

Merchant Administration

Version 4.6.0

For TNSPay 4.6

Disclaimer

Copyright © 2011 TNS Payment Technologies Pty Ltd ("TNS"). All rights reserved.

This document is provided by TNS on the basis that you will treat it as confidential. No part of this document may be reproduced or copied in any form by any means without the written permission of TNS. Unless otherwise expressly agreed in writing, the information contained in this document is subject to change without notice and TNS assumes no responsibility for any alteration to, or any error or other deficiency, in this document.

All intellectual property rights in the Document and in all extracts and things derived from any part of the Document are owned by TNS and will be assigned to TNS on their creation. You will protect all the intellectual property rights relating to the Document in a manner that is equal to the protection you provide your own intellectual property. You will notify TNS immediately, and in writing where you become aware of a breach of TNS' intellectual property rights in relation to the Document.

The names "TNS", any product names of TNS including "Dialect" and "QSI Payments" and all similar words are trademarks of TNS and you must not use that name or any similar name.

TNS may at its sole discretion terminate the rights granted in this document with immediate effect by notifying you in writing and you will thereupon return (or destroy and certify that destruction to TNS) all copies and extracts of the Document in your possession or control.

TNS does not warrant the accuracy or completeness of the Document or its content or its usefulness to you or your merchant cardholders. To the extent permitted by law, all conditions and warranties implied by law (whether as to fitness for any particular purpose or otherwise) are excluded. Where the exclusion is not effective, TNS limits its liability to \$100 or the resupply of the Document (at TNS' option). Data used in examples and sample data files are intended to be fictional and any resemblance to real persons or companies is entirely coincidental.

TNS does not indemnify you or any third party in relation to the content or any use of the content as contemplated in these terms and conditions.

Mention of any product not owned by TNS does not constitute an endorsement of that product.

This document is governed by the laws of New South Wales, Australia and is intended to be legally binding.

Contents

Preface	5
Welcome to TNS	5
Who Should Read This Guide.....	5
Where to Get Help.....	5
Introduction	7
Requirements	7
Types of Merchant Profiles	7
About the Payment Server	7
Managing Your Transactions with Payment Server.....	8
Types of Orders	8
Getting Started	9
Logging in to Merchant Administration	10
The Home Page.....	13
Working with Orders	15
Creating an Order.....	16
The Create Order Entry Page	17
The Create Order Response Page	20
Creating a Capture Only Entry Order	23
Searching for Orders.....	23
Order Search Page	24
Viewing Orders - The Order List Page.....	26
Viewing an Individual Order - The Order Details Page.....	27
Address Verification Details	28
Card Details	28
Payment Plan Details.....	29
Action	29
History	29
Risk Assessment Details	31
Performing Actions on Orders.....	40
Capturing an Order Amount.....	40
Completing an Order.....	41
Refunding a Transaction.....	41
Voiding a Transaction	42
Settling Orders	43
Dealing with Unsettled Transactions.....	43
Unsettled Transactions Summary Page	44
Transactions by Currency	44
Batch Closure Receipt Page.....	45
Searching for Settlements.....	45
Settlement Search Page	46
Settlement List - Settled Batches.....	46
Settlement Details Page	47
Financial Transactions	49
Searching for Financial Transactions.....	49
Financial Transactions Search Page	50
Viewing the Financial Transactions List.....	51
Viewing an Individual Financial Transaction.....	52
Downloading the Transactions File	56

Downloading Transaction Files.....	56
Payment Authentications	57
Payment Authentication Information Flow	58
Payment Authentications Status.....	59
Searching for Payment Authentications	59
Payment Authentications Search Page	60
Viewing the Payment Authentications List	61
Viewing an Individual Payment Authentication	62
Downloading Payment Authentication Information	65
Downloading Transaction Files.....	65
Reports	67
Gateway Reports.....	67
Gateway Report Search Page	67
Viewing a Gateway Report	68
Admin	69
Configuring Your Settings	69
Configuration Details.....	69
Editing Your Configuration Settings.....	71
Managing Merchant Administration Operators	72
Types of Operators	73
Creating a New Merchant Administration Operator	73
Editing Operators	77
Unlocking an Operator Account.....	78
Managing Passwords.....	79
Changing an Operator's Password	79
Changing Your Own Operator Password	80
Manage Banamex Payment Plans.....	80
Adding a Payment Plan	81
Using Payment Plans.....	82
Acquirer Link Selection	82
Downloading Software and Documentation.....	83
Managing Risk	85
Introduction to Internal Risk	86
Risk Management Architecture.....	87
Basic Concepts	90
Accessing Internal Risk.....	92
Viewing Risk Management Summary.....	92
Risk Assessments for Review.....	93
Failed Risk Reversals	93
Working with Rules.....	94
Trusted Cards	95
Suspect Cards.....	98
Configuring IP Address Range Rules	101
Configuring IP Country Rules	106
Configuring Card BIN Rules.....	110
Configuring 3-D Secure Rules	113
Configuring AVS Rules	118
Configuring CSC Rules.....	122
Searching for Orders Based on Risk Recommendation	124
Index	125

CHAPTER 1

Preface

Welcome to TNS

TNS Payment Technologies Pty Ltd. ("TNS") is a global provider of payment solutions, connecting merchants and retailers to the world's leading banks, acquirers, and processors, to enable secure, efficient and cost-effective delivery and processing of payments. TNS' payments division provides a wide array of pre-packaged, end-to-end managed solutions designed specifically for the payments industry, enabling customers to focus on their core businesses.

TNS' Payment Gateway, TNSPay Gateway, is a managed gateway service offering, enabling merchants to authorize and settle card transactions securely, reliably and economically, while ensuring full card data security. TNSPay Gateway is designed to meet the demanding needs of MOTO (mail order/telephone order) merchants and web/eCommerce retailers. Today, TNSPay Gateway represents the platform of choice for over 30,000 merchants, two global card associations, and over 70 banks worldwide. In addition, the solution utilizes our resilient, state-of-the-art global network that transports billions of transactions each year.

For more information on how TNS can help you with your payment processing needs, visit our website at <http://www.tnsi.com> <http://www.tnsi.com>

Who Should Read This Guide

This guide is specifically aimed at merchants and operations personnel using Merchant Administration, and assumes knowledge of the following:

- Web applications
- Commercial practices
- The card processor's merchant operational procedures
- Transaction systems operations.

Where to Get Help

If you need assistance with the Merchant Administration, please contact TNS.

CHAPTER 2

Introduction

Merchant Administration allows you to monitor and manage your electronic orders through a series of easy to use screens.

Requirements

To use Merchant Administration, you need:

- Access to the Internet through Internet Explorer versions 6 or 7
- Your Merchant ID
- Your Operator ID and the corresponding password

Types of Merchant Profiles

Two types of merchant profiles are created for you by Transaction Network Services' registration process:

Test merchant profile – Use this to perform test transactions against an emulator of the transaction processing system. The test merchant profile always has TEST prefixed to the production Merchant ID. Using the test profile is an ideal way to become familiar with Merchant Administration as it allows you to create orders, test transactions and use other areas of the system without affecting your production system.

Production merchant profile – Use this to perform transactions directly against the live transaction processing system when you are satisfied with your test transactions. Be aware that funds will be transferred from the cardholders' accounts.

About the Payment Server

The Payment Server processes merchant transaction requests in real time.

The Payment Client sends the transaction requests to the Payment Server. Transaction requests provide the cardholder's information to the Payment Server enabling it to process the transaction. After the transaction has been processed, the Payment Server sends a transaction response to the Payment Client, indicating whether the transaction was successful.

Managing Your Transactions with Payment Server

You can use one of two methods to manage your transactions:

- **Merchant Administration** – uses a browser interface to interactively perform various types of transactions, and to perform set up activities. These functions are described in this guide.
- **Advanced Merchant Administration** – allows you to use the Payment Client to directly access the Payment Server to perform all transaction-related actions integrated with a merchant's own payment software interfaces. Information on how to integrate Advanced Merchant Administration with your software application is provided in the Payment Client Integration Guide.

Note: For the purposes of this guide, a *financial transaction*, or sometimes just *transaction*, will refer to an individually executed action, such as a capture, performed against an order. This should not be confused with the term *shopping transaction*, which is sometimes used to describe the *order* itself.

Types of Orders

You can choose to create only an "Auth and Capture" order on this system.

Auth and Capture

Requires two transactions to debit the funds from a cardholder's account. First, an authorization(Auth) transaction is used to reserve the funds on the cardholder's card, followed separately by a capture transaction to actually debit the funds from the cardholder's card when the goods or services have been shipped.

The full amount of the goods or service is used to verify that the funds are available in the cardholder's card account. The funds are reserved until captured by you and transferred to your account.

The Auth transaction reserves the funds for a predetermined period of time as determined by the acquirer. If the cardholder performs another transaction, the current authorization transaction is taken into account and reduces the cardholder's available funds as though the transaction had taken place.

Purchase

The Purchase transaction effectively combines an Authorize and a Capture into one transaction. A single transaction is used to authorize the payment and initiate the debiting of funds from a cardholder's credit card account. Usually the order is completed and the goods are shipped immediately.

Auto-Capture

Auto-capture is a variant of Purchase transaction, which enables a Purchase mode merchant to use an acquirer that only supports Auth/Capture transaction mode. The Purchase transaction submitted by the merchant is transformed into an Authorization followed by an auto-triggered Capture.

The Transaction ID for both Authorize and Capture request will be the Transaction ID supplied by the merchant in the original Purchase transaction.

Note: Auto-Capture may also be performed on a referred Authorization transaction, by providing the manual authorization code.

Getting Started

Merchant Administration allows you, as an authorized Operator, to monitor and manage your electronic orders. Authorized Operators can log in from the Login screen and use the various features of Merchant Administration.

Authorized merchant personnel must be set up as Operators before they can log in. For more information see Managing Operators.

Logging in to Merchant Administration

To log in, from the **Merchant Administration Login** on page 10 page:

- 1 Enter your Merchant ID.
- 2 Enter your *Operator ID*.
- 3 Enter your *Password*. If you have forgotten your password, click the **Forgot Password** on page 11 link.
- 4 Click the **[LOG IN]** button. The Merchant Administrator Main Menu page displays.

Note: To log in to Merchant Administration for the first time after your merchant profile has been created and approved, you must use the default account username "Administrator".

The Merchant Administration Main menu allows you to choose various options relating to transactions, and Merchant Administration Operator records. These options are described in detail in the sections that follow.

Note: The options that are displayed on the Merchant Administration Main menu depend on your user privileges. For more information on user privileges, see Merchant Administration Operator Details page

Your merchant profile is set up to allow you to first process transactions in Test mode. When you are satisfied that testing is complete, you can request Transaction Network Services' to have Production mode enabled so that you can process transactions in real time.

Login Field Definitions

The Merchant Administration Login screen requires the following information.

Login Field Definitions

Field	Description
Merchant ID	The merchant's unique alphanumeric identifier. There is a unique Merchant ID for each merchant account/profile.
Operator ID	The operator ID.
Password	The password must be at least eight characters long and contain at least one alphabetical character and numeric character. The password is case sensitive.

Note: Your password should have been provided to you by your Merchant Services Organization (MSO). If you forget your password, you can have it reset using the Forgot Password Link on the Login screen. See **Resetting a Forgotten Password** on page 11.

Changing Your Password at Login

During the log in process you may be prompted to change your password. This could be because you are logging in for the first time as the "Administrator" or your password has expired.

Note: You cannot use the Administrator Operator ID to process transactions. If you wish to process transactions, you must log in with an Operator ID. See Creating a New Operator.

Resetting a Forgotten Password

Note: The Forgot Password link is displayed only if Password Reset functionality is supported by your MSO.

The Forgot Password link takes you to a page where you can request a temporary password for logging in to Merchant Administration. If you have made five or more unsuccessful log-in attempts using an incorrect password, your password must be reset. You have two options to reset your password:

- Use the Forgot Password link. You must have the operator privilege "Change Their Own Password" enabled.
- Contact the Administrator for a password reset, if one more more of the following is true:
 - you do not have an email address recorded against your operator profile.
 - you have the "Enable Advanced Merchant Administration Features" privilege enabled.
 - you have the "Perform Operator Administration" privilege enabled.
 - you are the primary operator (Administrator) for the merchant profile.
 - your account is locked because the "Lock Operator Account" privilege is enabled on your profile by an operator with administration privileges. If you have successfully authenticated then you will notified to contact the Administrator to unlock your account.

Note: For information on how an Administrator can change an Operator's password, see *Changing an Operator's Password*. on page 79

How to request a temporary password

- 1 Enter your Merchant ID and Operator ID and click **[Request Password]** button.
- 2 The Password Reset Requested page appears notifying you that an email with a temporary password has been sent. Click **[Continue]** to accept the notification and return to the Login page.

You will receive an email containing the temporary password on your registered email address. When you log in using the temporary password you will be prompted to change the password. Once you change the password, you will be logged out of Merchant Administration and must log in again using the new password.

Selecting Merchant Administration Menu Options

The following menu administration options are available in Merchant Administration.

Menu Option	Description
Search	Access orders, financial transactions, and payment authentications
Orders	Create an initial order manually, or perform an address verification.
Reports	Select and view reports.
Admin	Create new Operators, change and delete existing Operator records and privileges, change passwords and edit merchant configuration details.
Translation Portal	Translate screen labels. Note: This menu is only available if the merchant profile has the <i>Enable Translation Portal</i> privilege.
Logout	Log out and return to the login page.

The administration options available to you depend on the features provided by Transaction Network Services' and/or the features that you requested. The options available to you will also depend on your Operator privileges. For more information, please refer to **Privileges** on page 73.

Note: You may not see all of the options described.

- 1 Select a menu option to display the submenu for that menu option. For example, if you click Search, the Search home page displays and the submenu is visible on the left hand side of the page.
- 2 Select an option from the submenu. The selected page displays.

Logging Out

You can log out of Merchant Administration at any stage. If you do not log out, you will be logged out automatically after 15 minutes of inactivity.

How to Logout

- 1 Click the *Logout* link in the top right corner of the screen.
- 2 The login screen is displayed when you have successfully logged out.

The Home Page

The home page of Merchant Administration displays the News items for the day, Terms and Conditions (if any), and some useful links.

If Terms and Conditions have been set, the home page first displays the online user acceptance agreement. Read the agreement and click **[Accept]** to accept the agreement else click **[Reject]**. If you reject the online user acceptance agreement, you will be logged out of the system.

To view the full news article click the news headline in the News section. The content of the news item displays below the headline.

The home page works as a dashboard by providing quick access to tasks that you might need to do. The tasks are divided into two submenus:

- **Action Items**

These are pending tasks that require some action to proceed. Currently, only items pertaining to the Risk Management module are available for action.

For more information, see **Action Items** on page 93.

- **Shortcuts**

These are quick links to common tasks the merchant is likely to perform on a day-to-day basis. Clicking a link takes you the relevant page from where you can decide to either proceed or cancel the task. The currently available links are:

- Create a New Order

See The Create Order Entry Page.

- View Orders Created Today

Searches for orders with today's date and displays a list of orders that match the criteria. See Order Search Page.

- View Transactions Processed Today

Searches for transactions with today's date and displays a list of transactions that match the criteria. See Financial Transactions Search Page.

CHAPTER 3

Working with Orders

Merchant Administration allows you to create, process, save and review orders or lists of orders. In its most simple form of an "order" the card holder provides their card details to a merchant, via mail order or by telephone (including Interactive Voice Response (IVR) systems) to make immediate or later payment for goods or services. An order can also include a range of other actions, depending on your privileges, and the acquirer that you are authorised to use.

Note: To create orders you must have the user privilege *MOTO* . See ***Merchant Administration Operator Details page*** on page 74.

Once orders are created they are available for further processing, for example, if a refund has to be made. Existing orders can be located by order, or financial transaction details. They can also be viewed under the View Orders option of the Orders menu.

Creating an Order

Cardholders can provide card and transaction information to a merchant by a variety of means. These include telephone, fax, email or IVR. The merchant can use this information to process an order.

Note: You may see fewer or more fields than shown in the sample pages, depending on your privileges and the country of use. All sample pages are illustrative only, and do not necessarily represent what you will actually see on your system.

To create an order:

- 1 On the main menu, click *Orders > Create Order*.
- 2 The Create Order Entry page displays.
- 3 There are at least three required fields on this page; *Amount*, *Card Number*, and *Card Expiry*. Complete these and others as required.
- 4 Click the *Submit* button. If you selected an installment plan in the Order Entry page, an Payment Plan Confirmation page appears, that enables you to view details and confirm the payment plan. Click *Submit*.

Note: This page only appears in countries where this is a mandatory requirement.

- 5 The Create Order Response page displays showing whether or not the transaction has been approved.
- 6 You can proceed in one of the following ways:
 - Click *New transaction with Current Data* to return to perform another order for the same cardholder. This will redisplay the page, enabling you to enter further orders for the same cardholder, with the same data.
 - Click the *New Transaction with Default Data* to create a new order. This will redisplay the page, with all fields cleared, enabling you to enter a new order.
 - Click *Capture Now* to capture the order.
- 7 The Order Details page appears, with all the details of the order as entered. You can now Capture the full or part amount of the order.
- 8 In the Action section, enter the *Capture Amount*.
- 9 Click the **[Capture]** button if this is a part or full amount or click the **[Complete]** button if no further amounts will be captured for this order.
- 10 The Order Details Response page displays showing whether or not the transaction has been approved. It also displays the History section containing the financial transaction details of the order.
- 11 In case you have wrongly entered the order as *Complete* (capture), you can click the **[Incomplete]** button to indicate that the transaction has not been completely captured. If you performed a capture or complete capture, a refund button appears, allowing you to perform a refund if necessary.
- 12 Select any option from the menu or navigation menu to continue.

The Create Order Entry Page

Complete all mandatory fields, and others as required.

Note: You may not see all the fields listed here, depending on your privileges and the country of use.

Field	Description
Order Reference	A merchant-supplied identifier for the order. This will typically be used by the customer to identify their order (for example, a booking reference number).
Amount	The total amount of the order in the transaction currency. For example, AUD \$100.00.
Card Holder Name	The name of the cardholder.
Currency	The currencies supported by the merchant acquirer relationships, displayed with the currency code and the full name. Examples include: <ul style="list-style-type: none"> ▪ AUD - Australian Dollar ▪ USD - US Dollar ▪ EUR - Euro ▪ GBP - UK Pound Sterling
<p>Note: If the merchant supports only one currency across all acquirer relationships then only the currency code and name is displayed instead of the currency selection drop-down list.</p>	
Card Number	The card number used in the order. Depending on your profile, the format used for displaying card numbers is one of the following: <ul style="list-style-type: none"> ▪ 0.4 Format, for example (xxxxxxxxxxx1234) ▪ 6.3 Format, for example (654321xxxxxxxx123) ▪ The full card number is displayed ▪ The card number is not displayed
Card Expiry	The expiry date of the card, in mm/yy format.
Card Security Code	This is a security feature used for card not present transactions. For example: <ul style="list-style-type: none"> ▪ on Visa and MasterCard credit cards, it is the three digit value printed on the signature panel on the back, following the credit card account number. ▪ on American Express credit cards, the number is the four digit value printed on the front, above the credit card account number.
Airline Ticket Number	Originally aimed at the airline industry, this is an optional field where extra information about the transaction can be stored.
Address	The street details of the cardholder's billing address.
City/Town	The city or town of the cardholder's billing address.
State/Province	The state or province of the cardholder's billing address.
Zip/Postal Code	The zip or postal code of the cardholder's billing address.
Country	The country of the cardholder's billing address.

Merchant Transaction Source	<p>The method by which the merchant received the order. Typical transaction sources include:</p> <ul style="list-style-type: none">▪ Call Centre▪ Mail Order▪ MOTO▪ Telephone Order
Merchant Transaction Frequency	<p>Specifies the payment scheme used to process the order. Depending on your configuration, the available frequencies can include:</p> <ul style="list-style-type: none">▪ Single Transaction This indicates to the acquirer that a single payment is used to complete the cardholders order.▪ Recurring Transaction This indicates to the acquirer that the payment is a recurring bill payment under the card scheme rules. Recurring payments are those originating from automated billing applications for ongoing goods/services (for example to automatically pay a telephone bill each month) with cardholders authorising the merchant to automatically debit their accounts for bill or invoice payments.▪ Installment Transaction This indicates to the acquirer that the payment is an installment payment under the card scheme rules. Installment payments are those where the cardholder authorises the merchant to deduct multiple payments over an agreed period of time for a single purchase.▪ Default The Payment Server will use the Default Transaction Frequency specified in the merchant profile, for the acquirer processing the order.

Payment Plan

Specifies the payment plan for cardholders that offer a Deferred Payment Plan (DPP) option — an option to make payments in a number of installments.

Depending upon the card type entered (American Express or Bankcard) the relevant payment plans (American Express or Banamex) will be displayed in the drop-down list. For example, for an American Express card, the options are:

- None
- Plan N — Plan 'N' is a financial payment option available in some countries. Plan N, allows cardholders to defer payments for purchases from an eligible merchant into monthly installments. The merchant determines the number of installments and accepts the applicable charges and payment plan conditions with American Express. The card member is billed in installments without any interest while the merchant is paid in the agreed payment plan less the applicable charges. Generally there is a maximum of 24 installments.
- Plan Amex — Plan 'Amex' or Deferred Payment Plan (DPP) is a payment method available to cardholders in some markets. In Plan 'Amex', the merchant is paid in full less applicable discount rate and the cardholder is billed in installments plus the applicable interest rate. Plan 'Amex' transactions in Brazil are done as an initial inquiry followed by an authorization. This is to satisfy statutory requirements in that country to provide information about the amount of interest charged to the customer

The Banamex payment plans are configured by the merchant operator based on the cardholder's requirements. Only plans that are enabled are displayed for selection. See **Manage Payment Plans** on page 80.

Note: Banamex Payment Plans are applicable only to transactions using Mexican Peso currency.

Payment Terms

Specifies the maximum number of installments and/or deferrals for the specified plan. The number of installments and deferrals vary from plan to plan.

Only plans that include deferrals display the option to specify the number of deferral months.

Note: An error is returned if the combination of currency and card type is not supported by any of the merchant's acquirer links.

The Create Order Response Page

Note: You may not see all the fields described here, depending on your merchant configuration and area of operation.

