Risk assessment management

Back Office user manual

Document version 1.5.2

Contents

1. HISTORY OF THE DOCUMENT.......... 3

2. GENERAL CONCEPT.......... 4
    2.1. Risk assessment.......... 4
    2.2. Control modes.......... 4

3. SIGNING IN TO MERCHANT BACK OFFICE.......... 6

4. ACCESSING THE RISK MANAGEMENT MODULE.......... 7

5. CARD NUMBER CONTROL.......... 8
    5.1. Viewing the list of greylisted cards.......... 8
    5.2. Greylisting a card via a transaction.......... 8
    5.3. Editing the card greylist.......... 9
    5.4. Removing a card from the greylist.......... 9

6. IP ADDRESS CONTROL.......... 11
    6.1. Viewing the list of greylisted IP addresses.......... 11
    6.2. Greylisting an IP address via a transaction.......... 11
    6.3. Editing the IP addresses greylist.......... 12
    6.4. Removing an IP address from the greylist.......... 12

7. BIN CODE CONTROL.......... 14
    7.1. Viewing the list of greylisted BIN codes.......... 14
    7.2. Greylisting a BIN code via a transaction.......... 14
    7.3. Editing the greylist of BIN codes.......... 15
    7.4. Removing a BIN code from the greylist.......... 15

8. CONTROL OF THE PAYMENT METHOD ISSUER COUNTRY.......... 17
    8.1. Viewing the list of greylisted countries.......... 17
    8.2. Editing the country greylist.......... 17

9. CONTROL OF THE IP ADDRESS COUNTRY.......... 18
    9.1. Viewing the list of countries with greylisted IP addresses.......... 18
    9.2. Editing the greylist of IP address countries.......... 18

10. VELOCITY CHECK.......... 19

11. CONTROL OF CARDS WITH UNCONDITIONAL AUTHORIZATION.......... 20

12. CONTROL OF E-CARTE BLEUE.......... 21

13. COUNTRY CONSISTENCY CONTROL.......... 22

14. CONTROL OF COMMERCIAL CARDS.......... 23

15. VIEWING THE RESULT OF TRANSACTION RISK ASSESSMENT.......... 24

16. ACCESSING RISK ASSESSMENT RESULTS.......... 25

17. CREATING NOTIFICATION RULES SPECIFIC TO RISK ASSESSMENT.......... 26

18. OBTAINING HELP.......... 28

1. HISTORY OF THE DOCUMENT

Version	Author	Date	Comment
1.5.2	La Banque Postale	6/13/2023	Added clarification on the choice of control mode.
1.5.1	La Banque Postale	12/1/2022	Update of the *General concept*.
1.5	La Banque Postale	5/11/2021	Update of the chapter *Creating notification rules specific to risk assessment*.
1.4	La Banque Postale	10/22/2020	Document overhaul
1.3	La Banque Postale	8/30/2019	Initial version

2. GENERAL CONCEPT

Scellius is a PCI-DSS compliant highly secure payment solution. To accept a payment request, the cardholder's bank makes an authorization request. It allows to check the card type, its expiry date and whether it has been declared stolen.

In order to reinforce compulsory checks, Scellius provides various tools to help the merchant combat fraud. The merchant can configure these tools manually via the Merchant Back Office.

Note:

In order to benefit from the **Risk assessment** option, please contact the E-Banking Merchant Support Service.

2.1. Risk assessment

The risk assessment module allows to define the criteria that the merchant wishes to supervise. These criteria are specific to each merchant website depending on its sector of activity.

Examples of checks:

- Detection of cards with unconditional authorization
- Identification of foreign cards
- Outstanding balance on a card on the merchant website
- Detection of an e-carte bleue
- Consistency check between the country of the IP address, of the card and of the buyer
- Card greylist
- IP address greylist
- BIN code greylist
- etc.

2.2. Control modes

For all risk assessment processes, the merchant can choose between three modes:

- **No control (default value)**

  Verification disabled.

  No checks are carried out in this case.
- **Informative control**

  Verification completed after authorization request. Informative control identifies questionable transactions without refusing them.

  To be notified by e-mail, create a specific rule (see *Creating notification rules specific to risk assessment* chapter).
- **Blocking control**

  Verification completed before authorization request. Blocking control leads to the refusal of questionable transactions.

When setting up module **Risk assessment**, it is **essential** to change the default control mode (No control) via the **Settings** tab.

