



Gestion des risques - Nouvelle interface

Manuel d'utilisation du Back Office

Sommaire

1. PRÉSENTATION DU SERVICE.....	3
1.1. Prérequis.....	3
2. PRINCIPE DE FONCTIONNEMENT.....	4
2.1. Gestion des risques et authentification 3D Secure.....	4
2.2. Les critères.....	6
2.3. Les actions.....	11
3. GESTION DES LISTES GRISES.....	13
3.1. Consulter les listes grises.....	13
3.2. Ajouter une entrée dans la liste grise.....	14
3.2.1. Depuis la liste des transactions.....	14
3.2.2. Depuis la gestion des risques.....	14
3.3. Supprimer une entrée dans la liste grise.....	15
4. GESTION DES RÈGLES.....	16
4.1. Créer une nouvelle règle.....	16
4.2. Rechercher / filtrer les règles.....	17
4.3. Activer / Désactiver une règle.....	17
4.4. Editer une règle.....	19
4.5. Supprimer une règle.....	19
5. TRANSMETTRE LES DONNÉES UTILES À LA GESTION DES RISQUES.....	20
6. RESTITUTION DE LA GESTION DU RISQUE DANS L'IPN.....	21
7. ETRE NOTIFIÉ EN CAS DE RISQUE DE FRAUDE.....	23
8. CONSULTER LE DÉTAIL D'UNE TRANSACTION.....	25
9. VALIDER MANUELLEMENT UNE TRANSACTION.....	27

1. PRÉSENTATION DU SERVICE

De manière à fournir un haut niveau de sécurité, la plateforme de paiement met à votre disposition des outils permettant :

- De minimiser les risques d'impayés en refusant des transactions jugées frauduleuses ;
- D'ajouter des contrôles en cas de suspicion de fraude.

Des filtres pertinents sont mis à disposition pour définir des actions préventives en fonction du niveau de risque et des spécificités de votre activité sans pour autant pénaliser vos ventes. Le service peut être configuré en tenant compte des risques connus ou des problèmes de fraude vécus par le passé.

1.1. Prérequis

Le marchand bénéficie de la fonction **Gestion des risques avancée**. Il accède à sa configuration depuis son Back Office Marchand.

2. PRINCIPE DE FONCTIONNEMENT

Le risque peut être évalué plusieurs fois lors de la création d'un paiement :

- après la validation des données d'entrée ;
- après l'authentification du porteur ;
- après l'autorisation.

A chaque fois, le service retourne potentiellement une ou plusieurs actions qui impactent le processus de paiement.



En cas d'indisponibilité, de configuration incorrecte, ou de dysfonctionnement, le paiement s'effectue sans contrôle du risque.

Vous avez accès à un ensemble de règles de gestion de risque. Chaque règle peut être activée ou désactivée.

Une règle est constituée de :

- un ou plusieurs **critères** à valider ;
- une ou plusieurs **actions** qui seront déclenchées si tous les critères de la règle sont validés.

Exemples :

- Une règle simple avec un seul critère et une seule action : si le montant cumulé sur une semaine est supérieur à 500 EUR, refuser le paiement.
- Une règle plus complexe avec deux critères et une action : si le pays de l'acheteur est différent du pays de votre boutique et que le montant est supérieur à 100 EUR, vous devez valider manuellement la transaction.

2.1. Gestion des risques et authentification 3D Secure

Le dispositif 3D Secure permet de réduire le risque d'impayés, grâce au transfert de responsabilité du marchand à la banque du porteur de la carte.

Lors du paramétrage des règles, vous pouvez définir un mode d'authentification lorsque 3D Secure v2 est activé sur au moins un vos contrats associés à la boutique.

En fonction des protocoles disponibles sur vos contrats, ces actions vous permettent :

- D'exprimer votre souhait de demander une authentification forte au porteur,
- De demander une authentification 3D Secure v2 sans interaction du porteur, si les options de la boutique le permettent.



Vous pouvez éventuellement définir le mode d'authentification depuis les requêtes de paiement.

Cette fonctionnalité peut être utilisée en complément des règles de risque sous réserve d'accord préalable de Société Générale.

Pour cela, la boutique doit disposer de l'option "Frictionless 3DS2".

Le choix transmis dans le champ **strongAuthentication** de l'API REST ou **vads_threeds_mpi** de l'API Formulaire est prioritaire sur le choix défini dans les règles de risque.

Retrouvez toutes les informations utiles sur l'authentification 3DS dans le [guide du 3D Secure](#).

D'autres règles peuvent s'appliquer en priorité sur celles que vous avez définies (dans les requêtes de paiement ou depuis les règles de risque) :

- Certaines cartes de paiement nécessitent une authentification du porteur. C'est le cas des cartes Maestro.
- American Express se réserve le droit d'effectuer une authentification forte en fonction de règles qui lui sont propres, même si vous avez fait une configuration différente.

2.2. Les critères

- Critères relatifs au montant



Contrôle sur le montant	Ce contrôle permet de définir l'action à déclencher lorsque le montant de la transaction est compris entre les seuils renseignés en paramètre. Vous pouvez créer plusieurs règles sur le montant.
Contrôle sur le montant minimum	Ce contrôle permet de définir l'action à déclencher lorsque le montant de la transaction est inférieur à celui renseigné en paramètre. Vous pouvez créer plusieurs règles sur le montant minimum.
Contrôle sur le montant maximum	Ce contrôle permet de définir l'action à déclencher lorsque le montant de la transaction est supérieur à celui renseigné en paramètre. Vous pouvez créer plusieurs règles sur le montant maximum.
Contrôle du montant cumulé sur une période*	Ce contrôle permet de définir l'action à déclencher lorsque le montant cumulé des paiements effectués avec le même moyen de paiement est supérieur à celui renseigné en paramètre. Vous définissez la période de référence.