The Order Response page displays the following information for an order:

- Response Details
- Risk Assessment Details

Orders - Create Order Response

0 - Approved

Response Details	
Order ID	26
Financial Transaction ID	26
Date	3/3/10 8:02 PM
Order Reference	
Amount	MXN P200.00
Card Type	Amex
Card Number	345678901234564
Card Expiry	05/13
Authorisation Code	000003
Acquirer Response Code	00
Response Code	0 - Approved
RRN	006312000026
Installments	12
Deferrals	3
Payment Plan	banamex2 - Pay in installments after a deferral period, with interest

New Transaction With Current Data

New Transaction With Default Data

Capture Now

Field	Description
Order ID	A unique number used to identify an order.
Transaction Number	An automatically generated number uniquely identifying the transaction. This identifier is unique within the merchant.
Date	The user-locale date and time at which the order was created.
Order Reference	A merchant-supplied identifier for the order. This will typically be used by the customer to identify their order (for example, a booking reference number).
Amount	The total amount of the order in the transaction currency. For example, AUD \$100.00.
Card Type	The card brand used for the transaction.
Card Holder Name	The name of the cardholder.
Card Number	<p>The card number used in the order. Depending on your profile, the format used for displaying card numbers is one of the following:</p> <ul style="list-style-type: none"> ▪ 0.4 Format, for example (xxxxxxxxxxx1234) ▪ 6.3 Format, for example (654321xxxxxxxx123) ▪ The full card number is displayed ▪ The card number is not displayed
Card Expiry	The expiry date of the card, in mm/yy format.
Authorisation Code	An identifier returned by the card-issuer indicating the result of the authorisation component of the order.
Acquirer Response Code	The response code from the acquirer indicating success or otherwise of the transaction.
Response Code	<p>A code and brief description summarizing the result of attempting to process the order. Example response codes are:</p> <ul style="list-style-type: none"> ▪ '0 - Approved' ▪ '3 - Timed Out'
RRN	The Retrieval Reference Number, which helps the Acquirer to identify a transaction that occurred on a particular day.
Country	The country of the cardholder's billing address.
Merchant Transaction Source	<p>The method by which the merchant received the order. Typical transaction sources include:</p> <ul style="list-style-type: none"> ▪ Call Centre ▪ Mail Order ▪ MOTO ▪ Telephone Order

Merchant Transaction Frequency	<p>Specifies the payment scheme used to process the order. Depending on your configuration, the available frequencies can include:</p> <ul style="list-style-type: none">▪ Single Transaction This indicates to the acquirer that a single payment is used to complete the cardholders order.▪ Recurring Transaction This indicates to the acquirer that the payment is a recurring bill payment under the card scheme rules. Recurring payments are those originating from automated billing applications for ongoing goods/services (for example to automatically pay a telephone bill each month) with cardholders authorising the merchant to automatically debit their accounts for bill or invoice payments.▪ Installment Transaction This indicates to the acquirer that the payment is an installment payment under the card scheme rules. Installment payments are those where the cardholder authorises the merchant to deduct multiple payments over an agreed period of time for a single purchase.▪ Default The Payment Server will use the Default Transaction Frequency specified in the merchant profile, for the acquirer processing the order.
Installments	The number of installments in this order. This field only displays if the order is part of a payment plan.
Deferrals	The number of deferrals in this order. This field only displays if the order is part of a payment plan, and if the payment plan supports deferrals.
Payment Plan	The name of the custom payment plan.
The following fields are displayed only if American Express Payment Plans are used.	
Payment Amount	The amount of the payment.
Final Amount	The outstanding amount of the payment plan.
Interest Amount	The interest amount in this order.

Creating a Capture Only Entry Order

A Capture Only order is used to capture an amount for an order which was authorised manually, or in an external system.

Note: In order to create a Capture Only order, both the operator and the merchant must have the Stand Alone Capture privilege enabled. This privilege is applicable to EMEA and GNS regions only.

To create a capture only entry:

- 1 On the Main menu, click *Orders > Capture Only*.
- 2 The Capture Only Entry page is displayed. See The Create Order Entry Page. The Capture Only Entry page includes an additional field, *Authorisation Code*, which uniquely identifies the authorisation performed outside Merchant Administration.
- 3 Enter the details of the order, ensuring that all mandatory fields are completed (these are indicated with an asterisk).
- 4 Click the **[Submit]** button. The Capture Only Response page displays showing whether or not the transaction has been approved.
- 5 You can proceed in one of the following ways:
 - Click *New transaction with Current Data* to perform another capture against the same cardholder.
 - Click *New Transaction with Default Data* to create another capture against a new cardholder.

Note: The fields displayed on the *Capture Only Entry* page include all those displayed on the *Create Order Entry* page, and one additional field called 'Authorisation Code'. The Authorisation Code is a mandatory field which identifies the authorisation for the order made in an external system.

Searching for Orders

To locate an order, use the search options of Merchant Administration.

To search for an order:

- 1 From the Main menu, select *Search > Order Search*. The Merchant Administration **Order Search** on page 24 displays.
- 2 Enter the search parameters. If you enter multiple search parameters, the records returned will match all the search criteria.
- 3 Click the **[Submit]** button. The **Order List page** on page 26 displays. The Order List page details information for each transaction.
- 4 Click on an individual *Transaction No.* to view its details. The Order Details page displays.

Order Search Page

Identify the orders you wish to retrieve on the Merchant Administration Order Search page, by populating the relevant search criteria. Click the **[Submit]** button to start the search.

The available search fields are:

Field	Description
From/To	Search for orders within a date range. If you clear the From field, all transactions up to the current date are displayed. The default From and To Dates are at the date of the users local time zone.
Order ID	Search for a specific order by its unique Order ID.
Order Reference	Search for orders created with specific Order Reference text.
Card Number	Search for orders made against a specific credit card.
Authorisations Pending Capture	Search for orders that have authorised amounts against them which have not yet been captured. Note: The orders returned will exclude outstanding authorisations marked as complete.
Outstanding Verifications	Search for orders that have credit cards verified but the order amount is not yet captured. Note: The orders returned will exclude outstanding verifications marked as complete.
Acquirer ID	Search for orders processed by a particular acquirer (for example, Mastercard NAB).
Currency	Search for orders processed by a particular currency or all currencies.
Card Type	Search for orders processed by a particular card type or all card types.
Merchant Transaction Source	Search for orders created using a specific facility (for example, Telephone Order).
Transaction Success	Search for orders having a specific success status (for example, successful, failed, or referred).
Risk Recommendation	Search for orders having a specific risk recommendation: Valid values are: <ul style="list-style-type: none"> ▪ Accept — indicates that the order was processed normally. ▪ Review — indicates that the order was marked for review. ▪ Reject — indicates that the order was rejected. ▪ All — indicates orders with one or more of the aforementioned risk recommendations.
Only Show Orders Where Risk Review Decision Required	Search for orders where a decision has not been taken on whether to accept or reject the order based on risk recommendation. This option provides merchants the flexibility to include only those orders where risk review decision is pending; and ignore orders where the decision has been made. Note: This field is displayed if <i>Risk Services</i> privilege is enabled for a merchant.

Number of Results to Display on Each Result Page Enter the number of rows of search results that you wish to see on a single page.
Leave this field blank for the default number of search results to be displayed.

Viewing Orders - The Order List Page

The Order List page displays all the orders that match the criteria of the **Order Search** on page 24.

Field	Description
Acquirer ID	The unique identifier of the card-processor to which the order was directed for processing.
Order ID	A unique number used to identify an order.
Order Reference	A merchant-supplied identifier for the order. This will typically be used by the customer to identify their order (for example, a booking reference number).
Amount	The total amount of the order in the transaction currency. For example, AUD \$100.00.
Date	The user-locale date and time at which the order was created.
Response Code	A code and brief description summarizing the result of attempting to process the order. Example response codes are: <ul style="list-style-type: none"> ▪ '0 - Approved' ▪ '3 - Timed Out'
Status	The result of the most recent action performed on the order (for example, 'Authorised' or 'Captured'.)
Capture	A check box enabling the operator to select orders against which funds are to be captured.

The Totals field is displayed only when all orders listed in the Order List page are for the same currency. Three page totals are displayed, as follows:

- **Authorised** — total of all successful authorisations. For merchants in Purchase mode, this should be the same as the Captured total.
- **Captured** — total of all successful captures. For merchants in Purchase mode, this is all successful purchases. Subsequent void captures are not deducted from the total.
- **Refunded** — total of all successful refunds.

Please note that:

- Totals are calculated for successful transactions only. Authorisations, Captures or Refunds that are declined or referred will not be added to the total.
- Voids are not included in the calculations. For example, if a Capture has been voided, the voided amount will not be subtracted from the total captured amount.
- If the capture or refund occurs outside the bounds of the search date, but the order date falls within the search date, the capture or refund will be included in the total.

Select an *Order ID* to see the details of that order. The Order Details page displays.

Use the **[Select All]** button if you wish to capture all the orders. Click the **[Capture]** button to perform a capture on any orders that have been selected for capture in the Order List.

Note 1: These buttons display only if you have the *Perform Bulk Captures* privilege.

Note 2: You can bulk capture orders with Level 2 data only if your merchant profile has "Allow Level 2 Order Creation" privilege enabled.

Viewing an Individual Order - The Order Details Page

The Order Detail page lists the following information for an order:

- Order Details
- Address Verification Details
- Card Details
- Payment Plan Details
- Risk Assessment Details
- Action
- History

Order Details

Field	Description
Acquirer ID	The unique identifier of the card-processor to which the order was directed for processing. Note: If an acquirer link is configured to have multiple acquirer relationships, then the acquirer link is suffixed with the Bank Merchant ID following a hyphen. For example, ANZ via FDRA — 12345 where "ANZ via FDRA" is the acquirer link and "12345" is the Bank Merchant ID.
Order ID	A unique number used to identify an order.
Date	The user-locale date and time at which the order was created.
Order Reference	A merchant-supplied identifier for the order. This will typically be used by the customer to identify their order (for example, a booking reference number).
Airline Ticket Number	Originally aimed at the airline industry, this is an optional field where extra information about the transaction can be stored.
Amount	The total amount of the order in the transaction currency. For example, AUD \$100.00.
Authorised Amount	The amount of the order that has been successfully authorised by the issuer, displayed with the currency code and the currency symbol. For example, AUD \$10.00.
Captured Amount	The amount of the order that has been successfully captured by the merchant, displayed with the currency code and the currency symbol. For example, AUD \$10.00.
Refunded Amount	The amount of the order that has been successfully refunded by the merchant, displayed with the currency code and the currency symbol. For example, AUD \$10.00.
Authorisation Code	An identifier returned by the card-issuer indicating the result of the authorisation component of the order.

Merchant Transaction Source	<p>The method by which the merchant received the order. Typical transaction sources include:</p> <ul style="list-style-type: none"> ▪ MOTO ▪ Telephone Order ▪ Mail Order ▪ Voice Response
Merchant Transaction Frequency	<p>Indicates whether the transaction was a single, recurring or part of an installment payment. Depending on your configuration the available frequencies can include:</p> <ul style="list-style-type: none"> ▪ Single Transaction This indicates to the acquirer that a single payment is used to complete the cardholders order. ▪ Recurring Transaction This indicates to the acquirer that the payment is a recurring bill payment under the card scheme rules. Recurring payments are those originating from automated billing applications for ongoing goods/services (for example to automatically pay a telephone bill each month) with cardholders authorising the merchant to automatically debit their accounts for bill or invoice payments. ▪ Installment Transaction This indicates to the acquirer that the payment is an installment payment under the card scheme rules. Installment payments are those where the cardholder authorises the merchant to deduct multiple payments over an agreed period of time for a single purchase.
Response Code	<p>A code and brief description summarizing the result of attempting to process the order. Example response codes are:</p> <ul style="list-style-type: none"> ▪ '0 - Approved' ▪ '3 - Timed Out'

Address Verification Details

Field	Description
Address	The street details of the cardholder's billing address.
City/Town	The city or town of the cardholder's billing address.
State/Province	The state or province of the cardholder's billing address.
Zip/Postal Code	The zip or postal code of the cardholder's billing address.
Country	The country of the cardholder's billing address.
AVS Result Code	Code and description returned by the AVS server.
Dialect AVS Result Code	Code and description summarising the outcome of the address verification attempt. For example: 'X (Exact match, 9-digit zip)'.

Card Details

Field	Description
Card Type	The card brand used for the transaction.

Card Number	The card number used in the order. Depending on your profile, the format used for displaying card numbers is one of the following: <ul style="list-style-type: none"> 0.4 Format, for example (xxxxxxxxxxxx1234) 6.3 Format, for example (654321xxxxxx123) The full card number is displayed The card number is not displayed
Card Expiry	The expiry date of the card, in mm/yy format.
Card Start Date	The start date of the card, if provided.
Issue Number	The issue number, if provided.
Acquirer CSC Result Code	Card security code validation result code as provided from the acquirer.
Dialect CSC Result Code	Card security code validation result code in standard payment server result format.

Payment Plan Details

Note: These fields are displayed only if the order is part of a payment plan.

Field	Description
Number of Installments	The number of installments in this order. This field only displays if the payment plan supports installments.
Number of Deferrals	The number of deferrals in this order. This field only displays if the payment plan supports deferrals.
Payment Plan	The name of the custom payment plan.
The following fields are displayed if American Express Payment Plans are used.	
Number of Installments	The number of payments in this order.
Interest Amount	The interest amount displayed with the currency code and symbol.
Interest Rate	The interest rate.
Payment Amount	The amount of each payment displayed with the currency code and symbol.
Final Amount	The total amount of the order displayed with the currency code and symbol.

Action

This section will contain only those actions that are applicable to the order.

Note: You may see none or more of the following fields.

For the steps required to use these field correctly, see Performing Actions on Orders.

Field	Description
Capture Amount	Enter the amount to be captured in this transaction.
Refund Amount	Enter the amount to be refunded to the cardholder.

History

Field	Description
Response Code	<p>A code and brief description summarizing the result of attempting to process the order. Example response codes are:</p> <ul style="list-style-type: none"> ▪ '0 - Approved' ▪ '3 - Timed Out'
Date	The user-locale date and time at which the order was created.
Transaction Type	<p>The type of transaction performed. An example may be:</p> <ul style="list-style-type: none"> ▪ Authorisation ▪ Capture ▪ Refund.
Amount	The total amount of the order in the transaction currency. For example, AUD \$100.00.
Operator ID	The identifier of the merchant operator that performed the action.
Transaction ID	A merchant generated unique identifier for the financial transaction (or system generated if one is not provided). This identifier is unique within the order.
Merchant Transaction Reference	A unique merchant specific identifier used in Payment Client transactions.
Transaction Source	<p>Indicates the integration facility used to generate the transaction. Typical transaction sources include:</p> <ul style="list-style-type: none"> ▪ PC — the transaction source is Payment Client. ▪ MOTO — the transaction source is Merchant Administration. ▪ Direct — the transaction source is Web Services API. ▪ Batch — the transaction source is Batch. ▪ Auto (Risk) — the transaction source is risk assessment. For example, an order on which a financial transaction is performed is rejected due to risk assessment it is automatically attempted for a reversal by the system. ▪ Auto — the transaction source is system. Auto indicates that the system initiated the transaction automatically. For example, an automatically-triggered Capture transaction when a Purchase transaction is submitted by a merchant for a processor that only supports Auth/Capture. ▪ Risk Override — the transaction source is a request to override a Reject risk recommendation for a transaction that has been assessed by external risk.





Risk Assessment Details

The Order Response and Order Details screens display the risk assessment details for an order, which include the recommended risk decision and details about the decision. The result of the individual risk rules that resulted in the risk recommendation are displayed under Risk Rules.

Note: The Risk Assessment Details for an order are displayed only if *May Use Risk Management* privilege is enabled for a merchant.

The screen shot below shows risk assessment details for an order that was assessed using **internal risk** only.

Risk Assessment Details				
Risk Recommendation	Review			
Risk Review Resolution	Rejected			
Order Reversal Status	OK			

Risk Rules				
Rule	Result	Details	Source	
Merchant BIN Range	 Review	525895	Merchant Rules	
Suspect Card List	 No Action		Merchant Rules	
Trusted Card List	 No Action		Merchant Rules	
MSO BIN Range	 No Action	525895	MSO Rules	

Field	Description
Risk Recommendation	<p>This field indicates the final action taken on the order based on the risk assessment performed.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> ▪ Accept — indicates that the order was processed normally. ▪ Not Checked — indicates that the order was processed by bypassing risk assessment using the <i>Bypass Risk Management</i> option. It also implies a condition where neither MSO nor merchant risk rules are configured in the system. ▪ Review — indicates that the order was marked for review. ▪ Reject — indicates that the order was rejected. ▪ System Reject — indicates that the order was rejected at the system (MSO) level. <p>For more information, see Implications of Risk Recommendation.</p>
Risk Review Resolution	<p>The decision made by the merchant operator in response to an order receiving a risk review decision of Review. This field is displayed only when Risk Recommendation is set to Review.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> ▪ Accepted — indicates that the order can be processed normally. ▪ Rejected — indicates that the order was rejected and cannot proceed. ▪ Decision Required — indicates that the risk review decision is yet to be made. ▪ No Decision Required — indicates that the risk review decision is not required because the transaction failed. For example, declined by acquirer after risk assessment is performed.
Order Reversal Status	<p>This field indicates the result of an order reversal for each authorization or purchase that occurred due to risk assessment.</p> <p>This field is displayed only for orders that were rejected due to risk assessment after the financial transaction was initiated/performed; or orders cancelled during a review decision. Rejected/cancelled orders are automatically attempted for a reversal by the system.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> ▪ OK— indicates that the order was reversed successfully. ▪ FAILED — indicates that the attempt to reverse the order failed. ▪ Not Supported — indicates that the acquirer does not support reversal of the required transaction so the reversal failed. ▪ Manual Override — indicates that a Reject risk recommendation for a transaction that was assessed by external risk has been manually overridden. <p>Currently, CSC/AVS rules are the only rules, which by default are processed after the financial transaction. To allow these rules to be processed before the financial transaction, you must have the merchant privilege "Perform Verification Only for AVS/CSC Risk Assessment" enabled.</p> <p>Verification Only allows the system to verify cardholder information without performing a financial transaction.</p>





Internal Risk Only

This section describes the implications of risk recommendation when only internal risk is enabled. The possible values for risk recommendation are:

- Accept
- Not Checked
- Reject
- System Reject
- Review

When Risk Recommendation is Set to Accept

A risk recommendation of "Accept" is displayed in the Order Details screen if the risk rules have been configured to process the order normally (No Action) or configured to the "Always Accept" action.

Risk Assessment Details				
Risk Recommendation		Accept		
Risk Rules				
Rule	Result	Details	Source	
Trusted Card List	 No Action		Merchant Rules	
Suspect Card List	 No Action		Merchant Rules	
Merchant BIN Range	 No Action	512345	Merchant Rules	
MSO BIN Range	 No Action	512345	MSO Rules	

Use Cases

Case A: 3DS Rule with Clash Rule Configuration

Let's say the cardholder who initiated the transaction is enrolled for 3DS and the following system and merchant rules apply. Let's also assume that the 3DS authentication returns "Verification Attempted" as the authentication result.

Rule Type	System Rules	Merchant Rules	Risk Recommendation
3DS Rule (Verification Attempted)	No Action	Always Accept	Accept
Suspect Cards	-	Always Reject	Reject

The merchant operator can perform one of the following actions on order:

- Go to the 3DS Rules Configuration page and configure the Clash Rule to "Always Accept" to proceed with the order. For more information on Clash Rule, see **Adding a 3DS Rule** on page 114.
- Go to the 3DS Rules Configuration page and configure the Clash Rule to "Always Reject" to reject the order. By default, the clash rule is set to "Always Reject".

Case B: 3DS Rule when failed authentication is rejected by the system

Let's say the cardholder who initiated the transaction is enrolled for 3DS and the following system and merchant rules apply.

Rule Type	System Rules	Merchant Rules	Risk Recommendation
3DS Rule (Verification Attempted)	No Action	Always Accept	Accept
Trusted Cards	-	Always Accept	Accept

Based on the Risk Recommendation, it seems that this transaction should be accepted; however, if the 3DS authentication returns "Authentication Failed" as the authentication result, then the Payment Server blocks the transaction at the system level itself thus bypassing all risk checks. This means the 3DS rule (Verification Attempted) configured to action "Always Accept" is bypassed and so is the Trusted Cards rule.

When Risk Recommendation is Set to Not Checked

A risk recommendation of "Not Checked" is displayed in the Order Details screen if the order was created by bypassing risk checks using the *Bypass Risk Management* option (and the MSO rules did NOT evaluate to a Reject). It also implies a condition where neither MSO nor merchant risk rules are configured in the system.

Risk Assessment Details				
Risk Recommendation			Not Checked	
Risk Rules				
Rule	Result	Details	Source	
MSO BIN Range	No Action	554983	MSO Rules	

An order with risk recommendation of "Reject" can be recreated and submitted by enabling the *Bypass Risk Management* option. See next.

When Risk Recommendation is Set to Reject

A risk recommendation of "Reject" is displayed in the Order Details screen if the MERCHANT risk rules have been configured to reject the order. Based on the rules configured the order can be rejected before or after the financial transaction. If the order is rejected after the financial transaction then the system automatically attempts to reverse the order and displays the results in the *Order Reversal Status* field.

Order Rejected Before the Financial Transaction

Risk Assessment Details				
Risk Recommendation				Reject
Risk Rules				
Rule	Result	Details	Source	
Suspect Card List		No Action		Merchant Rules
Trusted Card List		No Action		Merchant Rules
Merchant BIN Range		Reject	540275	Merchant Rules
MSO BIN Range		No Action	540275	MSO Rules

Order Rejected After the Financial Transaction

Risk Assessment Details				
Risk Recommendation				Reject
Order Reversal Status				OK
Risk Rules				
Rule	Result	Details	Source	
Merchant CSC		Reject	U	Merchant Rules
Trusted Card List		No Action		Merchant Rules
Suspect Card List		No Action		Merchant Rules
Merchant BIN Range		No Action	498765	Merchant Rules
MSO CSC		No Action	U	MSO Rules
MSO BIN Range		No Action	498765	MSO Rules

Occasionally, order reversals can fail due to the acquirer not supporting reversals or an acquirer being unavailable. In such a case, the Order Reversal Status is set to "Failed " as shown below. You can retry an order reversal on a failed reversal by clicking the **[Retry Order Reversal]** button.

Risk Assessment Details	
Risk Recommendation	Reject
Order Reversal Status	Failed
<input type="button" value="Retry Order Reversal"/>	

A successful reversal changes the status to "OK". If the acquirer does not support reversals, the status changes to "Not Supported".

