Payment Express® Risk Management

User Manual

paymentexpress®

www.paymentexpress.com

Version 0.1

paymentexpress®

Risk Management

User Manual

Document Revision Information

Version	Date	Revision Information
0.1	01/02/2017	Initial version

Risk Management

User Manual

Copyright

98 Anzac Avenue
PO Box 8400
Auckland, 1150
New Zealand
www.paymentexpress.com

Proprietary Notice

The information described in this document is proprietary and confidential to Payment Express. Any unauthorised use of this material is expressly prohibited except as authorised by Payment Express in writing.

paymentexpress®

Risk Management

User Manual

Contents

1. Overview

Payment Express offers an extensive library of customizable Risk Management rules which are used to enforce security, prevent fraudulent activity, and provide in-depth knowledge of card-holder behaviour to the merchant.

Prior to validation by the acquiring bank, the Risk Management rule sets are used to vet the transaction inputs, analyse metadata, and assess the risk associated with any given transaction based on the recorded transaction velocity of a given card.

Merchants using the Payment Express Risk Management rule sets are able to reduce their exposure to potentially fraudulent behaviour. Static allow and block lists, the ability to block or allow ranges of cards by type, and real-time transaction notifications allow merchants to put in place rules which bolster their security without alienating genuine customers. Merchants are encouraged to set rules which work for them and their business model.

Merchants with an effective array of Risk Management rules would expect to see a reduction in exposure to financial risk. By identifying suspicious purchases in advance, the merchant can make an informed choice on whether to provide goods and services. Reduced charge-backs and better control over stock will allow for merchants to reduce financial costs associated with credit/debit card fraud.

The Payment Express Risk Management rules give merchants the option of receiving real-time notification for all transactions. Real-time notification provides merchants with the ability to review transactions, learn about card-holder behaviour, and most importantly learn how to set effective risk-management rules.
Risk Management rules are accessible for review and customization via Payline.

Production - https://sec.paymentexpress.com/pxmi3/logon
Testing - https://uat.paymentexpress.com/pxmi3/logon

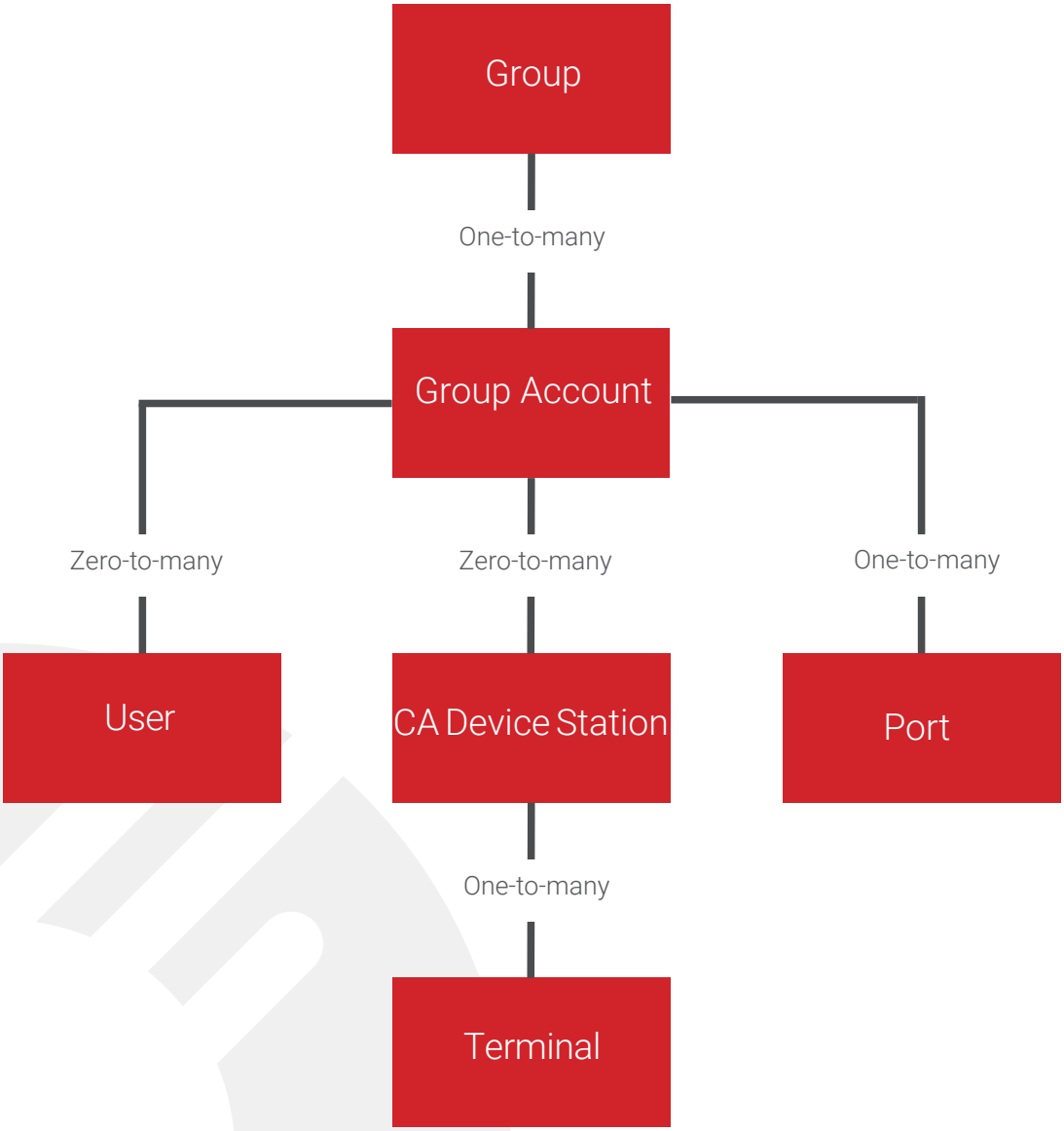
For additional information regarding the Risk Management rule sets and how these can benefit your business, please contact our sales team:
Phone: 0800 PAYMENT (729 6368)
Email: sales@paymentexpress.com

2. Your setup

For every customer, an account is set up to hold all of their custom settings, transactional information, and contact details.

At the highest level of abstraction, a Group contains important technical information about a customer. Each Group contains a number of general purpose settings which are applied across the board to each and every element of the customer's Payment Express experience.

Each Group has one or more Group Accounts associated with it, whereas a Group Account contains a reference to one and only one Group. Group Accounts are used to differentiate between elements of the merchant's payment faculties. Most Groups will have only one Group Account, however in some cases (for example a large business or franchise) it is necessary to further split the information in order to assess where transactions are occurring.



Each Group and Group Account are linked to one or more Ports, and each Port applies to only one Group and Group Account. The Port controls the link between Payment Express and the bank.

All e-commerce payments and Host Initiated Transactions utilize a Payment Express User. Each User relates to only one Group and Group Account, however there are no limits on the number of users that can be set up with the same Group and Group Account. For card-present transactions (both attended and unattended) a CA Device station serves to control the settings of a specific terminal or group of terminals, like the User, each CA Device station has a zero-to-many relationship to the Group and Group Account. When transacting with e-commerce of HIT, the main Payment Express tool you will be using is your User. When transacting in a card-present environment (not including HIT) the main tool is the CA Device Station.

3. Use Cases and Rule Exceptions

Payment Express Risk Management allows for customizable control over transactions. Cards can be explicitly added to allow and block lists, transactions can be restricted by various inputs, and risk management rules can be applied based on previous transaction history over a configurable time period.

When a generic range of transactions have been blocked (see section 5.0), there may be cases where cards are used in a non-fraudulent manner, however these cards will still be blocked by the rules.

Instead of disabling the rule and exposing merchants to potential fraudulent behaviour, the cards can be added to an Allowed Cards list (see section 4.0). These Allowed Cards will apply to particular groups and allow for merchants to maintain their own security without discriminating against potential customers.

Conversely a merchant may not wish to implement a blanket rule preventing payments from all card holders based on certain criteria. A block list exists which allows for merchants to block specific cards without also blocking all other potential customers.

When a transaction fails due to a Risk Management rule being broken, the **LR ReCo** will be returned.

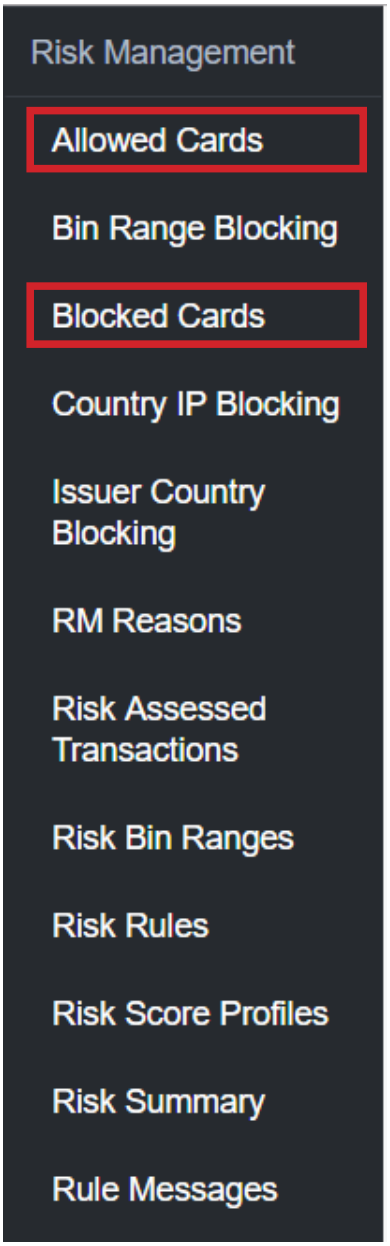
4. Block or Allow Individual Cards

At the merchant's discretion, individual cards can be blocked or allowed. The use of Blocked and Allowed lists offers merchants a much finer level of control over which potential customers can and cannot make purchases. Instead of creating (or modifying) rule sets, Allowed and Blocked lists will look only at individual card numbers and treat these differently from other cards with similar properties e.g. card issuer or issuing country.

In many cases it is easier and safer to simply add a card to either the Blocked list or the Allowed list instead of modifying rules to take into account exceptional cards.

When a potential customer is known to be genuine, despite having a card which is blocked by one or more of the Payment Express Risk Management Rules, it is a straight forward process to add their card to an Allowed list; this requires no modification of the existing rule sets which have been put in place. The Allowed List option is ideal when there are very few cards which need to be added; if there is a very frequent need to add new cards and there is a clear pattern that these cards follow, it may be worthwhile reviewing the Risk Management rules and making modifications.

If a specific card is being used in a fraudulent manner, this card can be added to the Blocked list. This requires no updates to existing rule sets and will allow for a card which would otherwise not trigger any of the Risk Management rules to automatically be declined. This option is ideal when the fraudulent card is similar to many other cards which are not being used in a fraudulent manner. If there is an increasing number of cards which have the same properties being added to the Block List, it may be worthwhile reviewing the existing rule sets and blocking these cards using the Risk Management rules.

