payment page
- **fraudManagement.riskAssessments.results** for the REST API

The possible values are:

Values	Description
ENABLE_3DS	3D Secure enabled.
DISABLE_3DS	3D Secure disabled.
MANUAL_VALIDATION	The transaction has been created via manual validation. The payment capture is temporarily blocked to allow the merchant to perform all the desired verification processes.
REFUSE	The transaction is refused.
RUN_RISK_ANALYSIS	Call to an external risk analyzer if the Merchant has a contract.
INFORM	A warning message appears. The Merchant is notified that a potential problem has been identified. The Merchant is informed via one or several notification center rules (IPN, e-mail or SMS).

