



Risk assessment management

Back Office user manual

Document version 1.3

Contents

1. HISTORY OF THE DOCUMENT.....	3
2. OBTAINING HELP.....	4
Viewing online documentation.....	4
Getting in touch with technical support.....	4
3. GENERAL CONCEPT.....	5
4. RISK ASSESSMENT.....	6
5. SIGNING IN TO THE MERCHANT BACK OFFICE.....	7
6. ACCESSING THE RISK MANAGEMENT MODULE.....	8
7. CONFIGURING RISK MANAGEMENT.....	9
7.1. Country consistency control.....	9
8. CREATING A COUNTRY GREYLIST.....	10
9. CREATING AN IP ADDRESS GREYLIST.....	11
10. CREATING AN BIN CODE GREYLIST.....	12
11. CREATING A COUNTRY GREYLIST.....	13
12. CREATING A GREYLIST IP ADDRESSES BY COUNTRY.....	14
13. VIEWING THE RESULT OF TRANSACTION RISK ASSESSMENT.....	15

1. HISTORY OF THE DOCUMENT

Version	Author	Date	Comment
1.3	Lyra Network	7/15/2019	Adding description of the countries consistency control.
1.2	Lyra Network	11/3/2016	Documentation update
1.1	Lyra Network	12/6/2015	Addition of details

This document and its contents are confidential. It is not legally binding. No part of this document may be reproduced and/or forwarded in whole or in part to a third party without the prior written consent of Lyra Network. All rights reserved.

2. OBTAINING HELP

Viewing online documentation

Need some help? Please, check online documentation

In Germany	https://payzen.io/de-DE/faq/sitemap.html
In Europe	https://payzen.io/en-EN/faq/sitemap.html
In Latin America (except Brazil)	https://payzen.io/lat/faq/sitemap.html
In Brazil	https://payzen.io/pt-BR/faq/sitemap.html
In India	https://payzen.io/in/faq/sitemap.html

We are constantly improving the understanding and proper use of our technical documentation. We appreciate any constructive remarks on your part.

Please send your comments and suggestions about the documentation to the e-mail address pole.documentation@lyra-network.com.

Getting in touch with technical support

For technical inquiries or support, you can reach us from Monday to Friday, between 9am and 6pm

	By phone	By e-mail
In France	0811708709 <small>Service fee 0,06 € / min + call charge</small>	support@payzen.eu
In Europe	+33 820902103 <small>Service fee 0,12 € / min + call charge</small>	support@payzen.eu
In Latin America (except Brazil)	N/A	soporte@payzen.lat
In Brazil	+55 (11) 3336-9217 +55 (11) 3336-9209	suporte@payzen.com.br
In India	+91 (022) 33864910 / 932	operations.department@lyra-network.co.in

and via your Merchant Back Office, menu **Help** > **Contact support**

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

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

3. GENERAL CONCEPT

PayZen is a PCI-DSS compliant highly secure payment solution. Each payment attempt systematically involves an authorization request sent to the cardholder's bank. It allows to check the card type, its expiry date and whether it has been declared stolen.

In order to reinforce compulsory checks, PayZen 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 administrator of the payment gateway.

4. 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
- Bank card details
- Detection of an e-carte bleue
- Consistency check between the country of the IP, the card and the buyer
- Card greylist
- IP address greylist
- BIN code greylist
- etc.

5. SIGNING IN TO THE MERCHANT BACK OFFICE

Sign in the Back Office:

<https://de.payzen.eu/vads-merchant/>

PayZen **MERCHANT BACK OFFICE**
Powered by Lyra

ID

Password

[Forgotten password or locked account?](#)

SIGN IN

Help | Terms and conditions
Copyright LYRA © 2019 All rights reserved

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 on 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.

6. ACCESSING THE RISK MANAGEMENT MODULE

Select **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

7. CONFIGURING RISK MANAGEMENT

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

- **No control measures**
Verification disabled.
- **Informative control**
Verification completed after authorization request. Informative control identifies questionable transactions without refusing them.
- **Blocking control**
Verification completed before authorization request. Blocking control leads to the refusal of questionable transactions.

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.

Note:

The merchant can request to receive an e-mail notification once these controls have been completed.

7.1. 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).

IMPORTANT


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.

What are the cases that allow to validate this check?

