



DATA CASH

A MASTERCARD COMPANY

DataCash MiGS Merchant Administration Guide

August 2014
Software version: MR 29.6

Copyright

MasterCard and its vendors own the intellectual property in this Manual exclusively. You acknowledge that you must not perform any act which infringes the copyright or any other intellectual property rights of MasterCard or its vendors and cannot make any copies of this Manual unless in accordance with these terms and conditions.

Without our express written consent you must not:

- Distribute any information contained in this Manual to the public media or quote or use such information in the public media; or
- Allow access to the information in this Manual to any company, firm, partnership, association, individual, group of individuals or other legal entity other than your officers, directors and employees who require the information for purposes directly related to your business.

License Agreement

The software described in this Manual is supplied under a license agreement and may only be used in accordance with the terms of that agreement.

Trademarks

Trademark notices and symbols used in this manual reflect the registration status of MasterCard trademarks in the United States. Please consult with the Customer Operations Services team or the MasterCard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

MasterCard Asia-Pacific (Australia)

Level 8, 100 Arthur Street

North Sydney, NSW 2060

Australia

www.mastercard.com

Contents

1	About Merchant Administration	1
	Introduction	1
	Administrator Account	3
	Frequently Asked Questions	4
2	Getting Started	7
	Logging in to Merchant Administration	7
	Changing Your Password at Login	8
	Selecting Merchant Administration Menu Options	8
	Creating New Operators	9
	Setting Privileges	11
	Configuring details	14
	Locked-out users	15
	Changing Own Password	15
	Logging Out	16
3	Working with Orders	17
	Creating an Order	18
	Searching for Orders	24
	Risk Assessment Details	31
	Performing Actions on Orders	38
	Voiding a Transaction	42
	Capture Completed	42
4	Working with Financial Transactions	43
	Searching for Financial Transactions	43
	Viewing the Financial Transaction List	46
	Downloading Transaction Files	49
5	Working with Payment Authentications	51
	Payment Authentication Information Flow	51
	Payment Authentications Status	52
	Searching for Payment Authentications	53
	Viewing Payment Authentications	54
	Downloading Payment Authentication Information	60
6	Working with Reports	61
	Searching for a Gateway Report	61
	Viewing a Gateway Report	62
7	Admin Options	64
	Configuring Your Settings	64
	Managing Merchant Administration Operators	70
	Managing Passwords	77
8	Managing Risk	80

	Introduction to the Risk Management Module	80
	Accessing Risk Management	85
	Viewing Risk Management Summary	85
	Working with Rules	87
	Trusted Cards	88
	Suspect Cards	89
	Configuring IP Address Range Rules	92
	Configuring IP Country Rules	96
	Configuring Card BIN Rules	100
	Configuring 3-D Secure Rules	101
	Configuring AVS Rules	107
	Configuring CSC Rules	110
	Searching for Orders Based on Risk Assessment	112
9	Glossary	113
10	Appendix A	116

1 About Merchant Administration

Introduction

MiGS Merchant Administration (MA) is an Internet-based portal that allows merchants to monitor and manage their online processing and administration of payments through a series of easy to use pages. Merchant Administration can be accessed via an Internet browser – the appropriate URL will be provided by your bank.

To use Merchant Administration, a merchant profile is required. The profile is a record of merchant details and the permitted functionality that the merchant has within the MA portal. All details are stored on the MiGS Server.

Two types of merchant profile are created through the bank's enrolment process:

- **TEST merchant profile**—allows merchants, within the test facility, to perform transactions against an emulator of the bank's transaction processing system. This profile will always exist for testing purposes. To access this facility, precede the merchant ID with the word TEST, i.e. MERCHANT01 becomes TESTMERCHANT01.
- **PRODUCTION merchant profile**—activates merchants within the production system, allowing them to process transactions directly against the MiGS live transaction processing system. This profile is only activated once testing has been deemed sufficient by the bank.

The MiGS "Virtual Payment Client"—clientless software provided by the bank—is required to provide the interface between the MiGS Payment Server and your merchant Shop & Buy application.

