



Advanced risk assessment

Back Office user manual

Document version 2.0

Contents

1. HISTORY OF THE DOCUMENT.....	4
2. PRESENTATION OF THE SERVICE.....	5
2.1. Prerequisites.....	5
2.2. Understanding the control process.....	6
3. OPERATING PRINCIPLE.....	7
3.1. Risk assessment and 3D Secure authentication.....	7
3.2. Criteria.....	8
3.3. Actions.....	9
4. CONFIGURING THE ADVANCED RISK ASSESSMENT VIA THE MERCHANT BACK OFFICE.....	11
4.1. Configuration tab.....	12
4.2. 3D Secure result tab.....	13
4.2.1. 3D Secure payment with a cardholder whose authentication cannot be verified.....	15
4.2.2. Card not enrolled in the 3D Secure program.....	15
4.2.3. 3D Secure payment with a card whose enrollment cannot be verified.....	16
4.2.4. Liability shift.....	16
4.3. Amount tab.....	17
4.3.1. Amount control.....	17
4.3.2. Minimum amount limit control.....	18
4.3.3. Maximum amount limit control.....	19
4.3.4. Control of the total amount for a payment method over a week.....	20
4.4. Payment method tab.....	21
4.4.1. Control of corporate cards.....	21
4.4.2. Control of corporate cards depending on their origin.....	22
4.4.3. Control of prepaid cards.....	23
4.4.4. Control of cards with unconditional authorization.....	24
4.4.5. Control of e-Carte Bleue.....	25
4.4.6. Control of personal credit cards.....	26
4.4.7. Control of personal debit cards.....	27
4.5. Shopping cart tab.....	28
4.5.1. Control of the number of items in the cart.....	28
4.5.2. Shopping cart items control.....	29
4.6. Country tab.....	30
4.6.1. Customer country control (billing address).....	30
4.6.2. Control of the shipping country.....	31
4.6.3. Control of diversity of countries.....	32
4.6.4. Control of card types issued by certain countries.....	33
4.6.5. Country control for SDD payments.....	34
4.7. Velocity tab.....	35
4.7.1. Velocity of an e-mail address within a week.....	35
4.7.2. Velocity of an IP address within a week.....	36
4.7.3. Velocity of a payment method over a week.....	36
4.8. Media tab.....	37
4.9. SafeKey result tab.....	38
4.9.1. Card not enrolled in SafeKey program.....	38
4.9.2. Payment with a card for which it is impossible to verify the enrollment into SafeKey program.....	39
5. CREATING NOTIFICATION RULES SPECIFIC TO RISK ASSESSMENT.....	40
6. TRANSMITTING USEFUL DATA TO THE ADVANCED RISK ASSESSMENT.....	42
6.1. Transmitting order details.....	42
6.2. Transmitting buyer details.....	44

6.3. Transmitting shipping details.....	46
7. VIEWING TRANSACTION DETAILS FROM THE MERCHANT BACK OFFICE.....	48
8. MANUAL VALIDATION OF A TRANSACTION.....	50
9. RETURN OF THE ADVANCED RISK ASSESSMENT MODULE RESULT IN THE IPN.....	51
10. OBTAINING HELP.....	52

1. HISTORY OF THE DOCUMENT

Version	Author	Date	Comment
2.0.	La Banque Postale	8/17/2022	<ul style="list-style-type: none">Update of the description of the vads_risk_assessment_result field values in the chapter <i>Restitution of the advanced risk assessment module result in the IPN</i>.
1.9	La Banque Postale	9/30/2021	<ul style="list-style-type: none">Update of the action description.New action available for 3D Secure v2.Update of the Configuration tab.Update of the chapter <i>Creating notification rules specific to risk assessment</i>.Update of the description of the vads_risk_assessment_result field values in the chapter <i>Restitution of the advanced risk assessment module result in the IPN</i>.
1.8	La Banque Postale	4/23/2021	<ul style="list-style-type: none">Update of the <i>Liability shift</i> chapter:<ul style="list-style-type: none">Amex transactions now benefit from liability shift.The “Liability shift” rule does not apply if 3DS is disabled or if the transaction is not eligible for 3DS.Addition of the 3DS2 schematic diagram in the chapter <i>3D Secure result tab</i>.
1.7	La Banque Postale	4/22/2020	<ul style="list-style-type: none">Addition of the equivalence between the Hosted Payment Page and REST API fields.
1.6	La Banque Postale	8/30/2019	Initial version

This document and its contents are confidential. It is not legally binding. Any reproduction and / or distribution of all or part of this document or its content to a third party is strictly prohibited or subject to prior written authorization from La Banque Postale. All rights reserved.

2. PRESENTATION OF THE SERVICE

The Scellius payment gateway is a PCI-DSS certified highly secure payment solution. Each payment attempt systematically involves an authorization request sent to the cardholder's bank. In case the merchant is enrolled with CB, Visa, Mastercard, American Express or Diners Club, the payment process also includes cardholder authentication.