* De 1 minute à 3 jours, le calcul de la période de référence tient compte de la date et de l'heure de la première transaction. Au-delà, le calcul se base uniquement sur la date.

- Critères relatifs aux listes grises

Contrôle du numéro de carte	Ce contrôle permet de définir l'action à déclencher lorsqu'une carte bancaire préalablement mise en exception effectue un paiement sur la boutique. Vous gérez intégralement la mise en exception des cartes, également appelée mise sur liste grise. Voir : Ajouter une entrée dans la liste grise à la page 14.
Contrôle du code BIN	Ce contrôle permet de définir l'action à déclencher lorsqu'une transaction est réalisée avec une carte dont le numéro commence par une valorisation donnée. Le BIN correspond habituellement aux six (ou huit) premiers caractères du numéro de carte. Vous gérez intégralement la mise en exception des BIN, également appelée mise sur liste grise. Voir : Ajouter une entrée dans la liste grise à la page 14.
Contrôle de l'adresse IP	Ce contrôle permet de définir l'action à déclencher lorsqu'une adresse IP préalablement mise en exception effectue un paiement sur la boutique. Vous gérez intégralement la mise en exception des adresses IP, également appelée mise sur liste grise. Voir : Ajouter une entrée dans la liste grise à la page 14.





- Critères relatifs à la commande

Contrôle sur le nombre de références produits dans le panier	<p>Ce contrôle permet de définir l'action à déclencher lorsque le nombre de références produits contenues dans le panier dépasse le seuil renseigné en paramètre.</p> <div> Lorsque vous activez ce contrôle, vous devez vous assurer de transmettre les données utiles à la gestion des risques.</div>
Contrôle des produits du panier	<p>Ce contrôle permet de définir l'action à déclencher lorsque le panier contient au moins un des articles dont le code produit mis en exception.</p> <p>Vous gérez intégralement la liste des codes article interdits depuis le paramétrage de la règle.</p> <div> Lorsque vous activez ce contrôle, vous devez vous assurer de transmettre les données utiles à la gestion des risques.</div>
Type de média utilisé	Ce contrôle permet de définir l'action à déclencher en fonction du type d'équipement utilisé lors du paiement.

- Critères relatifs à l'analyse de la carte

Contrôle des e-Carte Bleue	<p>Une e-Carte Bleue est une carte virtuelle qui fournit un numéro de carte éphémère pour chaque transaction réalisée sur Internet. Ainsi un numéro de carte bancaire « réel » ne transite pas sur Internet.</p> <p>Ce contrôle permet de définir l'action à déclencher lorsqu'une transaction est réalisée avec une e-Carte Bleue.</p> <p>Vous choisissez le type de transactions sur lesquelles s'applique le contrôle.</p>
Contrôle des cartes à autorisation systématique	<p>Ce contrôle permet de définir l'action à déclencher lorsqu'une transaction est réalisée avec une carte à autorisation systématique parmi lesquelles les plus couramment rencontrées sont les cartes cadeau, les cartes Maestro et Electron.</p> <p>Vous choisissez le type de transactions sur lesquelles s'applique le contrôle.</p>
Contrôle des cartes prépayées	<p>Ce contrôle permet de définir l'action à déclencher lorsqu'une transaction est réalisée avec une carte prépayée.</p> <p>Vous choisissez la ou les marques de carte pour lesquelles activer le contrôle.</p>
Contrôle des cartes commerciales suivant leur provenance	<p>Ce contrôle permet de définir l'action à déclencher lorsqu'une transaction est réalisée avec une carte commerciale provenant d'un pays mis en exception.</p> <p>Vous sélectionnez les pays pour lesquels activer le contrôle.</p> <p>Vous choisissez la ou les marques de carte pour lesquelles activer le contrôle.</p>
Contrôle des cartes commerciales	<p>Une carte commerciale est une carte de société. Elle est délivrée par exemple à un salarié à des fins professionnelles.</p> <p>Ce contrôle permet de définir l'action à déclencher lorsqu'une transaction est réalisée avec une carte commerciale.</p> <p>Vous choisissez la ou les marques de carte pour lesquelles activer le contrôle.</p>

	Vous choisissez le type de transactions sur lesquelles s'applique le contrôle.
Contrôle des cartes personnelles de débit	<p>Une carte personnelle de débit est une carte de paiement. Le compte est prélevé au fur et à mesure que les transactions sont transmises par les marchands bénéficiaires.</p> <p>Ce contrôle permet de définir l'action à déclencher lorsqu'une transaction est réalisée avec une carte de débit.</p> <p>Vous choisissez la ou les marques de carte pour lesquelles activer le contrôle.</p>
Contrôle des cartes personnelles de crédit	<p>Une carte personnelle de crédit est une carte de paiement. Le compte est débité en différé de la totalité des achats effectués pendant une période définie.</p> <p>Ce contrôle permet de définir l'action à déclencher lorsqu'une transaction est réalisée avec une carte de crédit.</p> <p>Vous choisissez la ou les marques de carte pour lesquelles activer le contrôle.</p>
<ul style="list-style-type: none"> • Critères relatifs au résultat de 3D Secure 	
Carte non enrôlée au programme SafeKey	Ce contrôle permet de définir l'action à déclencher lorsqu'une transaction est réalisée avec une carte American Express non enrôlée au programme SafeKey (NOT_ENROLLED).
Paiement avec une carte dont l'enrôlement au programme SafeKey ne peut pas être vérifié	Ce contrôle permet de définir l'action à déclencher lorsqu'une transaction est réalisée avec une carte American Express dont l'enrôlement au programme SafeKey ne peut pas être vérifié (3DS_UNAVAILABLE).
Paiement 3D Secure avec un porteur dont l'authentification ne peut pas être vérifiée	Ce contrôle permet de définir l'action à déclencher lorsque le statut d'authentification 3D Secure du porteur est "ATTEMPT" (preuve d'authentification fournie).
Carte non enrôlée au programme 3D Secure	Ce contrôle permet de définir l'action à déclencher lorsqu'une transaction est réalisée avec une carte non enrôlée au programme 3D Secure ("NOT_ENROLLED").
Paiement 3D Secure avec une carte dont l'enrôlement ne peut pas être vérifié	Ce contrôle permet de définir l'action à déclencher lorsqu'une transaction est réalisée avec une carte dont l'enrôlement au programme 3D Secure ne peut pas être vérifié ("3DS_UNAVAILABLE").
Transfert de responsabilité	Ce contrôle permet de définir l'action à déclencher lorsqu'une transaction ne bénéficie pas du transfert de responsabilité (le porteur de carte ne peut pas transférer la responsabilité d'un impayé pour le motif "Contestation du porteur" vers vous).
<ul style="list-style-type: none"> • Critères relatifs aux pays 	
Contrôle du pays émetteur du moyen de paiement	<p>Ce contrôle permet de définir l'action à déclencher lorsqu'une transaction est réalisée avec une carte bancaire émise dans un pays mis en exception.</p> <p>Vous sélectionnez les pays pour lesquels activer le contrôle.</p>
Contrôle du pays de l'adresse IP	<p>Ce contrôle permet de définir l'action à déclencher lorsqu'une transaction est réalisée avec une adresse IP située dans un pays mis en exception.</p> <p>Vous sélectionnez les pays pour lesquels activer le contrôle.</p>