For more information on the Virtual Payment Client (VPC), ask your bank for the "MiGS Virtual Payment Client Integration Guide".

Managing 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 Virtual 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 Virtual 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

There are two types of orders available to choose from when creating an order:

- Auth and Capture
- Purchase

Auth and Capture

This requires two transactions to debit the funds from a cardholder's account. First, an authorisation (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 authorisation transaction is taken into account and reduces the cardholder's available funds as though the transaction had taken place.

Purchase

A single transaction is used to authorise 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.

Help

At any time when using the Merchant Administration facility, you can click on the  icon as it appears and it will display a window giving an explanation of that particular field on the screen.

Certain tabs and functions may not be available to you as a user, depending upon the privileges that have been set for your account. Therefore you may not see certain features that are documented in this manual.

Prerequisites

- Access to the Internet through an Internet browser
- Your Merchant ID
- Your Operator ID and the corresponding password.

Administrator Account

The “Administrator” account within Merchant Administration is the top-level account and the only one created on merchant setup by the bank. This is not an operator account for daily use and only has the ability to search for transactions and perform operator administration tasks. As such, this account should be safeguarded as an operator administration or manager’s account only. It is the only account within MA that is not removable and consequently provides the only access should all other accounts be disabled. It should therefore be under the ownership of a Manager or Supervisor.

To initially log on as the Administrator, the bank will provide you with access details and you will automatically be granted the privileges as explained above. Once you have accessed the system, click on the **Admin** tab at the top of the page. From the options in the left side menu select the **Operators** link and the following page is displayed:



Merchant Administration - Operator List

[Create an Operator](#)

[Create a new Merchant Administration Operator](#)

[Edit an Operator](#)

Operator ID	Operator Name	Description	
Administrator	superuser		Edit

Initially, the Administrator account is the only account.

- 1 Click the **Edit** link to enter the Administrator profile.
- 2 Enter the operator's description and email address.
- 3 Click **Submit** to update the details for this account.

All the available privileges are automatically enabled for the Administrator user and these are:

- Ability to perform operator administration tasks, and
- Ability to use the transaction search function.

Once the Administrator account has been configured accordingly, the user should then create an alternative operator account for daily use as previously advised. This allows the Administrator account to be maintained as a supervisory account to perform administration tasks as necessary. To create a new operator account, see *Creating New Operators* on page 9.

Frequently Asked Questions

Getting Started

Q. Why would I use Merchant Administration?

A. Merchant Administration is used by merchant personnel to monitor and manage their online processing and administration of payments.

Q. How do I access Merchant Administration for the first time?

A. You need the MiGS Merchant Administration URL, your merchant ID, user name and password to access the MA system. These details will be provided by your bank (see *Logging in to Merchant Administration* on page 7).

Q. How do I create additional operator accounts for access to Merchant Administration?

A. You need to have the **Perform Operator Administration** privilege in order to create new users on the system. If you have this privilege, you will need the new operator's details, including name, position and the privileges that they are to be configured with (see the *Creating New Operators* on page 9).

Q. What happens if I lock myself out of Merchant Administration?

A. You have five attempts to correctly enter your password into the MA login screen before your account is disabled. If this happens, you will need a Supervisor or Administrator—someone with the **Perform Operator Administration** privileges—to enter the system and unlock your account. The same password is valid (see the *Locked-out users* on page 15).

Q. Why can I not see all the functionality that is described here in this manual?

A. All operator accounts are created individually. Some users may be set with different privileges to others, depending on the purpose of their access to Merchant Administration. The privileges you have are normally set by your Administrator or Supervisor. This manual describes the features of all functions within MA, some of which you as a user may not have.

Transactions

Q. In Merchant Administration, what is the difference between an Order and Financial Transaction?

A. An Order is the original purchase transaction for goods or services. A financial transaction refers to all transactions – the original order and all subsequent actions, i.e. voids or refunds (see *Working with Financial Transactions*).