Otherwise, no check will be carried out.

The merchant has the possibility to refine the control according to the type, origin and use of cards:

- **Card control**

  Identification of cards with unconditional authorization, e-carte bleue cards and commercial cards (cards issued by companies), card number control, BIN code control.

- **Contextual control**

  Control of the buyer’s IP address, of the payment method’s issuing country, of the IP address country, consistency check.

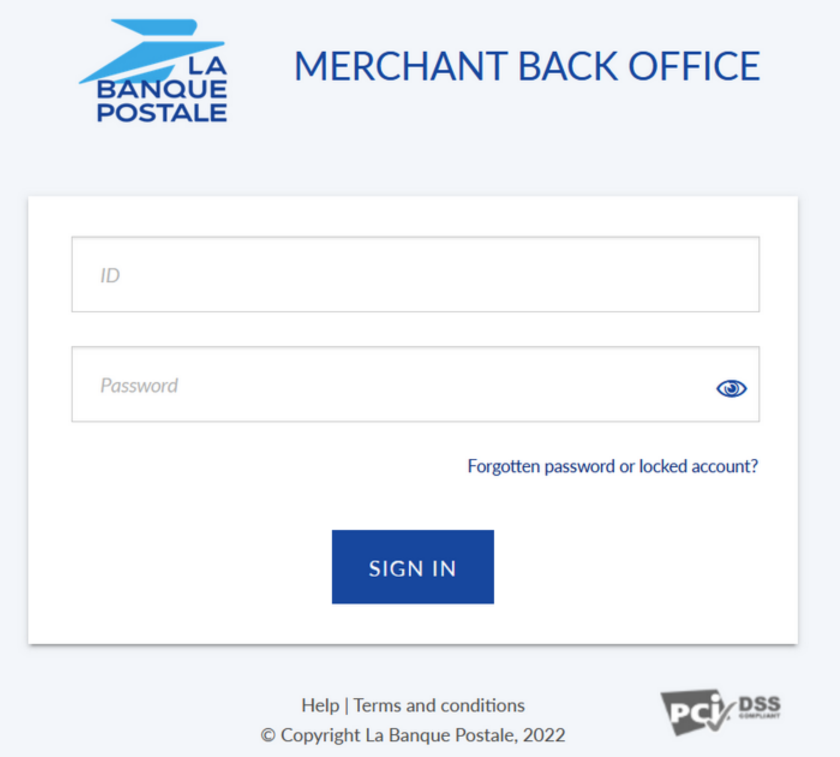
- **Use**

  Velocity control.

3. SIGNING IN TO MERCHANT BACK OFFICE

Sign in to the Back Office:

https://scelliuspaiement.labanquepostale.fr/vads-merchant/


LA BANQUE POSTALE
MERCHANT BACK OFFICE
ID
Password
Forgotten password or locked account?
SIGN IN
Help | Terms and conditions
© Copyright La Banque Postale, 2022
PCI DSS

1. Enter your login.

   The login is sent to the merchant's e-mail address (the subject of the e-mail is **Connection identifiers- [your shop name]**.

2. Enter your password.

   The password is sent to the merchant's e-mail address (the subject of the e-mail is **Connection identifiers- [your shop name]**.

3. Click **Sign in**.

   After 3 password entry errors, the user’s account is locked. Click on the link **Forgotten password or locked account** to reset it.

> ! A user's password is valid for 90 days. Beyond this period, a renewal will be requested when connecting.

4. ACCESSING THE RISK MANAGEMENT MODULE

Select the **Settings** > **Risk assessment** > [your shop].

The parameters are presented in several tabs:

- General settings
- Card greylist
- IP address greylist
- BIN code greylist
- Check of the countries that issue the payment method
- Check of IP addresses by country

5. CARD NUMBER CONTROL

This control allows to block some of the bank cards or to be notified when a card which has been set as an exception makes a payment in the shop.

The merchant fully manages the card exception, also known as greylisting. However, for security and PCI-DSS compliance purposes, the merchant does not have access to the full numbers of greylisted cards.

To configure this control:

1. Open the **Settings** > **Risk assessment** > [your shop name] menu.
2. Search for the box **Card number control**.
3. Select the control mode from the drop-down list.

> ! By default, **No control** is selected. No checks are carried out in this case. To activate this setting, you **absolutely** must choose a control mode from the list (informative or blocking).