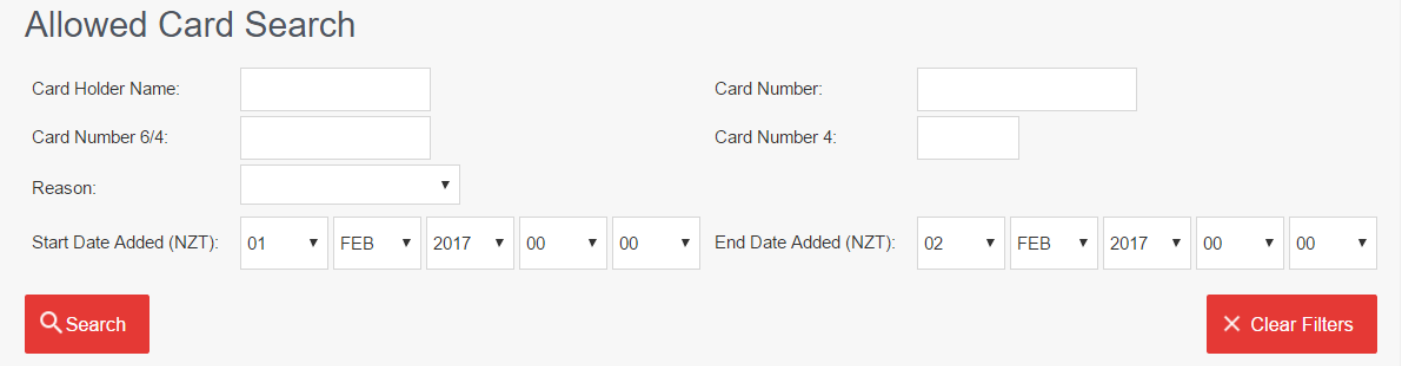


4.1 Searching Allowed and Blocked List Cards

To search for cards which have already been added to the Allowed or Blocked lists, navigate to Payline and select either Allowed Cards or Blocked Cards under Risk Management; if this is not visible please contact your account manager.

These will be displayed on the left hand side of the screen when accessing Payline.

Both Allowed and Blocked card lists will display the following search options, these can be used to refine the results and look for specific cards.

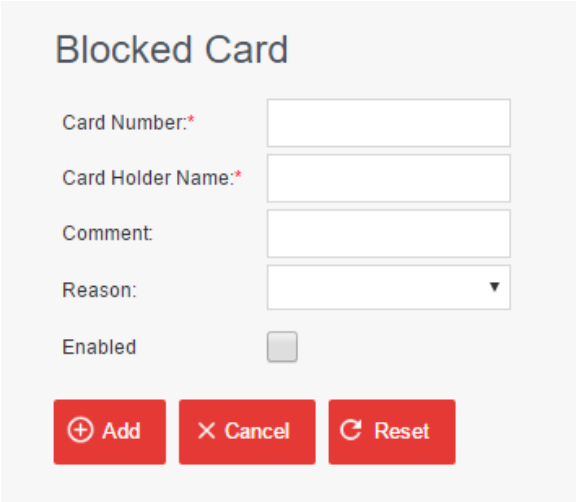


4.2 Adding a New Card to the Blocked List

To add a new card to the Blocked List, sign into the Payment Express Payline service and navigate to Blocked Cards under Risk Management. Clicking the add button will open the following screen where cards can be added to the Blocked list. Identifying information about the card is required.

Comments can be added in a free text field, this can be used to give an explanation of why the card has been blocked in addition to the Risk Management reason. The reason is selected from a drop down of existing options, additional options can be added using the RM Reasons screen.

The Enabled radio button allows for the merchant to turn the rule off or on essentially treating the card as though it was not in the Blocked list without deleting it.

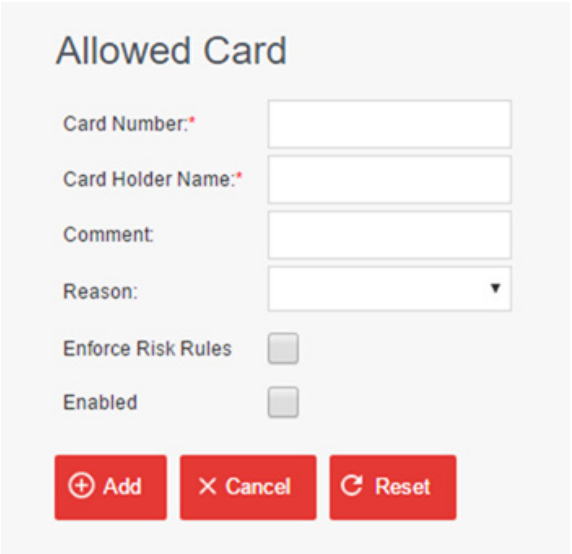


4.3 Adding a New Card to the Allowed List

To add a new card to the Allowed List, sign into the Payment Express Payline service and navigate to Allowed Cards under Risk Management. Clicking the add button will open the following screen where cards can be added to the Allowed list. Identifying information about the card is required.

The Enforce Risk Rules radio button enables merchants to choose whether or not to apply Risk Management rules to this card. If this option is enabled, the card will be treated as though it was any other valid card and will be subject to additional checks which will analyse the transaction history of the card. If this option is not checked any valid transaction will be approved.

The Enabled radio button allows for the merchant to treat the card as though it was not in the Allowed list without deleting it. This radio button allows merchants to enable or disable individual cards.

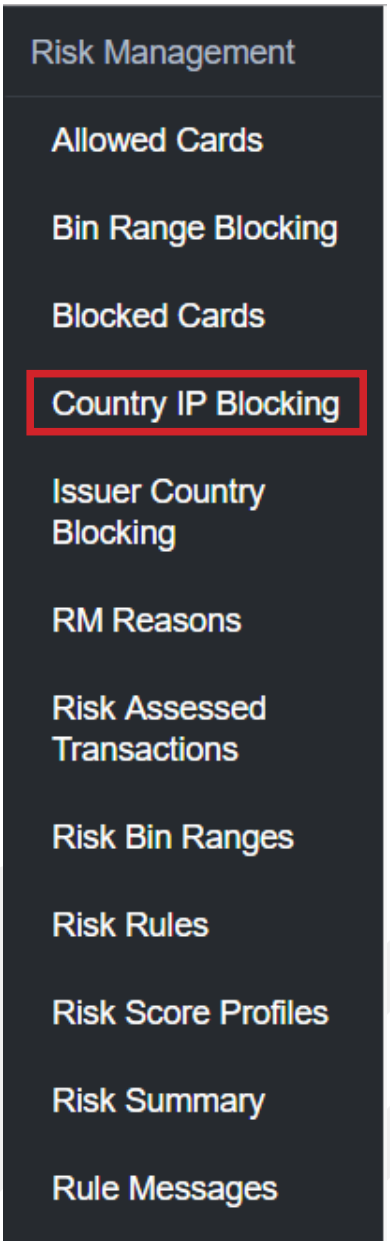


5. Static Blocked and Allowed Lists

The Payment Express Risk Management rule sets incorporate static allow lists and block lists. When a transaction is made, the Risk Management software will analyse the transaction details and either block or allow the transaction based on these static lists.

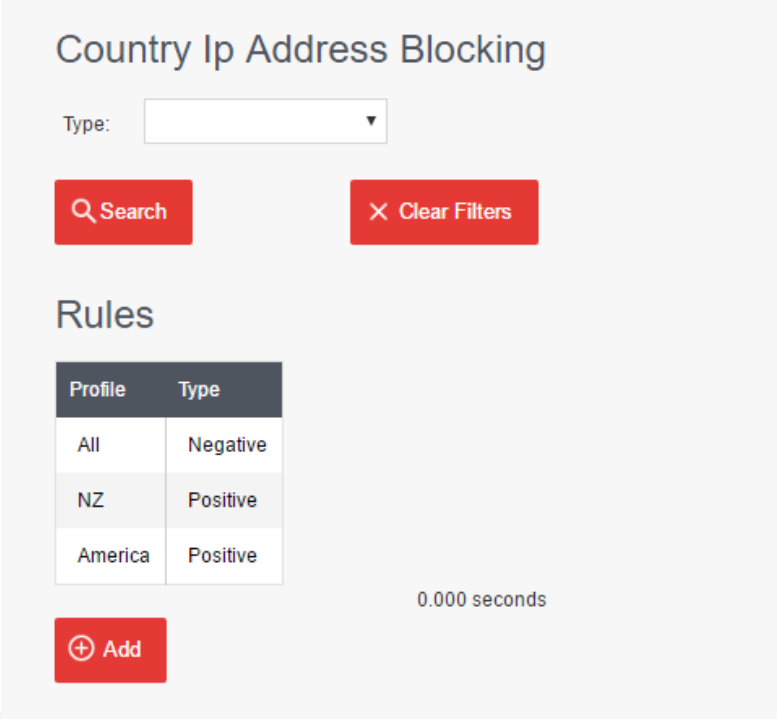
Any allow listed value will take precedence over a block listed value, this allows a large range of values to be blocked and a subset to be allowed. A wide range of cards can be blocked and then another range of cards can be allowed. The allowed cards will always take precedence over blocked ones.

These lists act as blanket rules which are used to limit transactions based on any of the following factors:



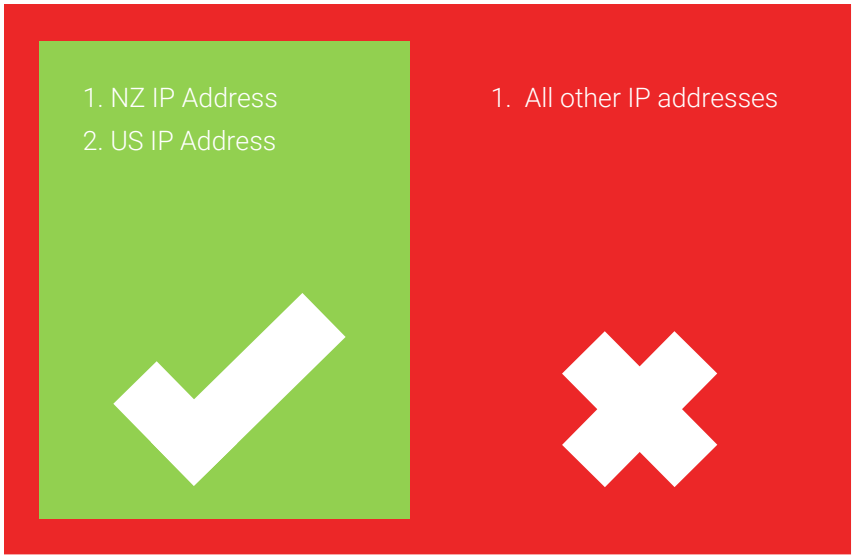
5.1 Blocking Countries by IP Address

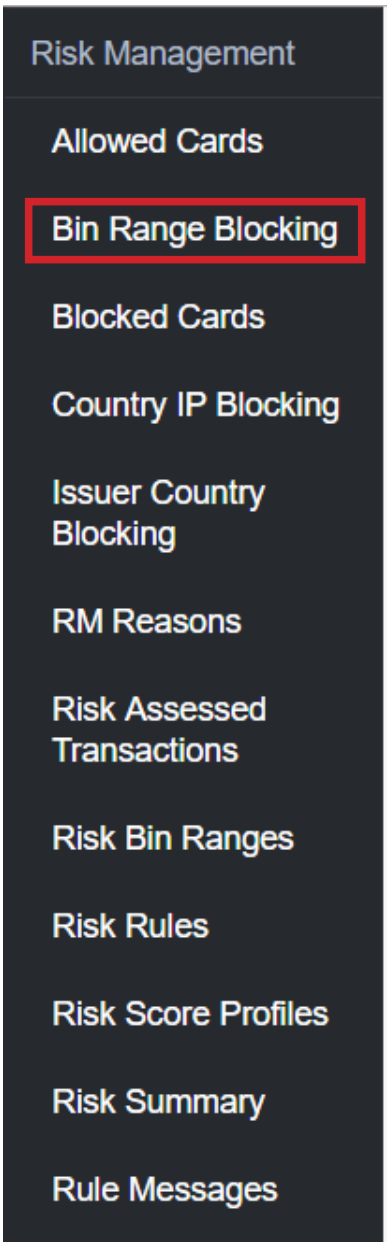
Country Ip Address Blocking can be found by navigating to the Risk Management drop down in Payline and selecting Country IP Blocking:



Risk Management gives merchants the power to either block or allow transactions coming from an IP address originating in any given country. This is done by enabling one or more country IP profiles and setting them to allowed or blocked. When a transaction is made, the originating IP address is compared to the values in the chosen Country IP Address profile.

In the example above, three country IP Address profiles have been enabled. The first profile "All" is Blocked. The second and third profiles will be triggered if the originating IP address is found to have been from either New Zealand or the United States and will successfully go through. Instead of individually blocking all countries except for New Zealand and the United States, Risk Management allows merchants to apply a blanket rule against all IP addresses and then allow a subset of countries to be specifically allowed.





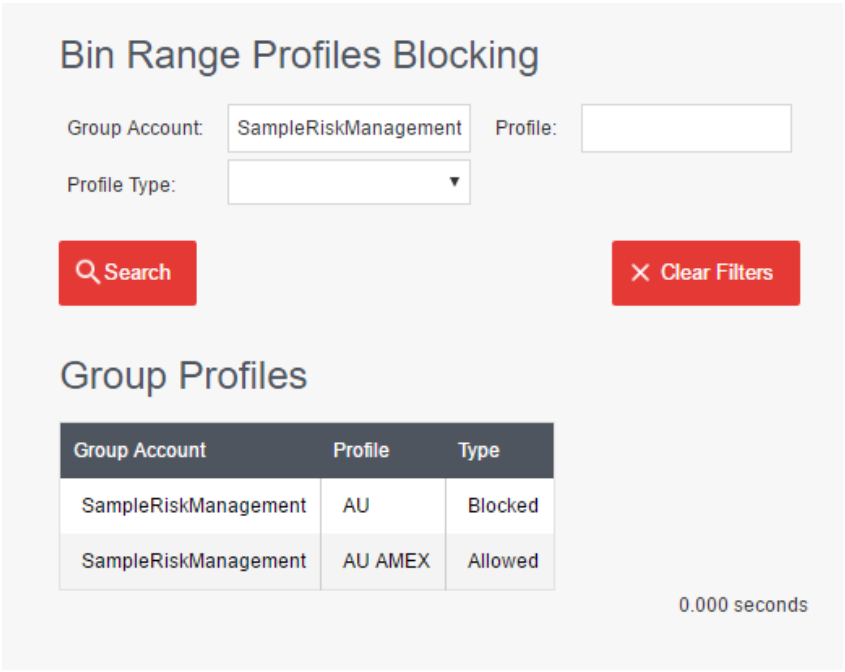
5.2 Blocking BIN Ranges

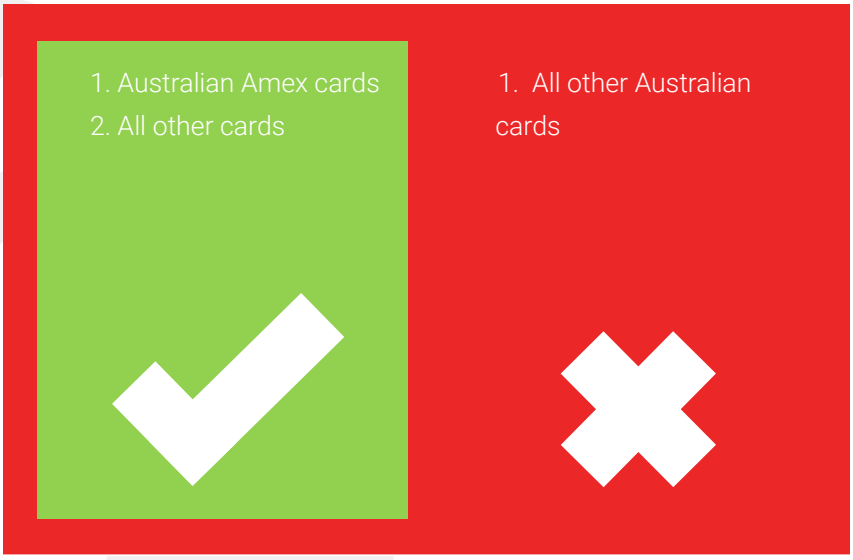
Bin Range Profiles Blocking can be found by navigating to the Risk Management drop down in Payline and selecting Bin Range Blocking:

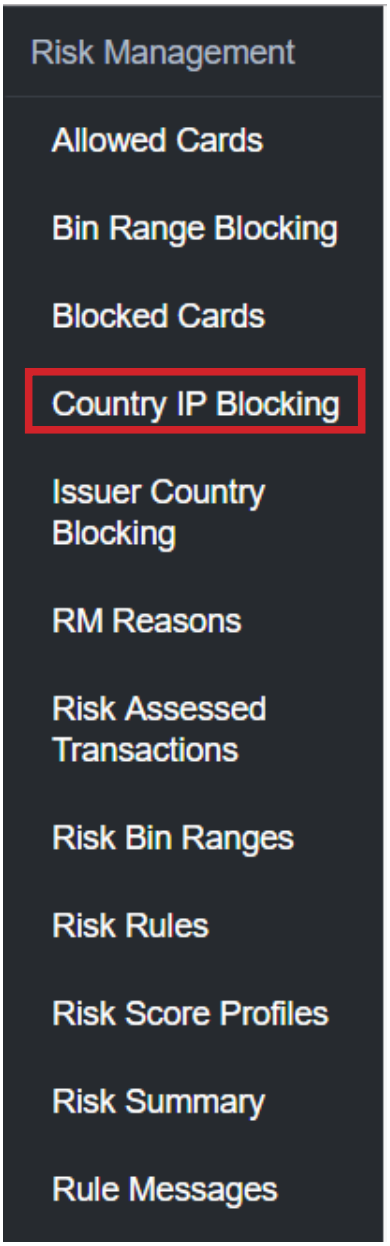
Using Risk Management rules, it is possible to block transactions based on the BIN range of the customer's card. BIN Range blocking will associate the merchant with a BIN range profile and the option to either Block or Allow cards with the given BIN ranges.

Any given BIN range profile is set by Payment Express and will contain a list of associated BIN ranges.

In the example below, the BIN range profile "AU" contains the BIN ranges of all cards issued in Australia and another profile called "AU AMEX" which contains the BIN ranges of all Amex cards issued in Australia. The Group Account "SampleRiskManagement" disallows any cards issued within Australia unless those cards happen to be Amex.

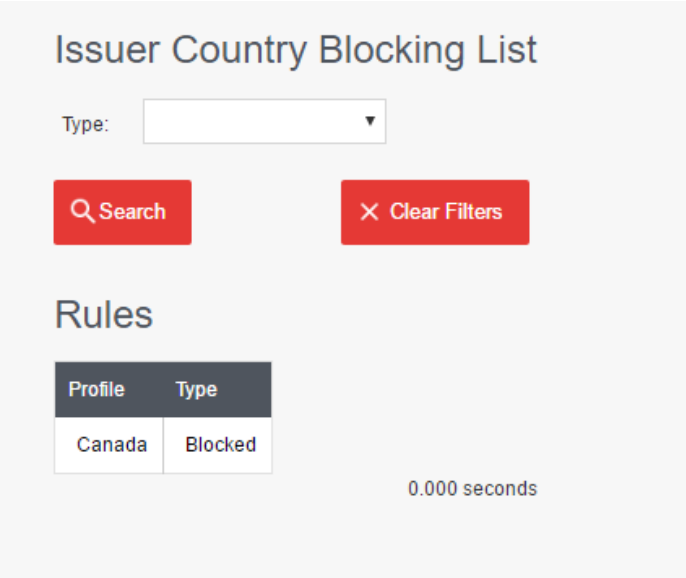






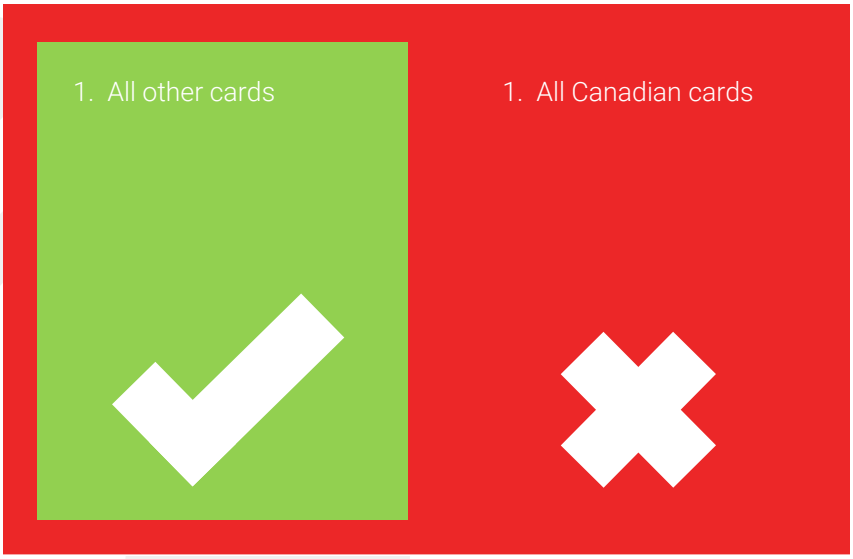
5.3 Blocking Cards by Issuing Country

Issuer Country Blocking List can be found by navigating to the Risk Management drop down in Payline and selecting Issuer Country Blocking:



Similar to the BIN range allow and block lists, Risk Management also provides the more straight-forward option to block cards issued in a particular country. In the above example, all Australian issued cards were blocked using the BIN range profile "AU" an alternative to using BIN range profiles is the Issuer Country Blocking List.