However, distance selling can present risks of chargebacks that are detrimental to your business.

In order to **provide an additional level of security to the merchant**, the payment gateway provides the **Advanced risk assessment** feature.

This functionality allows you to:

- Minimize the risk of chargeback by refusing transactions deemed fraudulent.
- Add verifications in case of suspected fraud.

The **Advanced risk assessment** service provides a tailored and comprehensive service to help you fight fraud. Specific filters are provided for defining preventive actions according to the level of risk and the characteristics of your activity while avoiding negative impact on your sales. Advanced risk assessment can be configured by taking into account known risks or previous issues with fraud. It is now up to you to adapt your rules according to the profile of your buyers and the transactions they make.

2.1. 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 E-Banking Merchant Support Service.

2.2. Understanding the control process

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

- Maximum 3 times:
 - After validation of the input data
 - After cardholder authentication
 - After authorization

With each call, the service 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.

3. OPERATING PRINCIPLE

The gateway provides a number of risk assessment 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 rule criteria are validated.

Examples:

- A simple rule with one criterion and one action: if the amount over a week is higher than EUR 500, refuse the payment.
- A more complex rule with two criteria and one action: if the buyer's country is different from the merchant's country and the amount is higher than EUR 100, the transaction will have to be validated manually.

3.1. 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 [3D Secure result tab](#) on page 13 chapter for more information).

The advanced risk assessment allows to perform two specific actions when configuring the rules:

- "Enable 3D Secure" and "Disable 3D Secure" when 3D Secure v1 is enabled for at least one of the contracts associated with the store.
- "Define an authentication mode" when 3D Secure v2 is also enabled on at least one of the contracts associated with the store.

Based on the protocols available for their contract, these actions allow the merchant:

- In 3D Secure v1, to enable or disable 3D Secure authentication.
- In v2 3D Secure, to express their desire to challenge the buyer with strong authentication during the payment.

Via the payment requests, authorized merchants can:

- Enable or disable the 3D Secure v1 authentication (requires the "Selective 3DS1" option).
- Request 3D Secure v2 authentication without cardholder interaction or frictionless, if an exemption applies (see "[Application of exemptions](#)") and if the shop has the "Frictionless 3DS2" option).

For this, they use the **strongAuthentication** field of the REST API or the **vads_threeds_mpi** field of the Hosted Payment Page.

This functionality 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.

Application of exemptions:

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 their payment requests or via the risk assessment module):

- Some payment cards require cardholder authentication. This is the case of Maestro cards.
- 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.

3.2. 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.
- **Velocity criteria**
These include the criteria that evolve depending on the activity of the card, of the e-mail, etc. in the merchant shop.

3.3. Actions

Several actions are available to the Merchant.

Action	Description
Validate manually	<p>This action allows to temporarily block the payment capture. In the meantime, the Merchant can verify the transaction and decide if they wish to validate or cancel it.</p> <p>The transaction is then created via manual validation. It can be validated as long as the capture delay has not passed. After this delay, the payment takes the Expired status. This status is final.</p> <p>When the transaction is created in manual validation mode following the application of a risk rule, the merchant is notified via the instant payment notification.</p> <p>The vads_risk_assessment_result field is set to MANUAL_VALIDATION.</p> <p>The merchant cannot define a specific notification rule to be notified about this action.</p> <p>This action can be combined with other actions, such as Raise an alert or Define an authentication mode.</p>
Refuse the payment	<p>This action allows to refuse a payment.</p> <p><u>Example</u>: refuse a payment if the used card is a corporate card.</p> <p>Refuse action has priority over Validate manually.</p>
Raise an alert	<p>This action allows to warn the merchant that a risk has been identified.</p> <p><u>Examples</u>: the amount of the transaction is higher than EUR 1000, the transaction has been made with a card from a country considered as high-risk for online fraud, etc.</p> <p>This action can be combined with other actions, such as Validate manually or Define an authentication mode.</p> <p>The alert allows the merchant to trigger processing or verification for the transaction, such as placing the delivery process on hold until checks can be performed on the transaction.</p> <p>The merchant is warned:</p> <ul style="list-style-type: none"> • Via the instant payment notification: The vads_risk_assessment_result field is set to INFORM. • By e-mail: The merchant must create a specific e-mail notification rule to receive the alert by e-mail. The condition for triggering the notification rule is Informative risk assessment = Failed. For more information on the notification configuration process, please see chapter Creating notification rules specific to risk assessment on page 40.
Define an authentication mode.	<p>This action is only available if 3D Secure v2 is enabled for at least one of the contracts associated with the shop.</p> <p>It allows to change the default authentication mode (NO_PREFERENCE) applied upon the payment.</p> <p>The available choices depend on the store's options.</p> <p>If your store has the "Frictionless 3DS2" option and is associated with an activated 3DS2 contract, you will have the choice between the following authentication modes:</p> <ul style="list-style-type: none"> • Authentication request with buyer interaction (Challenge)

Action	Description
	<ul style="list-style-type: none"><li data-bbox="547 159 1358 190">• Authentication request without buyer interaction (Frictionless) <p data-bbox="547 215 1441 315">If “Frictionless” is selected, 3D Secure v2 authentication will be performed with the merchant preference forced to Frictionless if an exemption applies (<i>see “Application of exemptions”</i>).</p> <p data-bbox="547 327 1214 358">For additional information, click “?” in the Help column.</p> <p data-bbox="547 367 1139 398"><i>Action not available in the “3D Secure result” tab.</i></p>

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

The advanced risk assessment is accessible via the Back Office.