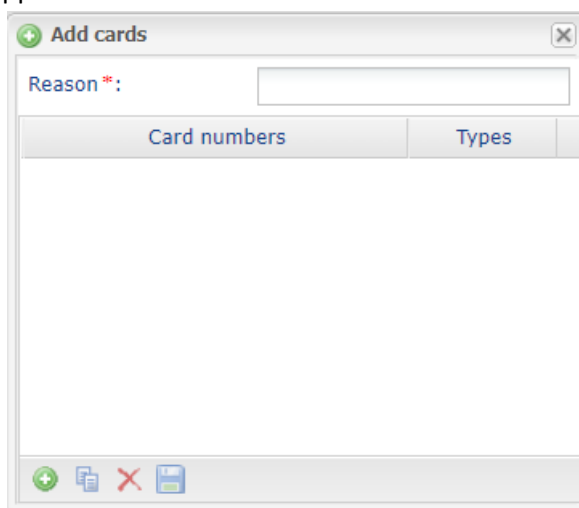
- The 3 countries are identical.
- The country of the payment method and the buyer's country are identical.
- The country of the payment method and the country of the IP address are identical.



All the other cases lead to a KO control.

8. CREATING A COUNTRY GREYLIST



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

The **Add card** 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 .
- The provided information is analyzed in order to check its validity.

It is also possible to:

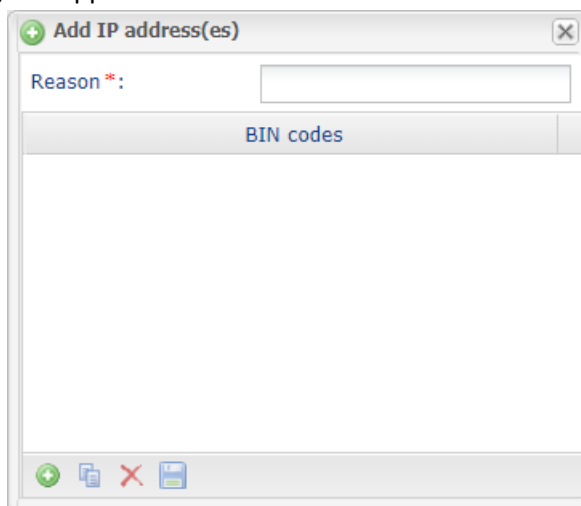
Description	Icon
Duplicate an entry	
Delete an entry	



8. Select the desired control mode (**Informative control** or **Blocking control**) via the **Settings** tab.

9. CREATING AN IP ADDRESS GREYLIST



1. Select the tab **IP address greylis**t.
2. Click the  **Add** button at the bottom of the screen or right click > **Add several IP addresses to the greylis**t.

The **Add IP address** 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 .

It is also possible to:

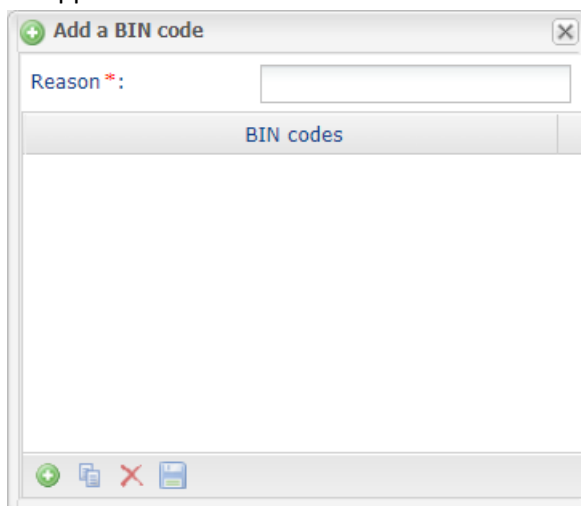
Description	Icon
Duplicate an entry	
Delete an entry	



7. Select the desired control mode (**Informative control** or **Blocking control**) via the **Settings** tab.

10. CREATING AN BIN CODE GREYLIST



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

The **Add 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 .

It is also possible to:

Description	Icon
Duplicate an entry	
Delete an entry	

7. Select the desired control mode (**Informative control** or **Blocking control**) via the **Settings** tab.

11. CREATING A COUNTRY GREYLIST

1. Select the tab **Payment method issuer country check**.

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

2. Select one or several countries.

3. Drag them to the **Forbidden countries** column or click the **Forbid** button.

- If the merchant is in greylist mode, all the cards issued by a bank established in one of the countries on the **Forbidden countries** list will be blocked.
- If the merchant is in whitelist mode, only the cards issued by a bank established in one of the countries on the **Authorized countries** list will be accepted.

4. Click **Save**.

5. Select the desired control mode (**Informative control** or **Blocking control**) via the **Settings** tab.

12. CREATING A GREYLIST IP ADDRESSES BY COUNTRY

1. Select the tab **IP addresses' countries on the greylist**.




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

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

13. VIEWING THE RESULT OF TRANSACTION RISK ASSESSMENT

1. Double click or right click a transaction > **Display transaction details**.
2. 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.