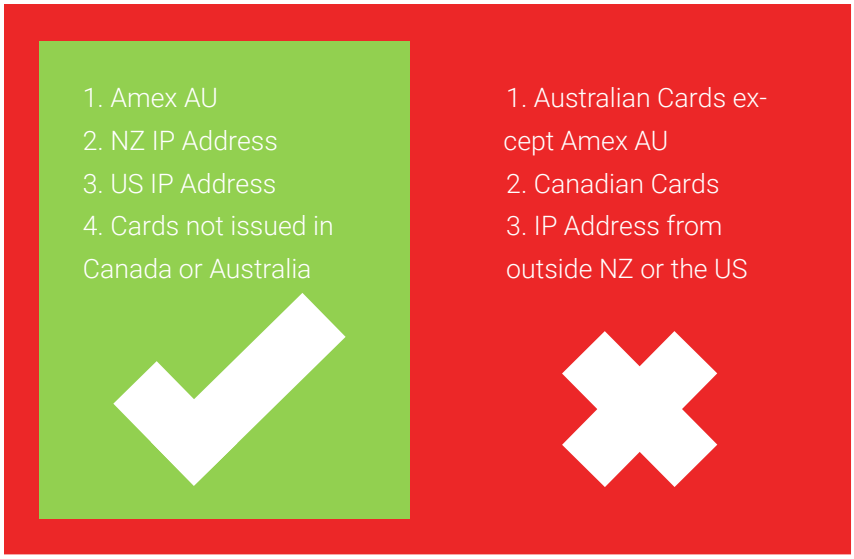
In the example below, all cards issued in Canada will be blocked.

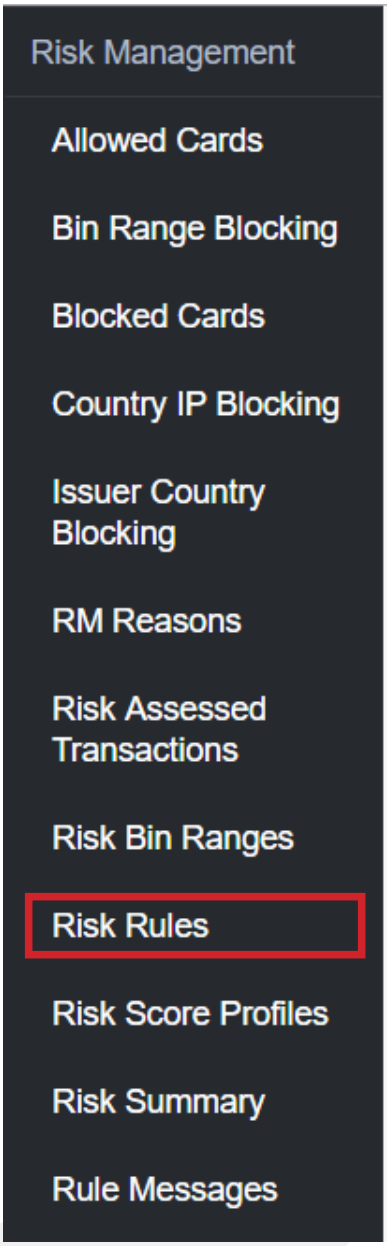


5.4 Summary of Examples

In the above examples, the transaction's IP address must be from either New Zealand or the United States and any cards issued in either Canada or Australia will be blocked (with the exception of Australian Amex cards).

These rules work in conjunction to provide the merchant a set of generalized blanket conditions which restrict where and how transactions are made.

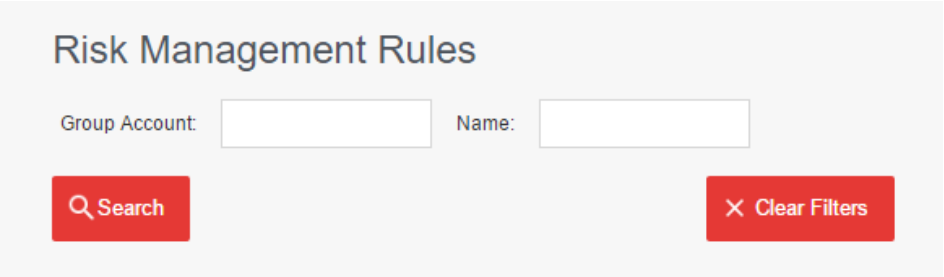




Risk Rules can be navigated to by selecting Risk Rules from the Risk Management option in Payline:

Risk Rules provides merchants with the ability to monitor, enforce, and fine tune highly customizable rule sets. Merchants are able to modify existing rules or request new rules to be implemented by the Payment Express support team.
The customer Risk Rules apply a more specific set of conditions to transactions. Transactions can be blocked depending on the card metadata.

It is possible to use custom risk rules to block transactions over a certain financial value.

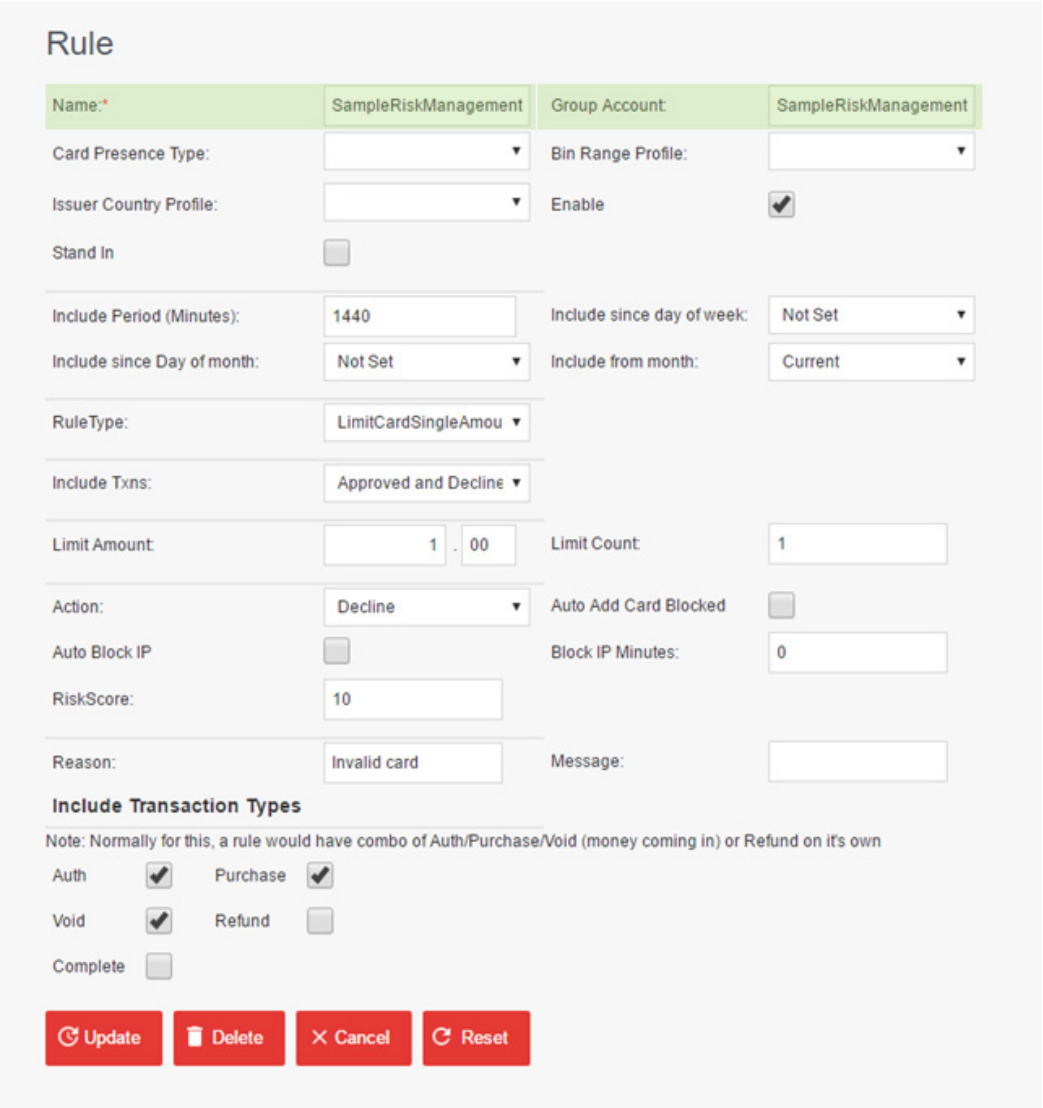


An example rule can be found in section 6.5

Each rule can be broken down into three key parts:

6.1 Identifying Your Rules

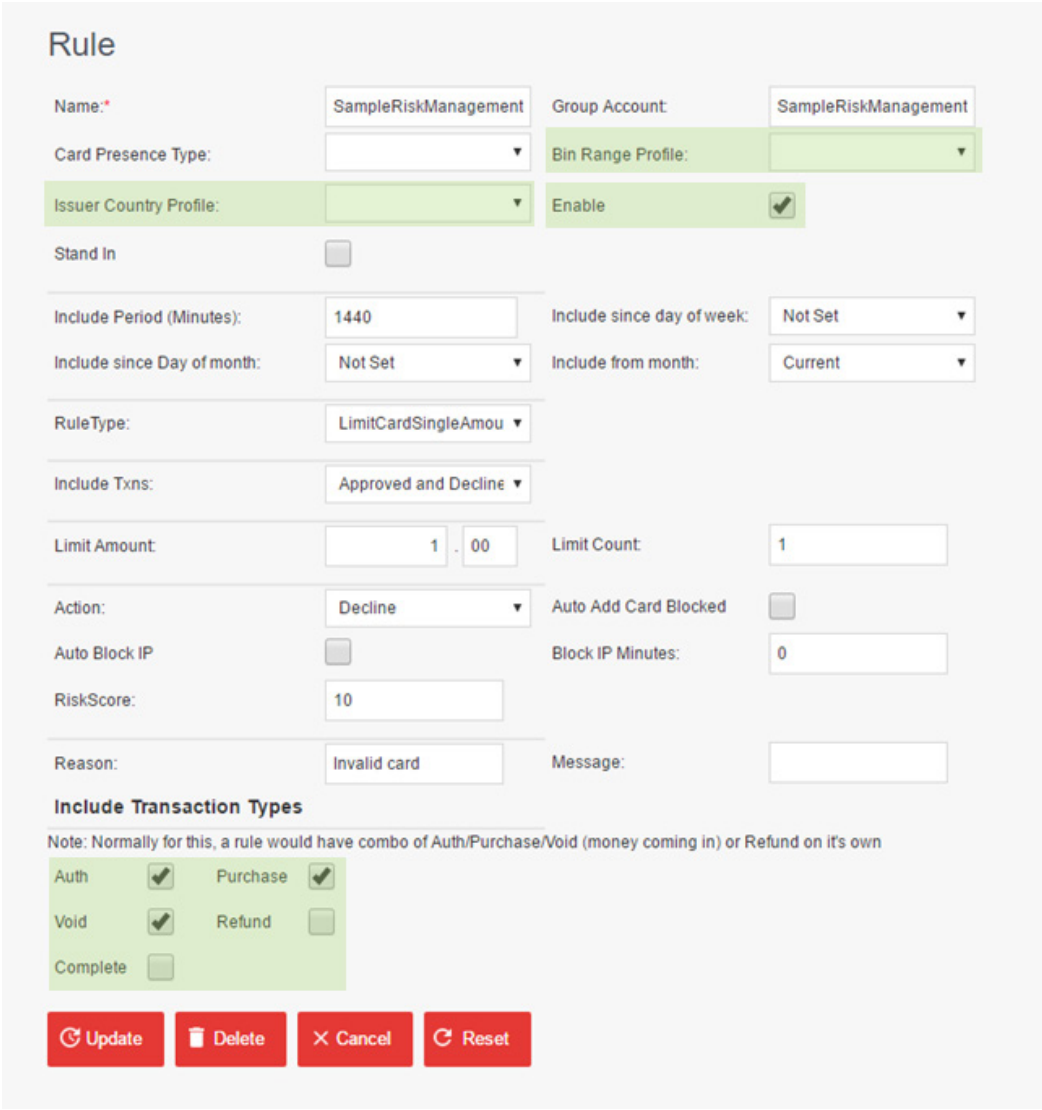
Every rule is uniquely identified using a name and is associated with a Group Account. This allows the merchant to quickly look up rules based on either of these fields.