To access it:

1. Sign in to the Back Office: <https://scelliuspaiement.labanquepostale.fr/vads-merchant/>.
2. Select **Settings** > **Advanced risk assessment** menu.

Note:

If you have multiple shops, select a shop.

Controls are grouped by tabs:

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

4.1. Configuration tab

This tab indicates the shop's "3D Secure by default behavior".

 **Advanced risk assessment module**

Default **3D Secure** store behavior: 3D Secure v2 authentication request with merchant preference set to "No requested" / 3D Secure v1 enabled.

If the card is enrolled for 3D Secure v2, authentication is performed with the merchant preference set to "No preference". In this case, the issuing bank decides which authentication mode is most suitable based on the characteristics of the transaction.

If the card is enrolled for 3D Secure v1, authentication is attempted in the 3D Secure v1.

If the card is not enrolled for 3D Secure, there is no prior authentication of the buyer **and you will not benefit from the liability shift.**

4.2. 3D Secure result tab

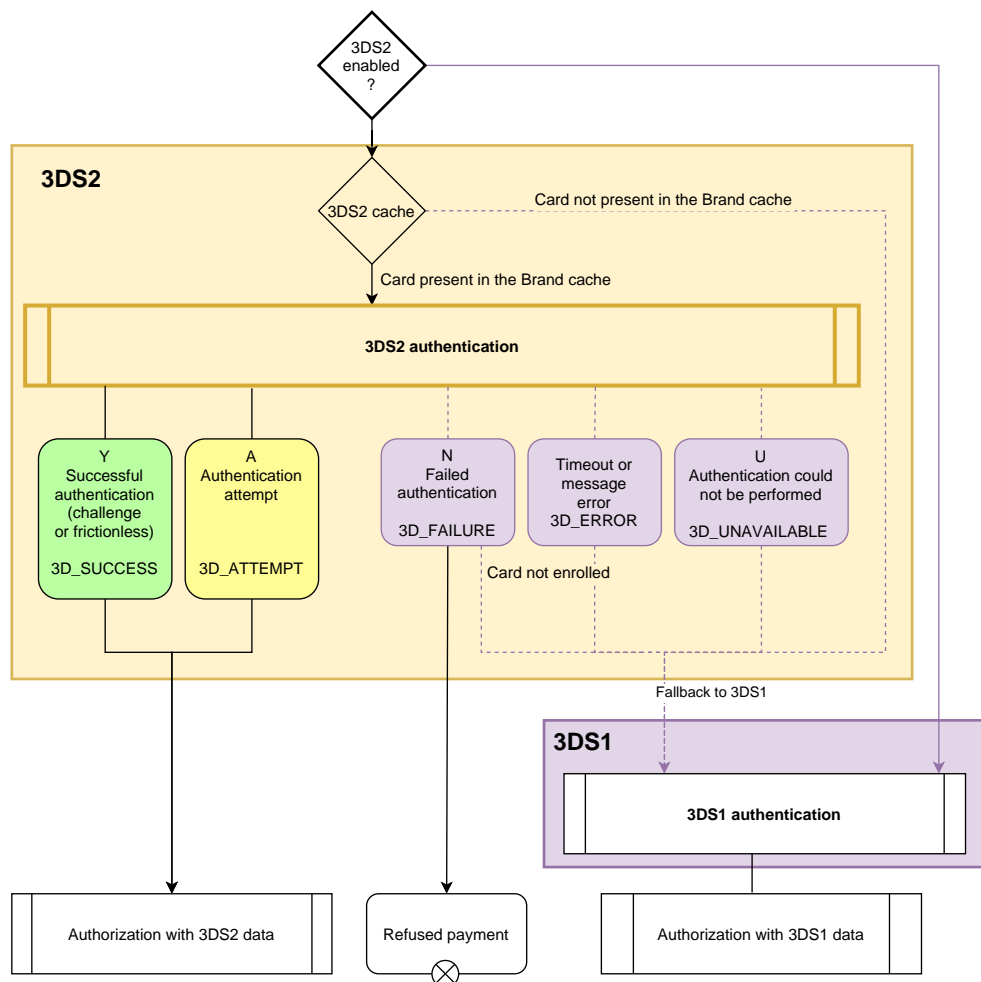
3D Secure (also called "*Paiement sécurisé*" by CB, "*Visa Secure*" by Visa, "*Mastercard Identity check*" by Mastercard and "*Safekey*" by American Express) is an international protocol standard used for securing online transactions.