Q. How do I search for a transaction?

A. If you are searching for the original purchase transaction, see *Working with Orders* on page 17. If you are looking for a financial transaction (e.g. refund, void) see *Working with Financial Transactions*. If you are searching for an authentication transaction (e.g. MasterCard SecureCode™ or Verified by Visa™), see Searching for Payment Authentications.

Q. How do I search for transactions belonging to a particular batch?

A. A batch is a group of transactions that are awaiting settlement with the Acquiring bank. If you are looking for a transaction within a particular batch, you will need the batch number that the transaction is in to enter into the search field (see *Working with Financial Transactions*). You can also search for transactions by transaction type, transaction number and payment method.

Q. How do I find a failed transaction?

A. All transactions can be searched for by “Transactions Success” – failed or successful. Additional criteria can be used to narrow down your search. To find a failed transaction, see *Working with Financial Transactions*, and select the search criteria for failed transactions.

Q. How do I perform refunds and voids?

A. You are required to have the necessary privileges to perform both refunds and voids. You need to find the original transaction and for a refund, you can process multiple, partial or full amounts. A void is the cancellation of the previous action performed or “last purchase”. The void amount is fixed and cannot be altered (see *Working with Orders* on page 17).

Q. Why is the void option not always available?

A. A void is the cancellation of a transaction so that no funds are transferred, and the transaction will not appear on the cardholder's statement. However, voids can only be performed on transactions that have not yet been sent to the acquiring bank for settlement. If this is the case, then the void option for this particular transaction is no longer displayed.

Q. What do I do about a referred transaction?

A. A referred transaction requires an authorisation code to be processed. You can either:

- Treat it as a decline, and the referred transaction will not be settled unless it is further actioned.
- Contact the issuing bank and query the authorisation. If the authorisation is manually granted by the Issuer, they will give you an Authorisation Code. This code can then be entered into a field that can be accessed in Merchant Administration, via the transaction Order Search.

Card Transactions

Q. How do I perform card transactions on behalf of the customer?

A. A manually entered card transaction in MiGS is referred to as "MOTO". To perform a MOTO transaction, you will need the cardholder's details including card number, expiry date, CSC if applicable, and all the details of the transaction (i.e. order no., merchant references, etc. if applicable) (see *Working with Orders* on page 17).

Reports

Q. How do I get a list of totals for a week's transactions?

A. Reports can be obtained on a daily, weekly, monthly or yearly basis and can also be selected by Acquirer - see *Working with Reports* on page 61 to access daily, weekly, monthly or yearly transaction reports.

2 Getting Started

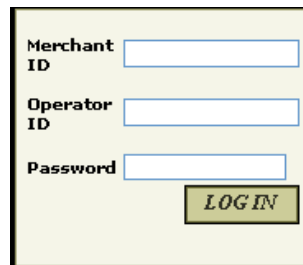
Merchant Administration allows you, as an authorised Operator, to monitor and manage your electronic orders. Authorised Operators can log in from the Login screen and use the various features of Merchant Administration.

Authorised merchant personnel must be set up as Operators before they can log in. For more information see *Managing Merchant Administration Operators*.

Logging in to Merchant Administration

To log in, from the Merchant Administration Login page:

1. Enter your Merchant ID.
2. Enter your Operator ID.
3. Enter your Password-
4. Click **LOG IN**.



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 Operator ID "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* on page 72.

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 your Payment Provider 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.

Table 1 Login Field Definitions

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

Note: Your password should have been provided to you by your Merchant Services Organisation (MSO).

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 New Operators*.

Selecting Merchant Administration Menu Options

The administration options available to you depend on the features provided by your Payment Service Provider and the features that you requested. The options available to you will also depend on your Operator privileges. For more information, see *Creating a New Merchant Administration Operator* on page 71.

The following menu administration options are available in Merchant Administration.

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

Table 2 Merchant Administration Menu Options

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.

Menu Option	Description
Translation Portal	Translate screen labels. Note: This menu is only available if the merchant profile has the Enable Translation Portal privilege.
Logout	Log out and return to the login page.