4. Click **Save** to take the configuration changes into account.

> i This control is available only for PRODUCTION transactions.

5.1. Viewing the list of greylisted cards

Go to **Settings** > **Risk assessment** > [your shop name] and click on the **Card greylist** tab.

For each card on the greylist, the interface lists:

- The partially masked card number
- The card type
- The source (transaction or entry interface)
- The reason for greylisting the card
- The user who performed the action
- The date of greylisting the card
- Buyer details (e-mail, name)
- The reference of the order that was used for greylisting
- The reference of the transaction that was used for greylisting

It is also possible to view the details of the transaction that was used for greylisting.

To do this, make a right click on the card, then select **Search the associated transaction** in the context menu.

5.2. Greylisting a card via a transaction

Cards can be greylisted via the list of transactions.

To do so:

1. Go to **Management** > **Transactions** menu and search for the transaction in question.

2. Make a right click on the transaction and select **Add this card to the greylist** from the context menu.

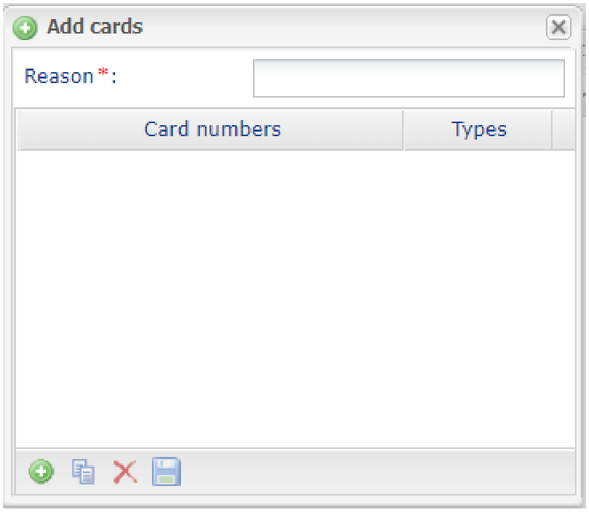
   A confirmation message appears.
3. Click **Yes** to proceed.
4. Enter the reason for greylisting (e.g. “fraud”) and click **OK**.

The card is added to the greylist.

5.3. Editing the card greylist

1. Select the **Card greylist** tab.
2. Click the ⊕ **Add** button at the bottom of the screen or right click > **Add several card numbers to the greylist**.

   The **Add cards** dialog box appears.



3. Enter the **Reason** for adding this card.
4. Click the ⊕ button to add a card number.
5. Enter the card number.
6. Select the card type from the list.
7. Click on ⧉ to duplicate a line.
8. Click on ✕ to delete a line.
9. Click on 💾 to save your greylist.
10. Make sure you have selected the desired control mode (Informative control or Blocking control) via the **Settings** tab.

5.4. Removing a card from the greylist

Go to **Settings** > **Risk assessment** > [your shop name] and click on the **Card greylist** tab.

1. Select the card in question and right-click on it.
2. Select **Remove the card from the greylist** in the context menu.

A confirmation message appears.

3. Click **Yes** to proceed.

   A second confirmation message appears.

4. Click **OK** to finish.

6. IP ADDRESS CONTROL

This control allows to block some of the user's IP addresses or to be notified when an IP address which has been set as an exception makes a payment in the shop.

The merchant fully manages the IP address exception, also known as greylisting.

To configure this control:

1. Open the **Settings** > **Risk assessment** > [your shop name] menu.
2. Search for the box **IP address control**.
3. Select the control mode from the drop-down list.

   ! By default, **No control** is selected. No checks are carried out in this case. To activate this setting, you **absolutely** must choose a control mode from the list (informative or blocking).

4. Click **Save** to take the configuration changes into account.

i This control is available only for PRODUCTION transactions.

6.1. Viewing the list of greylisted IP addresses

Go to **Settings** > **Risk assessment** > [your shop name] and click on the **IP address greylist** tab.

For each card on the greylist, the interface lists:

- The IP address
- The reason for greylisting the card
- The user who performed the action
- The date of greylisting the card
- Buyer details (e-mail, name)
- The reference of the order used for greylisting
- The reference of the transaction used for greylisting

It is also possible to view the details of the transaction used for greylisting.

To do this, make a right click on the corresponding line and select **Search for the associated transaction** from the context menu.