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.

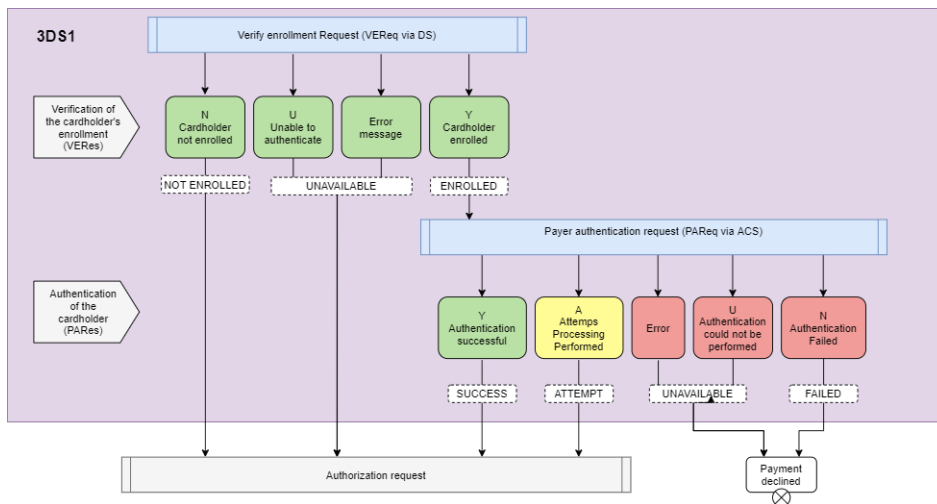
Its purpose is to:

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

The diagram below illustrates the principle of the 3D Secure 2 authentication:



The diagram below illustrates the principle of the 3D Secure 1 authentication:



Thus, depending on the results returned, the payment gateway provides several profiles to trigger actions.

4.2.1. 3D Secure payment with a cardholder whose authentication cannot be verified

In order to trigger one or several actions when the cardholder's 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.

For more information, please see chapter [Actions](#) on page 9.

3. If you want to define one or more other actions, click **Add**.

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

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

4.2.2. 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.

For more information, please see chapter [Actions](#) on page 9.

3. If you want to define one or more other actions, click **Add**.

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

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

4.2.3. 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.

For more information, please see chapter [Actions](#) on page 9.

3. If you want to define one or more other actions, click **Add**.

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

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

4.2.4. 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 “Cardholder dispute”.

This rule is not triggered if 3D Secure is disabled (only possible in 3DS1) or if 3DS is not applicable for the transaction (e.g. MOTO payment).

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.

For more information, please see chapter [Actions](#) on page 9.

4. If you want to define one or more other actions, click **Add**.

5. Select another action that you want 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.

4.3.1. Amount control

Depending on the payment amount, amount control can be enabled.

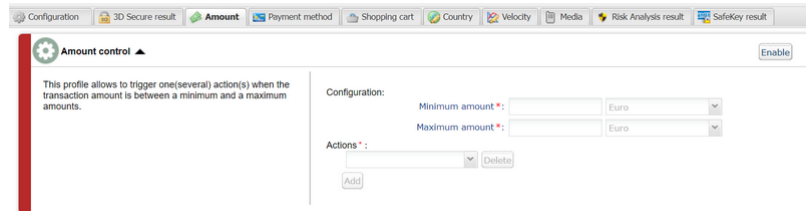


Figure 1: Amount tab

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.

For more information, please see chapter [Actions](#) on page 9.

5. If you want to define one or more other actions, click **Add**.

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

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

4.3.2. Minimum amount limit control

It is possible to enable a control from a minimum amount.

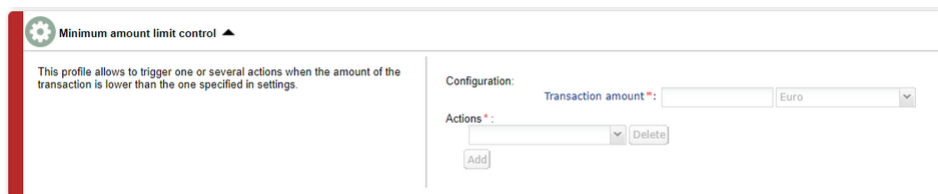


Figure 2: Minimum amount limit control

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.
For more information, please see chapter [Actions](#) on page 9.
5. If you want to define one or more other actions, click **Add**.
6. Select another action that you want to trigger when the profile appears.
7. Click **Save** at the bottom of the page.

4.3.3. Maximum amount limit control

It is possible to enable a control from a maximum amount.