Note: If you wish to make an exception to a particular cardholder you can choose to override the merchant rules. To achieve this, you must recreate and submit the order by bypassing risk assessment. See *Bypass Risk Management* option.

Use Cases

Case A: IP Country Rule

Let's say the cardholder who initiated the transaction is currently present in country "Country_A" and the following system and merchant rules apply.

Rule Type	System Rules	Merchant Rules	Risk Recommendation
IP Country (Country_A)	No Action	Reject	Reject

The merchant operator can perform one of the following actions on the order:

- If the cardholder has a good transaction history and you want to make an exception to this particular cardholder, re-submit the order by enabling *Bypass Risk Management* option.
- As the cardholder appears trustworthy, add the cardholder to the Trusted Cards list to ensure that review decisions on this cardholder, if any, in the future, can be bypassed. A cardholder added to the trusted cards list is always accepted unless rejected at the MSO level.

Case B: CSC Rule

Let's say the cardholder who initiated the transaction has a CSC (Card Security Code) that does not match the data in card issuer's database, and the following system and merchant rules apply.

Rule Type	System Rules	Merchant Rules	Risk Recommendation
CSC (No CSC Match)	No Action	Reject	Reject

CSC/AVS rules by default are processed after the financial transaction unless the merchant has the privilege to perform Verification Only for AVS/CSC Risk Assessment enabled. Verification Only allows the system to verify cardholder information before performing a financial transaction. If the CSC rule is processed after the financial transaction and the risk assessment rejects the order, then the Risk Assessment Details section displays an additional field "Order Reversal Status", which indicates the result of the order reversal performed for an authorization or a purchase. Orders rejected due to risk assessment after the financial transaction are automatically attempted for a reversal by the system.

The History section displays the details of the transactions performed for the order reversal. Transactions reversed due to risk assessment are indicated with the "Auto (Risk)" label in the Transaction Source column. See History in the Order Details Page.

The merchant operator can perform one of the following actions on the order:

- If the cardholder has a good transaction history and you want to make an exception to this particular cardholder, re-submit the order by enabling *Bypass Risk Management* option.
- As the cardholder appears trustworthy, add the cardholder to the Trusted Cards list to ensure that review decisions on this cardholder, if any, in the future, can be bypassed. A cardholder added to the trusted cards list is always accepted unless rejected at the MSO level.

When Risk Recommendation is Set to System Reject

A risk recommendation of "System Reject" is displayed in the Order Details screen if the MSO level risk rules are configured to reject the transaction. An order rejected at the MSO level cannot be accepted by any means unless the risk rules are re-configured to accept the transaction.

Risk Assessment Details

Risk Recommendation System Reject

Risk Rules

Rule	Result	Details	Source
MSO BIN Range	No Action	498765	MSO Rules
MSO IP Address Range	Reject	53.255.255.255	MSO Rules
MSO IP Country	No Action	DEU	MSO Rules

Note: MSO risk rules always override merchant level rules; they cannot be bypassed by enabling *Bypass Risk Management* option in the Create Order screen.

When Risk Recommendation is Set to Review

A risk recommendation of "Review" is displayed in the Order Details screen if the merchant operator has not taken a risk assessment decision on the order yet. In such a case, the merchant operator with the privilege "May Perform Risk Assessment Review" is required to take a decision on whether to approve or reject the order. No subsequent transactions will be allowed until the operator takes an action on the order. For example, for an "Auth Then Capture" transaction type, if the authorization returns a risk recommendation of "Review" then a subsequent Capture transaction will not be allowed till the operator takes a decision. The decision may be based on the individual risk assessment results for the rule types defined for the merchant and MSO and/or the transaction history of the cardholder.

Click **[Accept Order]** to proceed with the order else click **[Reject Order]**.

Risk Assessment Details

Risk Recommendation Review

Risk Review Resolution Decision Required

Risk Rules

Rule	Result	Details	Source
Merchant BIN Range	Review	525895	Merchant Rules
Suspect Card List	No Action		Merchant Rules
Trusted Card List	No Action		Merchant Rules
MSO BIN Range	No Action	525895	MSO Rules

The reviewed orders will display the risk review resolution under Risk Assessment Details as shown below.

Risk Review Resolution when the Reviewed Order is Accepted

Risk Assessment Details

Risk Recommendation Review

Risk Review Resolution Accepted

Risk Review Resolution when the Reviewed Order is Rejected

Risk Assessment Details	
Risk Recommendation	Review
Risk Review Resolution	Rejected
Order Reversal Status	OK

For a merchant transaction in Auth Then Capture mode, if the merchant operator decides to reject the order, then the system will attempt to void the authorization and mark the transaction as complete if the acquirer supports Void Authorization. However, if the acquirer does not support Void Authorization, the system will just mark the transaction as complete.

In a Purchase mode, if the merchant operator decides to reject the order, the system will attempt to void the purchase and mark the order as complete if:

- the acquirer supports Void Purchase,
- if the order is in an unreconciled batch, and
- if the order is not a P2P transaction.

However, if the acquirer does not support Void Purchase, the system will perform a refund on the captured amount and mark the transaction as complete.

Note: Merchant operators will not be allowed to perform bulk capture on orders with the Risk Recommendation of "Review".

Use Cases

Case A: IP Country Rule

Let's say the cardholder who initiated the transaction is currently present in country "Country_A" and the following system and merchant rules apply.

Rule Type	System Rules	Merchant Rules	Risk Recommendation
IP Country (Country_A)	No Action	Review	Review

The merchant operator can perform the review in the following ways:

- Proceed with the order if the cardholder has a good transaction history though the country from which the transaction originates is under Review. As the cardholder appears trustworthy, add the cardholder to the Trusted Cards list to ensure that review decisions on this cardholder, if any, in the future, can be bypassed.
- Reject the order if the cardholder has a fraudulent transaction history or has no previous records of transaction — it's perhaps not worth the risk! As the cardholder appears untrustworthy, add the cardholder to the Suspect Cards list to ensure that review decisions on this cardholder, if any, in the future, can be bypassed.

Case B: Card BIN Rule

Let's say the cardholder who initiated the transaction belongs to the BIN range (457199 - 457999) and the following system and merchant rules apply.

Rule Type	System Rules	Merchant Rules	Risk Recommendation
Card BIN (457199 - 457999)	No Action	Review	Review

The merchant operator can proceed with the review decision in the following ways:

- Reject the order as the Card BIN range is under Review and if the cardholder has a fraudulent transaction history, add the cardholder to the Suspect Cards list to ensure that review decisions on this cardholder, if any, in the future, can be bypassed.
- Proceed with the order if the merchant operator identifies the risk rule as false and re-configure the risk rules for Card BIN ranges.

- Proceed with the order if the cardholder has a good transaction history and you want to make an exception to this particular cardholder. As the cardholder appears trustworthy, add the cardholder to the Trusted Cards list to ensure that review decisions on this cardholder, if any, in the future, can be bypassed.

Performing Actions on Orders

The *Action* section on the Orders Details page allows the operator to perform actions upon a Order. These actions will vary according to the payment type, and to the stage of the payment cycle. For example, an order which has authorised amount and awaiting capture may display as shown in the example.

Action	
Capture Amount	R\$ <input type="text" value="00.00"/>
<input type="button" value="Capture"/>	
<input type="button" value="Complete"/>	Mark the order as completely captured if you do not expect to be capturing the outstanding authorised amount

Actions which may be available for a transaction are:

- Capture
- Complete (Capture)
- Incomplete (Capture)
- Refund

Note: To perform any action you must have the required user privilege, for example, *Refunds* or *Captures*.

Capturing an Order Amount

You may capture some or all of the authorised amount of a transaction.

To capture funds for an authorised transaction:

- 1 Enter the amount in the *Capture Amount* field.
- 2 Click the **[Capture]** button.

Completing an Order

In several situations, it is useful to consider an order to be complete, even though only a portion of the authorised amount of the order has been captured.

Consider, for example, a book-supplier who authorises an order for three books, but then discovers that only two of the ordered books can be found on their shelves. The supplier may want to capture the portion of the authorised amount corresponding to the value of the two books they can find, and then tag the order as complete to indicate that no more funds will be charged to the customer's card for this order. Similarly, when a guest books a hotel room, the hotel may authorise an amount which is intended to cover both room rental and any anticipated room-service charges. If, on checking out of the hotel, the guest has incurred no room-service charges, the hotel will only capture the portion of the authorised amount corresponding to rental of the room, and will then consider the order to be complete.

Whenever the authorised amount of an order has not been completely captured, it is possible to mark the order as complete, so that no further captures may be made against it.

To tag a partially captured order as complete:

- Click the **[Complete]** button. The refreshed order details page displays. The *Amount* field is now appended with the word 'Completed', and the only actions now available for the order are **[Refund]** and **[Incomplete]**.

Note: Complete orders will not be retrieved by an order search specifying Outstanding Authorisations.

If you decide that a further capture is required against a complete order (if the book-seller finds the missing book at the last minute, for example), it is possible to re-tag the order as incomplete, so that a further capture can be made.

To tag a complete order as incomplete:

- Click the **[Incomplete]** button. The refreshed order details page displays. The word 'Completed' is now removed from the Amount field, and the actions now available for this order are **[Refund]**, **[Complete]**, and **[Capture]**.

Refunding a Transaction

A refund is cancelling any purchases performed on a pre-authorised amount.

Note: Refunding a transaction is not supported by all card types.

Refunds are performed for many reasons, for example, the return of unwanted, incorrect or faulty goods.

To refund an OrderID (shopping transaction) :

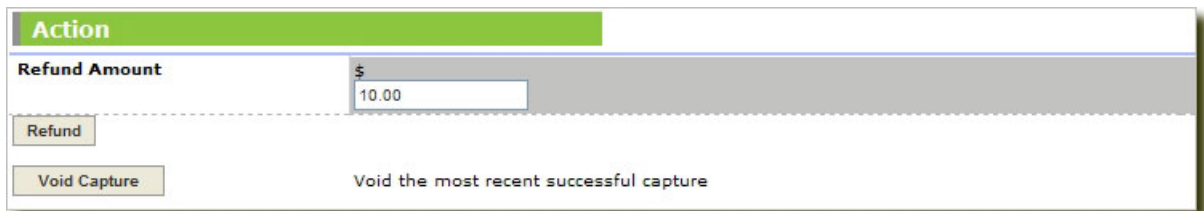
- 1 Enter the *Amount* to be refunded in the Refund box.
- 2 Click the *Refund* button. The refreshed Orders Details page displays and includes the new transaction.

Voiding a Transaction

A void is the cancellation of a previous transaction on an Order. Voids can only be performed if the transaction is in a batch that has not already been reconciled.

You can void an authorisation, refund, purchase, or a capture. The option displayed depends on the action you last performed. A void performed on an authorisation will immediately release any reserved funds. In all other transaction types, the void will prevent the funds transfer from occurring.

Only the last refunded amount is voidable. You are unable to input an amount during this process.



The screenshot shows a dialog box titled "Action" with a green header. Below the header, there is a section labeled "Refund Amount" with a dollar sign (\$) and a text input field containing "10.00". Below this, there are two buttons: "Refund" and "Void Capture". The "Void Capture" button is highlighted, and its tooltip text reads "Void the most recent successful capture".

To void a Order:

- 1 Click the **[Void Authorisation]**, **[Void Purchase]**, **[Void Refund]**, **[Void Capture]**, or **[Void Auth and Capture]** button. The refreshed Order details page displays and includes the new transaction.

The "Void Auth and Capture" button becomes available only for a Purchase transaction that has been auto-captured. When you void this transaction, the payment gateway:

- attempts a "Void Capture" for the Capture transaction.
- if the "Void Capture" is successful, then a "Void Authorization" is attempted for the Authorization. If the "Void Capture" is unsuccessful, then the response indicates that the void failed; the Void Authorization is not attempted.

CHAPTER 4

Settling Orders

Merchant Administration allows you to settle your customer's orders automatically or manually with your acquirer. Settlement allows you to view the set of orders that have been billed to the customer but still have to be settled with the acquirer.

Note: To perform a manual Settlement you require Merchant and User privileges to *View Settlement pages* and *Initiate Manual Batch Closure*. User privileges are found in the Operator Detail page under the Admin menu.

Settlements are balance operations between a merchant's accounts and an acquirer's records. Depending on how your merchant profile is set up, settlement can be done automatically (the time is set when creating your merchant profile) or manually (you can settle your orders yourself).

Settlement is divided into two sections:

- Settlement - Display the orders in the current settlement that are to be settled.
- Settlement History Selections - Allows you to search for and view orders that have already been settled.

Dealing with Unsettled Transactions

To view the current orders awaiting settlement:

- 1 Select *Settlement > Pre-settlement Summary*. If you have multiple acquirer links, the Settlement Acquirer Link Selection page displays. Note that the card types and currencies configured for the acquirer link are also displayed. Select the Acquirer ID and click the **[Submit]** button. The ***Unsettled Transactions Summary*** on page 44 page displays.
- 2 The Settlement page shows the current orders awaiting settlement. It details a settlement by **Currency**. Each row for a currency provides details for transactions processed by a specific card type.
- 3 If you have the *Initiate Manual Batch Closure* privilege, a **[Settle Now]** button displays. Click this to settle the batch. The ***Batch Closure Receipt*** on page 45 page displays.

Unsettled Transactions Summary Page

The Unsettled Transactions Summary page displays lists of transactions by currency, and provides a **[Settle Now]** button that allows you to settle all pending orders.

Settlement - Unsettled Transactions Summary

Merchant and Acquirer Settlement Details

Number Of Batch Currently Open	4
Merchant ID	TESTUSDONLY
Acquirer ID	AMEX

USD - US Dollar

Card Type	Number Debits	Total Debits	Number Credits	Total Credits
American Express	2	USD \$5,200.00	0	
Total	2	USD \$5,200.00	0	USD \$0.00

The fields are as follows:

Field	Description
Number of Batch Currently Open	The number of the batch that is currently open.
Merchant ID	The merchant's unique alphanumeric identifier. There is a unique Merchant ID for each merchant account/profile.
Acquirer ID	The unique identifier of the card-processor to which the order was directed for processing.

Transactions by Currency

The transactions are grouped into sections by the transaction currency.

Field	Description
Card Types	The card types in this summary, for example: <ul style="list-style-type: none"> ▪ JCB ▪ Visa ▪ MasterCard ▪ American Express ▪ Diners ▪ Bankcard ▪ JCB ▪ Discover
Debits Count	The number of debits in the settlement batch.
Total Debits or Debits Amount	The total debit amount in the settlement batch.
Number Credits	The number of credits in the settlement batch.
Total Credits	The total credit amount in the settlement batch.

Batch Closure Receipt Page

The Batch Closure receipt page contains the following details about the batch that was settled using the *Settle Now* button on the **Unsettled Transactions Summary** on page 44 page.

Field	Description
No. of Batch being Closed	The number of the batch that is being closed in this transaction.
Merchant ID	The merchant's unique alphanumeric identifier. There is a unique Merchant ID for each merchant account/profile.
Acquirer ID	The unique identifier of the card-processor to which the order was directed for processing.
	<p>Note: If an acquirer link is configured to have multiple acquirer relationships, then the acquirer link is suffixed with the Bank Merchant ID following a hyphen. For example, ANZ via FDRA — 12345 where "ANZ via FDRA" is the acquirer link and "12345" is the Bank Merchant ID.</p>
Status	The batch status.

Searching for Settlements

To view current or completed settlements:

- 1 Click *Settlement > Settlement Search* . The **Settlement Search** on page 46 page displays.
- 2 Enter the search criteria for the type of settlements to locate.
- 3 Click the **[Submit]** button. The **Settlement List** on page 46 page displays.
- 4 To view a particular batch, select the batch number. The **Settlement Details** on page 47 page displays the details of the settlement.

Settlement Search Page

Specify your search by using the fields to enter the search parameters. Click **[Submit]** to start the search.

The available search parameters are:

Field	Description
From/To	Search for orders within a date range. If you clear the From field, all transactions up to the current date are displayed. The default From and To Dates are at the date of the users local time zone.
Batch Number	Select settlements belonging to a particular batch.
Settlement Result	Select settlements according to result: <ul style="list-style-type: none"> ▪ All Settlement responses ▪ Successful Settlements ▪ Pending Settlements ▪ Failed Settlements
Acquirer ID	Search for orders processed by a particular acquirer (for example, Mastercard NAB).

Settlement List - Settled Batches

This page lists the details of the settled batches.

Field	Description
Acquirer ID	The unique identifier of the card-processor to which the order was directed for processing.
Settlement Batch Number	The identifier for the batch to which the transactions belong.
Settlement Date and time	The date on which the batch was settled. or The date and time on which the batch was settled.
Debits Count	The number of debits in the settled batch.
Credits Count	The number of credits in the settled batch.

Settlement Details Page

The Settlement Details page consists of two sections, Merchant and Acquirer Details and Merchant and Acquirer Details Comparison. The transactions in the Merchant and Acquirer Details Comparison section are grouped by currencies.

Merchant and Acquirer Settlement Details

Field	Description
Merchant ID	The merchant's unique alphanumeric identifier. There is a unique Merchant ID for each merchant account/profile.
Acquirer ID	The unique identifier of the card-processor to which the order was directed for processing.
	Note: If an acquirer link is configured to have multiple acquirer relationships, then the acquirer link is suffixed with the Bank Merchant ID following a hyphen. For example, ANZ via FDRA — 12345 where "ANZ via FDRA" is the acquirer link and "12345" is the Bank Merchant ID.
Settlement Batch Number	The identifier for the batch to which the transactions belong.
Submission Date	The date on which the settlement occurred.
Settlement Response	The response received back from the acquirer.
Payment Method	The method of funds transfer used for the transaction. For example, Credit.

Merchant and Acquirer Settlement Details Comparison

Field	Description
Currency	The currency used for the transaction.
Debits Count	The number of debits in the settlement batch.
Total Debits or Debits Amount	The total debit amount in the settlement batch.
Number Credits	The number of credits in the settlement batch.
Total Credits	The total credit amount in the settlement batch.

CHAPTER 5

Financial Transactions

Financial Transactions represent the flow of information between the cardholder, the merchant and the acquirer when purchasing goods and services. They include transactions for purchasing goods immediately, authorizing and billing goods on order, and performing refunds when necessary.

Searching for Financial Transactions

To locate a financial transaction, use the search options of Merchant Administration.

To search for a financial transaction:

- 1 From the Main menu, select *Search > Financial Transaction Search*. The Merchant Administration Financial Transaction Search page displays.
- 2 Enter the search parameters. If you enter multiple search parameters, the records returned will match all the search criteria.
- 3 Click the **[Submit]** button. The ***Financial Transactions List*** on page 51 page displays.
- 4 Select an individual Transaction ID to view its details. The ***Financial Transaction Details page*** on page 52 displays.

Financial Transactions Search Page

Use the fields on the Financial Transaction Search page to enter the search parameters.

The search parameters are as follows:

Field	Description
From/To	Search for orders within a date range. If you clear the From field, all transactions up to the current date are displayed. The default From and To Dates are at the date of the users local time zone.
Transaction Number	Select a transaction by its system generated unique identifier for the financial transaction. This identifier is unique within the merchant.
Batch Number	Select transactions belonging to a particular batch.
RRN	The RRN (Reference Retrieval Number) allows the Acquirer to uniquely identify a transaction.
Merchant Transaction Reference	A unique merchant specific identifier used in Payment Client transactions.
Transaction Type	Search for transactions of a particular type, for example: <ul style="list-style-type: none"> ▪ All ▪ Authorisation ▪ Capture ▪ Refund ▪ Void Refund ▪ Void Capture
Payment Method	Search for transactions according to the payment method. Valid values are: <ul style="list-style-type: none"> ▪ Credit ▪ PayPal
Acquirer ID	Search for orders processed by a particular acquirer (for example, Mastercard NAB).
Currency	Search for orders processed by a particular currency or all currencies.
Transaction Success	Search for orders having a specific success status (for example, successful, failed, or referred).
Authentication Type	Search for a particular type of 3DS authentication. Click the drop down arrow and select an authentication type from the list, or leave the default entry to display all authentication types. The available types of authentication are: <ul style="list-style-type: none"> ▪ IGNORE ▪ All Authenticated Transactions ▪ All Non-Authenticated Transactions ▪ Verified by Visa ▪ MasterCard SecureCode ▪ JCB J/Secure ▪ American Express SafeKey

Authentication State	<p>Search for transactions with a particular authentication status. Click the drop down arrow and select an authentication status from the list, or leave the default entry to display all authentication status. The available types of authentication status are:</p> <ul style="list-style-type: none"> ▪ IGNORE ▪ All Authenticated Transactions ▪ All Non-Authenticated Transactions ▪ Authenticated Transactions – Successful ▪ Authenticated Transactions – Failed ▪ Authenticated Transactions – Undetermined ▪ Authenticated Transactions – Not Enrolled
Number of Results to Display on Each Result Page	<p>Enter the number of rows of search results that you wish to see on a single page. Leave this field blank for the default number of search results to be displayed.</p>

Click **[Submit]** to start the search. The Financial Transactions List page displays.

Viewing the Financial Transactions List

To view financial transactions, use the search methods described in Searching for Financial Transactions.

The Financial Transaction List page details the following information for each transaction:

Field	Description
Acquirer ID	The unique identifier of the card-processor to which the order was directed for processing.
Transaction Number	An automatically generated number uniquely identifying the transaction. This identifier is unique within the merchant.
Merchant Transaction Reference	A unique merchant specific identifier used in Payment Client transactions.
Transaction Type	The type of transaction performed. An example may be: <ul style="list-style-type: none"> ▪ Authorisation ▪ Capture ▪ Refund.
Amount	The total amount of the order in the transaction currency. For example, AUD \$100.00.
Date	The user-locale date and time at which the order was created.
Response Code	A code and brief description summarizing the result of attempting to process the order. Example response codes are: <ul style="list-style-type: none"> ▪ '0 - Approved' ▪ '3 - Timed Out'

Click an individual *Financial Transaction ID* to view its details. The ***Financial Transaction Details*** on page 52 page displays.

Viewing an Individual Financial Transaction

After the *list of financial transactions* on page 51 displays, you can click an individual Financial Transaction ID to view its details. The Financial Transaction Details page displays all the details of an individual financial transaction.