<p>Contrôle du pays de livraison</p>	<p>Ce contrôle permet de définir l'action à déclencher lorsqu'une transaction est réalisée avec un pays de livraison mis en exception.</p> <p>Vous sélectionnez les pays pour lesquels activer le contrôle.</p> <div data-bbox="715 271 1442 405" style="border: 1px solid #add8e6; padding: 5px;"> <p> Lorsque vous activez ce contrôle, vous devez vous assurer de transmettre les données utiles à la gestion des risques.</p> </div>
<p>Contrôle du pays du client (adresse de facturation)</p>	<p>Ce contrôle permet de définir l'action à déclencher lorsqu'une transaction est réalisée avec une adresse de facturation située dans un pays mis en exception.</p> <p>Vous sélectionnez les pays pour lesquels activer le contrôle.</p> <div data-bbox="715 584 1442 719" style="border: 1px solid #add8e6; padding: 5px;"> <p> Lorsque vous activez ce contrôle, vous devez vous assurer de transmettre les données utiles à la gestion des risques.</p> </div>
<p>Contrôle de la cohérence des pays</p>	<p>Ce contrôle permet de vérifier la cohérence entre :</p> <ul style="list-style-type: none"> • le pays de l'acheteur (que vous transmettez dans votre formulaire de paiement ou dans votre requête Web Service), • le pays du moyen de paiement (déterminé par la plateforme de paiement), • le pays de l'adresse IP de l'acheteur (déterminé par la plateforme de paiement). <p>Ce contrôle permet de définir l'action à déclencher lorsqu'aucune des conditions ci-dessous n'est validée :</p> <ul style="list-style-type: none"> • les 3 pays sont identiques, • le pays du moyen de paiement et le pays de l'acheteur sont identiques, • le pays du moyen de paiement et le pays de l'adresse IP sont identiques. <div data-bbox="715 1317 1442 1451" style="border: 1px solid #add8e6; padding: 5px;"> <p> Lorsque vous activez ce contrôle, vous devez vous assurer de transmettre les données utiles à la gestion des risques.</p> </div>
<p>Contrôle de la variété des pays</p>	<p>Ce contrôle permet de définir l'action à déclencher lorsque le nombre de pays concernés par la transaction dépasse un seuil et le montant de la transaction est compris entre un montant minimum et maximum.</p> <div data-bbox="715 1637 1442 1771" style="border: 1px solid #add8e6; padding: 5px;"> <p> Lorsque vous activez ce contrôle, vous devez vous assurer de transmettre les données utiles à la gestion des risques.</p> </div>
<p>Contrôle sur des produits carte provenant de certains pays</p>	<p>Ce contrôle permet de définir l'action à déclencher lorsqu'une transaction est réalisée avec une carte émise dans un pays mis en exception.</p> <p>Vous sélectionnez les pays pour lesquels activer le contrôle. Vous choisissez le ou les types de carte pour lesquels activer le contrôle parmi la liste suivante :</p> <ul style="list-style-type: none"> • carte personnelle de crédit • carte personnelle de débit

- carte personnelle
- carte commerciale
- carte prépayée

Contrôle des pays pour les paiements SDD	Ce contrôle permet de définir l'action à déclencher lorsque le pays du compte bancaire (IBAN) fait partie de la liste des pays sélectionnés.
--	---

- **Critères de vélocité**

Contrôle du nombre de tentatives de paiement pour une adresse IP sur une période*	Ce contrôle permet de définir l'action à déclencher lorsque de multiples tentatives de paiement sont détectées avec une adresse IP identique. Vous définissez la période de référence.
---	--

Contrôle du nombre de tentatives de paiement pour une adresse mail sur une période*	Ce contrôle permet de définir l'action à déclencher lorsque le nombre de tentatives de paiement avec une adresse e-mail identique est supérieur au seuil renseigné en paramètre. Vous définissez la période de référence.
---	---


Contrôle du nombre de tentatives de paiement pour un moyen de paiement sur une période*	Ce contrôle permet de définir l'action à déclencher lorsque de multiples tentatives de paiement sont détectées avec un moyen de paiement (carte ou IBAN) identique. Vous définissez la période de référence.
---	--

Contrôle du nombre de paiements acceptés sur une période*	Ce contrôle permet de définir l'action à déclencher lorsque le nombre de paiements acceptés avec le même moyen de paiement est supérieur au seuil renseigné en paramètre. Vous définissez la période de référence.
---	--

* De 1 minute à 3 jours, le calcul de la période de référence tient compte de la date et de l'heure de la première transaction. Au-delà, le calcul se base uniquement sur la date.