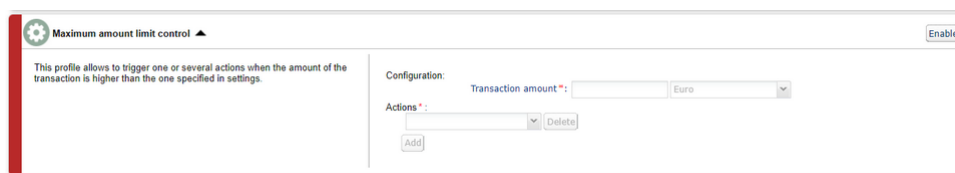


Figure 3: Maximum amount limit control

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.

For more information, please see chapter [Actions](#) on page 9.

5. If you want to define one or more other actions, click **Add**.

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

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

4.3.4. Control of the total amount for a payment method over a week

It is possible to enable a verification of the total amount paid with a payment method over a week.

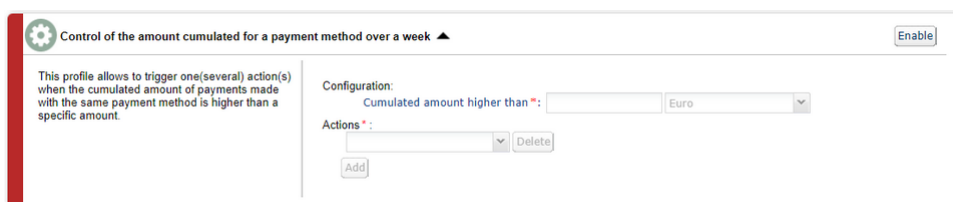


Figure 4: Control of the total amount

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 total amount.
4. Select the action that you wish to trigger when the profile appears.
For more information, please see chapter [Actions](#) on page 9.
5. If you want to define one or more other actions, click **Add**.
6. Select another action that you want 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.

4.4.1. Control of corporate cards

A corporate 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 corporate 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.

The controlled cards are :

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

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

For more information, please see chapter [Actions](#) on page 9.

4. If you want to define one or more other actions, click **Add**.

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

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

4.4.2. Control of corporate cards depending on their origin

A corporate 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 corporate 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.

The controlled cards are :

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

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

For more information, please see chapter [Actions](#) on page 9.

5. If you want to define one or more other actions, click **Add**.

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

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

4.4.3. 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.

The controlled cards are :

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

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

For more information, please see chapter [Actions](#) on page 9.

4. If you want to define one or more other actions, click **Add**.

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

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

4.4.4. 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.

For more information, please see chapter [Actions](#) on page 9.

4. If you want to define one or more other actions, click **Add**.

5. Select another action that you want 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.

4.4.5. Control of e-Carte Bleue

An e-Carte Bleue is a virtual card that provides a temporary 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.

For more information, please see chapter [Actions](#) on page 9.

3. If you want to define one or more other actions, click **Add**.

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

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

4.4.6. 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.

The controlled cards are :

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

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

For more information, please see chapter [Actions](#) on page 9.

4. If you want to define one or more other actions, click **Add**.

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

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

4.4.7. 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.

The controlled cards are :

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

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

For more information, please see chapter [Actions](#) on page 9.

4. If you want to define one or more other actions, click **Add**.

5. Select another action that you want 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.

4.5.1. 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.

For more information, please see chapter [Actions](#) on page 9.

4. If you want to define one or more other actions, click **Add**.

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

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

4.5.2. 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.

For more information, please see chapter [Actions](#) on page 9.

4. If you want to define one or more other actions, click **Add**.

5. Select another action that you want 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.

4.6.1. 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.

For more information, please see chapter [Actions](#) on page 9.

4. If you want to define one or more other actions, click **Add**.

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

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

4.6.2. 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.

For more information, please see chapter [Actions](#) on page 9.

4. If you want to define one or more other actions, click **Add**.

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

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

4.6.3. 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.

For more information, please see chapter [Actions](#) on page 9.

6. If you want to define one or more other actions, click **Add**.

7. Select another action that you want to trigger when the profile appears.

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

4.6.4. 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, corporate 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**

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.).

- **Corporate card**

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

- **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.

For more information, please see chapter [Actions](#) on page 9.

5. If you want to define one or more other actions, click **Add**.

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

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

4.6.5. Country control for SDD payments

This profile allows to trigger actions when the bank account (IBAN) country is on the list of selected countries.

All the countries are accepted by default.

To trigger one or more actions:

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.

For more information, please see chapter [Actions](#) on page 9.

4. If you want to define one or more other actions, click **Add**.

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

6. 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.

4.7.1. 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.

For more information, please see chapter [Actions](#) on page 9.

4. If you want to define one or more other actions, click **Add**.

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

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

4.7.2. 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.
For more information, please see chapter [Actions](#) on page 9.
4. If you want to define one or more other actions, click **Add**.
5. Select another action that you want to trigger when the profile appears.
6. Click **Save** at the bottom of the page.

4.7.3. 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.
For more information, please see chapter [Actions](#) on page 9.
4. If you want to define one or more other actions, click **Add**.
5. Select another action that you want 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) device(s) from the list: “Computer, Tablet, Mobile Phone”.