6.2 When Does Your Rule Get Looked At?

Any rule will require conditions upon which it will be looked at by risk management.

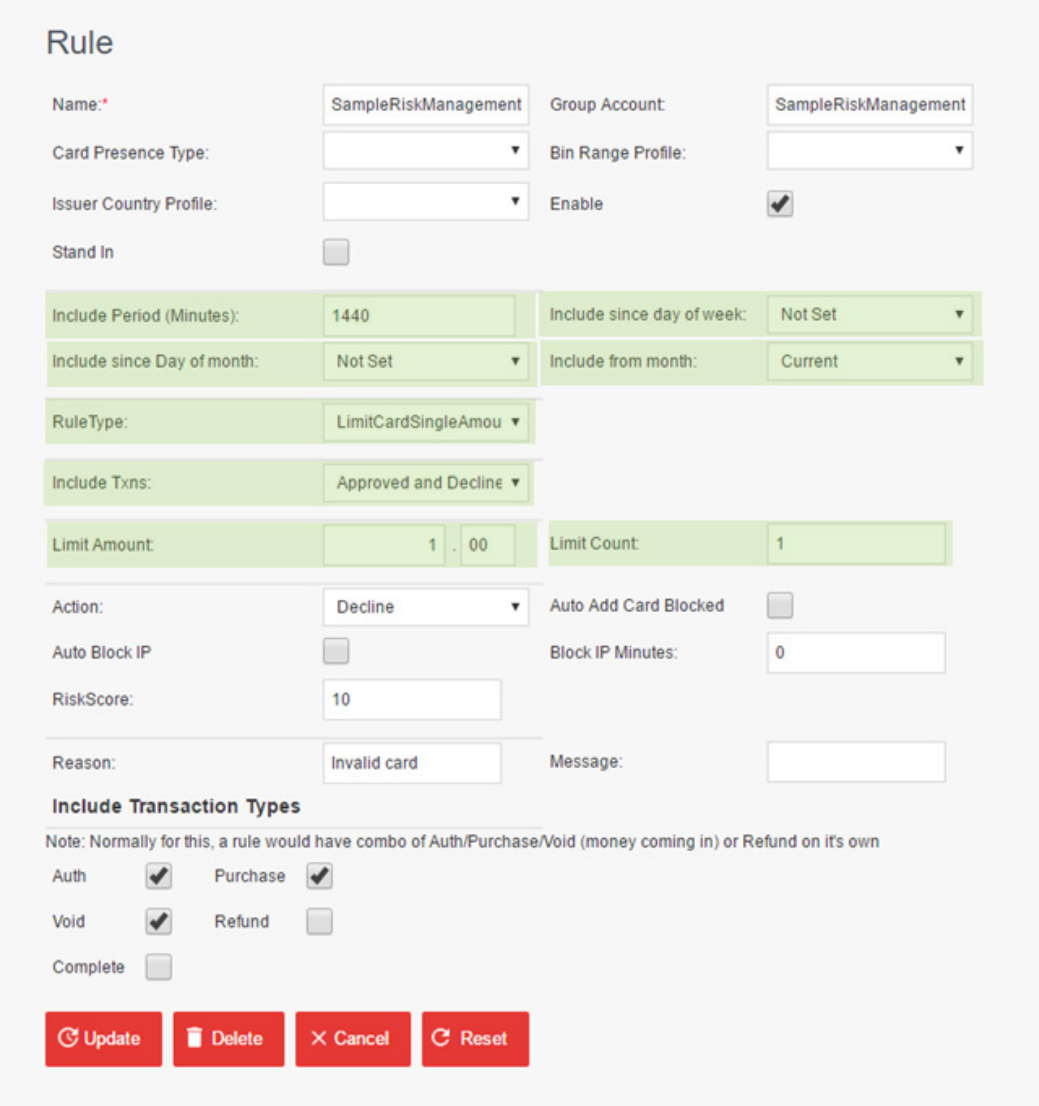
The example below explores the various parameters which can be associated with the "SampleRiskManagement" rule.



Field	Description
BIN Range Profile	Applies a BIN range profile, for the rule to break the card used must be within this profile.
Issuer Country Profile	Applies a Country Profile, the rule will only break if the card is issued from one of the selected countries.
Enable	Allows the rule to be turned on/off.
Include Transaction Types	Controls which transaction types will trigger the rule.

6.3 When Does Your Rule Get Triggered?

If Risk Management looks at a rule, it will trigger based on how the following fields are set.



Field	Description
Include Period (Minutes)	These values are used to set the period for rules limiting transactions over a certain time frame.
Include Since Day Of Week	
Include Since Day Of Month	
Include From Month	
Rule Type	Looks at both the medium used to make a transaction and information about the transaction and/or transaction history. Please see section 5.3.1 for a full set of examples on each rule.
Include Txns	Will apply the rule to Approved and/or Declined transactions only.
Limit Amount	Sets the financial limit on transactions which are restricted by a monetary value.
Limit Count	Sets the numeric limit on transactions which are restricted by a count.

6.3.1 Risk Rules

If Risk Management looks at a rule, it will trigger based on how the following fields are set.

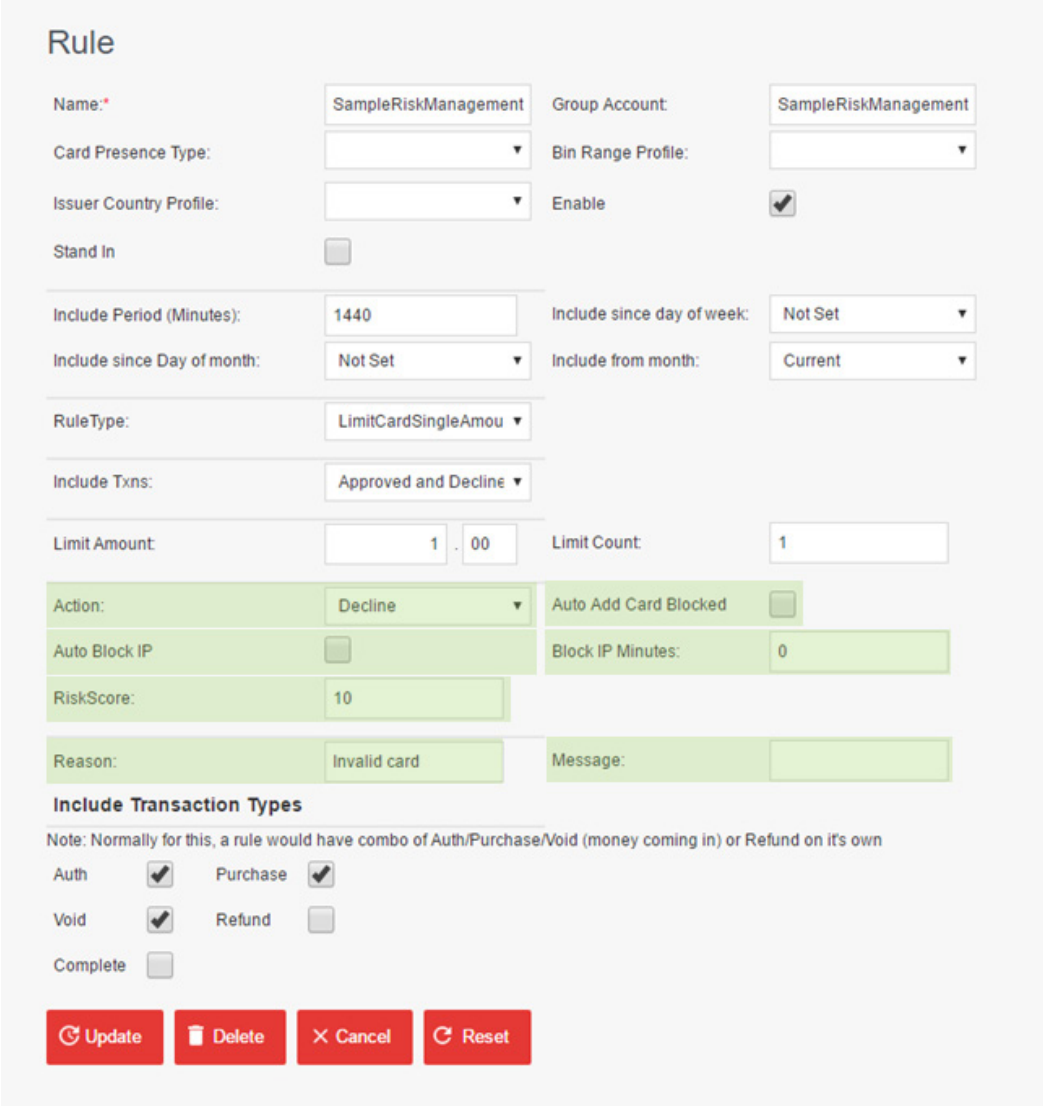
Rule Prefix	Description
LimitAccount	The Account parameter pertains to the optional <AccountInfo> XML tag sent in a transaction.
LimitCard	Refers to the Card Number being transacted against.
LimitPhoneNumber	The Phone Number parameter pertains to the optional <PhoneNumber> XML tag sent in a transaction.
LimitIpAddress	Refers to the originating IP Address the transaction was made from.