6.2. Greylisting an IP address via a transaction

IP addresses can be greylisted via the list of transactions.

To do so:

1. Go to **Management** > **Transactions** menu and search for the transaction in question.
2. Make a right click on the transaction and select **Add this IP address to the greylist** from the context menu.

   A confirmation message appears.

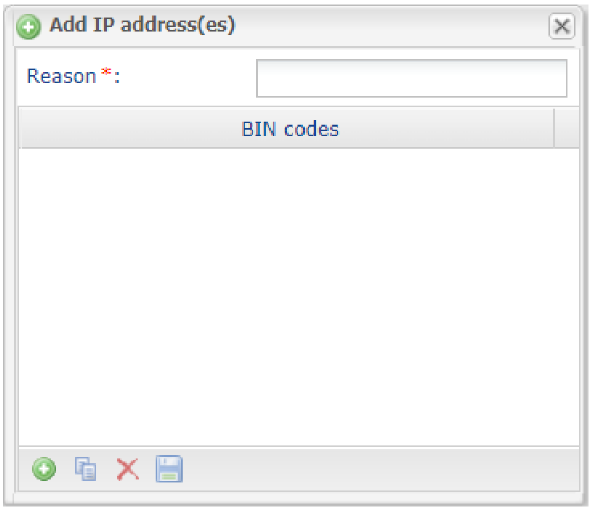
3. Click **Yes** to proceed.
4. Enter the reason for greylisting (e.g. “fraud”) and click **OK**.

The IP address is added to the greylist.

6.3. Editing the IP addresses greylist

1. Select the **IP address greylist** tab.

2. Click the ⊕ **Add** button at the bottom of the screen or right click > **Add several IPs to the greylist**.
   The **Add IP address(es)** dialog box appears.



3. Enter the **Reason** for adding this card.

4. Click the ⊕ button to add an IP address.

5. Enter the IP address.

6. Click on ⧉ to duplicate a line.

7. Click on ✕ to delete a line.

8. Click on 💾 to save your greylist.

9. Make sure you have selected the desired control mode (Informative control or Blocking control) via the **Settings** tab.

6.4. Removing an IP address from the greylist

Go to **Settings** > **Risk assessment** > [your shop name] and click on the **IP address greylist** tab.

1. Select the card in question and right-click on it.
2. Select **Remove the IP address from the greylist** in the context menu.

   A confirmation message appears.
3. Click **Yes** to proceed.

   A second confirmation message appears.

4. Click **OK** to finish.

7. BIN CODE CONTROL

This control allows to automatically identify or refuse transactions made with cards whose number begins with a specific value.

The BIN usually corresponds to the six (soon to be eight) first digits of the card number.

To configure this control:

1. Open the **Settings** > **Risk assessment** > [your shop name] menu.
2. Search for the box **BIN code control**.
3. Select the control mode from the drop-down list.

   ! By default, **No control** is selected. No checks are carried out in this case. To activate this setting, you **absolutely** must choose a control mode from the list (informative or blocking).

4. Click **Save** to take the configuration changes into account.

i This control is available only for PRODUCTION transactions.

7.1. Viewing the list of greylisted BIN codes

Go to **Settings** > **Risk assessment** > [your shop name] and click on the **IP address greylist** tab.

For each card on the greylist, the interface lists:

- The BIN code
- The reason for greylisting the card
- The user who performed the action
- The date of greylisting the card
- Buyer details (e-mail, name)
- The reference of the order that served for greylisting
- The reference of the transaction that served for greylisting

It is also possible to view the details of the transaction that served for greylisting.

To do this, make a right click on the corresponding line, then select **Search the associated transaction** in the context menu.

7.2. Greylisting a BIN code via a transaction

BIN codes can be greylisted via the list of transactions.

To do so:

1. Go to **Management** > **Transactions** menu and search for the transaction in question.
2. Make a right click on the transaction and select **Add this BIN code to the greylist** from the context menu.

   A confirmation message appears.