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

For more information, please see chapter [Actions](#) on page 9.

4. If you want to define one or more other actions, click **Add**.

5. Select another action that you want 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.

4.9.1. 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.

For more information, please see chapter [Actions](#) on page 9.

3. If you want to define one or more other actions, click **Add**.

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

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

4.9.2. 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.

For more information, please see chapter [Actions](#) on page 9.

3. If you want to define one or more other actions, click **Add**.

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

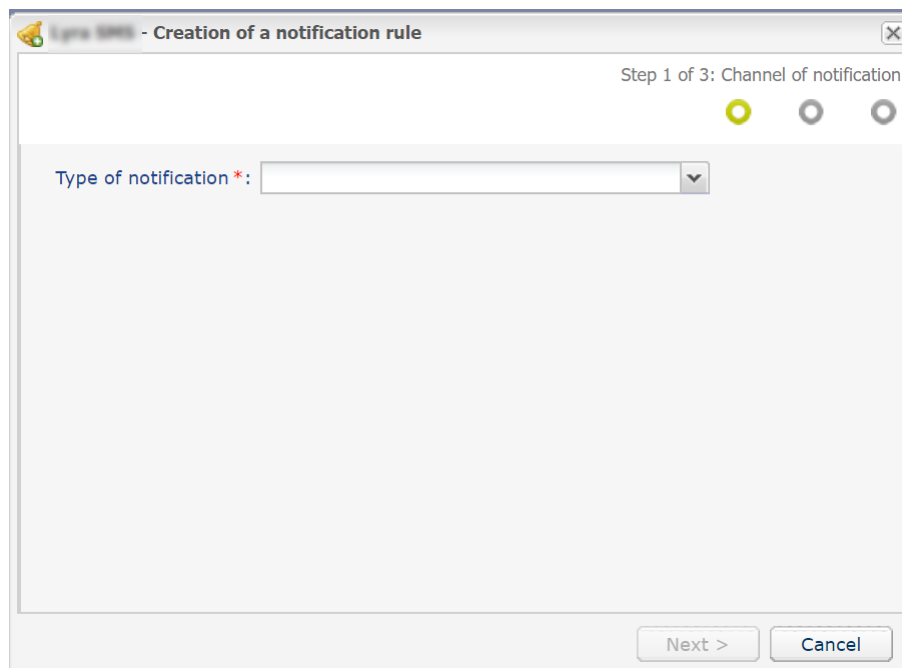
5. Click **Save** at the bottom of the page.

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.

To create the associated notification rule:

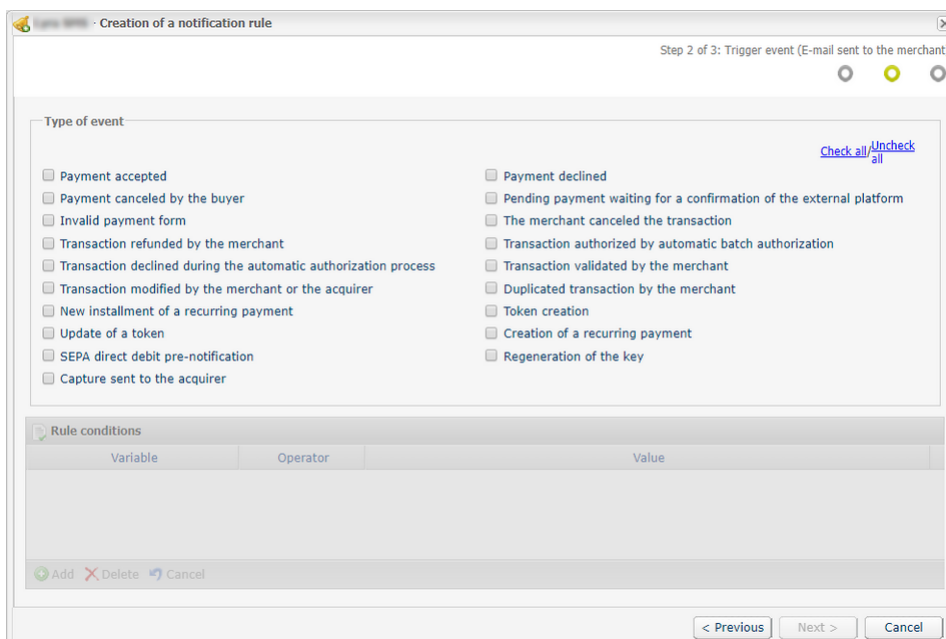
1. In your Merchant Back Office, go to the following menu: **Settings > Notification rules**.
2. Click the **Create a rule** button in the bottom left corner of the screen.
3. Select **Advanced notification**.



The screenshot shows a dialog box titled "Lycos 2000 - Creation of a notification rule". The window title bar includes a close button (X). The main content area is titled "Step 1 of 3: Channel of notification" and features three progress indicators: the first is a yellow circle, the second and third are grey circles. Below the title, there is a label "Type of notification *:" followed by a dropdown menu. At the bottom right, there are two buttons: "Next >" and "Cancel".