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 side of the page.
2. Select an option from the submenu. The selected page displays.

Creating New Operators

To create new operators on the system, select the *Admin* tab from the Main menu.

1. Click on the "Operators" link from the menu options on the left. The **Admin - Operator List** will display a register of all operator accounts enabled on the system.

Admin - Operator List

Create an Operator

[Create a new Merchant Administration Operator](#)

Edit an Operator

Operator ID	Operator Name	Description	Change Password	Edit	Delete
Administrator	superuser				
MIGSTEST	Ilan				

2. Click on the [Create a new Merchant Administration Operator](#) link under the **Create an Operator** heading. This will take you to the **Admin - Operator Detail** screen where the new user's details must be entered.

Admin - Operator Details

Operator Details

Merchant	<input type="text" value="M00001"/>
Operator ID	<input type="text"/>
Operator Name	<input type="text"/>
Description	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
Email Address	<input type="text"/>
Locale	<input type="text" value="English (Australia)"/>
TimeZone	<input type="text" value="Australia/Sydney"/>

Security

Lock Operator Account	<input type="checkbox"/>
Change Their Own Password	<input type="checkbox"/>
Must Change Password At Next Login	<input type="checkbox"/>
Password Reset Required	No

Transactions

Perform MOTO Transactions	<input type="checkbox"/>
Perform Purchases	<input type="checkbox"/>
Perform Voids	<input type="checkbox"/>
Perform Stand Alone Captures	<input type="checkbox"/>
Perform Refunds	<input type="checkbox"/>
Perform Stand Alone Refunds	<input type="checkbox"/>

Merchant Maintenance

Modify The Merchant Configuration	<input type="checkbox"/>
Perform Operator Administration	<input type="checkbox"/>

General

View Report Pages	<input type="checkbox"/>
Enable Advanced Merchant Administration Features	<input type="checkbox"/>
Download Order Search Results	<input type="checkbox"/>
Download Transaction Search Results	<input type="checkbox"/>
Allow Software Download	<input type="checkbox"/>
Allow Payment Client Download	<input type="checkbox"/>
Allow Merchant Admin Documentation Download	<input type="checkbox"/>
May Configure Risk Rules	<input type="checkbox"/>
May Perform Risk Assessment Review	<input type="checkbox"/>
May Bypass Risk Management	<input type="checkbox"/>

Complete all the required fields, entering a password that you will later give to that operator. The password validity should be set to "Must change their password at next login" allowing the operator to choose a password they will remember and for security reasons. Passwords must be a minimum of eight characters with at least one alphabetical character and one number and not including the external operator ID. All operators are prompted to change their user password every 90 days.

There is an additional "Lock Operator Account" field in this section which is displayed when the operator has been locked out due to repeated login failures, or a supervisor or Administrator suspends the operator's privileges.

The operator's privileges must then be set, taking care to set only those that are required by that particular user. For example, **Operator Administration** privileges allow those operators to create new users, but also to delete and modify existing ones. It is advised that only supervisors or a select few have this privilege to avoid misuse of its function. For a description of each function, see the Setting Privileges section below.

One privilege to note is **Enable Advanced Merchant Administration Features** (under *General*) as this must only be set for those operators who wish to function only through the Virtual Payment Client directly. Once this has been selected for an operator, they will not be able to log into Merchant Administration via a web browser. All operators wishing to log into the MA portal to enter manual transactions or complete administrative tasks should not enable this privilege.

When all fields have been completed or checked, click **Submit** and a screen is generated confirming the success of creating the new operator.

This process should be completed for each operator that is to be configured on the system. Operator profiles can be edited and deleted by clicking on the appropriate link. The "Administrator" operator account cannot be deleted.

Setting Privileges

The privileges set can differ between operators and should be tailored to each user according to their function within MA. The privileges available to all users are listed below with a brief description of what they allow the operator to do.