3. Click **Yes** to proceed.
4. Enter the reason for greylisting (e.g. “fraud”) and click **OK**.

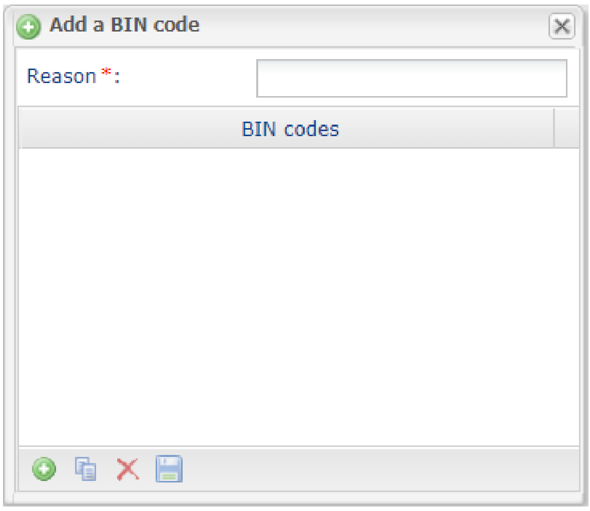
The BIN code is added to the greylist.

7.3. Editing the greylist of BIN codes

1. Select the **BIN code greylist** tab.

2. Click the ⊕ **Add** button at the bottom of the screen or right click > **Add several BIN codes to the greylist**.

   The **Add a BIN code** dialog box appears.



3. Enter the **Reason** for adding this card.

4. Click the ⊕ button to add a BIN code.

5. Enter the BIN code.

6. Click on ⧉ to duplicate a line.

7. Click on ✕ to delete a line.

8. Click on 💾 to save your greylist.

9. Make sure you have selected the desired control mode (Informative control or Blocking control) via the **Settings** tab.

7.4. Removing a BIN code from the greylist

Go to **Settings** > **Risk assessment** > [your shop name] and click on the **BIN code greylist** tab.

1. Select the card in question and right-click on it.
2. Select **Remove the BIN code from the greylist** in the context menu.

   A confirmation message appears.
3. Click **Yes** to proceed.

   A second confirmation message appears.

4. Click **OK** to finish.

8. CONTROL OF THE PAYMENT METHOD ISSUER COUNTRY

This control allows to:

- Block cards issued in certain countries.
- Be notified when a transaction is made with a card issued in a country specified as an exception.

By default, all countries are authorized.

The merchant has total control over the list of authorized and forbidden countries.

To configure this control:

1. Open the **Settings** > **Risk assessment** > [your shop name] menu.
2. Select the tab **Payment method issuing country control**.
3. Select the control mode from the drop-down list.

   > ! By default, **No control** is selected. No checks are carried out in this case. To activate this setting, you **absolutely** must choose a control mode from the list (informative or blocking).

4. Click **Save** to take the configuration changes into account.

8.1. Viewing the list of greylisted countries

Go to **Settings** > **Risk assessment** > [your shop name], click on **Payment method issuer country check**.

The interface lists all the countries (authorized and forbidden).

8.2. Editing the country greylist

1. Select the **Payment method issuing country control** tab.

   By default, all countries are listed in the **Authorized countries** column.

2. Select one or several countries.
3. Drag them to the **Forbidden countries** column or click the **Forbid** button.
4. Click **Save**.
5. Make sure you have selected the desired control mode (Informative control or Blocking control) via the **Settings** tab.

9. CONTROL OF THE IP ADDRESS COUNTRY

This control allows to:

- Block IP addresses located in certain countries.
- Be notified when a transaction is made with an IP address located in a country specified as an exception.

By default, all countries are authorized.

The merchant has total control over the list of authorized and forbidden countries.

To configure this control:

1. Open the **Settings** > **Risk assessment** > [your shop name] menu.
2. Search for the box **IP address country control**.
3. Select the control mode from the drop-down list.

   ! By default, **No control** is selected. No checks are carried out in this case. To activate this setting, you **absolutely** must choose a control mode from the list (informative or blocking).

4. Click **Save** to take the configuration changes into account.

9.1. Viewing the list of countries with greylisted IP addresses

Go to **Settings** > **Risk assessment** > [your shop name] and click on the **IP address countries on the greylist** tab.

The interface lists all the countries (authorized and forbidden).

9.2. Editing the greylist of IP address countries

1. Select the **IP address countries on the greylist** tab.

   By default, all countries are listed in the **Authorized countries** column.

2. Select one or several countries.
3. Drag them to the **Forbidden countries** column or click the **Forbid** button.
4. Click **Save**.
5. Make sure you have selected the desired control mode (Informative control or Blocking control) via the **Settings** tab.