The fields displayed are as follows:

Acquirer ID	The unique identifier of the card-processor to which the order was directed for processing.
	<p>Note: If an acquirer link is configured to have multiple acquirer relationships, then the acquirer link is suffixed with the Bank Merchant ID following a hyphen. For example, ANZ via FDRA — 12345 where "ANZ via FDRA" is the acquirer link and "12345" is the Bank Merchant ID.</p>
Transaction Number	An automatically generated number uniquely identifying the transaction. This identifier is unique within the merchant.
Merchant Transaction Reference	A unique merchant specific identifier used in Payment Client transactions.
Date	The user-locale date and time at which the order was created.
Transaction Type	The type of transaction performed. An example may be: <ul style="list-style-type: none"> ▪ Authorisation ▪ Capture ▪ Refund.
Payment Method or Payment Types	The account type: <ul style="list-style-type: none"> ▪ Credit Card.
Amount	The total amount of the order in the transaction currency. For example, AUD \$100.00.
Order ID	A unique number used to identify an order.
Settlement Batch Number	The identifier for the batch to which the transactions belong.
RRN	The Retrieval Reference Number, which helps the Acquirer to identify a transaction that occurred on a particular day.
Response Code	A code and brief description summarizing the result of attempting to process the order. Example response codes are: <ul style="list-style-type: none"> ▪ '0 - Approved' ▪ '3 - Timed Out'
Acquirer Response Code	The response code from the acquirer indicating success or otherwise of the transaction.
Authorisation Code	An identifier returned by the card-issuer indicating the result of the authorisation component of the order.

Integration Type	<p>The means by which the merchant accesses the Payment Server. The available integration types are:</p> <ul style="list-style-type: none"> ▪ PC (Payment Client) ▪ VPC (Virtual Payment Client) ▪ MA (Merchant Administration) ▪ API:REST (JSON) ▪ API:NVP ▪ BATCH:NATIVE
Integration Type Version	<p>The version of the software used to integrate to the Payment Server.</p> <hr/> <p>Note: This field is displayed only if the Integration Type is PC or VPC.</p>
Transaction Source	<p>Indicates the integration facility used to generate the transaction. Typical transaction sources include:</p> <ul style="list-style-type: none"> ▪ PC — the transaction source is Payment Client. ▪ MOTO — the transaction source is Merchant Administration. ▪ Direct — the transaction source is Web Services API. ▪ Batch — the transaction source is Batch. ▪ Auto (Risk) — the transaction source is risk assessment. For example, an order on which a financial transaction is performed is rejected due to risk assessment it is automatically attempted for a reversal by the system. ▪ Auto — the transaction source is system. Auto indicates that the system initiated the transaction automatically. For example, an automatically-triggered Capture transaction when a Purchase transaction is submitted by a merchant for a processor that only supports Auth/Capture. ▪ Risk Override — the transaction source is a request to override a Reject risk recommendation for a transaction that has been assessed by external risk. <hr/> <p>Note: The following fields are displayed only if the transaction was processed using a Corporate Purchase Card. Charge Description 1-4 are displayed for an American Express Corporate Purchase Card only.</p>
Tax Amount	The local tax amount in base currency units. It must not be greater than the total authorised amount. It is provided by the merchant.
Tax Reference Number	If applicable, a tax reference value associated with the transaction.
Customer Reference Number	The cardholder's reference number, for example their purchase order number.
Charge Description 1	Optional free form text field used to describe the nature of the charge associated with the order.
Charge Description 2	Optional free form text field used to provide further information about the charge associated with the order.
Charge Description 3	Optional free form text field.
Charge Description 4	Optional free form text field.

The following fields are displayed if airline data is passed in the transaction. You may not see all the fields listed here, depending on the charge type and the acquirer used to process the transaction.

Note: Click **More** to view more details about the field, and click **Less** to collapse the details.

Booking Reference	The record locator used to access a specific Passenger Name Record (PNR). PNR is a record in the database of a booking system that contains the itinerary for a passenger, or a group of passengers traveling together. Data may consist of a combination of numeric and alphabetic characters.
Document Type	The type of charge associated with the transaction. For example, passenger ticket, excess baggage, animal transportation charge, etc.

Note: Itinerary may include data on one or more travel legs, and the list number indicates the index for that leg.

Itinerary: Leg: Carrier Code	The 2-character IATA airline code of the airline carrier for the trip leg.
Itinerary: Leg: Conjunction Ticket Number	The ticket containing the coupon for this leg for an itinerary with more than four trip legs.
Itinerary: Leg: Coupon Number	The coupon number on the ticket for the trip leg. Each trip leg requires a separate coupon. The coupon within the series is identified by the coupon number.
Itinerary: Leg: Departure Airport	The 3 character IATA airport code of the departure airport for the trip leg.
Itinerary: Leg: Departure Date	Date of departure for the trip leg.
Itinerary: Leg: Departure Tax	Tax payable on departure for the trip leg.
Itinerary: Leg: Departure Time	Departure time in local time for the departure airport for this trip leg.
Itinerary: Leg: Destination Airport	The 3 character IATA airport code for the destination airport for the trip leg.
Itinerary: Leg: Destination Arrival Time	Arrival time in local time for the destination airport for this trip leg.
Itinerary: Leg: Endorsements Restrictions	Restrictions (e.g. non-refundable) or endorsements applicable to the trip leg.
Itinerary: Leg: Exchange Ticket Number	New ticket number issued when a ticket is exchanged for the trip leg.
Itinerary: Leg: Fare	Total fare payable for the trip leg.
Itinerary: Leg: Fare Basis	Code defining the rules forming the basis of the fare (type of fare, class entitlement, etc.)
Itinerary: Leg: Fees	Total fees payable for the trip leg.
Itinerary: Leg: Flight Number	The flight number for the trip leg.
Itinerary: Leg: Stop Over Permitted	Indicates if a stopover is permitted for the trip leg.
Itinerary: Leg: Taxes	Total taxes payable for the trip leg.
Itinerary: Leg: Travel Class	The industry code indicating the class of service (e.g. Business, Coach) for the leg.
Itinerary: Number In Party	Number of passengers associated with this booking.
Itinerary: Origin Country	The 3 character ISO 3166-1 alpha-3 country code of the country of origin for the itinerary.

Note: The booking may include data on one or more passengers, and the list number indicates the index for that passenger.

Passenger: First Name	First name of the passenger to whom the ticket is being issued.
Passenger: Last Name	Last name of the passenger to whom the ticket is being issued.
Passenger: Middle Name	Middle name of the passenger to whom the ticket is being issued.
Passenger: Specific Information	Passenger specific information recorded on the ticket.
Passenger: Title	Title of the passenger to whom the ticket is being issued.
Plan Number	Plan number supplied by the airline for this booking.
Ticket: Conjunction Ticket Indicator	Indicates if a conjunction ticket with additional coupons was issued. Conjunction ticket refers to two or more tickets concurrently issued to a passenger and which together constitute a single contract of carriage.
Ticket: Customer Reference	Information supplied by the customer. For example, Frequent Flyer number.
Ticket: eTicket	Indicates if an electronic ticket was issued.
Ticket: Exchanged Ticket Number	The original ticket number when this is a transaction for an exchanged ticket.
Ticket: Issue: Address	The address where the ticket was issued.
Ticket: Issue: Carrier Code	The 2-character IATA airline code of the airline carrier issuing the ticket.
Ticket: Issue: Carrier Name	Name of airline carrier issuing the ticket.
Ticket: Issue: City	The city/town where the ticket was issued.
Ticket: Issue: Country	The 3 character ISO 3166-1 alpha-3 country code of the country where the ticket was issued.
Ticket: Issue: Date	The date the ticket was issued.
Ticket: Issue: Travel Agent Code	Industry code of the travel agent issuing the ticket.
Ticket: Issue: Travel Agent Name	Name of the travel agent issuing the ticket.
Ticket: Restricted	Indicates if the issued ticket is refundable.
Ticket: Ticket Number	The airline ticket number associated with the transaction.
Ticket: Total Fare	Total fare for all trip legs on the ticket.
Ticket: Total Fees	Total fee for all trip legs on the ticket.
Ticket: Total Taxes	Total taxes for all trip legs on the ticket.
Transaction Type	The type of transaction performed against this airline booking.

Downloading the Transactions File

To use the download transaction information functionality, you must have been set up to do so by Transaction Network Services'.

The **[Download]** button on Financial Transactions Search, or Download Search Results link on the **Financial Transaction List** on page 51, allows you to download transaction information in a text or csv file. The file contains the orders with all the associated Financial Transaction data for the search criteria entered.

The format of the file is a Comma Separated Value file and ends with the extension .csv. This format is used to transfer data from one application to another. Most database systems can import and export comma-separated value files, which can be used in any spreadsheet program.

To download transaction information you must first enter your search criteria in the Financial Transaction Search page.

Note: If you are configured to download financial transactions in the multi-currency format, the Currency column is replaced by the Currency Code column, which displays the currency code instead of the currency symbol. An additional column for Bank Merchant ID/ SE Number is also displayed.

Downloading Transaction Files

- 1 From the Financial Transactions Search page, after you have entered the search criteria, click the **[Download]** button.
- 2 A dialog box displays, prompting you to choose whether you would like to open or save the file.
- 3 Click the required button and follow the prompts.
- 4 If you choose to *Save to Disk*, you can change the file name and select a location to save the file.
- 5 Or, if you choose to *Open* the file, for example, using Excel (the default option), the file opens in Excel.

Note: Ensure that you take necessary security measures to protect the data downloaded on to your computer.

CHAPTER 6

Payment Authentications

Verified by Visa™ (Visa 3-Domain Secure), MasterCard SecureCode™ (MasterCard 3-Domain Secure) and J-Secure Schemes, are Payment Authentications designed to stop credit card fraud by authenticating cardholders when performing transactions over the Internet.

Merchant Administration allows you to search for payment authentications and view the results.

Payment Authentication Information Flow

A payment authentication is performed immediately before a merchant performs an authorisation or purchase. Authenticating ensures that the card is being used by its legitimate owner. During a transaction, authentication allows a merchant to confirm the identity of the cardholder by redirecting them to their card-issuer where they enter a password that they had previously registered with their card issuer.

The cardholder must have registered their card and password with the issuing bank before they can use the authentication scheme.

The cardholder's browser acts as a path to transport messages between the web application, the Payment Server and the card-issuing bank's Access Control Server (ACS).

The following is the flow of information between all the parties in a payment authentication.

- 1 If the merchant collects the cardholder's details, the cardholder enters their card details into the merchant application payment page and submits the order, and their browser is redirected to the Payment Server.
If the Payment Server collects the cardholder's card details, the cardholder will now enter their card details on the payments page provided by the Payment Server.
- 2 The Payment Server determines if the card is enrolled in the Payment Authentications scheme by checking the card scheme database.

If the cardholder's card is registered in the scheme, the Payment Server redirects the cardholder's browser to the ACS site for authentication.
If the card is not enrolled, steps 3, 4 and 5 (below) are skipped, and the Payment Server continues processing the transaction.
- 3 The ACS displays the cardholder's secret message and the cardholder enters their response (password), which is checked with the Card Issuer database.
- 4 The cardholder is redirected back to the Payment Server and the card issuer sends an authentication message indicating whether or not the cardholder's password matched the message in the database.
- 5 The Payment Server continues processing the transaction.

Note: If the merchant profile has 3DS Blocking enabled, and the transaction fails authentication, the Payment Server will not continue to process the transaction, and the details of the transaction will not be saved.

- 6 The cardholder is redirected to the merchant, where the receipt is passed back to the cardholder.

Payment Authentications Status

Merchant Administration provides you with a record of every attempt at authentication by your cardholders.

The status of payment authentications are the values returned for every attempted authentication, showing, for example, whether the authentication passed or failed.

During the authentication process, while a cardholder is being authenticated, the merchant will see a status value of T. This changes to a value of "Y-Success" if the authentication is successful. The cardholder is then redirected to the payment section of the transaction.

If however, the cardholder cancelled the transaction in the authentication stage, then the value T is displayed in the merchant's records.

If the cardholder is enrolled but is not authenticated correctly, for example, because the customer may have entered their password incorrectly 3 times, then the value F is displayed to indicate that the cardholder failed the authentication process.

If the cardholder is not enrolled, the transaction is processed without the cardholder being redirected to be authenticated, but a value is returned to show that the cardholder was not enrolled.

Searching for Payment Authentications

The Payment authentication search page provides ways to select a single or set of payment authentications to view the results of the authentication.

To search for a payment authentication:

- 1 Select *Search* from the Main menu.
- 2 Select *Payment Authentications Selection* from the submenu. The Merchant Administration Payment Authentication Search page displays.
- 3 Enter your search parameters. If you enter multiple search parameters, the records returned will match all the search criteria.
- 4 After you have entered your search criteria you can view the results of your search on the next page.

Payment Authentications Search Page

Use the fields on the Payment Authentications Search page to find the required payment authentications.

The search parameters are as follows:

Field	Description
Merchant ID	Enter a Merchant ID or click the [Search] link to use the Merchant Search page.
From/To	Search for orders within a date range. If you clear the From field, all transactions up to the current date are displayed. The default From and To Dates are at the date of the users local time zone.
Authentication ID	Search for an order with a particular authentication ID.
Order Reference	Search for orders created with specific Order Reference text.
Currency	Search for orders processed by a particular currency or all currencies.
Authentication Type	Search for a particular type of 3DS authentication. Click the drop down arrow and select an authentication type from the list, or leave the default entry to display all authentication types. The options may include: <ul style="list-style-type: none"> ▪ IGNORE ▪ All Authenticated Transactions ▪ All Non-Authenticated Transactions ▪ MasterCard SecureCode ▪ Verified By Visa ▪ JCB J/Secure ▪ American Express SafeKey
Authentication State	Search for transactions with a particular authentication status. Click the drop down arrow and select an authentication status from the list, or leave the default entry to display all authentication status. The available types of authentication status are: <ul style="list-style-type: none"> ▪ IGNORE ▪ All Authenticated Transactions ▪ All Non-Authenticated Transactions ▪ Authenticated Transactions – Successful ▪ Authenticated Transactions – Failed ▪ Authenticated Transactions – Undetermined ▪ Authenticated Transactions – Not Enrolled
Number of Results to Display on Each Result Page	Enter the number of rows of search results that you wish to see on a single page. Leave this field blank for the default number of search results to be displayed.

Click the **[Submit]** button to start the search. The Payment Authentication List page displays.

Viewing the Payment Authentications List

To view the results of your search, click the **[Search]** button on the **Payment Authentication** on page 59 page. The results display on the Payment Authentication List page.

The Payment Authentication List page details the following information for each authentication:

Field	Description
Authentication ID	The unique payment authentication ID. Click on the ID to view the authentication details.
Authentication Type	The type of 3DS authentication. The available types of 3DS authentication are: <ul style="list-style-type: none"> ▪ All Authenticated Transactions ▪ All Non-Authenticated Transactions ▪ Verified by Visa ▪ MasterCard SecureCode ▪ JCB J/Secure ▪ American Express SafeKey
Order Reference	A merchant-supplied identifier for the order. This will typically be used by the customer to identify their order (for example, a booking reference number).
Amount	The total amount of the order in the transaction currency. For example, AUD \$100.00.
Date	The user-locale date and time at which the order was created.
Response Code	A code and brief description summarizing the result of attempting to process the order. Example response codes are: <ul style="list-style-type: none"> ▪ '0 - Approved' ▪ '3 - Timed Out'

Viewing an Individual Payment Authentication

To view the details of an individual payment authentication, click an authentication number displayed after a search on the **Payment Authentication** on page 59 page. The Payment Authentication Details page displays.

The Payment Authentication Details page displays the following information for a specific payment authentication.

Note: You may not see all the fields listed here. Depending on prior selections, your privileges and the country of use, some fields may be enabled or disabled.

Field	Description
Authentication ID	The unique payment authentication ID. Click on the ID to view the authentication details.
Date	The user-locale date and time at which the order was created.
Order Reference	This is also known as the Session ID. It is the merchant's unique identifier for each transaction. For example, the order number attached to the Digital Order from the Payment Client.
Card Number	The card number used in the order. Depending on your profile, the format used for displaying card numbers is one of the following: <ul style="list-style-type: none"> ▪ 0.4 Format, for example (xxxxxxxxxxxx1234) ▪ 6.3 Format, for example (654321xxxxxx123) ▪ The full card number is displayed ▪ The card number is not displayed
Amount	The total amount of the order in the transaction currency. For example, AUD \$100.00.
Authentication Type	The type of payment authentication, for example: <ul style="list-style-type: none"> ▪ Verified by Visa (Visa 3-D Secure) ▪ MasterCard SecureCode 3-D Secure ▪ JCB J-Secure ▪ American Express SafeKey

Authentication State	<p>A payment authentication specific field that indicates the status of the payment authentication, for example:</p> <p>Y – Success - The cardholder was successfully authenticated.</p> <p>M – Success - The cardholder is not enrolled, but their card issuer attempted processing.</p> <p>E – Not Enrolled - The cardholder is not enrolled.</p> <p>F – Failed - An error exists in the request format from the Merchant.</p> <p>N – Failed - Verification Failed.</p> <p>U – Undetermined - The verification was unable to be completed. This can be caused by network or system failures.</p> <p>T – Undetermined - The cardholder session timed out and the cardholder's browser never returned from the Issuer site.</p> <p>A – Undetermined - Authentication of Merchant ID and Password to the Directory Failed.</p> <p>D – Undetermined - Error communicating with the Directory Server.</p> <p>C – Undetermined - Card brand not supported.</p> <p>S – Failed - The signature on the response received from the Issuer could not be validated. This should be considered a failure.</p> <p>P – Failed - Error receiving input from Issuer.</p> <p>I – Failed - Internal Error.</p>
	<p>Note: New authentication codes are returned if "Use new 3DS response codes for VPC/PC" privilege is enabled for your merchant profile.</p>
Verification Security Level	<p>The Verification Security Level field shows the VISA ECI or MasterCard SLI or J/Secure value sent in the authorisation message. It is generated either by the Payment Server or your online store depending on your chosen implementation model. It is shown for all transactions except those with authentication status "Failure".</p> <p>These values are:</p> <p>05 - Fully Authenticated</p> <p>06 - Not authenticated (cardholder not participating)</p> <p>07 - Not authenticated (usually due to a system problem or invalid password)</p> <p>The actual value used may differ for some banks.</p>
Verification Token (CAVV)	<p>The Verification Token (CAVV = Cardholder Authentication Verification Value) is a Visa token generated at the card issuer to prove that the Visa cardholder authenticated satisfactorily.</p>
Verification Token (UCAF)	<p>The Verification Token (UCAF =Universal Cardholder Authentication Verification Value) is a MasterCard token generated at the card issuer to prove that the MasterCard cardholder authenticated satisfactorily.</p>
Verification Token (AEVV)	<p>The Verification Token (AEVV = American Express Verification Value) is an American Express token generated at the card issuer to prove that the American Express cardholder authenticated satisfactorily.</p>

3-D Secure VRes.enrolled	This value indicates whether or not the card used was enrolled for 3-D Secure at the time of the transaction. The available values are: Y - Yes N - No U - Undetermined. For example, the payment authentications system was unavailable at the time of the authentication.
3-D Secure XID	The unique identifier returned by the issuer for a successful authentication.
3-D Secure ECI	The 3-D Secure Electronic Commerce Indicator (ECI), as returned from the issuer in response to an authentication request.
3-D Secure PRes.status	Indicates the result of the cardholder authentication. The available values are: Y – Yes N – No A – Attempted Authentication but failed. For example the cardholder failed to enter their password after three attempts. U – Undetermined. The payment authentications system was unavailable at the time of the authentication.
Time taken (milliseconds)	A payment authentication specific field which indicates the time taken (in milliseconds) for the payment authentication.
Transaction Number	An automatically generated number uniquely identifying the transaction. This identifier is unique within the merchant.

Note: The following extended response fields are displayed only if an error message is returned from the Directory Server (DS) or Access Control Server (ACS).

Source	The source of the following fields. For example, ACS, DS.
Message Type	IREQ (Invalid Request Response) or Error
Error Message Version	The version of the message as returned by the ACS/DS
Error Code	The error code as returned by the ACS/DS
Error Detail	Detail message as returned by the ACS/DS
Vendor Code	Vendor code for the ACS/DS.
Error Description	Description of the error, as returned by the ACS/DS.

Downloading Payment Authentication Information

To use the download transaction information functionality, you must have been set up to do so by Transaction Network Services'.

The **[Download]** button on *Payment Authentications Search* on page 60, or Download Search Results link on the *Payment Authentications List* on page 61, allows you to download transaction information in a text or csv file. The file contains the orders with all the associated Payment Authentication data for the search criteria entered.

The format of the file is a Comma Separated Value file and ends with the extension .csv. This format is used to transfer data from one application to another. Most database systems can import and export comma-separated value files, which can be used in any spreadsheet program.

To download transaction information you must first enter your search criteria in the *Payment Authentications Search* on page 60 page.

Note: If you choose to download payment authentication information in the multi-currency format, the Currency column displays the currency code instead of the currency symbol. An additional column for Bank Merchant ID/ SE Number is also displayed.

Downloading Transaction Files

- 1 From the Financial Transactions Search page, after you have entered the search criteria, click the **[Download]** button.
- 2 A dialog box displays, prompting you to choose whether you would like to open or save the file.
- 3 Click the required button and follow the prompts.
- 4 If you choose to *Save to Disk*, you can change the file name and select a location to save the file.
- 5 Or, if you choose to *Open* the file, for example, using Excel (the default option), the file opens in Excel.

Note: Ensure that you take necessary security measures to protect the data downloaded on to your computer.

CHAPTER 7

Reports

A range of reports are available depending on the merchant operator's privileges.

Gateway Reports

Gateway reports display the details of all merchant's transactions that have been processed by the Payment Server. It allows you to search for and list the transaction details by date, transaction mode (test or production), time interval (daily, weekly, monthly) and currency.

To search for a Gateway report:

- 1 From the Main menu, select *Reports > Gateway Reports*. The Gateway Reports display.
- 2 Enter your *search parameters*.
If you enter more than one parameter the records returned match all your search criteria.
- 3 Click the **[Submit]** button. The Gateway Report Details page displays.

Gateway Report Search Page

Use the fields on the Gateway Report page to enter the search parameters for your order search.

The search parameters are as follows:

Field	Description
From/To	Search for orders within a date range. If you clear the From field, all transactions up to the current date are displayed. The default From and To Dates are at the date of the users local time zone.
Time Interval	The time span that the transactions occurred for example: <ul style="list-style-type: none"> ▪ Daily ▪ Weekly ▪ Monthly ▪ Yearly. If a two week period is entered with a daily time interval, 14 daily report totals are displayed.
Acquirer ID	Search for orders processed by a particular acquirer (for example, Mastercard NAB).
Currency	Search for orders processed by a particular currency or all currencies.