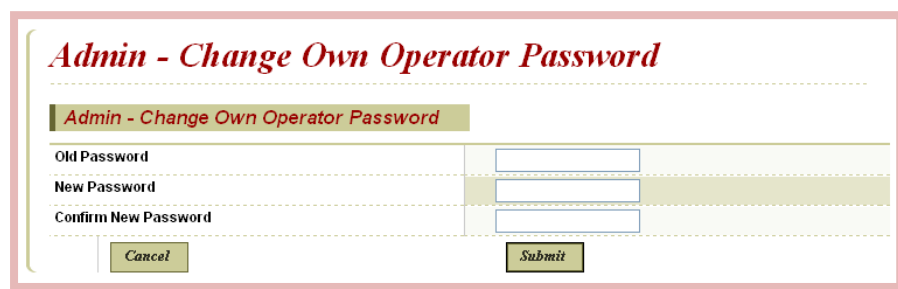
Security Privileges

- Lock Operator Account

This is automatically enabled if the operator repeatedly fails to enter the correct login details. An operator has five attempts to enter their password correctly before being locked out of the system. This option can also be checked to temporarily suspend an operator user.

- Change Their Own Password

This allows an operator to change their own password if necessary, without having to rely on a supervisor.



The screenshot shows a web form titled "Admin - Change Own Operator Password" in red text. Below the title is a green header bar with the same text in white. The form contains three input fields: "Old Password", "New Password", and "Confirm New Password". Each field has a corresponding label to its left. At the bottom of the form are two buttons: "Cancel" and "Submit".

- Must Change Password At Next Login

This will force the operator to change their password when they next log in. This should be checked for all new operators for security reasons.

Note: All operators are prompted to change their user passwords every 90 days.

Transactions

- Perform MOTO Transactions
This allows an operator to enter manual transactions within the MA portal on behalf of the cardholder.
- Perform Voids
This allows an operator to void a transaction. Voids can only be performed if the transaction has not been processed by the acquiring bank, i.e. the transaction is in the current batch date.
- Perform Captures
This allows an operator to perform split authorisation/capture transactions, and to perform a separate request to capture funds from the cardholder.
- Perform Stand Alone Captures
This allows an operator to perform a capture without performing the authorisation step (which may have been performed manually or in an external system).
- Perform Refunds
This allows an operator to process a refund to transfer funds from the merchant back to the cardholder.

Merchant Maintenance

- Modify The Merchant Configuration
This allows the operator to edit the merchant configuration details. These details are preset by the bank and **should not need changing**. Contact your bank should these details need changing.
- Perform Operator Administration
This allows an operator to perform administrative tasks within MA, including creating and deleting other operator accounts. It should only be given to supervisors or managers or those with the authority to carry out such changes.

General

- View Report Pages
This allows the operator access to view the merchant report pages. They can be viewed in either a daily, weekly, monthly or yearly format.

Reports - Gateway Reports

Gateway Reports

From: 8/10/10

To: 8/10/10

Time Interval: Daily

Acquirer: Daily

Currency: USD

Submit

- **Enable Advanced Merchant Administration Features**
This should **not** be enabled for those operators wishing to function through the Merchant Administration web portal. The Advanced Merchant Administration feature is to allow merchants to automatically carry out certain actions directly through the MiGS software (VPC), for example to run a QueryDR search for a transaction. If this privilege is enabled, the operator will not be able to log in to the MA web portal.
- **Download Order Search Results**
This allows the operator to download order information in a text file. The file contains the orders with all the associated financial transactions data
The format of the file is Comma Separated Value.
- **Download Transaction Search Results**
This allows an operator to download a set of transaction data from within MA to export as a .csv file.
- **Allow Software Download**
This allows an operator to download the Payment Client application.

Note: Payment Client is no longer available for new merchant integrations.

Configuring details

To edit Merchant Configuration details, click on **Configuration Details** from the menu on the left side of the page.

The merchant configuration details are preset by the bank and should not need changing. Only the Administrator account needs this privilege and should any changes be needed, the bank should be contacted first.