4. Select the notification type: **E-mail sent to the merchant**.

5. Click **Next**.



The screenshot shows the same dialog box, now at "Step 2 of 3: Trigger event (E-mail sent to the merchant)". The progress indicators show the second circle as yellow. The "Type of event" section contains a list of checkboxes for various events, such as "Payment accepted", "Payment declined", "Transaction declined during the automatic authorization process", etc. A link "Check all/Uncheck all" is visible on the right. Below this is a "Rule conditions" section with a table with columns "Variable", "Operator", and "Value". At the bottom, there are buttons for "< Previous", "Next >", and "Cancel".

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. Select the fields to be included in the e-mail.

By default, the information of the advanced risk assessment module is already included.

15. If you want to change the message body, click **Customize default text values** in the **E-mail settings** section.

16. Once you have completed the configuration, click **Create**.

When a risk rule configured with the **Raise an alert** action is triggered, the merchant receives an e-mail containing the details of the call to the advanced risk assessment module:

Details of the call to the risk assessment module

 **Raise an alert**

6. TRANSMITTING USEFUL DATA TO THE ADVANCED RISK ASSESSMENT

In order to perform the verification processes enabled and configured in the Merchant 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` / `customer.billingDetails.country`),
- Transmit the shipping details to know the shipping country (`vads_ship_to_country` / `customer.shippingDetails.country`).

6.1. Transmitting order details

The merchant can indicate in their payment form if they wish to transfer the order details (order reference, description, shopping cart contents, 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 Merchant Back Office (**Shopping cart** tab).

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.orderInfo1	Complementary order details	E.g.: Door code 3125
Hosted Payment Page : vads_order_info2 REST API : metadata.orderInfo2	Complementary order details	E.g.: No elevator
Hosted Payment Page : vads_order_info3 REST API : metadata.orderInfo3	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 barcode 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	E.g.: 32150

Field name	Description	Value
	item (0 for the first one, 1 for the second one, etc.).	
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
Hosted Payment Page : vads_product_qtyN REST API : cartItemInfo.productQty	Item quantity. N corresponds to the index of the item (0 for the first one, 1 for the second one, etc.).	E.g.: 1

Item type (vads_product_type / productType)

Value	Description
FOOD_AND_GROCERY	Food and grocery
AUTOMOTIVE	Cars / Moto
ENTERTAINMENT	Entertainment / Culture
HOME_AND_GARDEN	Home / Gardening
HOME_APPLIANCE	Household appliances
AUCTION_AND_GROUP_BUYING	Auctions / Group purchasing
FLOWERS_AND_GIFTS	Flowers / Presents
COMPUTER_AND_SOFTWARE	Computers / Software
HEALTH_AND_BEAUTY	Health / Beauty
SERVICE_FOR_INDIVIDUAL	Services for individuals
SERVICE_FOR_BUSINESS	Services for companies
SPORTS	Sports
CLOTHING_AND_ACCESSORIES	Clothes / Accessories
TRAVEL	Travel
HOME_AUDIO_PHOTO_VIDEO	Audio / Photo / 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 Merchant 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.: name@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.: Laurent
Hosted Payment Page : vads_cust_last_name REST API : customer.billingDetails.lastName	Last name	E.g.: Durant
Hosted Payment Page : vads_cust_legal_name REST API : customer.billingDetails.legalName	Buyer's legal name	E.g.: D. & Cie
Hosted Payment Page : vads_cust_cell_phone REST API : customer.billingDetails.cellPhoneN	Cell phone number	E.g.: 06 12 34 56 78
Hosted Payment Page : vads_cust_address_number REST API : customer.billingDetails.streetNumb	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	Address line 2	E.g.:

Field name	Description	Value
Hosted Payment Page : vads_cust_district REST API : customer.billingDetails.district	District	E.g.: Centre ville
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 REST API : customer.billingDetails.state	State / Region	E.g.: Occitanie
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, title, phone number etc.).

This information can be found in the transaction details in the Merchant Back Office (**Shipping 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.: Albert
Hosted Payment Page : vads_ship_to_last_name REST API : customer.shippingDetails.lastName	Last name	E.g.: Durant
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.phoneNu	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.streetNu	Street number	E.g.: 2
Hosted Payment Page : vads_ship_to_street	Postal address	E.g.: Rue Sainte Catherine

Field name	Description	Value
REST API : customer.shippingDetails.address		
Hosted Payment Page : vads_ship_to_street2 REST API : customer.shippingDetails.address2	Address line 2	
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 MERCHANT BACK OFFICE

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

To view the details of a transaction:

1. Select a transaction.
2. Right 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.

Details of a transaction in progress: 253128 (Order reference: 2524895)

Details | 3D Secure | Buyer | Risk assessment | Advanced risks assessment | Event log

Transaction identification

Transaction : 253128

Transaction UUID : 250342037db0470fb3b84277f4950291

Order reference : 2524895

Shop :

Current amount : 90.57

Type : Debit

Transaction life cycle

Status : Declined (Reason for refusal : Advanced risks assessment)

Error details : 147 : The risk assessment module asked for this transaction refusal.