Viewing a Gateway Report

A Gateway Report is grouped into sections by transaction currency and the payment method. Each row of the list provides aggregated details for transactions processed by a specific acquirer, using a specific currency, and occurring in a specific period. The size of the period is determined by the Time Interval selected on the Gateway Report Search page.

Note: A merchant may have multiple merchant acquirer relationships with the same acquirer.

Gateway Daily Reports								
Payment Method: Credit			Currency: USD					
Date	Acquirer	Merchant	No. Transactions	No. Settlements	Total Authorisations	Total Captures	Total Purchases	Total Refunds
4/1/11	Amex	TESTUSDONLY	1	0	USD \$10.00	USD \$0.00	USD \$0.00	USD \$0.00
Total:			0	0	USD \$10.00	USD \$0.00	USD \$0.00	USD \$0.00

Each row of the list specifies the details described in the following table.

Field	Description
Date	The start date of the period for which transactions are aggregated.
Acquirer	The name of the acquirer who processed the transactions.
Merchant ID	The merchant's unique alphanumeric identifier. There is a unique Merchant ID for each merchant account/profile.
No. Transactions	The number of transactions processed by the acquirer, in a given currency, during the reporting period.
No. Settlements	The number of transactions that were settled during the reporting period.
Total Authorisations	The total amount (specified using the currency and the currency symbol) of authorisations, less any voids or refunds in, the reported transactions.
Total Captures	The total amount (specified using the currency and the currency symbol) of captures, less any voids or refunds, in the reported transactions.
Total Purchases	The total amount (specified using the currency and the currency symbol) of purchases, less any voids or refunds, in the reported transactions.
Total Refunds	The total amount (specified using the currency and the currency symbol) of refunds in the reported transactions.

CHAPTER 8

Admin

The Admin option allows you to:

- Modify your configuration settings.
- Create, modify, and delete Operator details.
- Change your password.
- Download software.

Configuring Your Settings

How to configure your merchant settings

- 1 Select '*Admin*' from the Main menu.
- 2 Select '*Configuration Details*' from the submenu.
- 3 Click the **[Edit]** button.
- 4 Make changes as required and click the **[Submit]** button.
- 5 The message 'Configuration Changes Saved' is displayed on the Configuration Details screen and details redisplayed with changed information.

Configuration Details

The Configuration Details page allows you to view or edit some details of your configuration.

Configuration Details Definitions

Field	Description
Merchant Name	The merchant's registered business, trading or organization name.
Merchant ID	The merchant's unique alphanumeric identifier. There is a unique Merchant ID for each merchant account/profile.

Note: You cannot change the *Merchant Name* and *Merchant ID*. Should you require any changes to these fields, please contact your MSO.

International Definitions

The Internationalization section on the Configuration Details screen contains the following information:

Field	Description
Locale	The default language displayed in Merchant Administration unless overridden by the Operator.
Time Zone	The user's Time Zone. This is the local time on all merchant transactions unless overridden by the Operator.

Note: You cannot change these fields. Should you require any changes to these fields, please contact your MSO.

Configuration Details - Virtual Payment Client

Field	Description
Access Code	The access code is an identifier that is used to authenticate the merchant for Virtual Payment Client transactions. The access code is generated automatically when the merchant is granted the privilege to use the Virtual Payment Client.
Secure Hash Secret	The secure hash is generated automatically and assigned to you when you were granted the Virtual Payment Client privilege. It is unique for each merchant and you must always have at least one secure hash secret but may have up to two secure hash secrets. The secure hash is only relevant to 3-party Virtual Payment Client transactions, as the transaction is sent to the Payment Server using the cardholder's browser and the response is returned to your website using the cardholder's browser, the Secure Hash Secret is used to prevent a cardholder from trying to change the transaction details. The Secure Hash Secret is made up of alphanumeric characters which are appended to the transaction.
3-Party Return URL	The default return web address when using the Virtual Payment Client interface. The cardholder is returned to this URL at the completion of the transaction, where the merchant initiated the payment via the Virtual Payment Client without specifying a return URL. The Return URL must start with either http:// or https://and may be up to 255 characters.

Configuration Details - Payment Client

The Payment Client section on the Configuration Details page displays and allows you to edit configuration information associated with the use of the Payment Client interface.

Field	Description
Client 3-Party Return URL	<p>The default return web address for the Payment Client interface. The cardholder is returned to this URL at the completion of the transaction when the merchant initiated the payment using the Payment Client without specifying a return URL. It can be a complete URL that defines the exact location of the receipt page, or it can be a partial URL that starts with HTTP or HTTPS and defines the machine where the receipt file is located. The complete URL for defining the receipt page can be a combination of both components, the Merchant Administration component and the ReturnURL component in the digital order. When setting the web return address you can either:</p> <ul style="list-style-type: none"> ▪ Enter the complete URL in Merchant Administration. ▪ Enter the complete URL in the digital order. ▪ Enter part of the URL in Merchant Administration and the remaining part in the Digital Order. <p>Note: If the ReturnURL in the Digital Order starts with either HTTP or HTTPS, it overwrites any return URL that you enter in Merchant Administration. If you use the ReturnURL in the Digital Order, you do not need to provide a ReturnURL in Merchant Administration.</p>

Editing Your Configuration Settings

How to edit your configuration settings

- 1 Select '*Admin*' from the Main menu.
- 2 Select '*Configuration Details*' from the submenu.
- 3 Click the **[Edit]** button.
- 4 Some of the fields can be changed. Enter changes in the fields that permit changes and click the **[Submit]** button.
- 5 The ***Configuration Details*** on page 69 screen re-displays with the changed information.

Editing Merchant Configuration - Virtual Payment Client

On the Configuration Editor page, you can edit the following for the Virtual Payment Client:

- **Secure Hash Secret** on page 72
- **3- Party Return URL** on page 72

Note: Only the Secure Hash Secret and return URL can be edited. The Access Code cannot be edited. You can have a maximum of two secrets and a minimum of one.

To Add a Secure Hash Secret

To add a secure hash secret on the Configuration Editor page:

- 1 Click the **[Add]** button. The page refreshes and a second secure hash secret is added. There are now two secure hash secrets displayed on the page with a delete button next to each secret.
- 2 Click the **[Submit]** button. The Configuration Details page re-displays, with the updated information.

To Delete a Secure Secret Hash

On the **Configuration Editor** on page 72 page:

- 1 Click the **[Delete]** button to the right of the Secure Secret Hash that you want to permanently remove.
- 2 The page refreshes and the Secure Hash Secret is deleted to display the remaining secret with an add button next to it. If the first secret is deleted then what was previously the second secret becomes secret one.
- 3 Click the **[Submit]** button. The Configuration Details page re-displays, with the updated information.

To Edit ReturnURL

On the **Configuration Editor** on page 72 page:

- 1 Enter a URL in the Return URL field.
- 2 Click the **[Cancel]** button to undo any changes that you have just made, otherwise click the **[Submit]** button. The Configuration Details page re-displays, with the updated information.

Editing the Payment Client

On the Configuration Editor page:

- 1 Enter a URL in the *Client 3- Party Return URL* field.
- 2 Click the **[Submit]** button. The Configuration Details page displays with the changed information.

Managing Merchant Administration Operators

Merchant Administration allows you to create, modify, enable, and delete an Operator's details. Before you can perform these functions you must have the user privilege *Perform Operator Administration*. This is done in the Operator Details page from the *Admin* menu.

You can create and edit Merchant Administration Operators.

To manage Operators:

- 1 From the Main menu, select *Admin > Operators*. The Merchant Administration Operator List page displays.
- 2 You can choose to either create an Operator, edit an Operator, change an existing Operator's password, or delete an Operator.

Note: This page displays a list of all existing Merchant Administration Operators.

Types of Operators

There are three types of Operator:

- **Web-based Operators** - these are Operators who perform Administration functions using the Merchant Administration web interface as described in this guide.
- **Primary Operator** - When your merchant profile is created, a primary Operator (Administrator) is also created. This Operator is allocated privileges to create, modify and delete other Operators. This Operator can also be modified and viewed, but not deleted.
- **Payment Client Operators** - these are Operators who perform Administration functions using the Payment Client. This Operator must have the user privilege *Advanced Merchant Administration*. Advanced Merchant Administration uses the Payment Client to directly access the Payment Server to perform all transaction-related actions integrated with a merchant's own payment software interfaces. Information on how to integrate Advanced Merchant Administration with your software application is given in the Payment Client Integration Guide.

Note: An Operator with *Advanced Merchant Administration* privilege selected will not be able to log in to Merchant Administration.

Creating a New Merchant Administration Operator

To create a new Merchant Administration Operator:

- 1 From the Main menu, select *Admin > Operators*. The Merchant Administration Operator List page displays.
- 2 Select *Create a new Merchant Administrator Operator*. The **Merchant Administration Operator Details** on page 74 page displays.
It consists of sections for recording details, security and transaction privileges for new Operators.
- 3 Enter the details as required.
- 4 Click the **[Submit]** button.
- 5 The Merchant Administration Operator List re-displays and includes the new Operator.

Merchant Administration Operator Details page

To create a new Merchant Administration operator, fill in the following fields.

Mandatory fields on the screen are indicated by a red asterisk.

Operator Details

Field	Description
Merchant ID	The merchant's unique alphanumeric identifier. There is a unique Merchant ID for each merchant account/profile.
Operator ID	The unique identifier of the merchant Operator.
Operator Name	The name of the Operator.
Description	Extra description of the user (for example, job title, department or level of privileges allocated).
Email Address	The Operator's email address. If Password Reset functionality is supported by your MSO, then a temporary password is sent to this email address when the Operator uses the Forgot Password link on the Login screen to request a password reset.
Password	The password must be at least eight characters long and contain at least one alphabetical character and numeric character. The password is case sensitive.
Confirm Password	Enter the password again in this field for confirmation when adding a new password or changing an existing one.
Locale	The default language displayed in Merchant Administration unless overridden by the Operator.
Time Zone	The user's Time Zone. This is the local time on all merchant transactions unless overridden by the Operator.

Security

Field	Description
Lock Operator Account	Allows an Operator with administration privileges to lock out an Operator. The locked out operator will be unable to log on to Merchant Administration until an Operator with administration privileges clears the check box to re-enable the Operator. For an Operator with "Enable Advanced Merchant Administration Features" privilege, this check box is automatically selected as a result of five failed login attempts. Note: If Password Reset functionality is supported by your MSO, then selecting this check box will prevent the Operator from using the Forgot Password link on the Login screen to request a password reset.
Must Change Password at Next Login	If selected, the next time an Operator logs in they are required to change their password.
Password never expires	If selected, an Operator's password will not expire. If cleared, the password shall expire at the end of the default period.

Change Their Own Password	The Operator is allowed to change their own password. Note: If Password Reset functionality is supported by your MSO, then enabling this privilege will allow the Operator to use the Forgot Password link on the Login screen to request a password reset.
Password Reset Required	Indicates if password reset is required. This field is set to "Yes" after five failed login attempts else set to "No". You may request a password reset using the Forgot Password link on the Merchant Administration log-in screen provided you have "Change Their Own Password" privilege or contact the Administrator for a password reset. For information on how to reset an Operator's password, see Changing an Operator's Password on page 79.

Transactions

Field	Description
Perform MOTO Transactions	Allows the operator to create orders in Merchant Administration and allows user to mark orders as complete.
Perform Verification Only	Allows the operator to perform address verification on cardholders.
Perform Captures	Allows the operator to perform captures and allows user to mark orders as complete.
Perform Stand Alone Captures	Allows the operator to perform captures for orders authorised manually, or in an external system.
Perform Bulk Captures	Allows the operator to perform a capture against a set of selected orders.
Perform Refunds	Allows the operator to give refunds. A refund is the transfer of funds from a merchant to a card holder.

Merchant Maintenance

Field	Description
Modify the merchant configuration	Allows the operator to edit the merchant's configuration details.
Perform operator administration	Allows the operator to create, edit and delete other Operator's details. If Password Reset functionality is supported by your MSO, then enabling this privilege will prevent the Operator from using the Forgot Password link on the Login screen to request a password reset.

General Privileges

Field	Description
Perform Settlements	Operator may perform settlements.
Perform actions with a supervisor's password	This is a supervisor override. An operator who does not have the privileges to perform actions, such as purchases, refunds and voids, may still perform actions if they have this privilege. The supervisor's username and password may be used to perform actions available on the Order Details page. A Supervisor is any Operator who has the user privileges to perform the required actions.
View Gateway Reports	Operator can view Gateway Reports.
Advanced Merchant Administration	Allows the merchant to perform administration functions through an interface with the Payment Client. The merchant can access the Payment Gateway to directly perform all transaction-related actions (for example, voids, purchases, and refunds) integrated with merchants' software interfaces, rather than using the portal. Note: If this privilege is selected for a Merchant Administration Operator, the operator will not be able to use Merchant Administration or use the Forgot Password link on the Login screen to request a password reset. The latter is only applicable if the Password Reset functionality is supported by your MSO.
Download Transaction Search Results	Allows the Operator to download transaction information in a text file. The file contains the orders with all the associated Financial Transactions and Payment Authentication Transaction data. The format of the file is a Comma Separated Value file and ends with the extension .csv. This format is used to transfer data from one application to another. Most database systems can import and export comma-separated value files, which can be used in any spreadsheet program.
Allow Payment Client Download	Allows you to download the Payment Client software.
Allow Software Download	Allows the merchant to download software and documentation from the Payment Server. For example, the merchant may need to download the Payment Client. Note: This privilege is a prerequisite to the Payment Client Download and Documentation Download privileges.
Allow Merchant Administration Documentation Download	Allows the operator to download documentation from Merchant Administration portal.
Enable Translation Portal	Allows the Operator to use the translation portal to change the language of the interface
Permit Site Resource Bundle Translation	Allows the merchant to use the translation portal for a site.
Permit Merchant Group Resource Bundle Translation	Allows the merchant to use the translation portal for a merchant group.
Permit MSO Group Resource Bundle Translation	Allows the merchant to use the translation portal for a MSO group.
Permit MSO Resource Bundle Translation	Allows the merchant to use the translation portal for a MSO.
View Settlement Pages	Allows the merchant to view batch settlement details.
Initiate Manual Batch Closure	Allows the merchant to trigger settlement for a batch.

May Configure Risk Rules	Allows the Operator to configure risk rules for a merchant. See Using External Risk Only section to learn how to define operator privileges for use with Interceptas.
May Perform Risk Assessment Review	Allows the Operator to make a decision on whether to accept or reject an order based on the risk assessment results. See Using External Risk Only section to learn how to define operator privileges for use with Interceptas.
May Configure Integration Settings	Allows the operator to configure integration settings for a merchant. The integration methods include API or Hosted Batch, which allow the merchant application to directly connect to the payment gateway.
Allow Import Wizard Download	Allows the operator to download the import wizard.

Editing Operators

To edit a currently configured Operator:

- 1 From the Main menu, select *Admin > Operators*. The **Operator List** on page 72 page displays.
- 2 The *Edit an Operator* section lists all existing Operators. You can do any of the following:
 - To edit a particular Operator, click *Edit*. The Operator Details page displays.
 - To delete a particular Operator, click *Delete*. A message prompts you to confirm deletion. Click OK or Cancel as appropriate.
 - To change an Operator's password, click *Change Password* link. The Change Password page appears.

Note: The Change Password link does not display for the logged in user. Use *Admin > Change Password* on page 80 to change the password of the currently logged in Operator.

Unlocking an Operator Account

If a Merchant Administration Operator with administration privileges enables "Lock Operator Account" privilege for the Operator profile then the Operator gets locked out of Merchant Administration.

Note: To reinstate a locked out Merchant Administration Operator, you must have the *May Perform Operator Administration* user privilege.

To reactivate a locked out Merchant Administration Operator, log in as an activated Operator with the appropriate privileges:

- 1 From the Main menu, select *Admin > Operators*. The Merchant Administration Operator List page displays.
- 2 Identify the Operator to edit and select '*Edit*'. The Operator Details display, with the existing values and settings in the fields.
- 3 Clear the *Lock Operator Account* check box.
- 4 Click the **[Submit]** button to commit the changes. The Operator's account has now been unlocked and the Operator can log in with the existing password.

AMA Operator

For an operator with "Enable Advanced Merchant Administration Features" privilege enabled, the "Lock Operator Account" check box is automatically selected as a result of five failed login attempts. To reinstate a locked out AMA Operator, you must not only clear the *Lock Operator Account* check box (see steps 1-4) but also reset the password using the steps outlined below.

- a From the Main menu, select *Admin > Operators*. The Merchant Administration Operator List page displays.
- b Identify the Operator and click Change Password link. Enter a new password for the merchant in the *Password* field and retype that password in the *Repeat Password* field. You need to provide this new password to the Operator.
- c Click the **[Submit]** button to commit the changes. The AMA Operator's account has now been unlocked and a new password has been created.

Managing Passwords

You may need to change an Operator's password, unlock an Operator's login, or change your own password from time to time. Before you attempt to do this, you must be aware of the prerequisites and requirements.

Prerequisites

To change an Operator's password you must have *May Perform Operator Administration* operator privilege. See Operator Details.

Password Requirements

The password:

- Must be at least 8 characters, and include at least one alphabetic character and numeric character, for example, password_1
- Must not be the same as one of the previous 5 passwords.
- Must not be the same as the operator name.

Password Options

When creating or modifying an Operator record, you can select whether the Operator password expires on next login. The Operator is then prompted to change their password at the next login attempt. Alternatively, you can select '*Password never expires*' so that the Operator never needs to change their password. If '*Password never expires*' is left unchecked, the password shall automatically expire every thirty days.

If given the required privileges, Operators can change their password at any time, but they cannot re-use that password for the next five password changes. They can also reset their own password if the existing password has been forgotten. See Resetting a Password.

Changing an Operator's Password

Note: To change an Operator's password, you must have "May Perform Operator Administration" user privilege.

To change an Operator's password:

- 1 From the Main menu, select *Admin > Operators*. The Merchant Administration Operator List page displays.
- 2 Identify the Operator in the Edit Operator section, and click Change Password link. The Change Operator Password page displays.
- 3 Enter the *New Password*, and re-enter the new password in the *Confirm New Password* field.
- 4 Click the **[Submit]** button.

Changing Your Own Operator Password

Prerequisite

You must have *Change Own Password* operator privilege. See Operator Details.

To change your password:

- 1 From the Main menu, select *Admin* ▶ *Change Password*. The Change Password page displays.
- 2 Enter the *Old Password*, the *New Password*, and re-enter the new password in the *Confirm Password* field.
- 3 Click the **[Submit]** button.

The password is changed, and you will have to use the new password the next time you log in.

Manage Banamex Payment Plans

How to manage Payment Plans

- 1 Select '*Admin*' from the Main menu.
- 2 Select '*Manage Payment Plans*' from the submenu. The Manage Payment Plans page displays.

Note: If you have multiple acquirer links, the ***Acquirer Link Selection*** on page 82 page displays.

- 3 Add payment plans as required in the ***Add Payment Plan*** on page 81 section.
- 4 Manage your payment plans as required in the ***Payment Plans*** on page 82 section.

Note: Only merchant operators with administrator privileges can view and manage payment plans.

Adding a Payment Plan

Field	Description
Plan Name	A merchant-supplied identifier for the payment plan. The Payment Plan Name is unique per Payment Plan Type for the merchant. Note: The maximum field length is 20 characters.
Plan Type	The payment plan types enabled for the merchant. Only Payment Plans enabled in the merchant profile by the MSO are available for configuration.
Plan Terms (Cardholder Options)	The number of monthly installments and/or deferrals for each Payment Plan. The number of installments and deferrals vary from plan to plan.

How to Configure Payment Plan Terms

Payment Plan terms include:

- (Optional) Installments — number of monthly payments to pay for goods, if applicable to the plan.
- (Optional) Deferrals — number of months, payments can be deferred, if applicable to the plan.

To configure installments:

- 1 Review and select an installment term from the pre-defined set of default installment terms listed under **No of Installments, paid monthly**.
- 2 If you wish to add a new installment term, type the number of installments (less than 99 months) for the term in the **installments** text box and click the **[Add Installment]** button.
The new installment term displays in the **No of Installments, paid monthly** list box.
- 3 If you wish to delete any installment terms, click the **[Remove]** button. You can use the <Ctrl> key to select multiple installment terms.

To configure deferrals:

- 1 Review and select a deferral term from the pre-defined set of default deferral terms listed under **Deferral Months**.
- 2 If you wish to add a new deferral term, type the number of deferral months (less than 99 months) in the **deferral months** text box and click the **[Add Deferral]** button.
The new deferral term displays in the **Deferral Months** list box.
- 3 If you wish to delete any deferral terms, click the **[Remove]** button. You can use the <Ctrl> key to select multiple deferral terms.

After configuring the payment plan terms, click the **[Add]** button to add the payment plan to the **Using Payment Plans** on page 82 list. Click **[Cancel]** to reset the **Add Payment Plan** section.

Using Payment Plans

Payment Plans					
Plan ID	Payment Plan	# Of Installments	# Of Deferrals	Status	Action
BPWOI2	Bana2 - Pay in installments, interest-free	[3, 6, 12, 18]	[]	Disabled	Enable Edit
BPWOI1	Banamex21 - Pay in installments after a deferral period, with interest	[6, 9, 12]	[3, 6, 9]	Enabled	Disable Edit

Field	Description
Plan ID	A auto-generated unique identifier for the payment plan. The Plan ID is unique across all Payment Plan Types for the merchant.
Payment Plan	A concatenation of Payment Plan Name and Payment Plan Type (<Plan Name> - <Plan Type> as entered in the Add Payment Plan section. For example, Banamex - Pay without Interest.
# Of Installments	The installment terms in months configured for the payment plan. If installments are not applicable to the plan type, [] is displayed.
# Of Deferrals	The deferral terms in months configured for the payment plan. If deferrals are not applicable to the plan type, [] is displayed.
Status	The status of the payment plans. Valid values are: <ul style="list-style-type: none"> Enabled — enables the payment plan to be available for selection in the Create Order page. Disabled — makes the payment plan unavailable for selection in the Create Order page.
Action	Provides two actions: <ul style="list-style-type: none"> [Enable/Disable] button — allows you to either enable or disable the payment plan. Disabled payment plans are greyed out in the Payment Plans list. [Edit] button — allows you to edit the payment plan and apply changes, if any. Click [Save] button to save the changes or [Cancel] to exit the edit mode.

Note: You cannot edit the Plan ID field.

Acquirer Link Selection

If you have configured multiple acquirer links for the same acquirer, the Acquirer Selection page displays.