Rule Suffix	Description	Example
SingleAmount	Will not allow any transaction with an amount exceeding "Limit Amount"	If Limit Amount is set to $100, the transaction will always fail for payments exceeding $100.
TotalAmount	Will not allow transaction/s to be made where the cumulative total exceeds "Limit Amount"	If Limit Amount is set to $100, it is possible to only send a cumulative total of $100 in transactions. Any combination from 10,000 payments of $0.01 through to 1 payment of $100 would be allowed, but if the total value exceeds $100, the latest transaction will decline.
Txns	Will allow only a certain number of transactions and is limited by "Limit Count"	If Limit Count is set to 10, only 10 transactions can be performed. This is independent of financial value.
CountOverAmount	Will only allow a certain number of transactions over a certain amount. Controlled by both "Limit Count" and "Limit Amount"	If Limit Amount is set to $100 and Limit Count is set to 5, it would be possible to send an unlimited number of transactions not exceeding $99.99 and only up to 4 transactions exceeding $100.

Non-Financial Rules	Description
LimitAccountsPerCard	Limits the number of unique <AccountInfo> XML tags that can be associated with a given card.
LimitPhoneNumbersPerCard	Limits the number of unique <PhoneNumber> XML tags that can be associated with a given card.
LimitCardCountForAccount	Limits the number of cards that can be associated with any unique <AccountInfo> XML tag.
LimitCardCountForIpAddress	Limits the number of cards that can be associated with any unique IP address.
LimitCardCountForPhoneNumber	Limits the number of cards that can be associated with any unique <PhoneNumber> XML tag.

6.4 What Does Your Rule Do?

When a rule breaks, there will be some action taken. The example below looks at the possible consequences of the rule break.



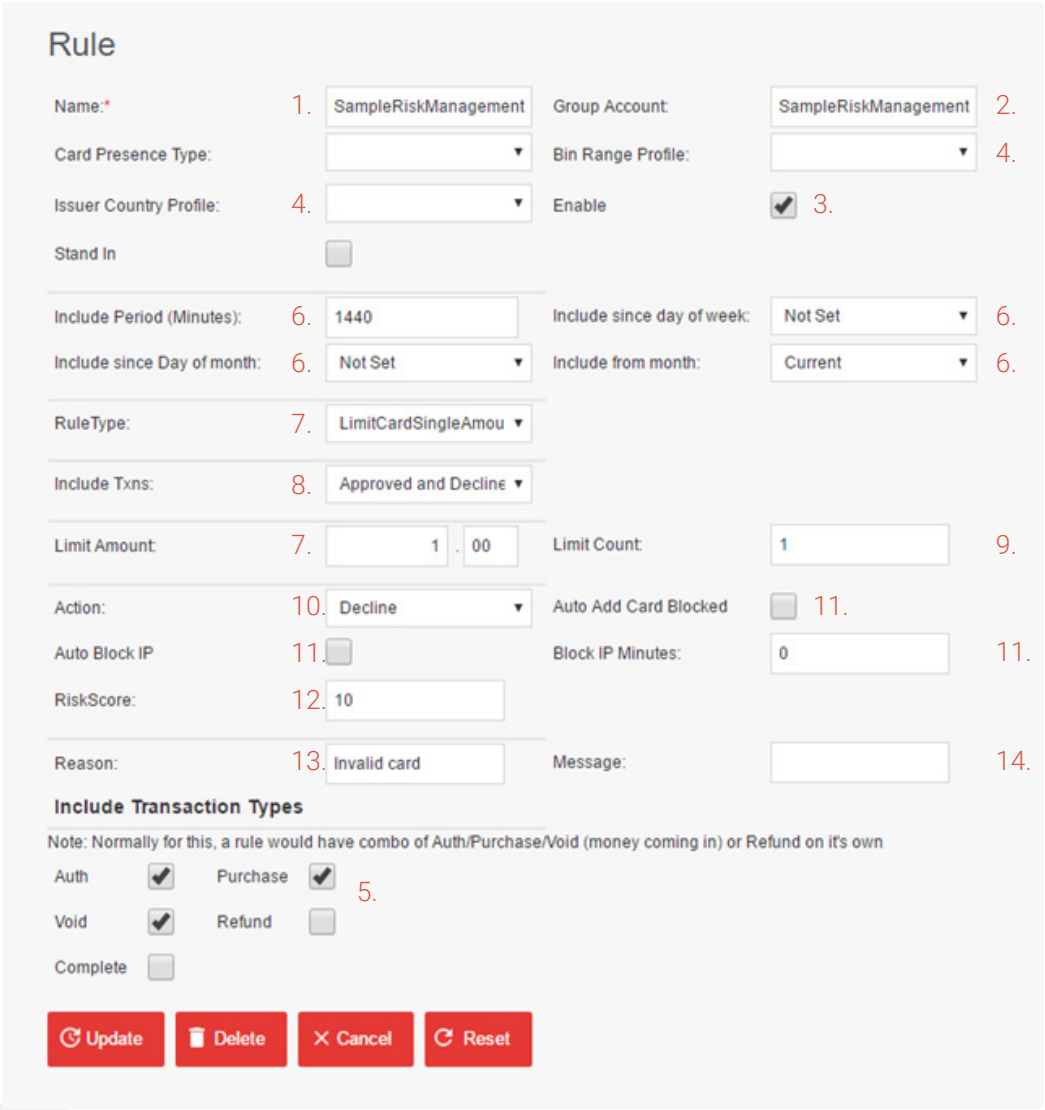
Non-Financial Rules	Description
Action	Determines whether the transaction will decline or be flagged. If Action is set to Decline, the transaction will return the LR ReCo and will fail prior to validation by the bank. A Declined transaction will also be flagged and provide the merchant with a notification of the failure. Flagged transactions will be invisible to the card holder, the notification will be sent solely to the merchant and there will be no indication of a rule break to the customer.
Auto Add Card Blocked	Allows for the card to be automatically added to the merchant's card block list.
Auto Block IP	Allows for the IP to be automatically added to the merchant's IP Address block list.
Block IP Minutes	Works with Auto Block IP to determine how long the IP should be blocked for.
Risk Score	Used in assessing the riskiness of any given transaction.
Reason	Returns the reason for failure, new reasons can be created in the Risk Management Reasons screen. This is only seen by the merchant. Should contain more in-depth information of the issue.
Message	Returns a failure message, new messages can be created in the Rule Messages screen. This is returned to the customer. Should contain a brief description appropriate to the customer.

6.5 Example RM Rule

The example rule below is called SampleRiskManagement (1) and it has been applied to the SampleRiskManagement Group Account (2).

The Rule is currently enabled (3) and does not have a BIN range profile, nor an issuer country profile applied to it (4).

Only Purchase, Auth, and Void transactions are assessed by this rule (5).



The rule will look at transactions occuring in the last 24 hours (1440 minutes), however will not be applied specifically to transactions from a given day of the week or month (6).

The RuleType is LimitCardSingleAmount and has a maximum value of $1.00, this means that for any transaction over a $1.00 the rule is triggered (7).

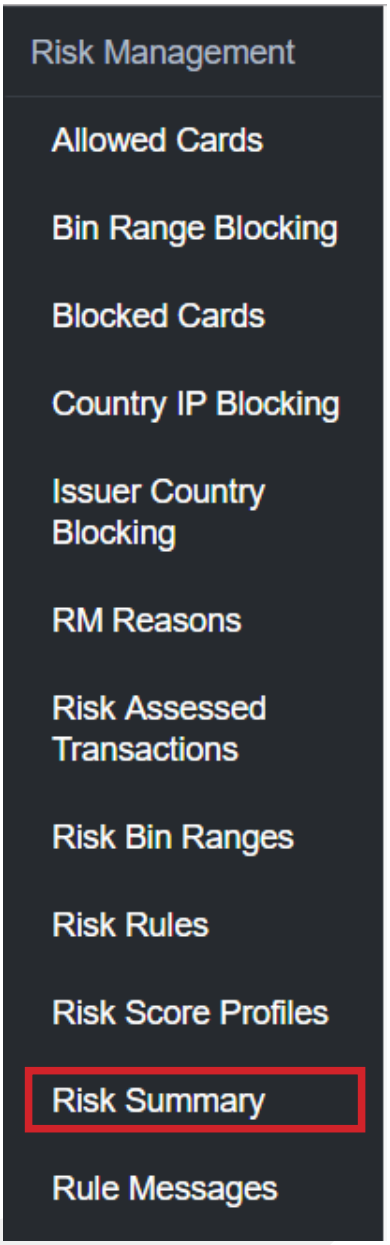
IncludeTxns (8) looks at both Approved and Declined transaction types after confirmation from the bank; in this case the rule is redundant as only one off transactions are reviewed. This is used when using Rules which look at the total number of transactions from a card, phone number, account, or IP address. Similarly, LimitCount (9) acts as a limit for rules which limit the number of transactions.

When the rule is triggered, the transaction will be declined (10). The card will not be automatically black listed, nor will the IP address be temporarily blocked for a configurable time period (11).

The rule has a risk score of 10 (12), see section 7 for more info on risk scores.

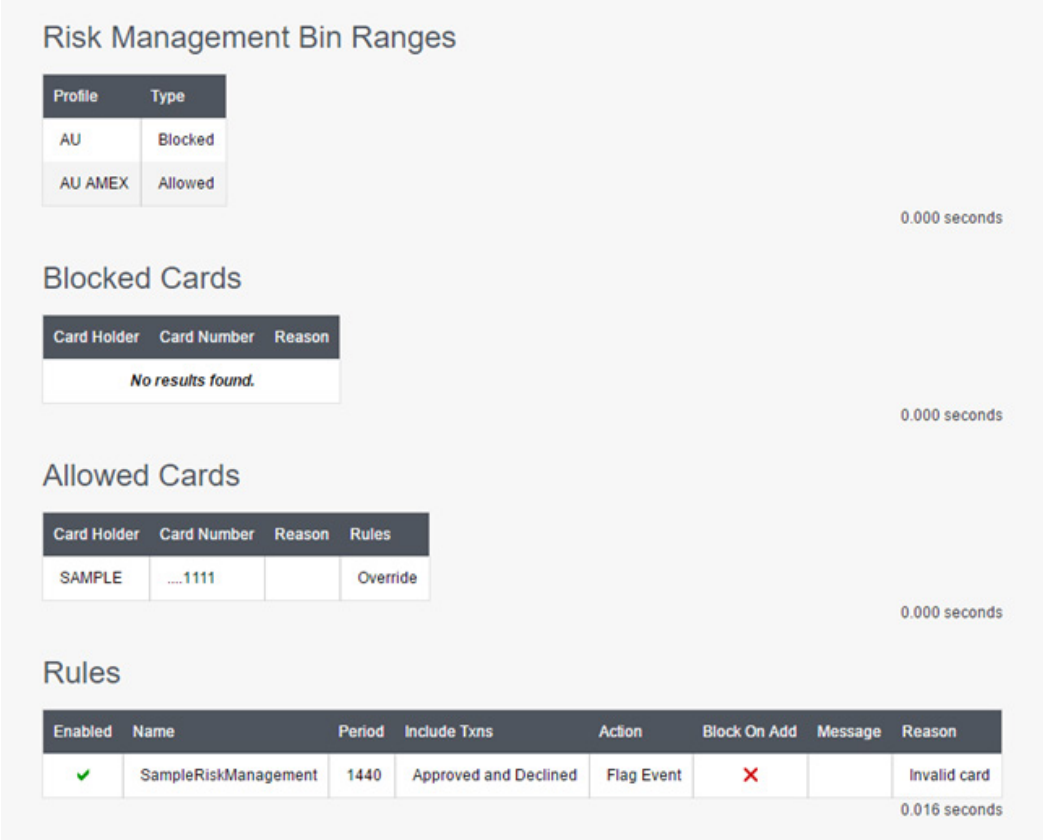
“Invalid Card” is returned in the response (13) and no additional message text is returned (14).