2.3. Les actions

Les actions disponibles dépendent des options de la boutique. Par défaut vous avez accès aux actions "Remonter une alerte" et "Refuser le paiement".

Action	Description
Valider manuellement	<p>Cette action permet de bloquer temporairement la remise du paiement. Pendant ce temps, vous pouvez vérifier la transaction et décider de la valider ou l'annuler.</p> <p>La transaction est créée en validation manuelle. Elle peut être validée tant que le délai de remise en banque n'est pas dépassé. Passé ce délai, le paiement prend le statut "Expiré". Ce statut est définitif.</p> <p>Lorsque la transaction est créée en validation manuelle suite à l'application d'une règle de risque, vous êtes averti via la notification de fin de paiement.</p> <p>La valeur MANUAL_VALIDATION est transmise dans vads_risk_assessment_result en mode redirection et fraudManagement.riskAssessments.results en mode embarqué.</p> <div data-bbox="544 748 1434 981" style="border: 1px solid #add8e6; padding: 10px;"><p> Pour recevoir une notification par e-mail lorsqu'un contrôle créé une transaction en validation manuelle, vous devez :</p><ul style="list-style-type: none">• ajouter l'action "Remonter une alerte" dans la configuration du contrôle et• créer une règle de notification spécifique à la gestion du risque.</div> <p>Cette action peut être cumulée avec d'autres actions, comme Remonter une alerte ou Définir un mode d'authentification.</p>
Refuser le paiement	<p>Cette action permet de refuser un paiement.</p> <p>Exemple : refuser un paiement si la carte utilisée est une carte commerciale.</p> <p>L'action Refuser est prioritaire sur l'action Valider manuellement.</p> <p>Le paiement est refusé et le détail de l'erreur (vads_payment_error / detailedErrorCode) est valorisé à 147.</p>
Remonter une alerte	<p>Cette action permet de vous avertir qu'un risque est identifié.</p> <p>Exemple : le montant de la transaction est supérieur à 1 000 EUR, la transaction a été réalisée avec une carte d'un pays jugé à risque.</p> <p>Cette action peut être cumulée avec d'autres actions, comme Valider manuellement ou Définir un mode d'authentification.</p> <p>L'alerte vous permet de déclencher des traitements ou des vérifications sur la transaction, comme par exemple, mettre en attente son processus de livraison le temps que des vérifications puissent être réalisées sur la transaction.</p> <p>Vous êtes averti :</p> <ul style="list-style-type: none">• via la notification de fin de paiement ; La valeur INFORM est transmise dans vads_risk_assessment_result en mode redirection et fraudManagement.riskAssessments.results en mode embarqué.• par e-mail. Vous devez créer une règle de notification par e-mail spécifique afin de recevoir l'alerte. La condition pour déclencher la règle de notification est Gestion des risques informative = Échouée. Pour plus d'informations sur la procédure de configuration de la notification, voir : Etre notifié en cas de risque de fraude à la page 23.
Définir un mode d'authentification.	<p>Cette action n'est disponible que si 3D Secure v2 est activé sur au moins un des contrats associés à la boutique.</p>

Elle permet de modifier le mode d'authentification par défaut (NO_PREFERENCE) appliqué lors du paiement.

Les choix disponibles dépendent des options de la boutique.

Si la boutique dispose de l'option "Frictionless 3DS2" et est associée à un contrat 3DS2 activé, vous aurez le choix entre les modes d'authentification suivants :

- Demande d'authentification avec interaction de l'acheteur (Challenge) ;
- Demande d'authentification sans interaction de l'acheteur (Frictionless).

En choisissant le choix "Frictionless", l'authentification 3D Secure v2 sera réalisée avec une préférence forcée à Frictionless si une exemption s'applique.

Retrouvez toutes les informations utiles sur les exemptions dans le [guide du 3D Secure](#).

3. GESTION DES LISTES GRISES

Vous avez accès à 3 listes grises qui permettent de mettre en exception :

- des adresses IP,
- des plages de cartes via le code BIN,
- des numéros de carte.

Pour que ces listes soient appliquées, vous devez créer une règle pour chaque liste et définir l'action à réaliser :

- Contrôle du code BIN
- Contrôle de l'adresse IP
- Contrôle du numéro de carte

Voir : [Les critères](#) à la page 6 pour plus de détails.

3.1. Consulter les listes grises

1. Ouvrez le menu **Paramétrage** > **Gestion des risques** > [libellé de votre boutique].
2. Cliquez sur **Gérer les listes grises**.

Adresse IP	Motif	Date	Utilisateur	Nom de l'acheteur	Commande
185.134.22.65		12/06/2024 10:13:58	Demo		

Les listes grises sont organisées par onglet. Cliquez sur l'onglet de votre choix pour afficher la liste correspondante.

L'interface liste pour chaque entrée de la liste grise :

- l'adresse IP, le code BIN ou le numéro de carte partiellement masqué,
- le motif de la mise sur liste grise,
- la date d'insertion sur la liste grise,
- l'utilisateur ayant procédé à l'action,
- le nom de l'acheteur,
- la référence de la commande ayant servi à la mise sur liste grise.

3.2. Ajouter une entrée dans la liste grise

3.2.1. Depuis la liste des transactions

1. Depuis le menu **Gestion > Transactions**, recherchez la transaction concernée.
2. Effectuez un clic droit sur la transaction.
3. Sélectionnez l'action à réaliser :
 - a. **Ajouter la carte à la liste grise**
 - b. **Ajouter l'adresse IP à la liste grise**
 - c. **Ajouter le code BIN à la liste grise**
4. Saisissez le motif de l'ajout en liste grise ("fraude" par exemple) puis cliquez sur **OK**.