Acquirer Selection

Acquirer	Card Types	Currencies
eGlobal — 213234234		MXN USD Show
eGlobal — 12345		MXN Show

The card types and currencies configured for the acquirer link are also displayed. Click the **[Show]** button next to the acquirer link against which you wish to configure payment plans.

The name of the acquirer link displays in the **Add Payment Plan** section label to indicate the acquirer link that's currently selected for configuration. Follow the steps outlined in **Adding a Payment Plan** on page 81 and **Using Payment Plans** on page 82 to configure and manage payment plans.

Add Payment Plan — eGlobal — 213234234

Plan Name *

Plan Type *

Plan Terms (Cardholder Options)

No of Installments, paid monthly

3 installments

6 installments

9 installments

12 installments

18 installments

24 installments

installments

Deferral Months

3 deferred months

6 deferred months

9 deferred months

deferral months

Payment Plans

Plan ID	Payment Plan	# Of Installments	# Of Deferrals	Status	Action
BPLWI1	banan - Pay in installments after a deferral period, with interest	3, 6, 9, 99	3, 12, 99	Enabled	<input type="button" value="Disable"/> <input type="button" value="Edit"/>

Downloading Software and Documentation

To download software and documentation you must have the Allow Merchant Administration Documentation Download privilege set.

How to download software and documentation

- 1 Select 'Admin' from the Main menu.
- 2 Select 'Software and Documentation' from the submenu.
- 3 Click the appropriate link and follow the prompts to download the required file.

CHAPTER 9

Managing Risk

With the incidence of credit-card fraud increasing year by year, providing a cost-effective fraud management solution is acknowledged as one of the primary challenges of the payment services industry today. Merchants and those providing payment solutions to merchants, specifically in the Card-Not-Present (CNP) domain, are exploring different avenues to combat fraudulent transactions and increase their profitability. TNS' Risk management solution simplifies fraud monitoring and detection, and has been devised to cater to most of the requirements of the Card-Not-Present (CNP) industry.

TNS' Risk management solution supports both internal risk management and external risk management to perform risk assessment of transactions. Internal risk management refers to merchant and MSO risk rules configured using Merchant Administration and Merchant Manager. External risk management refers to any external risk provider that integrates with the gateway to perform risk assessment of transactions processed through the gateway.

This chapter describes how to use both internal and external risk modules. It contains the following sections:

- Accessing Risk Management
- Using Internal Risk Only
- Using External Risk Only
- Using Both Internal Risk and External Risk
- ***Searching for Orders Based on Risk Recommendation*** on page 124

Throughout the documentation, the terms "internal risk" and "external risk" will be used to refer to internal risk management and external risk management respectively.

Note: The Internal Risk module is used to define rules for the Internal Risk Rules service only. Rules for the external risk provider will be defined in the external system and will not be visible through Merchant Administration.

Introduction to Internal Risk

The Internal Risk module enables MSOs and merchants to mitigate fraud effectively using a set of business risk rules. These risk rules are configured to identify transactions of high or low risk thereby enabling merchants to accept, reject, or mark transactions for review based on risk assessment.

Typically, merchants adopt a combination of fraud prevention tools, for example, Verified by Visa, MasterCard SecureCode, AVS, CSC (Card Security Code), manual screening of orders, etc., to combat fraud. These tools have proved to be highly useful and efficient with the merchants hosted on our payment server; however, with the introduction of the Risk Management solution, the merchants can now automate the process of accepting, rejecting, or reviewing the order based on the risk assessment results. The risk rules are evaluated to determine the action taken on the order thereby demanding merchant operator intervention only when an order qualifies for a review decision. This functionality also allows flexibility to bypass risk assessment for individual orders if the merchant operator deems the card holder to be trustworthy and decides to proceed with a rejected order (unless the order is rejected at the MSO level).

The solution introduces various rules for risk mitigation — IP Country, Card BIN (Bank Identification Number), Trusted Cards, Suspect Cards, 3-D Secure, IP Address Range, AVS, CSC — each rule contributes differently to the risk profile. IP Address Range and Card BIN rules enable blocking/reviewing transactions from high-risk IP address ranges and high-risk BIN ranges respectively. Trusted Cards and Suspect Cards allow you to create lists of trustworthy card numbers and suspected card numbers respectively. 3DS rules enable you to block/review/accept transactions based on authentication states and IP Country rules enable you to block/review countries with high-risk IP addresses. AVS/CSC rules allow you to block/review/accept transactions based on AVS/CSC response codes.

Rules can be configured at both the merchant level and MSO level; however, Suspect Cards, Trusted Cards, and AVS rules can be configured at the merchant level only. The risk assessment results and details are displayed in the order response and order details screens for risk analysis. You can also search for orders based on the risk assessment results.

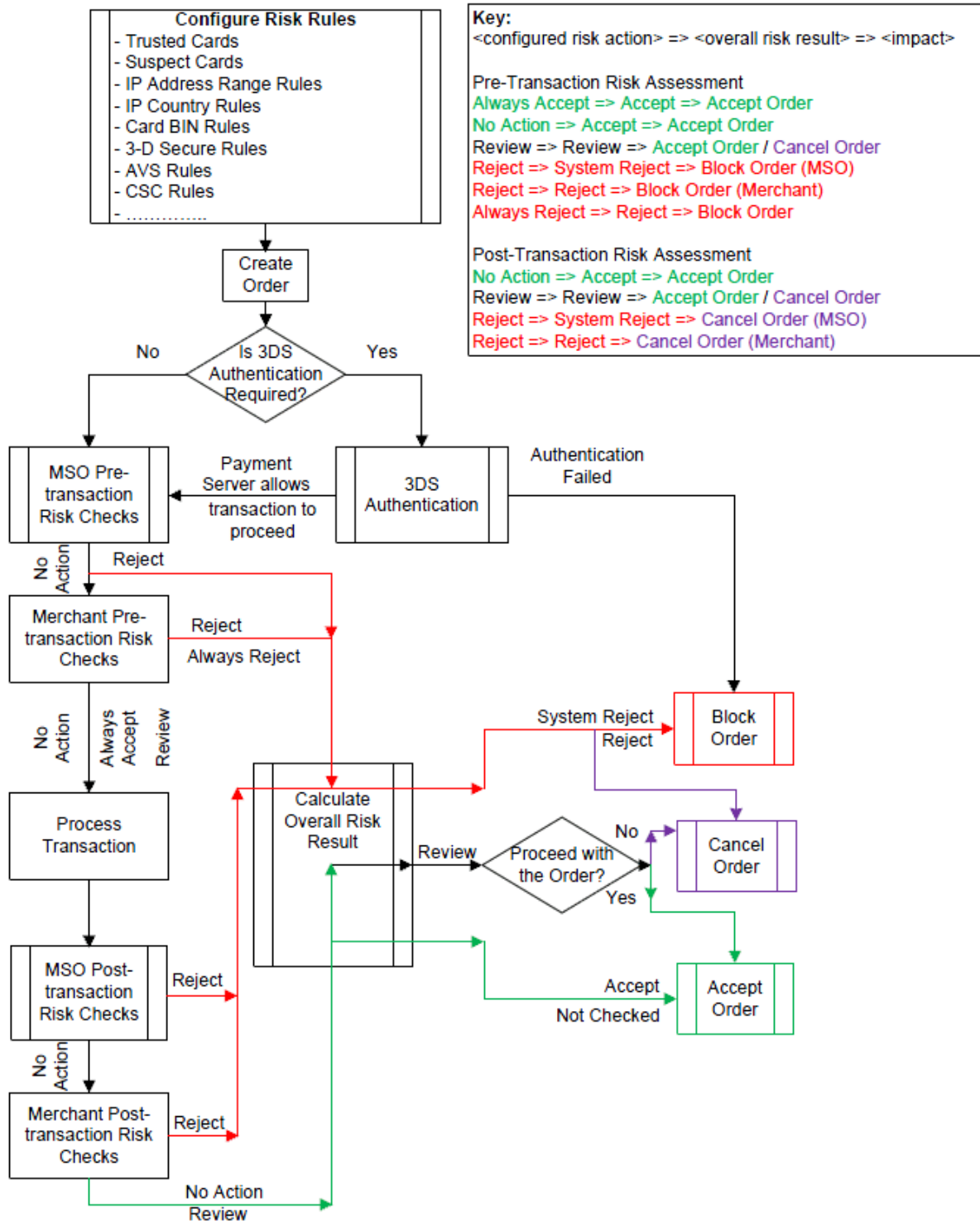
Risk Management Architecture

Risk Management primarily comprises of risk rule configuration and process management. You can choose to configure different types of risk rules based on your business needs. The results of risk assessment are processed automatically — the orders are either accepted, rejected, or marked for manual review. Orders marked for review may result in proceeding with the order or may be cancelled. You can also choose to resubmit rejected orders by bypassing all risk checks (unless the order is rejected at the MSO level).

Note 1: MSO level risk rules always override merchant level risk rules.

Note 2: You cannot bypass MSO level risk rules.

The diagram below illustrates the process flow of an order when risk management is enabled for a merchant.



¹3DS Authentication is required only if:

- the card type supports a 3DS authentication scheme;
- the merchant has the privilege to use this 3DS authentication scheme; and
- the merchant acquirer link has authentication details configured to use this 3DS authentication scheme.

Note: Risk assessment after the financial transaction (post-transaction risk assessment) is not applicable to Referred transactions (Authorisation or Purchase transactions that received a "Refer to Issuer" acquirer response).

Basic Concepts

To use the Risk Management module effectively, you must understand the following concepts:

Risk Rules

A set of rules defined to identify high or low risk transactions. For example, an IP Country rule definition that rejects "Country A" will treat all transactions from "Country A" as high risk; and a trusted card rule will treat all transactions from the specified trusted card number as low risk.

Risk Recommendation

The final action taken on the order based on the risk assessment performed. This action is determined after evaluating risk rules configured at the MSO and merchant level.

Internal Risk

Merchant and MSO risk rules configured using Merchant Administration and Merchant Manager.

External Risk

Any external risk provider that integrates with the gateway to perform risk assessment of transactions processed through the gateway.

Clash Action

The final action taken when results of two different risk rules have the same priority, i.e., one rule results in "Always Accept" and another in "Always Reject". As a processing guideline, "Always Accept" and "Always Reject" have the highest priority followed by "Reject", "Review" and "No Action".

MSO Rules

A set of rules configured at the MSO level. MSO rules always override merchant rules.

Merchant Rules

A set of rules configured at the merchant level.

Trusted Cards

A set of credit card numbers owned by those card holders whom the merchant considers trustworthy to transact with.

Suspect Cards

A set of credit card numbers owned by those card holders whom the merchant considers untrustworthy to transact with.

No Action

A type of action defined in the Risk Management tool, which enables the transaction to be processed normally.

Accept

A type of action defined in the Risk Management tool, which enables the transaction to be processed normally after risk assessment is performed.

Reject

A type of action defined in the Risk Management tool, which enables the transaction to be rejected automatically.

Review

A type of action defined in the Risk Management tool, which enables the transaction to be manually reviewed to be either accepted or cancelled.

System Reject

A type of action defined in the Risk Management tool, which enables the transaction to be rejected at the MSO level because the risk rules configured at the MSO level evaluate to reject the transaction.

Not Checked

A type of action defined in the Risk Management tool, which enables the transaction to be processed by bypassing risk assessment when the MSO rules do NOT evaluate to a risk result of Reject. It also implies a condition where neither MSO nor merchant risk rules are configured in the system.

Always Accept

A type of action defined in the Risk Management tool, which enables the transaction to be always processed normally. Trusted Cards are always set to this action; however, you can also choose to configure a 3-D Secure authentication state to "Always Accept". A rule configured to the action "Always Accept" overrides all other actions except "Always Reject".

Always Reject

A type of action defined in the Risk Management tool, which enables the transaction to be always rejected automatically. Suspect Cards are always set to this action. A rule configured to the action "Always Reject" overrides all other actions except "Always Accept".

Accessing Internal Risk

To use the internal risk module, the MSO must enable *Internal Risk Rules* privilege for the merchant. This enables the merchant to:

- grant risk management administration privilege to merchant operators,
- perform risk assessment of orders, and
- bypass risk assessment.

The privileges available for a merchant operator are:

- *May Configure Risk Rules* — enables the merchant operator to configure risk rules.
- *May Perform Risk Assessment Review* — enables the merchant operator to review the risk recommendation.
- *May Bypass Risk Management* — enables the merchant operator to process orders without performing risk checks.

For more information on these privileges, see Merchant Operator General Privileges.

Viewing Risk Management Summary


The Risk Management Summary page introduces the Risk Management module and provides various options for risk mitigation on the left pane.


The **Action Items** menu allows you to take action on some pending tasks associated with risk assessment. For more information, see **Action Items** on page 93.

The risk rules configuration submenu allows you to configure risk rules for IP Country, IP Address Range, Card BIN, Trusted Cards, Suspect Cards, 3-D Secure, AVS, or CSC. To do this, click the rule type, which takes you to the corresponding configuration page. See **Working with Rules** on page 94

Action Items

(x) the number "x" represents the count, i.e., the number of orders that require action.

 icon indicates a necessary action; it appears only when the count > 0

 icon indicates no action required; it appears only when the count = 0

The currently available links in Action Items are:

- Risk Assessments for Review

Note: This link appears only if the merchant operator has *May Perform Risk Assessment Review* privilege.

- Failed Risk Reversals

Risk Assessments for Review

Clicking this link takes you to the Risk Assessments for Review page on the Risk Management tab in the main menu. The **Action Items** menu and risk rules configuration submenu are displayed on the left pane. A list of orders awaiting review decision are displayed on the right pane.

Click the Order ID link to review the risk assessment. For more information, see Risk Assessment Details

Failed Risk Reversals

Clicking this link takes you to the Failed Risk Reversals page on the Risk Management tab in the main menu. The **Action Items** menu and risk rules submenu are displayed on the left pane. A list of orders with failed risk reversals are displayed on the right pane.

A failed risk reversal typically occurs when the system fails to automatically reverse a rejected/cancelled order that was assessed for risk. Orders rejected/cancelled due to risk assessment after the financial transaction are automatically attempted for a reversal by the system. The reversals can fail due to the acquirer not supporting reversals or an acquirer being unavailable. For more information on order reversals, see Risk Assessment Details.

Click the Order ID link to retry the order reversal. For more information, see section "When Risk Recommendation is Set to Reject" in Implications of Risk Recommendation.

Note: You can choose to dismiss review decisions or failed risk reversals such that they do not appear as an action item. For more information, see **Dismissing Review Decisions or Failed Risk Reversals** on page 94.

Dismissing Review Decisions or Failed Risk Reversals

In the Risk Assessments for Review or the Failed Risk Reversals page, you may choose to manually dismiss the review decision or a failed risk reversal for an order. You may want to do this because you have settled the order off-line directly with the customer or you have other high priority tasks and do not wish to take any action on alerts.

To dismiss a review decision or a failed risk reversal:

- 1 Select the **Dismiss** check box on the order for which you wish to dismiss the review decision or the failed risk reversal.
Click [**Select All**] to select all orders for dismissal.
- 2 Click the [**Dismiss**] button.

Working with Rules

Rules are the building blocks of the Risk Management functionality — they enable merchants to identify high risk transactions thereby preventing merchants from processing fraudulent transactions. The risk rules can be configured by the MSO or the merchant; however, the MSO's risk settings always override the merchant's risk settings. All updates to the risk rules are captured in the system's audit log.

Types of Rules

Currently, our Risk management solution supports the following types of rules:

- **IP Country Rules** on page 106 — enables you to block transactions based on IP addresses of countries.
- **IP Address Range Rules** on page 101 — enables you to block transactions based on IP addresses of transactions.
- **Card BIN Rules** on page 110 — enables you to block transactions based on BINs (Bank Identification Numbers).
- **Trusted Cards** on page 95 — enables you to always accept transactions from the card numbers identified as Trusted Cards.
- **Suspected Cards** on page 98 — enables you to always reject transactions from the card numbers identified as Suspect Cards.
- **3-D Secure Rules** on page 113 — enables you to block transactions based on 3DS authentication states.
- **AVS Rules** on page 118 — enables you to block transactions based on AVS (Address Verification Status) response codes.
- **CSC Rules** on page 122 — enables you to block transactions based on CSC (Card Security Code) response codes.

Trusted Cards

Trusted cards list is a set of credit card numbers owned by those card holders whom the merchant considers trustworthy to transact with. Typically, a card holder with a good record of transaction history has a high potential of being added to the trusted card list. Configuring trusted card rules ensures that transactions from trusted cards are always accepted.

Before you attempt to add trusted cards, you must be aware of the prerequisites.

Prerequisite

To add trusted cards, you must have *May Configure Risk Rules* operator privilege. See Merchant Operator General Privileges.

Adding a Trusted Card Number

How to add a trusted card number

- 1 From the Main menu, select *Risk Management > Trusted Cards*. The *Trusted Cards* page displays.
- 2 In *Add New Card Number* section, enter the following information.

Add New Card Number			
Card Number	Card Holder Name	Reason	
* 5123456789012346	Ian Hill	Good transaction histo	Add

Field	Description
Card Number	The credit card number of the card holder.
Card Holder Name	The name of the card holder. This is an optional field. Note: The card holder name cannot exceed 40 characters.
Reason	The reason for which you want to add the specified card number as a trusted card number. This is an optional field. Note: The reason cannot exceed 40 characters.

- Click the **[Add]** button. The Trusted Cards page re-displays with the updated current Trusted Card Numbers list sorted by card numbers. The card numbers are displayed in the 6.4 card masking format irrespective of the card masking format configured for the merchant.

Current Trusted Card Numbers

Select: **All** | **None** Filter By Card Number:

Select	Card Number	Card Holder Name	Reason	
<input type="checkbox"/>	345678xxxxx0007	Darrell Louis	Masked numbers are different	Edit
<input type="checkbox"/>	352812xx9012	Scott Adam	Short JCB	Edit
<input type="checkbox"/>	457199xxxxxx0003	Helton Serrao	Resulted in chargebacks last time	Edit
<input type="checkbox"/>	500000xxxxxxxxxx0005	Alan Harper		Edit
<input type="checkbox"/>	510112xxxxxx0003	Kitty Kugyela		Edit
<input type="checkbox"/>	512345xxxxxx2346	Ian Hill	Good transaction history	Edit

Reviewing Current Trusted Card Numbers

How to review the current trusted card numbers

- From the Main menu, select *Risk Management > Trusted Cards*. The *Trusted Cards* page displays. The *Current Trusted Card Numbers* section displays a list of all currently added trusted card numbers and their corresponding details.

If the list of trusted cards exceeds 20 entries, pagination triggers which allows you to navigate between multiple pages.

Current Trusted Card Numbers

Select: **All** | **None** Filter By Card Number:

Select	Card Number	Card Holder Name	Reason	
<input type="checkbox"/>	345678xxxxx0007	Darrell Louis	Masked numbers are different	Edit
<input type="checkbox"/>	352812xx9012	Scott Adam	Short JCB	Edit
<input type="checkbox"/>	457199xxxxxx0003	Helton Serrao	Resulted in chargebacks last time	Edit
<input type="checkbox"/>	500000xxxxxxxxxx0005	Alan Harper		Edit
<input type="checkbox"/>	510112xxxxxx0003	Kitty Kugyela		Edit
<input type="checkbox"/>	512345xxxxxx2346	Ian Hill	Good transaction history	Edit

- 2 To filter the list based on a card number:
 1. Enter the card number in the **Filter by Card Number** text box. Click **[Clear]** if you want to clear the filter string. Clearing the filter repopulates the entire list of card numbers.
 2. Click **[Go]**. Only card numbers that match the filter criteria are displayed in the Current Trusted Card Numbers list. The card numbers are sorted in ascending order.
- 3 To edit a card number:
 1. Click the **[Edit]** option next to the card number record.



2. Make changes to the required fields.

When you modify the card number, ensure that you enter the complete card number for validation purposes. Editing Card Holder name and Reason do not require you to enter the card number.
3. Click the **[Update]** button to process the changes.
4. Click **[Cancel]** if you want to cancel the changes.

Deleting Trusted Card Numbers

How to delete a trusted card number

- 1 From the Main menu, select *Risk Management > Trusted Cards*. The Trusted Cards page displays. The *Current Trusted Card Numbers* section displays a list of all currently added trusted card numbers and their corresponding details.

If the list of trusted cards exceeds 20 entries, pagination triggers which allows you to navigate between multiple pages.

- 2 Use the **Filter By Card Number** option to find card numbers you may want to delete. See *Reviewing Current Trusted Card Numbers* on page 96.

Select	Card Number	Card Holder Name	Reason	
<input checked="" type="checkbox"/>	345678xxxxx0007	Darrell Louis	Masked numbers are different	Edit
<input checked="" type="checkbox"/>	352812xx9012	Scott Adam	Short JCB	Edit
<input type="checkbox"/>	457199xxxxxx0003	Helton Serrao	Resulted in chargebacks last time	Edit
<input type="checkbox"/>	500000xxxxxxxxxx0005	Alan Harper		Edit
<input type="checkbox"/>	510112xxxxxx0003	Kitty Kugyela		Edit

- 3 Select the card number you want to delete by selecting the check boxes under the **Select** column. You may use **Select All /None** to select/clear all card numbers.
- 4 Click [**Remove Trusted Card Numbers**] to delete the selected card numbers.

Suspect Cards

Suspect cards list is a set of credit card numbers owned by those card holders whom the merchant considers untrustworthy to transact with. Typically, a card holder with fraudulent transaction history has a high potential of being added to the suspect card list. Configuring suspect card rules enable you to block transactions from suspected cards.

Before you attempt to add suspect cards, you must be aware of the prerequisites.

Prerequisite

To add suspect cards, you must have *May Configure Risk Rules* operator privilege. See Merchant Operator General Privileges.

Adding a Suspected Card Number

How to add a suspect card number

- 1 From the Main menu, select *Risk Management > Suspect Cards*. The *Suspect Cards* page displays.
- 2 In *Add New Card Number* section, enter the following information.

Field	Description
Card Number	The credit card number of the card holder.
Card Holder Name	The name of the card holder. This is an optional field. Note: The card holder name cannot exceed 40 characters.
Reason	The reason for which you want to add the specified card number as a suspect card number. This is an optional field. Note: The reason cannot exceed 40 characters.

- 3 Click the **[Add]** button. The *Suspect Cards* page re-displays with the updated current *Suspect Card Numbers* list sorted by card numbers. The card numbers are displayed in the 6.4 card masking format irrespective of the card masking format configured for the merchant.