Creation date : 25/02/2020 17:27:55

Requested capture date : 25/02/2020 17:27:55

Payment method

Payment method :

Card number : 597010XXXXX0042 (2021/06 - valid)

Issuing bank :

Authorization

Merchant ID (MID) : 5785350

Validate | Modify | Cancel | Duplicate | Receipt

Close

Figure 5: Details tab

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

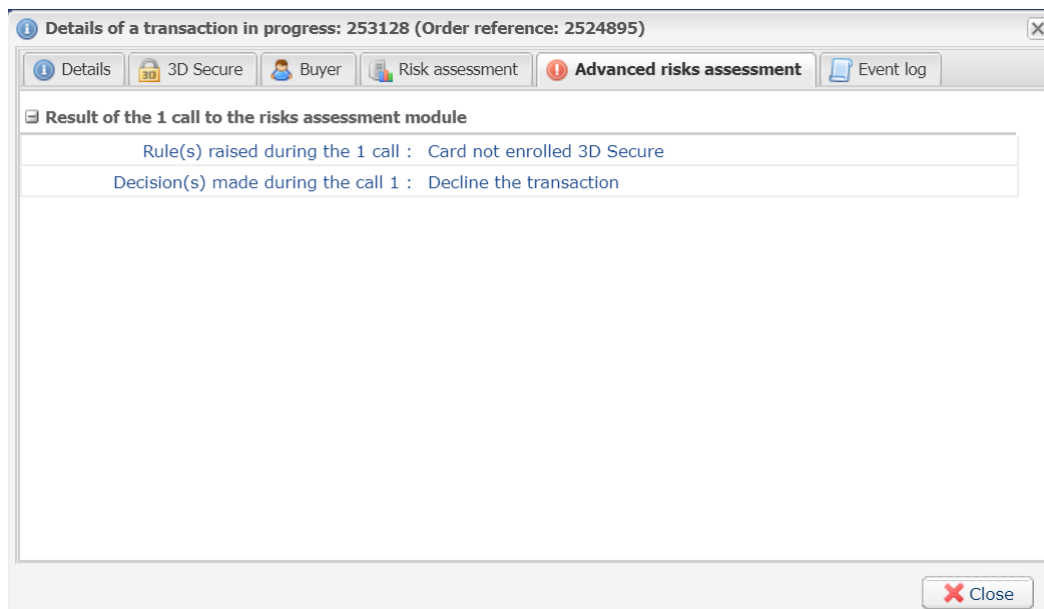


Figure 6: Advanced risks assessment tab

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. RETURN OF THE ADVANCED RISK ASSESSMENT MODULE RESULT IN THE IPN

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	<ul style="list-style-type: none">• 3DS1 card: The risk module has requested 3DS authentication.• 3DS2 card: The risk module has requested an authentication with cardholder interaction (challenge).
DISABLE_3DS	<ul style="list-style-type: none">• 3DS1 card: The risk module has requested 3DS deactivation.• 3DS2 card: The risk module has requested an authentication without cardholder interaction (frictionless).
NO_PREFERENCE	<ul style="list-style-type: none">• 3DS1 card: The risk module has requested 3DS authentication.• 3DS2 card: The risk module has requested 3DS authentication. The choice of the preference is transferred to the card issuer.
NO_CHALLENGE_REQUESTED	<ul style="list-style-type: none">• 3DS1 card: The risk module has requested 3DS deactivation.• 3DS2 card: The risk module has requested an authentication without cardholder interaction (frictionless).
CHALLENGE_REQUESTED	<ul style="list-style-type: none">• 3DS1 card: The risk module has requested 3DS authentication.• 3DS2 card: The risk module has requested an authentication with cardholder interaction (challenge).
CHALLENGE_MANDATE	<ul style="list-style-type: none">• 3DS1 card: The risk module has requested 3DS authentication.• 3DS2 card: The risk module has requested an authentication with cardholder interaction (challenge for regulatory reasons) for regulatory reasons.
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	Transaction is declined.
RUN_RISK_ANALYSIS	Call to an external risk analyzer if the Merchant has a contract. See the description of the TransactionDetails.FraudManagement.RiskAnalysis object to identify the list of possible values and their description.
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).

10. OBTAINING HELP

Looking for help? Check our FAQ on our website

<https://scelliuspaiement.labanquepostale.fr/doc/en-EN/faq/sitemap.html>

For any technical inquiries or if you need any help, contact [technical support](#).

In view of facilitating the processing of your requests, please specify your shop ID (an 8-digit number) in your query.

This information is available in the “registration of your shop” e-mail or in the Merchant Back Office (**Settings > Shop > Configuration**).