Par défaut aucun contrôle n'est activé. L'ajout seul en liste grise ne permet pas de bloquer le paiement. Vous devez [créer une règle](#) pour chaque liste grise et définir l'action à réaliser.

3.2.2. Depuis la gestion des risques

1. Ouvrez le menu **Paramétrage > Gestion des risques > [libellé de votre boutique]**.
2. Cliquez sur **Gérer les listes grises**.

Le screenshot montre l'interface 'Gestion des listes grises'. En haut, il y a trois onglets : 'Adresse IP', 'Code BIN' et 'Numéro de carte'. À droite, il y a des boutons 'Éditer', 'Supprimer' et '+ Ajouter'. En dessous, un tableau affiche une seule entrée avec les colonnes 'Adresse IP', 'Motif', 'Date', 'Utilisateur', 'Nom de l'acheteur' et 'Commande'. La valeur de l'adresse IP est '185.134.22.65', la date est '12/06/2024 10:13:58' et l'utilisateur est 'Demo'. En bas à gauche, il y a '1 - 1 sur 1' et 'Page 1'. En bas à droite, il y a un menu déroulant '25' et deux boutons 'Fermer' et 'Confirmer'.

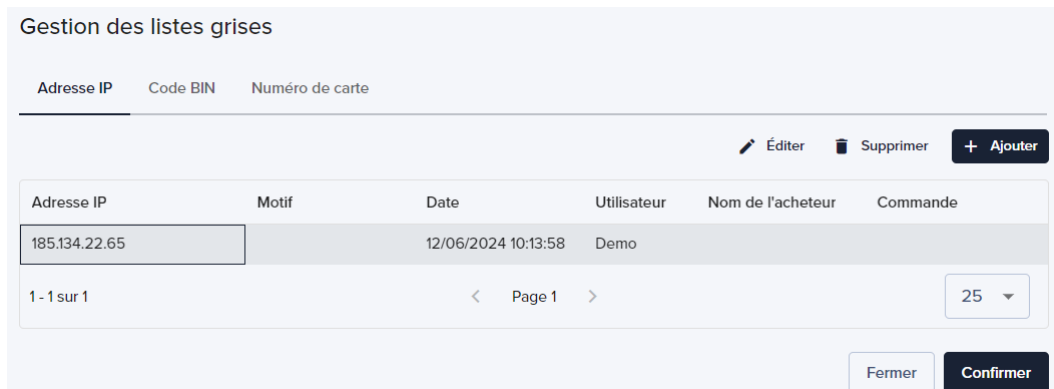
3. Cliquez sur l'onglet correspondant à la liste grise de votre choix :
 - a. **Adresse IP**
 - b. **Code BIN**
 - c. **Numéro de carte**
4. Cliquez sur **Ajouter** pour renseigner manuellement les données à mettre en liste grise.



Par défaut aucun contrôle n'est activé. L'ajout seul en liste grise ne permet pas de bloquer le paiement. Vous devez [créer une règle](#) pour chaque liste grise et définir l'action à réaliser.

3.3. Supprimer une entrée dans la liste grise

1. Ouvrez le menu **Paramétrage** > **Gestion des risques** > [libellé de votre boutique].
2. Cliquez sur **Gérer les listes grises**.
3. Cliquez sur l'onglet correspondant à la liste grise de votre choix :
 - a. **Adresse IP**
 - b. **Code BIN**
 - c. **Numéro de carte**
4. Sélectionnez l'entrée à supprimer.



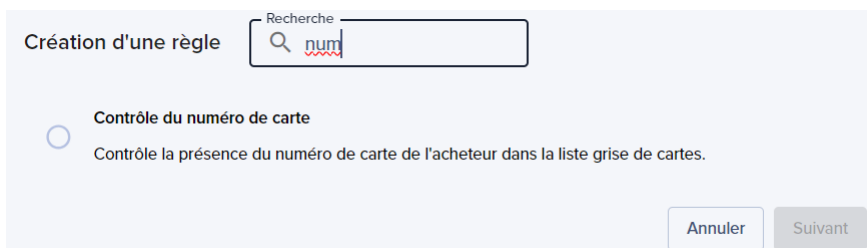
The screenshot shows the 'Gestion des listes grises' interface. At the top, there are three tabs: 'Adresse IP', 'Code BIN', and 'Numéro de carte'. Below the tabs, there are three buttons: 'Éditer', 'Supprimer', and '+ Ajouter'. A table with the following columns is displayed: 'Adresse IP', 'Motif', 'Date', 'Utilisateur', 'Nom de l'acheteur', and 'Commande'. The table contains one row with the following data: '185.134.22.65', an empty 'Motif' cell, '12/06/2024 10:13:58', 'Demo', and empty 'Nom de l'acheteur' and 'Commande' cells. Below the table, there is a pagination bar showing '1 - 1 sur 1', 'Page 1', and a dropdown menu set to '25'. At the bottom right, there are two buttons: 'Fermer' and 'Confirmer'.

5. Cliquez sur **Supprimer** puis confirmez la suppression.

4. GESTION DES RÈGLES

4.1. Créer une nouvelle règle

1. Ouvrez le menu **Paramétrage** > **Gestion des risques** > [libellé de votre boutique].
2. Cliquez sur **Créer une nouvelle règle**.
3. Utilisez le moteur de recherche pour trouver le contrôle à activer.
















4. Sélectionnez le contrôle puis cliquez sur **Suivant**.



5. **Nom de la règle** : Modifiez le nom de la règle si nécessaire.
6. **Paramètres** : Ils diffèrent en fonction des règles.
 - Champs de saisie à remplir
 - Liste déroulante
Maintenez la touche CTRL appuyée + clic gauche de la souris pour sélectionner plusieurs valeurs.
 - Liste de pays
Choisissez si vous souhaitez que la règle se déclenche ou ne se déclenche pas en fonction des pays sélectionnés.
Cochez les pays en fonction de votre besoin. Vous pouvez vous aider de la barre de recherche pour trouver un pays.