10. VELOCITY CHECK

This control allows to limit the purchases made in a shop within a defined period or to be alerted as soon as the velocity of transactions made with a given card exceed the amounts predefined by the merchant.

To configure this control:

1. Open the **Settings** > **Risk assessment** > [your shop name] menu.
2. Search for the box **Velocity check**.
3. Select the control mode from the drop-down list.

   > ! By default, **No control** is selected. No checks are carried out in this case. To activate this setting, you **absolutely** must choose a control mode from the list (informative or blocking).

4. Proceed to the configuration of the velocity control parameters:
   - Check the box **Maximum amount authorized** if you wish to limit the amount of each order. In this case, you must enter the maximum authorized amount.

     Example: if you enter an amount of €1000, the buyer will be able to place as many orders as they wish as long as the amount of each order is lower than €1000.

     If the order amount exceeds the maximum authorized amount, then, depending on the control parameter configuration, either an alert will be raised or the payment will be refused.
   - Enter the reference period in number of days.
   - Check the box **Maximum total amount for several orders** if you wish to limit the order amount for a specified period. In this case, you must enter the total maximum authorized amount.

     Example: if you enter a total amount of €1000, the buyer will be able to place as many orders as they wish as long as the total amount of these payments for the specified period is lower than €1000.

     If the total amount exceeds €1000, then, depending on the control parameter configuration, either an alert will be raised or the payment will be refused.
   - Check the box **Number of accepted payments** if you wish to limit the number of payments accepted over the specified period. In this case, you must enter the maximum authorized number of payments.
5. Click **Save** to take the configuration changes into account.

11. CONTROL OF CARDS WITH UNCONDITIONAL AUTHORIZATION

This control allows to automatically identify or refuse transactions made with systematic authorization cards, among which the most commonly encountered are Maestro, Electron and gift cards.

This control will only apply to CB and CB-approved cards.

To configure this control:

1. Open the **Settings** > **Risk assessment** > [your shop name] menu.
2. Search for the box **Control of cards with unconditional authorization**.
3. Select the control mode from the drop-down list.

> ! By default, **No control** is selected. No checks are carried out in this case. To activate this setting, you **absolutely** must choose a control mode from the list (informative or blocking).

4. Select the transaction type for which the control will be applied:
   - **All transactions**
   - **Recurring and Installment transactions**
5. Click **Save** to take the configuration changes into account.

12. CONTROL OF E-CARTE BLEUE

This control allows to automatically identify or refuse transactions made with an e-Carte Bleue.

To configure this control:

1. Open the **Settings** > **Risk assessment** > [your shop name] menu.
2. Search for the box **Control of e-Carte Bleue**.
3. Select the control mode from the drop-down list.

> ! By default, **No control** is selected. No checks are carried out in this case. To activate this setting, you **absolutely** must choose a control mode from the list (informative or blocking).

4. Select the transaction type for which the control will be applied:
   - **All transactions**
   - **Recurring and Installment transactions**
5. Click **Save** to take the configuration changes into account.

13. COUNTRY CONSISTENCY CONTROL

This setting allows to control the consistency between:

- The buyer's country (information transmitted by the merchant in his or her payment form or in the Web Service request).
- The country of the payment method (information provided by the payment gateway).
- The country of the buyer's IP address (information provided by the payment gateway).

What are the cases that allow to validate this control?

- The 3 countries are identical.
- The country of the payment method and the buyer's country are identical.
- The country of the payment method and the country of the IP address are identical.

All the other cases lead to a KO control.

> When the merchant enables this verification, he or she must make sure to transmit the information about the buyer's country. Without it, the check cannot be performed.

To configure this control:

1. Open the **Settings** > **Risk assessment** > [your shop name] menu.
2. Search for the box **Country consistency control**.
3. Select the control mode from the drop-down list.

   > By default, **No control** is selected. No checks are carried out in this case. To activate this setting, you **absolutely** must choose a control mode from the list (informative or blocking).

4. Click **Save** to take the configuration changes into account.

14. CONTROL OF COMMERCIAL CARDS

This control allows to automatically identify or refuse transactions made with a commercial debit or credit card, depending on its origin.

To configure this control:

1. Open the **Settings** > **Risk assessment** > [your shop name] menu.
2. Search for the box **Control of commercial cards**.
3. Select the control mode from the drop-down list.

> ! By default, **No control** is selected. No checks are carried out in this case. To activate this setting, you **absolutely** must choose a control mode from the list (informative or blocking).