Admin - Configuration Details

Merchant

Merchant Name	MasterCard Test 1
Merchant ID	MC0001

Internationalisation

Locale	English (Australia)
Time Zone	Australia/Sydney

Virtual Payment Client

Access Code	021F1D8F
Secure Hash Secret 1	FEAA04B99784CC24A65DF364734E143D
Secure Hash Secret 2	4CFE8D3160EE76188B4343B464192CFD

Only limited fields can be edited. Having checked the existing details, click **Edit**.

This displays the **Admin – Configuration Details** screen.

Admin - Configuration Details

Merchant

Merchant Name	MasterCard Test 1
Merchant ID	MC0001

Internationalisation

Locale	English (Australia)
Time Zone	Australia/Sydney

Virtual Payment Client

Access Code	021F1D8F
Secure Hash Secret 1	FEAA04B99784CC24A65DF364734E143D
	<input type="button" value="Delete"/>
Secure Hash Secret 2	4CFE8D3160EE76188B4343B464192CFD
	<input type="button" value="Delete"/>
3-Party Return URL	<input type="text"/>

Payment Client

Client 3-Party Return URL	<input type="text"/>
---------------------------	----------------------

You can amend the following fields for Virtual Payment Client and Payment Client.

Virtual Payment Client

- Secure Hash Secret 1

This allows you to add another Secure Hash Secret value if desired.

- 3-Party Return URL

This allows you to enter the default return web address where the cardholder is directed back to on completion of the transaction, if this is not included in the transaction message.

Payment Client

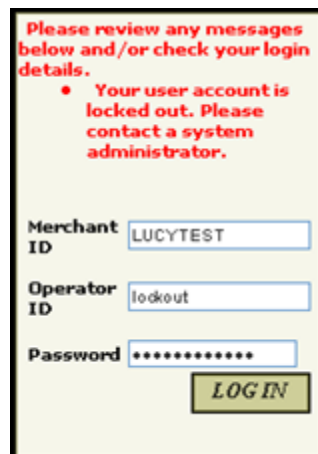
- Client 3-Party Return URL

This allows you to enter the default return web address where the cardholder is directed back to on completion of the transaction, if this is not included in the transaction message.

Click **Submit** or **Cancel** to either save or cancel any changes made and return to the previous screen.

Locked-out users

When logging into Merchant Administration, you have **five** attempts to enter your password correctly before your user account is disabled. If you log in incorrectly, an error message prompts you to check your credentials. If you repeatedly enter incorrect login details, after five attempts you are locked out and the following error message is displayed:

A screenshot of a login form with a yellow background. At the top, red text reads: "Please review any messages below and/or check your login details." Below this, a red bullet point states: "Your user account is locked out. Please contact a system administrator." The form contains three input fields: "Merchant ID" with the value "LUCYTEST", "Operator ID" with the value "logout", and "Password" with masked characters "*****". A green "LOGIN" button is positioned below the password field.

If this happens, contact your Administrator or Supervisor (someone who has the **Operator Administration** privileges) who is able to reset your account. The existing password will still be valid.

Changing Own Password

1. To change your own password, click on **Change Password** from the menu on the left side of the page. The **Admin – Change Own Operator Password** screen is displayed.

Admin - Change Own Operator Password

Admin - Change Own Operator Password

Old Password

New Password

Confirm New Password

2. Enter the old password, and then enter the new password and repeat to confirm. When choosing a new password, you may not enter any of the previous five passwords used for this particular operator account.
3. Click **Submit** to process the change. A confirmation screen is displayed.

Operators with **Operator Administration** privileges have the ability to change the passwords of other operators.

Note: This function will only be available to you if you have the selected privilege set in your operator profile.

Logging Out

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

To log out, select *Logout* from the Main menu. The Login screen is displayed.

3 Working with Orders

Merchant Administration allows an operator to process orders in which card details are provided to the merchant by mail order, telephone, or Interactive Voice Response (IVR) systems.

An order generally consists of two parts: Authorisation and Capture. The authorisation step ensures the validity of the cardholder details and the sufficiency of the cardholder's funds, while a capture is a request to transfer the funds from the cardholder's account.