La règle se déclenche pour les 0 pays sélectionné(s)

Recherche

 Afghanistan <input type="checkbox"/>	 Andorre <input type="checkbox"/>	Antilles néerlandaises
 Afrique du Sud <input type="checkbox"/>	 Angola <input type="checkbox"/>	 Arabie saoudite
 Albanie <input type="checkbox"/>	 Anguilla <input type="checkbox"/>	 Argentine
 Algérie <input type="checkbox"/>	Antarctique <input type="checkbox"/>	 Arménie
 Allemagne <input type="checkbox"/>	 Antigua-et-Barbuda <input type="checkbox"/>	 Aruba

Vous devez sélectionner au minimum un pays.

7. **Actions** : Cliquez sur **Ajouter** et sélectionnez l'action à réaliser dans la liste déroulante. Si vous souhaitez définir plusieurs actions, cliquez à nouveau sur **Ajouter**.

Voir : [Les actions](#) pour plus d'informations sur les actions disponibles.

8. Cliquez sur **Sauvegarder** pour enregistrer vos modifications.



- L'action **Remonter une alerte** nécessite la création d'une règle de notification spécifique.
- La liste des actions disponibles dépend des options de votre boutique.

4.2. Rechercher / filtrer les règles

1. Ouvrez le menu **Paramétrage** > **Gestion des risques** > [libellé de votre boutique].

2. Utilisez la barre de recherche pour retrouver rapidement les règles existantes

Recherche

3. Saisissez un mot clé présent dans le libellé de la règle, par exemple : "montant", pour retrouver toutes les règles dont le libellé comporte "montant".

Vous pouvez aussi utiliser les filtres disponibles pour lister les règles en fonction de leurs actions ou de leur état :

Toutes les règles Actives Inactives  Refuser  Manuel  Alerte  Mode d'authentification

4.3. Activer / Désactiver une règle

1. Ouvrez le menu **Paramétrage** > **Gestion des risques** > [libellé de votre boutique].


2. Recherchez la règle concernée.

Utilisez les filtres ou la barre de recherche pour retrouver facilement la règle.

3. Cliquez sur l'interrupteur à droite du détail de la règle.

> Contrôle du numéro de carte   


L'état de l'interrupteur indique le statut de la règle :

 : la règle est active. Vous pouvez la désactiver.



: la règle est désactivée. Vous pouvez l'activer. La règle s'applique alors instantanément sur les transactions de test comme sur les transactions de production.


4.4. Editer une règle

1. Ouvrez le menu **Paramétrage** > **Gestion des risques** > [libellé de votre boutique].
2. Recherchez la règle concernée.
Utilisez les filtres ou la barre de recherche pour retrouver facilement la règle.
3. Cliquez sur  à droite du détail de la règle.



4. Cliquez sur **Éditer** pour modifier la configuration de la règle.

4.5. Supprimer une règle

1. Ouvrez le menu **Paramétrage** > **Gestion des risques** > [libellé de votre boutique].
2. Recherchez la règle concernée.
Utilisez les filtres ou la barre de recherche pour retrouver facilement la règle.
3. Cliquez sur  à droite du détail de la règle.



4. Cliquez sur **Supprimer** puis confirmez la suppression.

5. TRANSMETTRE LES DONNÉES UTILES À LA GESTION DES RISQUES

Certains contrôles nécessitent des données particulières dans la demande de paiement afin d'évaluer le risque. Sans ces données le contrôle ne peut être réalisé.

Le tableau ci-dessous liste pour chaque contrôle concerné les données nécessaires à son exécution :

Contrôle	API Formulaire	API REST
Contrôle du nombre de tentatives de paiement pour une adresse mail sur une période	vads_cust_email	customer.email
Contrôle du pays du client (adresse de facturation)	vads_cust_country	customer.billingDetails.country
Contrôle de la cohérence des pays	vads_cust_country	customer.billingDetails.country
Contrôle du pays de livraison	vads_ship_to_country	customer.shippingDetails.country
Contrôle de la variété des pays	vads_ship_to_country, vads_cust_country	customer.shippingDetails.country, customer.billingDetails.country
Contrôle sur le nombre de références produits dans le panier	vads_nb_products	Géré automatiquement par la plateforme.
Contrôle des produits du panier	vads_product_refN	cartItemInfo.productRef

6. RESTITUTION DE LA GESTION DU RISQUE DANS L'IPN

Le résultat des contrôles effectués dans le cadre de l'analyse du risque est retourné dans l'IPN via les champs :

6. vads_risk_assessment_result / fraudManagement.riskAssessments.results

Valeurs	Description
ENABLE_3DS	Une authentification avec interaction du porteur (challenge) a été demandée.
DISABLE_3DS	Une authentification sans interaction du porteur (frictionless) a été demandée.
NO_PREFERENCE	Une authentification 3DS a été demandée. Le choix de la préférence est délégué à l'émetteur de la carte.
NO_CHALLENGE_REQUESTED	Une authentification sans interaction du porteur (frictionless) a été demandée.
CHALLENGE_REQUESTED	Une authentification avec interaction du porteur (challenge) a été demandée.
CHALLENGE_MANDATE	Une authentification avec interaction du porteur (challenge) a été demandée pour des raisons réglementaires.
MANUAL_VALIDATION	La transaction est créée en validation manuelle. La remise du paiement est bloquée temporairement pour vous permettre de procéder à toutes les vérifications souhaitées.
REFUSE	La transaction est refusée.
RUN_RISK_ANALYSIS	Appel à un analyseur de risque externe sous condition que vous possédez un contrat. Se référer à la description de l'objet vads_risk_analysis_result pour identifier la liste des valeurs possibles et leur description.
INFORM	Une alerte est remontée. Vous êtes averti qu'un risque est identifié. Vous êtes informé via une ou plusieurs des règles du centre de notification (URL de notification, e-mail ou SMS).