4. Select the transaction type with local cards for which the control will be applied:
   - **All transactions**
   - **Recurring and Installment transactions**
5. Select the control mode for foreign cards from the drop-down list.
6. Select the transaction type with foreign cards for which the control will be applied:
   - **All transactions**
   - **Recurring and Installment transactions**
7. Click **Save** to take the configuration changes into account.

15. VIEWING THE RESULT OF TRANSACTION RISK ASSESSMENT

1. Make a double click on a transaction or click to show the context menu of the transaction.
2. Click **Display transaction details**.
3. Select the **Risk assessment** tab.

   Depending on the result:

Symbol	Description
✅	The risk assessment is enabled but not launched. No risk detected.
⚠	The risk assessment is enabled and launched. A risk has been detected and a notification has been sent to the merchant.
⛔	The risk assessment is enabled and launched. A risk has been detected and the payment has been rejected.

16. ACCESSING RISK ASSESSMENT RESULTS

The risk assessment result can be accessed:

- Via the reports: **COMPLEMENTARY_INFO**
- Via the end of payment notifications (IPN):
  - **vads_risk_control** for the hosted payment page
  - **transactionDetails.fraudManagement.riskControl** object of the **Transaction** object for the REST API

17. CREATING NOTIFICATION RULES SPECIFIC TO RISK ASSESSMENT

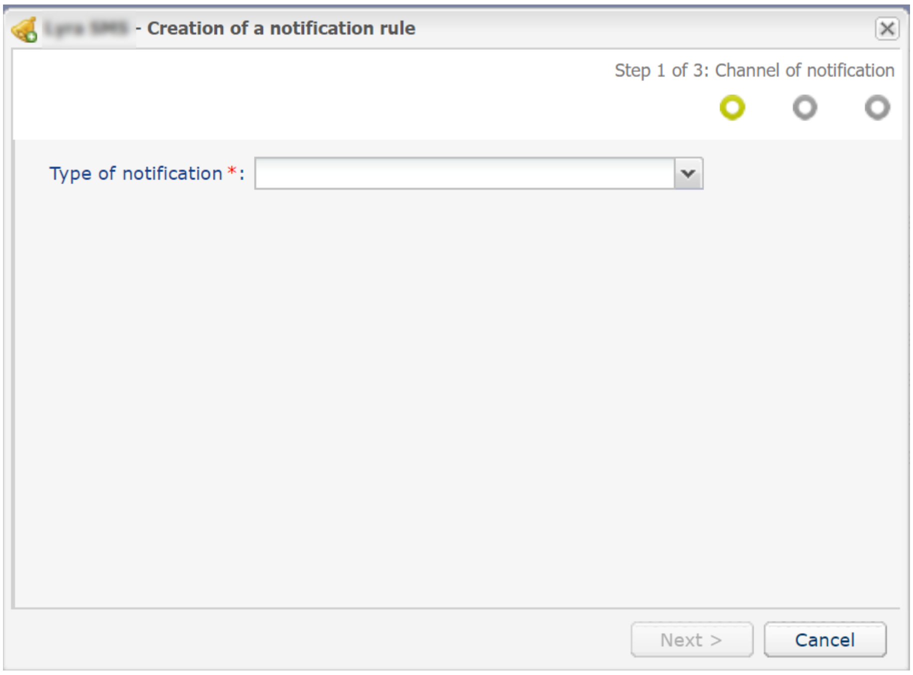
Use case: Risk assessment is set to **informative control**. The merchant wishes to receive an e-mail as soon as a verification process detects risk of fraud.

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**.