7. Risk Summary

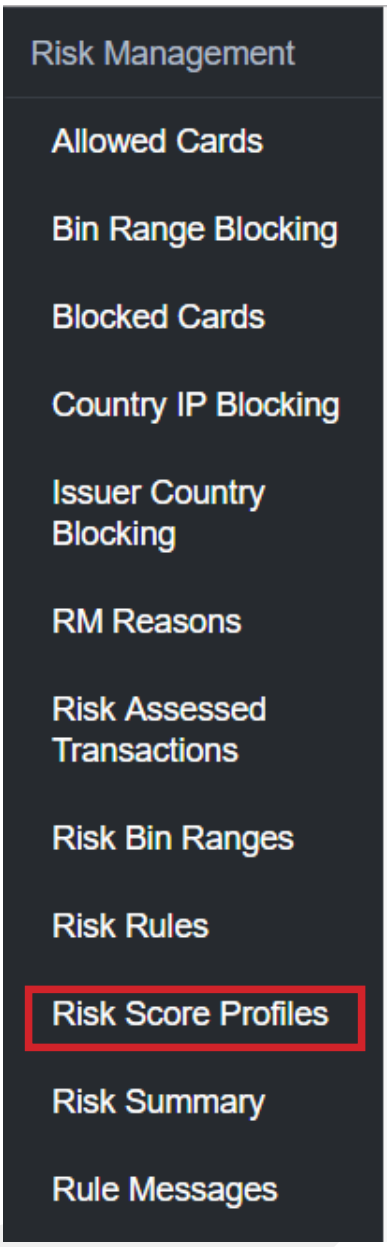


The Payment Express Risk Management tool contains an easy access summary screen which allows merchants to quickly review and access their Risk Management rules.

Access to the Risk Summary tool is achieved via Payline and navigating to Risk Summary under Risk Management.



8. Risk Scoring



Risk Scoring provides merchants with a finer level of control over which transactions will and will not be processed. If one rule is broken, the transaction may still be safe. If two rules are broken, the tranaction may appear suspicious. If three rules are broken, there is reason to block a card*.

Risk Scoring allows merchants to set a Risk Score profile which has a specifiable limit on what overall risk score is acceptable. If a rule is broken, the risk associated with the transaction increases. If the transaction breaks enough rules it will either decline or be flagged.

It is possible to view and amend risk-scoring profiles by navigating to Risk Score Profiles under Risk Management in Payline.

*These numbers might not apply to your Risk Management set up and are simply an indication of how Risk Scoring is used.

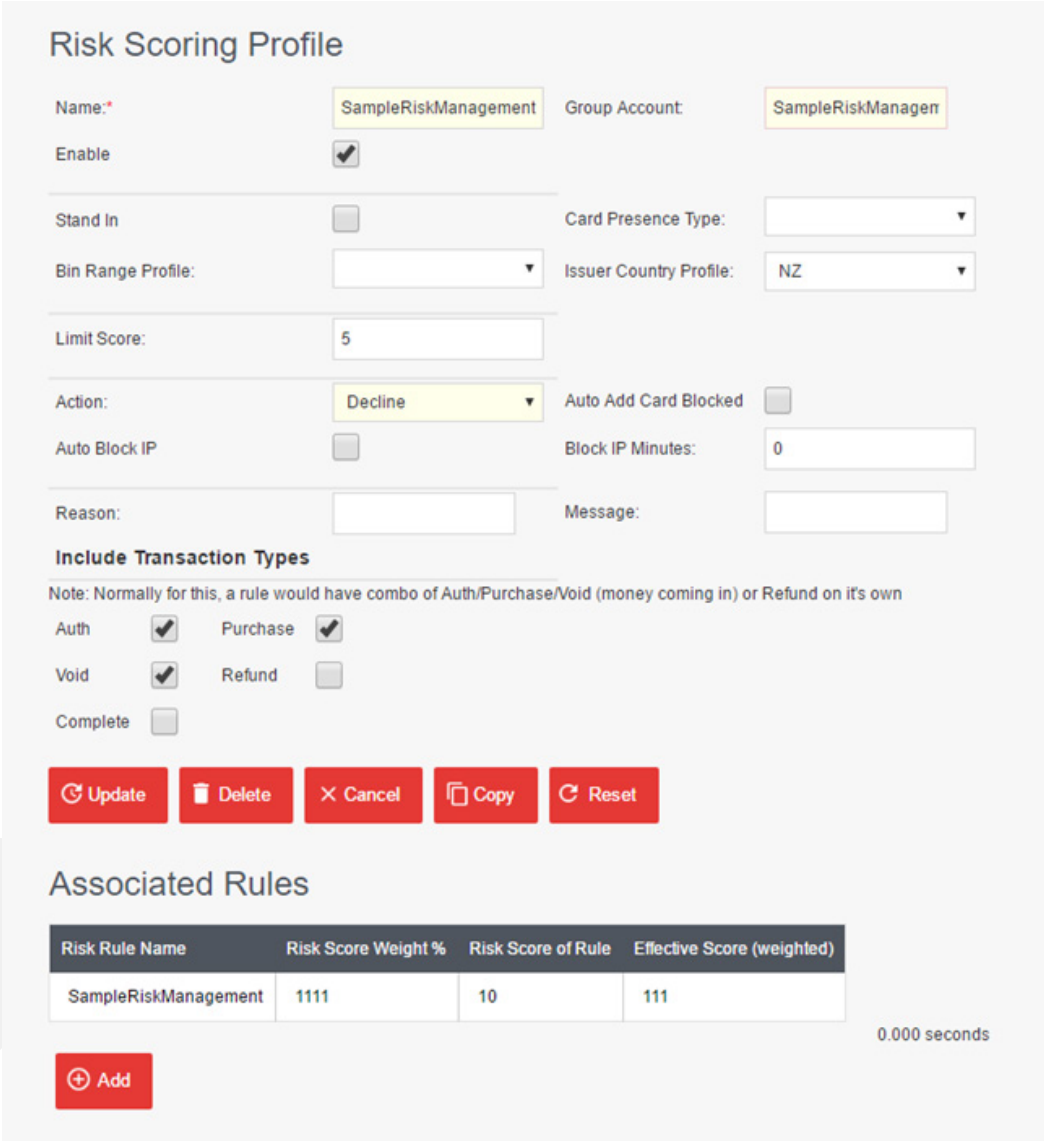
8.1 Risk Scoring Profiles

Each Risk Scoring Profile is associated with a name and the applicable group account, this information is used to identify individual profiles.

The Enable radio button allows the scoring profile to be turned off or on.

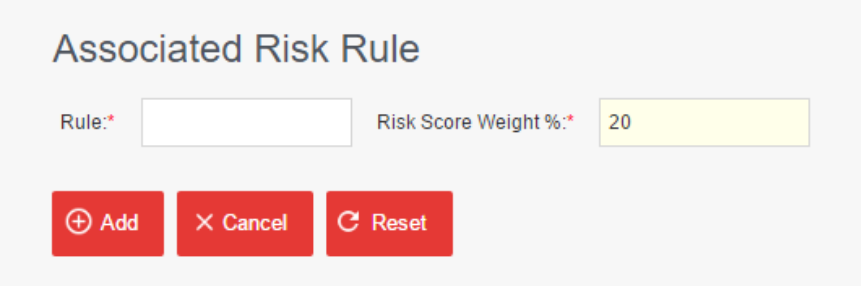
Each profile has a score limit, which can be set by the merchant. When a transaction is attempted, the score is calculated; if the score exceeds this limit, the transaction will either be flagged or declined.

Any number of rules can be associated with a given Risk Scoring Profile.



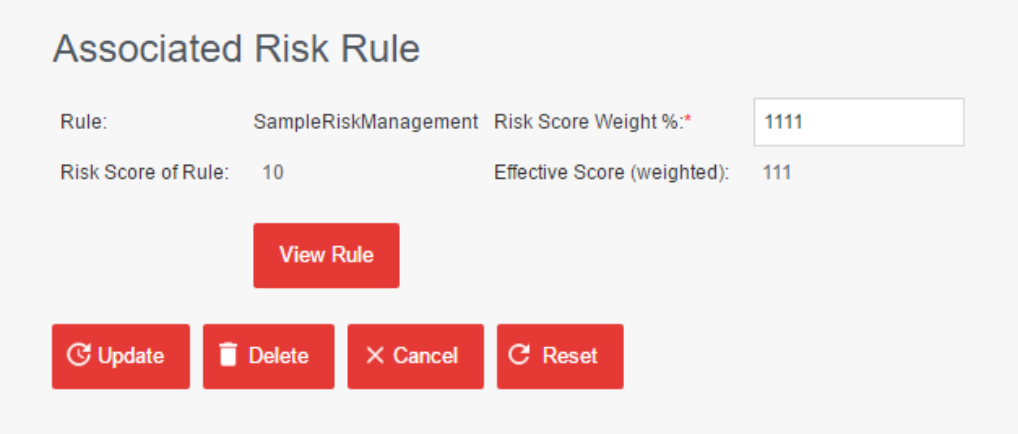
8.2 Associate a New Risk Scoring Rule

A new rule can be associated with the risk scoring profile and assigned a percentage weight. As the risk score is associated with the rule in the Rules screen (see section 5.4) the weighting allows for this score to be modified and used in more than one Risk Score Profile. This means you can keep the same Risk Score associated with the rule, but modify the weighting depending on the requirements of each profile.