The two parts can either be contained in a single MiGS request, or in two separate MiGS requests.

Sometimes the authorisation step is performed manually, or in an external system. When this happens, an operator having the **Standalone Capture** privilege may perform a capture without performing the authorisation step.

Note: The Payment Server also supports Standalone Refunds, which are refunds made without an initial order existing in the system. Currently, Standalone Refunds may be viewed, but not performed, in Merchant Administration.

Once orders are created they are available for further processing, for example, if a refund has to be made. Existing orders can be located using a number of search criteria.

Creating an Order

Cardholders can provide card and transaction information to a merchant using a variety of methods, including telephone, fax, email or IVR. The merchant can use this information to process an order.

To create an order:

1. From the Main menu, select **Orders > Create Order**. The **Orders - Create Order Entry** page displays.

Orders - Create Order Entry

Order Reference

Amount AUD - Australian Dollar

Card Holder Name

Card Number

Card Expiry / (mm / yy)

Card Security Code

Bypass Risk Management ☐

Airline Ticket Number

Address

City/Town

State/Province

Zip/Postal Code

Country Australia

Merchant Transaction Source MOTO

Transaction Frequency Default

2. Enter the details of the order, ensuring that all mandatory fields are completed (these are indicated with an asterisk).
3. Click **Submit**.
4. The **Orders - Create Order Response** page displays indicating whether or not the transaction has been successfully authorised.
5. You can proceed in one of the following ways:
 - Click **New Transaction With Current Data** to return to create another order for the same cardholder. This will redisplay the page, enabling you to enter further transactions 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. Continue with Step 6.
6. The **Orders - Order Details** page displays, with all the details of the order as entered.
7. In the Action section, enter the Capture Amount. You may capture a partial amount of the total order or the full amount.

Note: If you have the **Excessive Capture** privilege, you may also capture an amount in excess of the order amount. The maximum amount you may capture is displayed in a message below the Capture Amount field.

8. Click **Capture** to capture the amount specified in the Capture Amount field.
9. If no further amounts will be captured or refunded against the order in future, click **Complete**.
10. The **Orders –Order Details** page displays indicating whether or not the transaction has been successfully captured. This page also provides a **History** section displaying details of all transactions associated with the order.

Note: If you have incorrectly marked an order as **Complete**, click **Incomplete** to allow a further capture or refund to be performed against the order.

11. Select any option from the Main menu or submenu 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.

Table 3 Create Order Entry Page Options

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.
Currency	<p>The currencies supported by the merchant acquirer relationships, displayed with the currency code and the full name. Examples include:</p> <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 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 (654321xxxxxx123) • The full card number is displayed • The card number is not displayed.
Card Start Date	The start date of the card, if available, in mm/yy format.
Card Expiry	The expiry date of the card, in mm/yy format.

Field	Description
Card Security Code	<p>This is a security feature used for card not present transactions. For example:</p> <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.
No CSC Printed On Card	Indicates that although Card Security Codes are being used, no such code is available on the card being processed.
Issue Number	The current issue number, if available, for the card being used.
Bypass Risk Management	<p>Allows the merchant to process transactions without performing risk checks and assessment of orders. Typically, a merchant operator chooses this option for a rejected order if the risk results are identified as false. For Risk Management information, see <i>Managing Risk</i>.</p> <p>Note: You cannot bypass rules configured at the MSO level.</p>
Airline Ticket Number	Originally used for the airline industry, this is an optional field where extra information about the transaction can be stored.
Address	The street details of the cardholder billing address.
City/Town	The city or town of the cardholder billing address.
State/Province	The state or province of the cardholder billing address.
Zip/Postal Code	The zip or postal code of the cardholder billing address.
Country	The country of the cardholder 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"> Default Internet Card Present MOTO Telephone Order Mail Order Voice Response. Auto (Risk) - indicates that the system initiated the transaction due to risk assessment. Orders rejected due to risk assessment after the financial transaction are automatically reversed by the system. <p>Note: If "Default" is selected, the Payment Server will use the Default Transaction Source specified in the merchant profile for the acquirer processing the order.</p>

Field	Description
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"> • Default The Payment Server will use the Default Transaction Frequency specified in the merchant profile for the acquirer processing the order. • Single Transaction This indicates to the acquirer that a single payment is used to complete the cardholder's order. • Recurring 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 and 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. • Instalment Transaction This indicates to the acquirer that the payment is an instalment payment under the card scheme rules. Instalment payments are those where the cardholder authorises the merchant to deduct multiple payments over an agreed period of time for a single purchase.