6. vads_risk_control / fraudManagement.riskAssessments.riskControl

Format : contrôle1=résultat1;contrôle2=résultat2

Valeur possibles pour "contrôle[x]"	Description
CARD_FRAUD	Contrôle du numéro de carte
SUSPECT_COUNTRY	Contrôle du pays émetteur du moyen de paiement
IP_FRAUD	Contrôle de l'adresse IP
CREDIT_LIMIT	<ul style="list-style-type: none">• Contrôle du montant cumulé sur une période,• Contrôle sur le montant maximum,• Contrôle du nombre de paiements acceptés sur une période
BIN_FRAUD	Contrôle du code BIN

ECB	Contrôle des e-Carte Bleue
COMMERCIAL_CARD	Contrôle des cartes commerciales
SYSTEMATIC_AUTO	Contrôle des cartes à autorisation systématique
INCONSISTENT_COUNTRIES	Contrôle de la cohérence des pays
NON_WARRANTY_PAYMENT	Contrôle le transfert de responsabilité de la transaction.
SUSPECT_IP_COUNTRY	Contrôle du pays de l'adresse IP

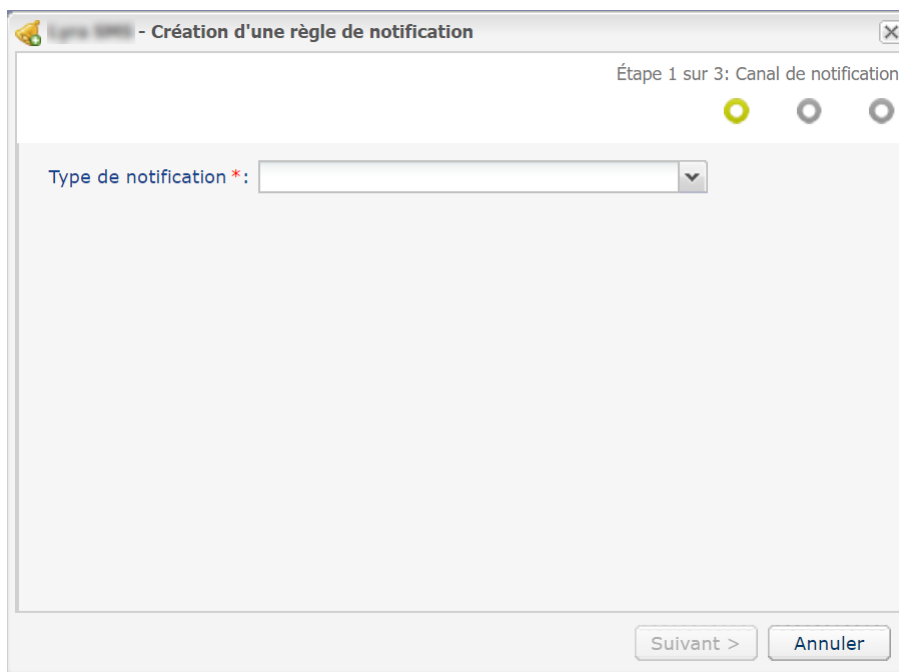
Valeurs pour "résultat[x]"	Description
OK	OK
WARNING	Le contrôle a remonté une alerte
ERROR	Le contrôle a refusé le paiement

7. ETRE NOTIFIÉ EN CAS DE RISQUE DE FRAUDE

Cas d'utilisation : L'action d'un contrôle de risque est configurée à **Remonter une alerte**. Vous souhaitez recevoir un e-mail spécifique dès lors qu'un contrôle détecte un risque de fraude.

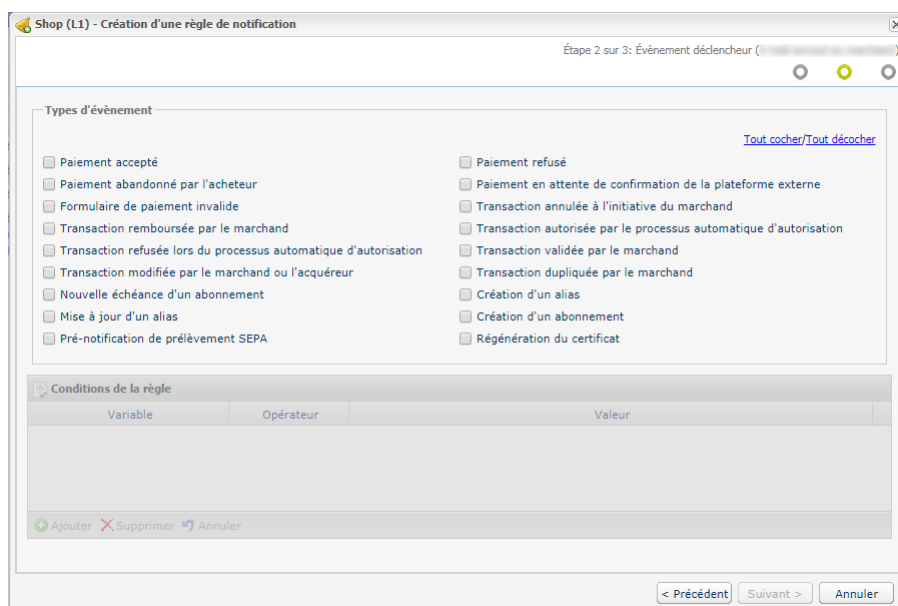
Pour créer la règle de notification associée :

1. Depuis votre Back Office Marchand, allez dans le menu : **Paramétrage > Règles de notifications**.
2. Cliquez sur le **Créer une règle** en bas à gauche de l'écran.
3. Sélectionnez **Notification avancée**.