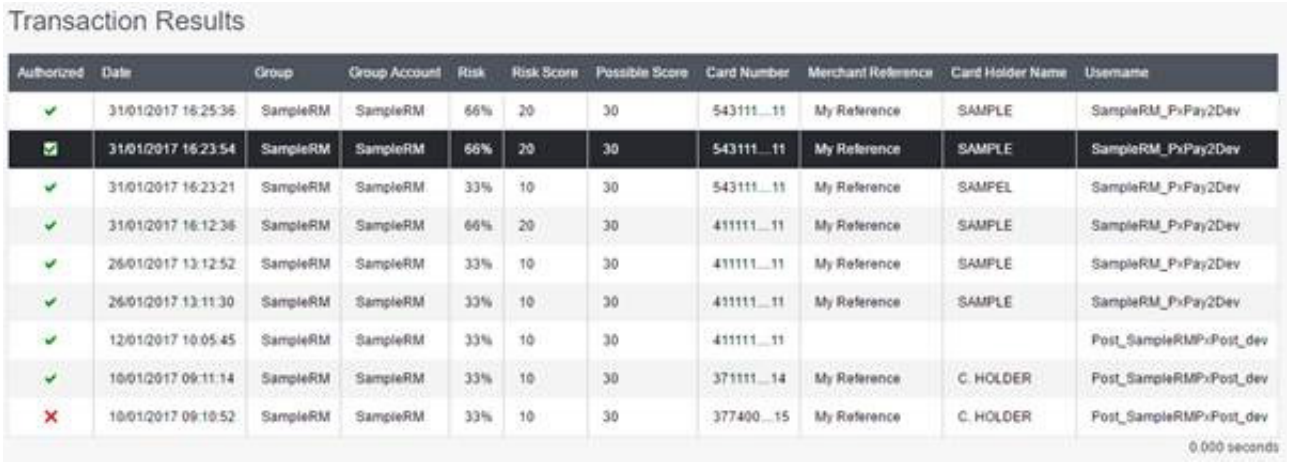
8.3 Update an Existing Risk Scoring Rule

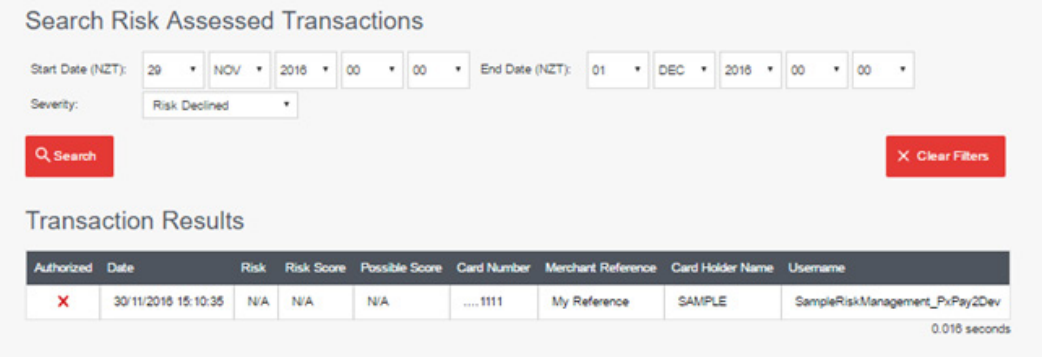
For existing risk rules, it is possible to update the percentage weight and view the associated rule.



9. Risk Assessed Transactions

For an overview of all transactions and their associated Risk Scores, navigate to Risk Assessed Transactions in Payline. The Risk Assessed Transactions tool shows all transactions and their associated level of risk. To aid with searching through individual transactions, the Group, Group Account, date range, and level of severity can be specified.
The Risk Score profile allocates a percentage of Risk to any given transaction as a ratio of Risk Score/Possible Score:





There are five levels of severity:

- No Risk 0%
- Low Risk 1% - 24%
- Medium Risk 25% - 74%
- High Risk 75% - 99%
- Risk Declined 100%

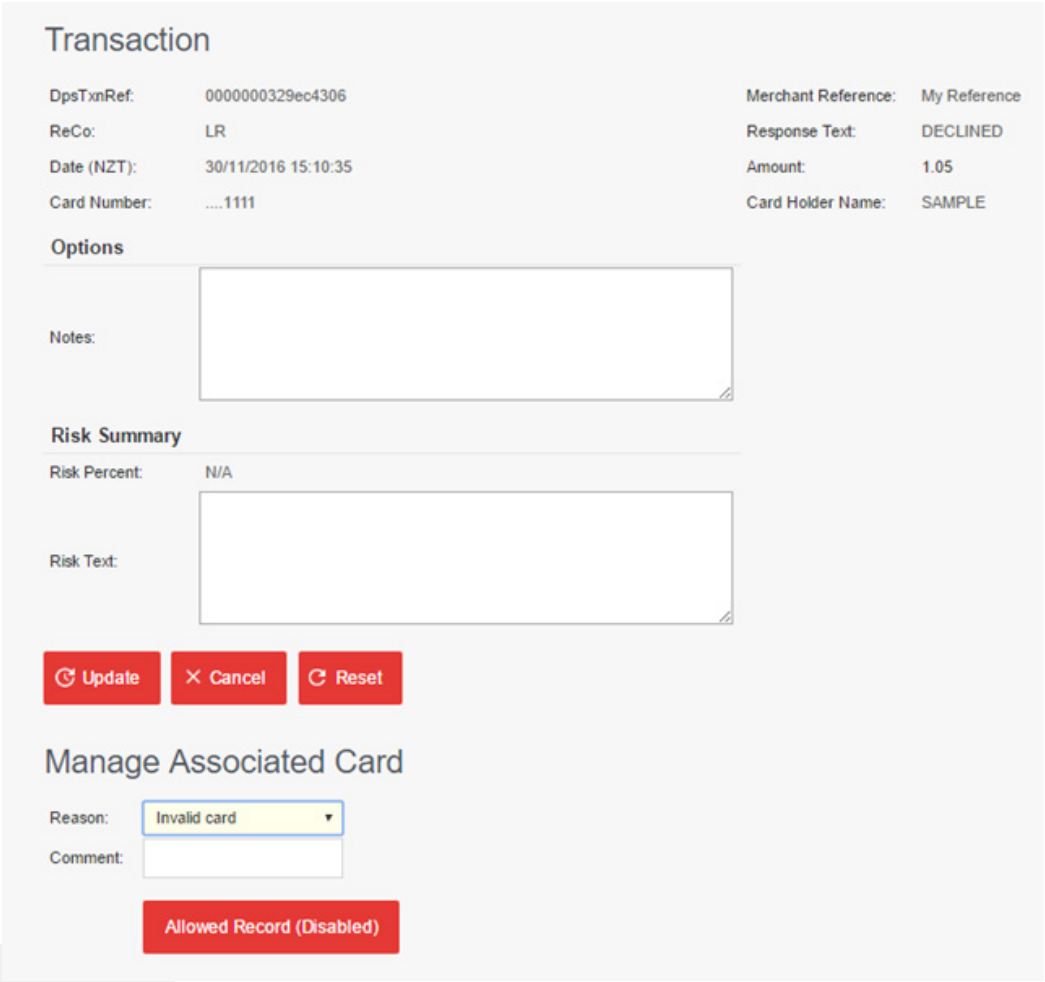
In the example above, each transaction is Medium Risk as the associated percentage is within the range 25% to 74%. Transactions will be declined automatically if they have an associated Risk of 100%.

For an in-depth view of individual transactions, click on any transaction from the Result list, this will display additional information specific to the chosen transaction.

It is possible to update the severity of the transaction as well as add any relevant notes. These features can be used to explain or differentiate an outlying transaction.

The Risk Summary shows the risk percentage as well as which rules were triggered when the transaction was made.

It is possible to add the card used on these transactions to the Allowed List or Blocked List.



10. Risk Notification

Payment Express Risk Management provides merchants with the option of receiving notifications when rules are triggered. When rules are broken the payment is either flagged or declined and a notification can be sent out either as an email and/or as an SMS message.

Notifications provide merchants with the opportunity to learn about their card holders and how transactions are made. Receiving notifications when a rule is triggered allows for merchants to stay abreast of their payments and how customers pay for goods and services.

The example below is for a transaction which has been flagged. Information about the transaction as well as the rule which has been triggered is displayed.

Dear Customer,

This payment was APPROVED, however one or more risk rules were triggered which might indicate fraudulent activity. Please review the details below.

Transaction Information

DpsTxnRef	000000032a022aea
Result	APPROVED
Amount	1.05NZD
Time	2016-12-02 15:51:42 NZT
Card Number	1111
Card Holder Name	SAMPLE
Merchant Reference	My Reference
TxnData1	Data 1
TxnData2	Data 2
TxnData3	Data 3
IP Address	192.168.102.113

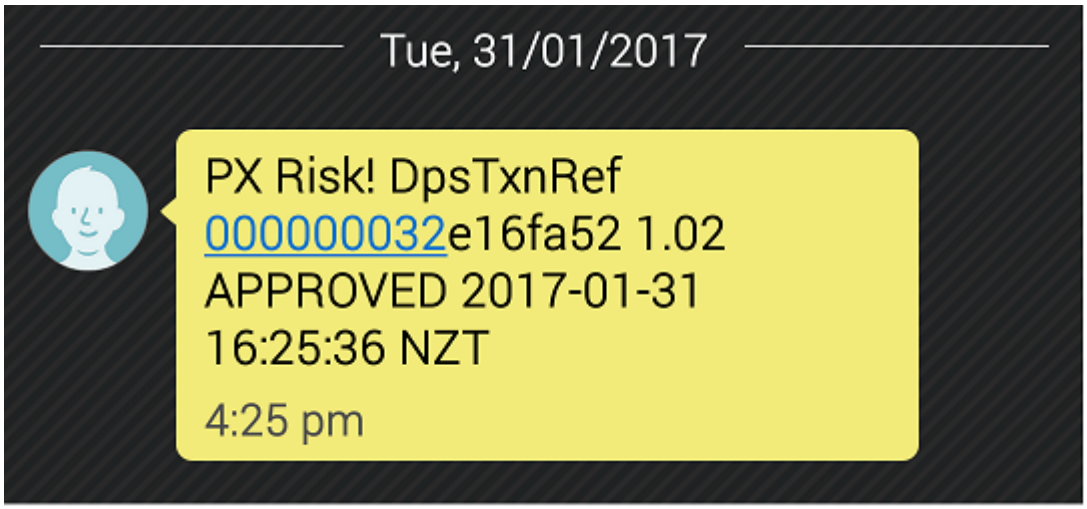
Triggered Rules

Rule Type	Detail
LimitCardSingleAmount	Transaction amount of 1.05 exceeds rule limit of 1.00

paymentexpress® Visit us online at www.paymentexpress.com

Thank you for using Payment Express!

In the example below, an SMS alert has been sent to the users phone notifying them of a flagged transacion. The SMS messages are more concise than email notifications and contain only the DpsTxnRef, the financial value of the transaction, the outcome, and a date/time string.



Please contact **Support** at **Payment Express** if you have any integration queries.

NZ: 0800 PAYMENT (729 6368)
AU: 1 800 006 254
UK: 0800 088 6040
US: 1 877 434 0003
Rest of the world: +64 9 309 4693

support@paymentexpress.com I www.paymentexpress.com

paymentexpress®
www.paymentexpress.com