Select	Card Number	Card Holder Name	Reason	Edit
<input type="checkbox"/>	493873xxxxxx0001	Lloyd Lane	Fraudulent transactions	Edit
<input type="checkbox"/>	512345xxxxxx2346	Terri Hill	Fraudulent history	Edit
<input type="checkbox"/>	514927xxxxxx0000	Kate Hilton	Bad transaction history	Edit

Reviewing Current Suspect Card Numbers

How to review the current suspect card numbers

- From the Main menu, select *Risk Management > Suspect Cards*. The *Suspect Cards* page displays. The *Current Suspect Card Numbers* section displays a list of all currently added suspected card numbers and their corresponding details.

If the list of suspect cards exceeds 20 entries, pagination triggers which allows you to navigate between multiple pages.

Select	Card Number	Card Holder Name	Reason	
<input type="checkbox"/>	493873xxxxxx0001	Lloyd Lane	Fraudulent transactions	Edit
	<input type="text" value="512345xxxxxx2346"/>	<input type="text" value="Terri Hill"/>	Fraudulent history	<input type="button" value="Update"/> <input type="button" value="Cancel"/>
	<input type="text" value="514927xxxxxx0000"/>	<input type="text" value="Kate Hilton"/>	Bad transaction history	<input type="button" value="Update"/> <input type="button" value="Cancel"/>

- To filter the list based on a card number:
 - Enter the card number in the **Filter by Card Number** text box. Click **[Clear]** if you want to clear the filter string. Clearing the filter repopulates the entire list of card numbers.
 - Click **[Go]**. Only card numbers that match the filter criteria are displayed in the Current Trusted Card Numbers list. The card numbers are sorted in ascending order.
- To edit a card number:
 - Click the **[Edit]** option next to the card number record.

- Make changes to the required fields.

When you modify the card number, ensure that you enter the complete card number for validation purposes. Editing Card Holder name and Reason do not require you to enter the card number.
- Click the **[Update]** button to process the changes.
- Click **[Cancel]** if you want to cancel the changes.

Deleting Suspect Card Numbers

How to delete a suspect card number

- From the Main menu, select *Risk Management > Suspect Cards*. The Suspect Cards page displays. The *Current Suspect Card Numbers* section displays a list of all currently added suspected card numbers and their corresponding details.
If the list of suspect cards exceeds 20 entries, pagination triggers which allows you to navigate between multiple pages.
- Use the **Filter By Card Number** option to find card numbers you may want to delete. See *Reviewing Current Suspect Card Numbers* on page 100.

Select	Card Number	Card Holder Name	Reason	
<input checked="" type="checkbox"/>	493873xxxxxx0001	Lloyd Lane	Fraudulent transactions	Edit
<input checked="" type="checkbox"/>	512345xxxxxx2346	Terri Hill	Fraudulent history	Edit
<input type="checkbox"/>	514927xxxxxx0000	Kate Hilton	Bad transaction history	Edit

- Select the card number(s) you want to delete by selecting the check boxes under the **Select** column. You can click **Select All / None** to select/clear all card numbers.
- Click [**Remove Suspected Card Numbers**] to delete the selected card numbers.

Configuring IP Address Range Rules

IP addresses can help in identifying the origin of the transaction and thus the location of the card holder. Configuring IP Address Range rules enable you to block or review transactions from a specific IP address or IP addresses within a range.

At the merchant level, you can configure IP address ranges to belong to only two categories:

- Review (processed or blocked manually)
- Reject (blocked automatically)

Before you attempt to configure IP Address Range rules, you must be aware of the prerequisites.

Prerequisite

To configure IP Address Range rules, you must have *May Configure Risk Rules* operator privilege. See Merchant Operator General Privileges.

Adding an IP Address Range Rule - Merchant

How to add an IP Address Range Rule

- 1 From the Main menu, select *Risk Management > IP Address Range Rules*. The *IP Address Range Rules* page displays.

Note: You cannot override the IP Address Range Rules configured by your MSO.

- 2 In *Add IP Address Range Rule* section, enter the following information to add a new range for blocking. You can choose to block a single IP address or an IP address range. For example, if you want to block IP Address 192.0.2.255, simply type 192.0.2.255 as the IP Address Range Start entry and choose the required action. To block an IP address range, say 192.0.2.222 to 192.0.2.255, type 192.0.2.222 and 192.0.2.255 as the start and end IP address ranges respectively.

Note 1: The IP address must be specified in IPv4 format between the range 0.0.0.0 and 255.255.255.255.

Note 2: If the defined IP ranges overlap to belong to both the categories (Review and Reject), then the action Reject overrides Review.

Add IP Address Range Rule		
IP Address Range Start	IP Address Range End	Action
* <input type="text" value="172.17.78.72"/>	<input type="text" value="172.17.78.79"/>	* <input type="radio"/> Review ? <input checked="" type="radio"/> Reject ?
		<input type="button" value="Add"/> ?

Field	Description
IP Address Range Start	The first IP address in the range to be blocked.
IP Address Range End	The last IP address in the range to be blocked.
Action	<p>The action you want to perform on the IP range. Valid options are:</p> <ul style="list-style-type: none"> ▪ Review — IP ranges with this status are manually reviewed and either accepted or rejected. ▪ Reject — IP ranges with this status are rejected automatically.

If the specified IP addresses form a large range then the system displays a warning "The rule you want to configure will apply to a very large number of IP addresses. Are you sure you want to add this rule?". Click **[OK]** if you want to continue else click **[Cancel]**.

- 1 Click the **[Add]** button. The IP Address Range Rules page re-displays with the updated current IP address range rules list.

Currently Blocked IP Address Ranges

Use the filter option to find an IP Address in a range or overlapping ranges, or to simply check if an IP Address is blocked currently. Filtering enables you to easily find overlapping ranges, and delete them as required.

Filter Mode: Off

Select: All | None Filter Ranges by IP Address: Go Clear ?

Delete

Select	Start	End
<input type="checkbox"/>	10.0.0.0	10.255.255.255
<input type="checkbox"/>	172.17.78.72	172.17.78.79
<input type="checkbox"/>	192.168.1.1	192.168.1.1
<input type="checkbox"/>	192.168.1.1	192.168.255.255

1

Reviewing Current IP Address Range Rules

How to review the current list of IP Address range rules

- From the Main menu, select *Risk Management > IP Address Range Rules*. The *IP Address Range Rules* page displays. The *Current IP Address Range Rules* section displays a list of all currently configured IP Address range rules in ascending order and their corresponding action status.

If the list of current IP Address Ranges exceeds 20 entries, pagination triggers which allows you to navigate between multiple pages.

Select	Start	End
<input type="checkbox"/>	10.0.0.0	10.255.255.255
<input type="checkbox"/>	172.17.78.72	172.17.78.79
<input type="checkbox"/>	192.168.1.1	192.168.1.1
<input type="checkbox"/>	192.168.1.1	192.168.255.255

- To filter the list based on an IP Address or to find an IP address in a range or overlapping ranges:
 - Enter the IP Address in the **Filter Ranges By IP Address** text box. Click **[Clear]** if you want to clear the filter string. Clearing the filter repopulates the entire list of IP address ranges and turns off the filter mode. **Filter Mode:Off** indicates that the filter option is not enabled on the IP Address Ranges list.

You can also use the filter option to check if an IP range is blocked currently.

- Click **[Go]**. Only IP ranges that match the filter criteria are displayed in the Current IP Address Range Rules list. The IP ranges are sorted in ascending order.

Filter Mode:On indicates that the filter option is enabled on the IP Address Ranges list.

Select	Start	End	Action
<input type="checkbox"/>	192.168.1.1	192.168.1.1	Reject
<input type="checkbox"/>	192.168.1.1	192.168.255.255	Reject

If you want to delete an IP address range, see *Deleting an IP Address Range Rule*. on page 105

Deleting an IP Address Range Rule

How to delete an IP Address Range Rule

- 1 From the Main menu, select *Risk Management > IP Address Range Rules*. The IP Address Range Rules page displays. The *Current IP Address Range Rules* section displays a list of all currently configured IP Address Range rules and their corresponding action status.

If the list of current IP Address Ranges exceeds 20 entries, pagination triggers which allows you to navigate between multiple pages.

- 2 Use the **Filter Ranges By IP Address** option to find an IP address in a range or overlapping ranges. See *Reviewing Current IP Address Range Rules*, on page 104

Current IP Address Range Rules

Use the filter option to find an IP Address in a range or overlapping ranges, or to simply check if an IP Address is blocked currently. Filtering enables you to easily find overlapping ranges, and delete them as required.

Filter Mode: On

Select: **All** | **None** Filter Ranges by IP Address: 192.168.1.1

Select	Start	End	Action
<input checked="" type="checkbox"/>	192.168.1.1	192.168.1.1	Reject
<input checked="" type="checkbox"/>	192.168.1.1	192.168.255.255	Reject

1

- 3 Select the IP Address range you want to delete. You may use **Select All/None** options to select/clear all the records.
- 4 Click the **[Delete]** button. A warning message displays, which alerts you about deleting IP ranges that may occur in multiple IP ranges if overlapping IP ranges have been defined.
- 5 Click **[Yes]** if you want to proceed with the deletion of the selected IP ranges. Click **[No]** to cancel the deletion.

Configuring IP Country Rules

IP addresses can help in identifying the location of the card holder. Configuring IP Country Rules enable you to block transactions originating from a pre-defined list of countries. You can also choose to configure additional rules to block countries identified as using IPs from unknown countries or IPs of anonymous proxies that mask the true origin of the request.

At the merchant level, you can configure countries to belong to three categories:

- No Action (processed normally)
- Review (processed or blocked manually)
- Reject (blocked automatically)

However, an MSO can configure countries to belong to only *No Action* and *Reject* categories.

Note: A country can belong to only one category at any given time.

Before you attempt to block countries, you must be aware of the prerequisites.

Prerequisite

To configure IP Country Rules, you must have *May Configure Risk Rules* operator privilege. See Merchant Operator General Privileges.

Adding an IP Country Rule

How to add an IP country rule

- 1 From the Main menu, select *Risk Management > IP Country Rules*. The IP Country Rules page displays with three list boxes:
 - **No Action** — lists countries you want to accept transactions from.
 - **Review** — lists countries you want to mark for review before proceeding with the order. Marking countries for review provides merchants with the flexibility to take a decision on whether to process or reject a transaction from the specified country.
 - **Reject** — lists countries you want to reject all transactions from.

Note: You cannot override the IP Country Rules configured by your MSO.

Add an IP Country Rule

Unknown Country	<input type="radio"/> No Action	<input checked="" type="radio"/> Review	<input type="radio"/> Reject	?
Anonymous Proxy	<input type="radio"/> No Action	<input type="radio"/> Review	<input checked="" type="radio"/> Reject	?

To select multiple countries, press Ctrl and select additional items. A country can belong to only one list at any given time.

<div style="background-color: #4CAF50; color: white; padding: 2px; font-weight: bold; text-align: center;">No Action ?</div> <div style="text-align: right; font-size: small; margin-bottom: 5px;">Select: All None</div> <div style="border: 1px solid #ccc; padding: 5px; min-height: 200px;"> <ul style="list-style-type: none"> China Christmas Island Cocos Islands Colombia Comoros Congo Cook Islands Côte d'Ivoire Croatia Cuba Cyprus Czech Republic Denmark Djibouti Dominica Dominican Republic Ecuador Egypt El Salvador Equatorial Guinea Eritrea Estonia Ethiopia </div> <div style="border-top: 1px dashed #ccc; padding-top: 5px; font-size: small; font-weight: bold;">Move Selected Countries To:</div> <div style="text-align: center; margin-top: 5px;"> <input type="button" value="Review"/> <input type="button" value="Reject"/> </div>	<div style="background-color: #4CAF50; color: white; padding: 2px; font-weight: bold; text-align: center;">Review ?</div> <div style="text-align: right; font-size: small; margin-bottom: 5px;">Select: All None</div> <div style="border: 1px solid #ccc; padding: 5px; min-height: 200px;"> <ul style="list-style-type: none"> Costa Rica Tajikistan Tanzania </div> <div style="border-top: 1px dashed #ccc; padding-top: 5px; font-size: small; font-weight: bold;">Move Selected Countries To:</div> <div style="text-align: center; margin-top: 5px;"> <input type="button" value="No Action"/> <input type="button" value="Reject"/> </div>	<div style="background-color: #4CAF50; color: white; padding: 2px; font-weight: bold; text-align: center;">Reject ?</div> <div style="text-align: right; font-size: small; margin-bottom: 5px;">Select: All None</div> <div style="border: 1px solid #ccc; padding: 5px; min-height: 200px;"> <ul style="list-style-type: none"> Guatemala Kuwait Kyrgyzstan </div> <div style="border-top: 1px dashed #ccc; padding-top: 5px; font-size: small; font-weight: bold;">Move Selected Countries To:</div> <div style="text-align: center; margin-top: 5px;"> <input type="button" value="No Action"/> <input type="button" value="Review"/> </div>
--	---	--

- 2 Under *Add an IP Country Rule* section, choose the action you want to perform on unknown countries and anonymous proxies.

Field	Description
Unknown Country	<p>A country that's not listed in Risk Manager or an IP address that does not resolve to a valid country in Risk Manager. For example, if country "Country A" is not listed in Risk Manager or if the IP address for this country is updated to a new value in the mapping list, by default, the transaction from this country will be accepted. However, you may choose to review or reject the transaction by selecting the Review or Reject option respectively. Valid options are:</p> <ul style="list-style-type: none"> ▪ No Action (default value) — an unknown country with this status is processed normally. ▪ Review — an unknown country with this status is manually reviewed and either accepted or rejected. ▪ Reject — an unknown country with this status is rejected automatically.
Anonymous Proxy	<p>IP address of a known anonymous proxy server. These addresses have been identified to mask the true origin of the request. For example, if IP address 172.17.78.25 belongs to an unknown country and is routed through an anonymous proxy server such that the actual IP address of the request is masked, then by default, the transaction from this country will be accepted. However, you may choose to review or reject the transaction by selecting the Review or Reject option respectively. Valid options are:</p> <ul style="list-style-type: none"> ▪ No Action (default value) — an unknown country with this status is processed normally. ▪ Review — an unknown country with this status is manually reviewed and either accepted or rejected. ▪ Reject — an unknown country with this status is rejected automatically.

- 1 To *mark a country for review*:
- a) Select the country from either the **No Action** or the **Reject** list box.
 - b) Click **[Review]** button to move the country to the **Review** list box. If you want to undo your action, select the country in the **Review** list box and click either the **[No Action]** or **[Reject]** button.

Note: Press CTRL to select multiple items.

- 2 To *reject a country*:
- a) Select the country from the **No Action** or the **Review** list box.
 - b) Click **[Reject]** button to move the country to the **Reject** list box. If you want to undo your action, select the country in the **Reject** list box and click either the **[No Action]** or **[Review]** button.
- 3 Click **[Save]** button to save the IP Country Rule.
- 4 Click **[Cancel]** button if you want to exit the IP Country Rules page without saving any changes.

Reviewing Currently Rejected IP Countries

How to review the current list of rejected countries

- From the Main menu, select *Risk Management > IP Country Rules*. The IP Country Rules page displays. The **Reject** list box displays all countries from which transactions are rejected currently. The countries marked for review are listed in the **Review** list box. Based on the merchant's review decision, countries marked for review may result in proceeding with the order or cancelling the order.

To select multiple countries, press Ctrl and select additional items. A country can belong to only one list at any given time.

No Action	Review	Reject
Select: All None China Christmas Island Cocos Islands Colombia Comoros Congo Cook Islands Côte d'Ivoire Croatia Cuba Cyprus Czech Republic Denmark Djibouti Dominica Dominican Republic Ecuador Egypt El Salvador Equatorial Guinea Eritrea Estonia Ethiopia	Select: All None Costa Rica Tajikistan Tanzania	Select: All None Guatemala Kuwait Kyrgyzstan
Move Selected Countries To: <input type="button" value="Review"/> <input type="button" value="Reject"/>	Move Selected Countries To: <input type="button" value="No Action"/> <input type="button" value="Reject"/>	Move Selected Countries To: <input type="button" value="No Action"/> <input type="button" value="Review"/>
<input type="button" value="Cancel"/> <input type="button" value="Save"/>		

Deleting an IP Country Rule

How to delete an IP Country Rule

- From the **Reject** list box, select the country for which you want to delete the IP Country Rule.

Note: Press CTRL to select multiple items.

- Click the **[No Action]** button to move the country to the **No Action** list box.
- Click **[Save]** button to process the IP Country Rule. All transactions from countries listed in the **No Action** list box will be processed normally.

Note: You cannot override the IP Country Rules configured by your MSO.

Configuring Card BIN Rules

The card Bank Identification Number (BIN) can help in identifying the location of the card issuer. Configuring Card BIN Rules enable you to block or review transactions from a specific BIN or all BINs within a range.

At the merchant level, you can configure Card BINs to belong to only two categories:

- Review (processed or blocked manually)
- Reject (blocked automatically)

Before you attempt to configure Card BIN rules, you must be aware of the prerequisites.

Prerequisite

To manage BIN blocking, you must have *May Configure Risk Rules* operator privilege. See Merchant Operator General Privileges.

Adding a Card BIN Rule

How to add a BIN rule

- 1 From the Main menu, select *Risk Management > Card BIN Rules*. The *Card BIN Rules* page displays.

Note: You cannot override the Card BIN Rules configured by your MSO.

- 2 In *Add BIN Rule* section, enter the following information to add a new range for blocking. You can choose to block a single BIN or a BIN range. For example, if you want to block BIN 123456, simply type 123456 as the BIN Range Start entry. To block a BIN range, say 111111 to 222222, type 111111 and 222222 as the start and end BIN ranges respectively.

Note: The BIN must be six numeric characters in length and cannot start with zero.

BIN Range Start	BIN Range End	Action	
* 345125	346125	* <input type="radio"/> Review ? <input checked="" type="radio"/> Reject ?	Add

Field	Description
BIN Range Start	The first BIN in the range to be blocked.
BIN Range End	The last BIN in the range to be blocked.
Action	<p>The action you want to perform on the BIN range. Valid options are:</p> <ul style="list-style-type: none"> ▪ Review — BIN ranges with this status are manually reviewed and either accepted or rejected. ▪ Reject — BIN ranges with this status are rejected automatically.

Note: If the defined BIN ranges overlap to belong to both the categories (Review and Reject), then the action Reject overrides Review.

- 1 Click the **[Add]** button. The Card BIN Rules page re-displays with the updated current BIN rules list.

Current BIN Rules			
Select: All None			
<input type="button" value="Delete"/>			
Select	Start	End	Action
<input type="checkbox"/>	345125	346125	Reject
<input type="checkbox"/>	345678	345678	Review
<input type="checkbox"/>	400939	400939	Reject
<input type="checkbox"/>	512345	512345	Review
1			

Reviewing Current Card BIN Rules

How to review the current list of BIN rules

- 1 From the Main menu, select *Risk Management > Card BIN Rules*. The *Card BIN Rules* page displays. The *Current BIN Rules* section displays a list of all currently configured Card BIN rules in ascending order and their corresponding action status.

If the list of current Card BIN ranges exceeds 20 entries, pagination triggers which allows you to navigate between multiple pages.

Current BIN Rules			
Select: All None			
<input type="button" value="Delete"/>			
Select	Start	End	Action
<input type="checkbox"/>	345125	346125	Reject
<input type="checkbox"/>	345678	345678	Review
<input type="checkbox"/>	400939	400939	Reject
<input type="checkbox"/>	512345	512345	Review

1

Deleting a Card BIN Rule

How to delete a blocked BIN range

- 1 From the Main menu, select *Risk Management > Card BIN Rules*. The *Card BIN Rules* page displays. The *Current BIN Rules* section displays a list of all currently blocked BIN ranges and their corresponding action status.

If the list of current Card BIN ranges exceeds 20 entries, pagination triggers which allows you to navigate between multiple pages.

Current BIN Rules			
Select: All None			
<input type="button" value="Delete"/>			
Select	Start	End	Action
<input checked="" type="checkbox"/>	345125	346125	Reject
<input checked="" type="checkbox"/>	345678	345678	Review
<input type="checkbox"/>	400939	400939	Reject
<input type="checkbox"/>	512345	512345	Review

1

- 2 Select the BIN range you want to delete. You may use **Select All/None** options to select/clear all the records.
- 3 Click the **[Delete]** button. A warning message displays, which alerts you about deleting BIN ranges that may occur in multiple BIN ranges if overlapping BIN ranges have been defined.
- 4 Click **[Yes]** if you want to proceed with the deletion of the selected BIN ranges. Click **[No]** to cancel the deletion.

Configuring 3-D Secure Rules

3-Domain Secure™ (3-D Secure or 3DS) is a protocol for authenticating cardholders, originally developed by Visa but now also adopted by MasterCard and JCB. It uses a Directory Server to determine whether the cardholder is enrolled for 3DS, then redirects the cardholder to an Access Control Server (ACS) where the cardholder enters a previously registered 3DS password for authentication. Authentication ensures that the card is being used by its legitimate owner.

A 3-D Secure transaction is performed immediately before a merchant performs a payment transaction, that is, an Authorisation transaction in the Auth/Capture mode, or a Purchase transaction in the Purchase mode. However, 3DS risk checks are applied only to transactions:

- that contain 3DS authentication data, namely, a standard 3-Party transaction; a 3-Party transaction where the merchant supplies full card details, or a 2-party pre-authenticated transaction, and
- transactions that are NOT blocked by the Payment Server at the system level due to a failed 3DS authentication state. For example, a 3DS verification status of N (Authentication Failed) instructs the Payment Server to block the transaction based on the default payment rule. In such a case, risk assessment will not be performed on this transaction.

Configuring 3DS rules enable merchants to either accept or block any transaction based on the 3DS authentication states. The authentication states are uniform across all authentication schemes and acquirers.

You can configure 3DS authentication states to belong to four categories:

- No Action (processed normally)
- Always Accept (always processed normally)
- Review (processed or blocked manually)
- Reject (blocked automatically)

However, an MSO can configure authentication states to belong to only *No Action* and *Reject* categories.

Note: An authentication state can belong to only one category at any given time.

Before you configure 3DS rules, you must be aware of the prerequisites.