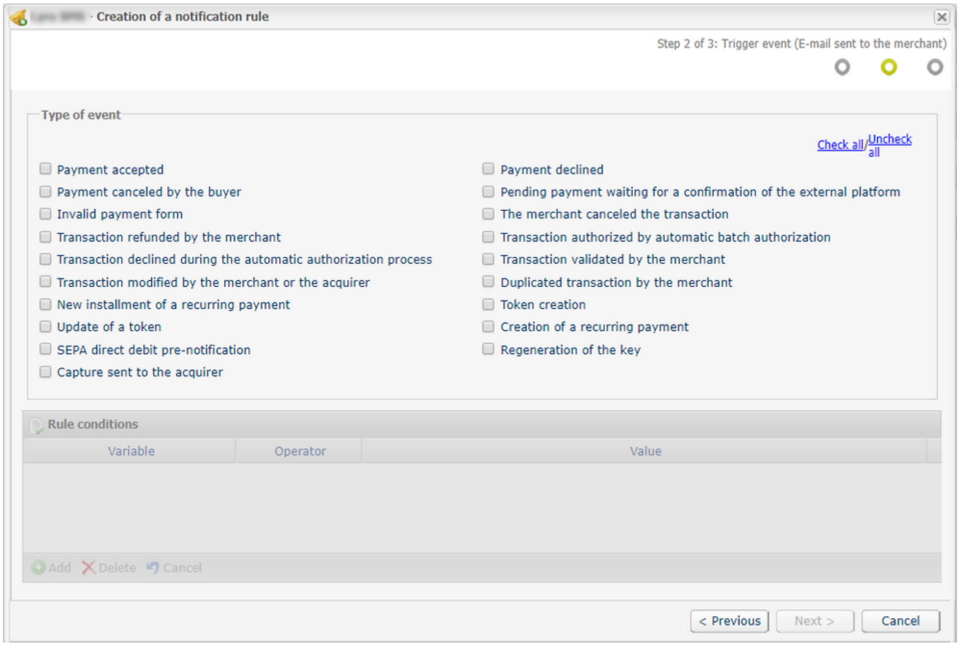
- Creation of a notification rule

Step 1 of 3: Channel of notification

Type of notification *:

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

5. Click **Next**.



- Creation of a notification rule

Step 2 of 3: Trigger event (E-mail sent to the merchant)

Type of event

☐ Payment accepted	☐ Payment declined
☐ Payment canceled by the buyer	☐ Pending payment waiting for a confirmation of the external platform
☐ Invalid payment form	☐ The merchant canceled the transaction
☐ Transaction refunded by the merchant	☐ Transaction authorized by automatic batch authorization
☐ Transaction declined during the automatic authorization process	☐ Transaction validated by the merchant
☐ Transaction modified by the merchant or the acquirer	☐ Duplicated transaction by the merchant
☐ New installment of a recurring payment	☐ Token creation
☐ Update of a token	☐ Creation of a recurring payment
☐ SEPA direct debit pre-notification	☐ Regeneration of the key
☐ Capture sent to the acquirer	

Rule conditions

Variable	Operator	Value

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**.

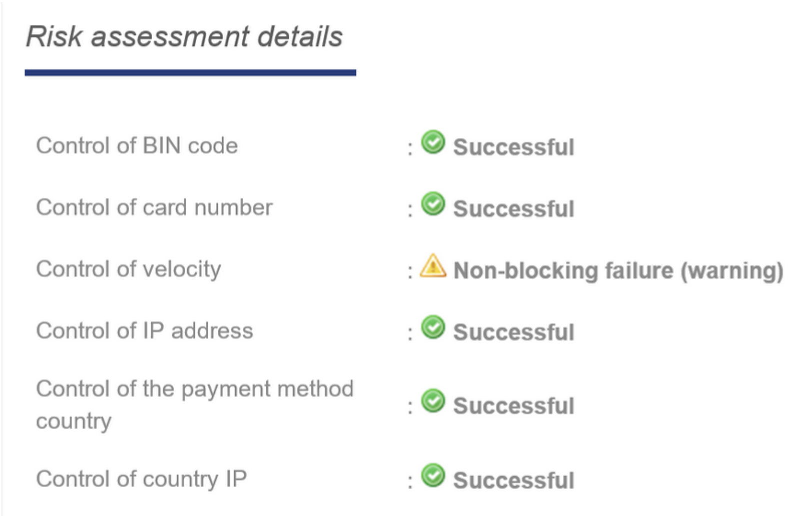
13. Enter the e-mail address to notify.

14. Select the fields to be included in the e-mail.
    By default, the risk assessment details are already included.

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**.

When risk assessment set to **informative control** fails, the merchant receives an e-mail containing the details of completed risk assessment processes:



Risk assessment details

Control of BIN code	: ✓ **Successful**
Control of card number	: ✓ **Successful**
Control of velocity	: ⚠ **Non-blocking failure (warning)**
Control of IP address	: ✓ **Successful**
Control of the payment method country	: ✓ **Successful**
Control of country IP	: ✓ **Successful**

18. 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**).