The screenshot shows a dialog box titled "Création d'une règle de notification" with a close button (X) in the top right corner. The progress indicator shows "Étape 1 sur 3: Canal de notification" with three circles, the first of which is highlighted in green. Below the progress indicator is a dropdown menu labeled "Type de notification *:". At the bottom of the dialog, there are two buttons: "Suivant >" and "Annuler".

4. Sélectionnez le type de notification **E-mail envoyé au marchand**.
5. Cliquez sur **Suivant**.



The screenshot shows the same dialog box, now at "Étape 2 sur 3: Évènement déclencheur". The progress indicator shows the second circle highlighted in green. The main area is titled "Types d'évènement" and contains a list of checkboxes for various events. A link "Tout cocher/Tout décocher" is visible on the right. Below the list is a section titled "Conditions de la règle" with a table structure for defining conditions. At the bottom, there are buttons for "Ajouter", "Supprimer", and "Annuler".

Variable	Opérateur	Valeur
----------	-----------	--------

6. Cochez les événements déclencheurs en fonction de votre besoin.

Exemple : **Paiement accepté** et **Création d'alias**.

7. Dans la section **Conditions de la règle**, cliquez sur **Ajouter**.
8. Dans la colonne **Variable**, sélectionnez **Gestion des risques informative**.
9. Sélectionnez l'opérateur **égal à**.
10. Sélectionnez la valeur **Échoués**.
11. Cliquez sur **Suivant**.
12. Renseignez le **Libellé de la règle**.
13. Renseignez l'adresse e-mail à notifier.
14. Choisissez les champs à inclure dans l'e-mail.
Par défaut, le détail de la gestion des risques est déjà inclus.
15. Cliquez sur **Paramétrage e-mail**.
Par défaut, le sujet du message est le même que l'e-mail de confirmation de paiement. Il est recommandé de modifier le sujet de l'e-mail pour identifier facilement ces e-mails d'alerte.
Ajoutez par exemple "Risque Fraude -" ou "Transaction à valider -" au début du sujet.
16. Une fois le paramétrage achevé, cliquez sur **Créer**.

Lorsqu'une règle de risque configurée avec l'action **Remonter une alerte** se déclenche, vous recevez un e-mail contenant le détail de la transaction et de la gestion des risques :

Détail de la gestion des risques

Contrôle d'encours :  Réussi

Contrôle de l'adresse IP :  Échec non bloquant

Détail de l'appel au module de gestion des risques avancée

 Lever une alerte

8. CONSULTER LE DÉTAIL D'UNE TRANSACTION

Les transactions sont visibles depuis le menu **Gestion > Transactions**.

Pour visualiser le détail d'une transaction :

1. Sélectionnez une transaction.
2. Effectuez un clic droit puis sélectionnez **Afficher le détail de la transaction**.
Dans le groupe **Cycle de vie de la transaction**, le statut de la transaction est spécifié.

Détail d'une transaction en cours : 253128 (Référence commande : 2524895)

Informations 3D Secure Acheteur Gestion des risques Gestion des risques avancée

Identification de la transaction

Id. Transaction :	253128
UUID Transaction :	250342037db0470fb3b84277f4950291
Référence commande :	2524895
Boutique :	[Masqué]
Montant actuel :	90
Type :	Débit

Cycle de vie de la transaction

Statut :	Refusé (Raison du refus : Gestion des risques avancée)
Détail de l'erreur :	147 : Le module de gestion de fraudes a demandé le refus de cette transaction.
Date de création :	25/02/2020 17:27:55
Date de remise demandée :	25/02/2020 17:27:55

Moyen de paiement

Moyen de paiement :	[Carte]
Numéro de carte :	597010XXXXXX0042 (06/2021 - en cours de validité)
Banque émettrice :	[Masqué]

Autorisation

Contrat commerçant :	[Masqué]
----------------------	----------

Validier | Modifier | Annuler | Dupliquer | Ticket

Fermer

En cas de paiement refusé le détail de l'erreur est valorisé à 147.

3. Cliquez sur l'onglet **Gestion des risques avancée** pour identifier la règle appliquée ainsi que l'action exécutée.

Détail d'une transaction en cours : 253128 (Référence commande : 2524895)

Informations 3D Secure Acheteur Gestion des risques **Gestion des risques avancée**




Résultat de l'appel 1 au module de gestion de fraudes

Règle(s) levée(s) lors de l'appel 1 :	Carte non enrôlée 3D Secure
Décision(s) prise(s) lors de l'appel 1 :	Refuser la transaction

Fermer

4. D'autres informations sont disponibles dans l'onglet **Gestion des risques** :

- les pays (IP, acheteur, moyen de paiement),
- le code produit et le type de produit de la carte,
- le résultat des différents contrôles.

Symbole	Description
	Le contrôle de risque est activé mais ne s'est pas déclenché. Aucun risque détecté.
	Le contrôle de risque est activé et s'est déclenché. Un risque a été détecté et une alerte a été envoyée au marchand.
	Le contrôle de risque est activé et s'est déclenché. Un risque a été détecté et le paiement a été refusé.

9. VALIDER MANUELLEMENT UNE TRANSACTION

Lorsqu'une règle de risque configurée à "Valider manuellement" se déclenche, la transaction est créée dans le statut "À valider".

Vous devez alors valider le paiement avant l'expiration de la demande d'autorisation. Dans le cas contraire le paiement expire.



Si vous souhaitez recevoir un e-mail spécifique lorsqu'une règle a créé une transaction en validation manuelle :

- Ajoutez l'action "Remonter une alerte" dans la configuration de la règle.
- [Créez une règle de risque spécifique à la gestion du risque.](#)

Pour valider une transaction depuis le Back Office Marchand :

1. Effectuez un clic droit sur une transaction dont le statut est "À valider".
2. Sélectionnez **Valider**.
3. Confirmez que vous souhaitez réellement valider la transaction sélectionnée.