Prerequisite

To configure 3DS Rules, you must have:

- the *May Configure Risk Rules* operator privilege. See Merchant Operator General Privileges.
- the privilege to at least one 3DS authentication scheme, namely *Verified by Visa*, *MasterCard SecureCode*, *J/Secure*, or *American Express SafeKey*. See Cardholder Verification in Merchant Privileges. If you do not have this privilege, the 3DS Rules option does not appear in the Risk Management submenu.
- the card type must support the 3DS authentication scheme.
- the merchant acquirer link must have authentication details configured for the 3DS authentication scheme.
- the *3-party gateways* privilege. See Gateways in Merchant Privileges.

Adding a 3-D Secure Rule

How to add a 3DS rule

- 1 From the Main menu, select *Risk Management > 3-D Secure Rules*. The 3DS Rules configuration page displays.

Note: Authentication states (X) - (W) are displayed only if "Use New 3DS Response Codes for VPC/PC" privilege is enabled for your merchant profile.

Configure Clash Action

Action Taken When Risk Rules Result In Both "Always Accept" And "Always Reject".

Always Accept Always Reject [?](#)

Configure Authentication States

Authentication State	No Action ?	Always Accept ?	Review ?	Reject ?
(Y) Card Holder Verified ?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(M) Verification Attempted ?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(E) Card Holder Not Enrolled ?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(U) Undetermined ?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(T) ACS Time Out ?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(D) Directory Server Communication Error ?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(A) Internal Error - Enrolment ?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(I) Internal Error - Authentication ?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(X) Authentication Undetermined ?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(Z) Invalid Enrollment Request ?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(V) Undetermined Invalid Request ?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(B) Enrollment Undetermined ?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(W) Enrollment Parse Error ?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- 2 In the *Clash Action* section, select the action you want to perform when risk rules evaluate to both "Always Accept" and "Always Reject". By default, the action is set to "Always Reject".

The Risk Management module evaluates rules based on the action associated with that rule. A risk recommendation is a summation of all types of rules associated with a transaction inclusive of the rules set at the MSO level. This risk result drives the final action performed on an order. For more information, see *Implications of Risk Recommendation*.

Occasionally, these rules can clash when they evaluate to both "Always Accept" and "Always Reject" and fail to determine the final action on the order. For example, if a card number is listed as a Suspect Card (Always Reject) and if the 3DS rule results in "Always Accept" for an authentication state, then the system encounters a rule deadlock requiring operator intervention to break the deadlock. In such a case, the action set in the Clash Rule configuration page comes into effect to determine the final action taken on the order.

- 3 Select the action you want to perform on the various 3DS authentication states. The following table lists the authentication states and their descriptions.

Field	Description
Card Holder Verified (Y)	Indicates that the cardholder was successfully authenticated.
Verification Attempted (M)	Indicates that the authentication could not be completed, but a proof of authentication attempt (CAVV) was generated. In some cases, a proof of authentication attempt can serve as a substitute for actual authentication.
Card Holder not enrolled (E)	Indicates that the cardholder is not enrolled in an authentication scheme, namely Verified by Visa, MasterCard SecureCode, J/Secure, or American Express SafeKey.
Undetermined (U)	Indicates that the issuer ACS (Access Control Server) is not responding and/or unavailable.
ACS Timeout (T)	Indicates that the response was not received or a timeout occurred waiting for a response from ACS.
Directory Server Communication Error (D)	Indicates that there was an error communicating with the Directory Server during card holder enrollment check.
Internal Error - Enrollment (A)	Indicates an internal system error during card holder enrollment check.
Internal Error - Authentication (I)	Indicates that authentication was attempted but was unsuccessful. The possible reasons for failure are: <ul style="list-style-type: none"> ▪ Authentication of Merchant ID and password to the Directory Server failed. ▪ Error communicating with the Directory Server.
Authentication Undetermined (X)	Indicates that the Access Control Server returned an Enrollment Status of "U".
Invalid Enrollment Request (Z)	Indicates that the Directory Server returned an Enrollment Status of "N" WITH an Invalid Request element. The Invalid Request indicates that the Directory Server rejected the contents of at least one field in the request, i.e., the request was invalid.
Undetermined Invalid Request (V)	Indicates that the Directory Server returned an Enrollment Status of "U" WITH an Invalid Request element.
Enrollment Undetermined (B)	Indicates that the Directory Server returned an Enrollment Status of "U" WITHOUT an Invalid Request element

Field	Description
Enrollment Parse Error (W)	Indicates that the system was unable to parse VERes received from the Directory Server.

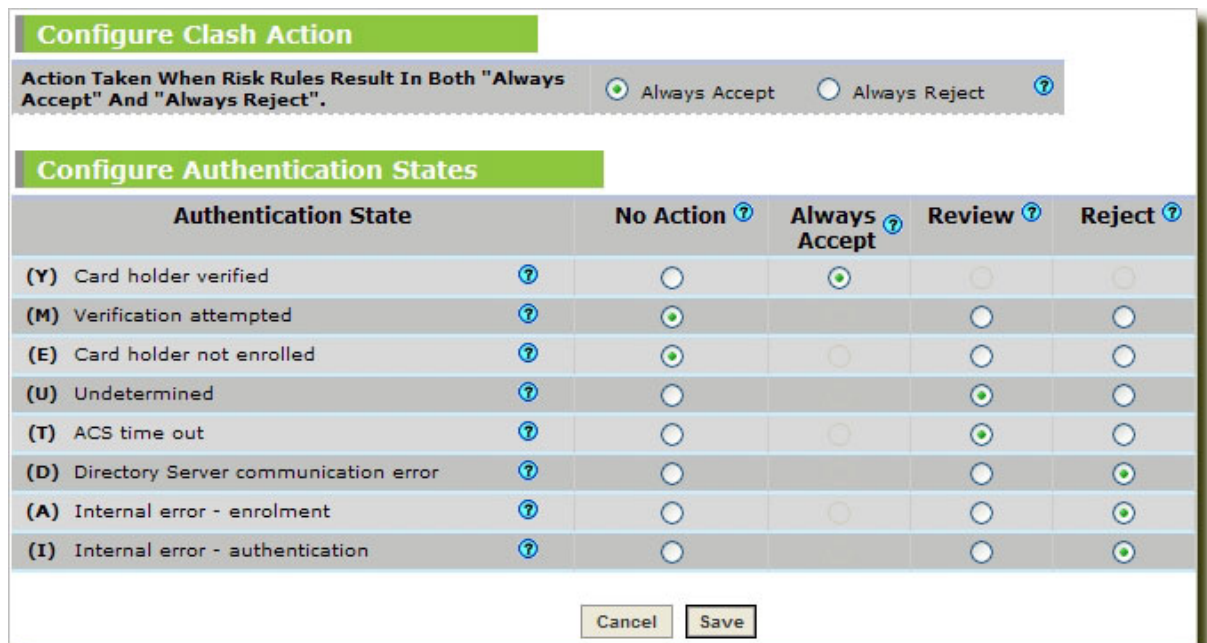
- For an authentication state, select the:
 - [No Action]** button if you want a transaction returning the selected authentication state to be processed normally.
 - [Reject]** button if you want a transaction returning the selected authentication state to be blocked automatically.
 - [Always Accept]** button if you want a transaction returning the selected authentication state to be always processed normally.
 - [Review]** button if you want a transaction returning the selected authentication state to be marked for manual review.
- Click **[Save]** button to save the 3DS Rule including the clash rule configuration. A success message, "Your changes have been saved successfully" displays.
- Click **[Cancel]** if you want to exit the 3DS Rules configuration page without saving any changes.

Note: A 3DS risk result of "Always Accept" returns an Risk Recommendation of "Accept".

Reviewing Currently Rejected 3-D Secure Authentication States

How to review the current list of rejected 3DS Authentication States

- From the Main menu, select *Risk Management > 3-D Secure Rules*. The 3DS Rules configuration page displays.



The **Reject** column displays the authentication states for which transactions are rejected currently. Note that "Always Accept" is enabled for the authentication state "Y-Card Holder Verified" only.

Deleting a 3-D Secure Rule

How to delete a 3-D Secure Rule

- 1 From the **Authentication State** column, select an authentication state for which you want to delete the 3DS Rule.
- 2 Select the **[No Action]** button to allow a transaction with the selected authentication state to be processed normally.
- 3 Click **[Save]** button to save the 3DS Rule.

Configuring AVS Rules

The Address Verification Service (AVS) is a security feature used for Card-Not-Present transactions. It compares the card billing AVS data that the cardholder supplies with the records held in the card issuer's database. Once the transaction is successfully processed and authorised, the card issuer returns a result code (AVS result code) in its authorisation response message. The result code verifies the AVS level of accuracy used to match the AVS data.

Note: The merchant can enforce the Card Holder name entry by enabling the *Enforce Card Holder Name entry for 3-party privilege* in Merchant Manager.

Merchants are encouraged to:

- include shipping data on all shipments, and
- to use the 205-Byte format to include shipping data on all shipments, even if Card member Billing and Ship-to addresses are identical, because this data enhances the ability to assess risk.

Configuring AVS rules enable merchants to either accept or block any transaction based on the AVS response codes. You can configure AVS response codes to belong to three categories:

- No Action (processed normally)
- Review (processed or blocked manually)
- Reject (blocked automatically)

However, an MSO can configure authentication states to belong to only *No Action* and *Reject* categories.

Note: A response code can belong to only one category at any given time.

Before you configure AVS rules, you must be aware of the prerequisites.

Prerequisite

To configure AVS Rules, you must have:

- the *May Configure Risk Rules* operator privilege. See Merchant Operator General Privileges.
- the *May Use AVS* merchant privilege. See Cardholder Verification in Merchant Privileges. If you do not have this privilege, the AVS Rules option does not appear in the Risk Management submenu.
- (optional) the *May Use Verification Only for AVS/CSC Risk Assessment* privilege. Verification Only allows the system to verify card holder information without performing a financial transaction. Enabling this privilege allows you to process AVS rules before the financial transaction; disabling the privilege processes AVS rules after the financial transaction. Any order rejected by the AVS rule after the transaction is automatically reversed by the system.

Note: The acquirer must support Verification Only messages for verifying a card holder successfully.

Adding an AVS Rule

How to add an AVS rule

- 1 From the Main menu, select *Risk Management > AVS Rules*. The AVS Rules configuration page displays.

Configure AVS Response Codes			
AVS Response Code	No Action ?	Review ?	Reject ?
(X) Exact match of 9 digit zip/postal code and street address	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(Y) Exact match of 5 digit zip/postal code and street address	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(A) Street address match only	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(W) 9 digit zip/postal code match only	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(Z) 5 digit zip/postal code match only	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(S) Service not supported	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(R) Issuer system unavailable	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(U) Address unavailable, no data from Issuer	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(N) No address or zip/postal code match	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(E) Not a mail/phone order	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(O) Address verification was not requested	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(G) International transaction, address information unavailable	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(D) International transaction, street address and postal code match	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(M) International transaction, street address and postal code match	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(B) International transaction, street address match but postal code not verified due to incompatible formats	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(P) International transaction, postal code match but street address not verified due to incompatible formats	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(C) International transaction, address not verified due to incompatible formats	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(I) International transaction, address not verified	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(K) Card holder name match only	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(F) Street address and postal code match, applies to U.K. only	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

- 2 Select the action you want to perform on the various AVS response codes. The descriptions next to the response codes indicate what the response codes mean.
- 3 For a response code, select the:
 - **[No Action]** button if you want a transaction returning the selected response code to be processed normally.
 - **[Reject]** button if you want a transaction returning the selected response code to be blocked automatically.
 - **[Review]** button if you want a transaction returning the selected response code to be marked for manual review.
- 4 Click **[Save]** button to save the AVS Rule. A success message, "Your changes have been saved successfully" displays.
- 5 Click **[Cancel]** if you want to exit the AVS Rules configuration page without saving any changes.

Reviewing Currently Rejected AVS Response Codes

How to review the current list of rejected AVS Response Codes

- 1 From the Main menu, select *Risk Management > AVS Rules*. The AVS Rules configuration page displays.

Configure AVS Response Codes			
AVS Response Code	No Action ?	Review ?	Reject ?
(X) Exact match of 9 digit zip/postal code and street address	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(Y) Exact match of 5 digit zip/postal code and street address	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(A) Street address match only	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
(W) 9 digit zip/postal code match only	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
(Z) 5 digit zip/postal code match only	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
(S) Service not supported	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
(R) Issuer system unavailable	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
(U) Address unavailable, no data from Issuer	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
(N) No address or zip/postal code match	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
(E) Not a mail/phone order	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
(O) Address verification was not requested	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(G) International transaction, address information unavailable	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(D) International transaction, street address and postal code match	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(M) International transaction, street address and postal code match	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
(B) International transaction, street address match but postal code not verified due to incompatible formats	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
(P) International transaction, postal code match but street address not verified due to incompatible formats	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
(C) International transaction, address not verified due to incompatible formats	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
(I) International transaction, address not verified	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
(K) Card holder name match only	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
(F) Street address and postal code match, applies to U.K. only	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

By default, the AVS response codes are set to **No Action**.

Deleting an AVS Rule

How to delete an AVS Rule

- 1 From the **AVS Response Code** column, select a response code for which you want to delete the AVS Rule.
- 2 Select the **[No Action]** button to allow a transaction with the selected response code to be processed normally.
- 3 Click **[Save]** button to save the AVS Rule.

Configuring CSC Rules

The Card Security Code (CSC) is a security feature for Card-Not-Present transactions. It is also known as also known as CVV(Visa), CVC2(MasterCard) or CID/4DBC(Amex) or CVV2.

It compares the Card Security Code on the card with the records held in the card issuer's database. For example, on Visa and MasterCard credit cards, it is the three digit value printed on the signature panel on the back following the credit card account number. For American Express, the number is the 4 digit value printed on the front above the credit card account number.

Once the transaction is successfully processed and authorised, the card issuer returns a result code (CSC result code) in its authorisation response message. This verifies the CSC level of accuracy used to match the card security code.

Configuring CSC rules enable merchants to either accept or block any transaction based on the CSC response codes. You can configure CSC response codes to belong to three categories:

- No Action (processed normally)
- Review (processed or blocked manually)
- Reject (blocked automatically)

However, an MSO can configure authentication states to belong to only *No Action* and *Reject* categories.

Note: A response code can belong to only one category at any given time.

Before you configure CSC rules, you must be aware of the prerequisites.

Prerequisite

To configure CSC Rules, you must have:

- the *May Configure Risk Rules* operator privilege. See Merchant Operator General Privileges.
- the *May Use CSC* merchant privilege. See Cardholder Verification in Merchant Privileges. If you do not have this privilege, the CSC Rules option does not appear in the Risk Management submenu.
- (optional) the *May Use Verification Only for AVS/CSC Risk Assessment* privilege. Verification Only allows the system to verify card holder information without performing a financial transaction. Enabling this privilege allows you to process CSC rules before the financial transaction; disabling the privilege processes CSC rules after the financial transaction. Any order rejected by the CSC rule after the transaction is automatically reversed by the system.

Note: The acquirer must support Verification Only messages for verifying a card holder successfully.

Adding a CSC Rule

How to add a CSC rule

- From the Main menu, select *Risk Management > CSC Rules*. The CSC Rules configuration page displays.

CSC Response Code	No Action ?	Review ?	Reject ?
(M) CSC match	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(S) CSC not present on card	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(U) Issuer is not certified for CSC processing	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(N) No CSC match	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
(P) Not processed	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

- Select the action you want to perform on the various CSC response codes. The following table lists the response code and their descriptions.

Field	Description
(M) CSC Match	Indicates a valid or matched CSC.
(S) CSC Not Present on Card	Merchant indicates that the CSC is not present on card.
(U) Issuer is Not Certified for CSC Processing	Indicates that the card issuer is not registered and/or certified.
(N) No CSC Match	Indicates that the CSC is invalid or not matched.
(P) Not Processed	Indicates that the CSC was not processed.

- For a response code, select the:
 - **[No Action]** button if you want a transaction returning the selected response code to be processed normally.
 - **[Reject]** button if you want a transaction returning the selected response code to be blocked automatically.
 - **[Review]** button if you want a transaction returning the selected response code to be marked for manual review.
- Click **[Save]** button to save the CSC Rule. A success message, "Your changes have been saved successfully" displays.
- Click **[Cancel]** if you want to exit the CSC Rules configuration page without saving any changes.

Reviewing Currently Rejected CSC Response Codes

How to review the current list of rejected CSC Response Codes

- 1 From the Main menu, select *Risk Management* > *CSC Rules*. The CSC Rules configuration page displays.

Configure CSC Response Codes			
CSC Response Code	No Action ?	Review ?	Reject ?
(M) CSC match	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(S) CSC not present on card	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
(U) Issuer is not certified for CSC processing	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
(N) No CSC match	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
(P) Not processed	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

The **Reject** column displays the response codes for which transactions are rejected currently. Note that response code "(M) CSC Match" has "Review" and "Reject" actions disabled.

Deleting a CSC Rule

How to delete a CSC Rule

- 1 From the **CSC Response Code** column, select a response code for which you want to delete the CSC Rule.
- 2 Select the **[No Action]** button to allow a transaction with the selected response code to be processed normally.
- 3 Click **[Save]** button to save the CSC Rule.

Searching for Orders Based on Risk Recommendation

The Risk Management module enables you to search for orders based on the risk assessment results. See Order Search. You can also view the Risk Assessment Details for individual orders in the Order Response and Order Details.

Index

A

About the Payment Server • 7
 Accessing Internal Risk • 92
 Acquirer Link Selection • 80, 83
 Action Items • 13, 92, 93
 Adding a 3-D Secure Rule • 34, 114
 Adding a Card BIN Rule • 110
 Adding a CSC Rule • 123
 Adding a Payment Plan • 80, 81, 83
 Adding a Suspected Card Number • 99
 Adding a Trusted Card Number • 95
 Adding an AVS Rule • 119
 Adding an IP Address Range Rule - Merchant
 • 102
 Adding an IP Country Rule • 107
 Admin • 69
 Auth and Capture • 8

B

Basic Concepts • 90
 Batch Closure Receipt Page • 43, 45

C

Capturing an Order Amount • 40
 Changing an Operator's Password • 11, 75, 79
 Changing Your Own Operator Password • 77,
 80
 Changing Your Password at Login • 10
 Completing an Order • 41
 Configuration Details • 69, 71
 Configuration Details - Payment Client • 71
 Configuration Details - Virtual Payment Client •
 70
 Configuration Details Definitions • 69
 Configuring 3-D Secure Rules • 94, 113
 Configuring AVS Rules • 94, 118
 Configuring Card BIN Rules • 94, 110
 Configuring CSC Rules • 94, 122
 Configuring IP Address Range Rules • 94, 101
 Configuring IP Country Rules • 94, 106
 Configuring Your Settings • 69
 Creating a Capture Only Entry Order • 23
 Creating a New Merchant Administration
 Operator • 12, 73
 Creating an Order • 16

D

Dealing with Unsettled Transactions • 43
 Deleting a 3-D Secure Rule • 117

Deleting a Card BIN Rule • 112
 Deleting a CSC Rule • 124
 Deleting an AVS Rule • 122
 Deleting an IP Address Range Rule • 104, 105
 Deleting an IP Country Rule • 109
 Deleting Suspect Card Numbers • 101
 Deleting Trusted Card Numbers • 98
 Disclaimer • 2
 Dismissing Review Decisions or Failed Risk
 Reversals • 93, 94
 Downloading Payment Authentication
 Information • 65
 Downloading Software and Documentation •
 84
 Downloading the Transactions File • 56
 Downloading Transaction Files • 56, 65

E

Editing Merchant Configuration - Virtual
 Payment Client • 71
 Editing Operators • 77
 Editing the Payment Client • 72
 Editing Your Configuration Settings • 71

F

Financial Transactions • 49
 Financial Transactions Search Page • 50

G

Gateway Report Search Page • 67
 Gateway Reports • 67
 General Privileges • 76
 Getting Started • 9

I

Internal Risk Only • 33
 International Definitions • 70
 Introduction • 7
 Introduction to Internal Risk • 86

L

Logging in to Merchant Administration • 10
 Logging Out • 12
 Login Field Definitions • 10

M

Manage Banamex Payment Plans • 19, 80
 Managing Merchant Administration Operators •
 72, 77

Managing Passwords • 79
Managing Risk • 85
Managing Your Transactions with Payment Server • 8
Merchant Administration Operator Details page • 15, 73, 74

O

Order Search Page • 23, 24, 26

P

Payment Authentication Information Flow • 58
Payment Authentications • 57
Payment Authentications Search Page • 60, 65
Payment Authentications Status • 59
Performing Actions on Orders • 40
Preface • 5
Purchase • 9

R

Refunding a Transaction • 41
Reports • 67
Requirements • 7
Resetting a Forgotten Password • 10, 11
Reviewing Current Card BIN Rules • 112
Reviewing Current IP Address Range Rules • 104, 105
Reviewing Current Suspect Card Numbers • 100, 101
Reviewing Current Trusted Card Numbers • 96, 98
Reviewing Currently Rejected 3-D Secure Authentication States • 116
Reviewing Currently Rejected AVS Response Codes • 121
Reviewing Currently Rejected CSC Response Codes • 124
Reviewing Currently Rejected IP Countries • 109
Risk Assessment Details • 31
Risk Management Architecture • 87

S

Searching for Financial Transactions • 49
Searching for Orders • 23
Searching for Orders Based on Risk Recommendation • 85, 124
Searching for Payment Authentications • 59, 61, 62
Searching for Settlements • 45
Selecting Merchant Administration Menu Options • 12
Settlement Details Page • 45, 47
Settlement List - Settled Batches • 45, 46
Settlement Search Page • 45, 46
Settling Orders • 43
Suspect Cards • 94, 98

T

The Create Order Entry Page • 17
The Create Order Response Page • 20
The Home Page • 13
To Add a Secure Hash Secret • 71, 72
To Delete a Secure Secret Hash • 72
To Edit ReturnURL • 71, 72
Trusted Cards • 94, 95
Types of Merchant Profiles • 7
Types of Operators • 73
Types of Orders • 8

U

Unlocking an Operator Account • 78
Unsettled Transactions Summary Page • 43, 44, 45
Using Payment Plans • 80, 82, 83

V

Viewing a Gateway Report • 68
Viewing an Individual Financial Transaction • 49, 51, 52
Viewing an Individual Order - The Order Details Page • 27
Viewing an Individual Payment Authentication • 62
Viewing Orders - The Order List Page • 23, 26
Viewing Risk Management Summary • 92
Viewing the Financial Transactions List • 49, 51, 52, 56
Viewing the Payment Authentications List • 61, 65
Voiding a Transaction • 42

W

Welcome to TNS • 5
Where to Get Help • 5
Who Should Read This Guide • 5
Working with Orders • 15
Working with Rules • 92, 94