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, area of operation and information entered on the Order Entry page.

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

- Response Details
- Risk Assessment Details.

Response Details

Table 4 Create Order Response Options

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.
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.
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.
Account Type	<p>The type of bank account – Savings or Cheque.</p> <p>Note: This field is displayed for Maestro cards only.</p>
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 summarising 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 billing address.

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: To create a Capture Only order, both the operator and the merchant must have the **Stand Alone Capture** privilege enabled.

To create a Capture Only entry:

1. On the Main menu, click **Orders > Capture Only**.

The **Capture Only Entry** page is displayed. The **Capture Only Entry** page includes an additional field, **Authorisation Code**, which uniquely identifies the authorisation performed outside Merchant Administration.

2. Enter the details of the order, ensuring that all mandatory fields are completed (these are indicated with an asterisk).
3. Click **Submit**.

The **Capture Only Response** page displays showing whether or not the transaction has been approved.

4. 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

Order Search Page

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 **Search – Order Search** page is displayed.

Search - Order Search

Search for Orders

From 5/6/13 12:00 AM ⓘ

To 5/6/13 11:59 PM

Order ID

Order Reference

Card Number

Outstanding Authorisations ☐

Acquirer ID All

Currency All Currencies

Card Type All Cards

Merchant Transaction Source All

Transaction Success All

Risk Recommendation All

Only Show Orders Where Risk Review Decision Required ☐

Number Of Results To Display On Each Result Page

Submit Download

2. Enter the search parameters. If you enter multiple search parameters, the records returned will match all the search criteria.

3. Click **Submit**.

The **Search - Order List** page details information for each transaction.

4. Click on an individual **Order ID** to view its details. The **Orders - Order Details** page displays.

Table 5 Order Search Page Options

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 user's 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.

Field	Description
Outstanding Authorisations	<p>Search for orders that have authorised amounts against them which have not yet been captured.</p> <p>Note: The orders returned will exclude outstanding authorisations marked as complete.</p>
Acquirer ID	Search for orders processed by a particular acquirer.
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, Internet or Telephone Order).
Transaction Success	Search for orders having a specific success status (for example, successful, failed, or referred).
Orders with High Fraud Score Only	<p>Search for orders that have been identified as high risk.</p> <p>Note: The process of flagging orders as high-risk is performed externally to Merchant Administration.</p>
Risk Recommendation	<p>Search for orders having a specific risk recommendation: Valid values are:</p> <ul style="list-style-type: none"> ▪ Accept — indicates that the order was processed normally. ▪ Not Checked — indicates that the order was not assessed for risk. This may occur: <ul style="list-style-type: none"> • if Bypass Risk Management option is activated for this particular transaction; • if 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. ▪ All — indicates orders with one or more of the aforementioned risk recommendations. <p>Note: This field is displayed if Risk Services privilege is enabled for a merchant.</p>
Only Show Orders Where Risk Review Decision Required	<p>Search for orders where a decision has not been taken on whether to accept or reject the order based on risk recommendation.</p> <p>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.</p> <p>Note: This field is displayed if Risk Services privilege is enabled for a merchant.</p>

Field	Description
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.

Table 6 Order Search Page Options

Field	Description
Acquirer ID	The unique identifier of the acquirer or bank who will process the transaction or order.
Transaction Number/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 summarising 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. Example values are: <ul style="list-style-type: none"> Authorised Captured.
Capture	A check box enabling the operator to select orders against which funds are to be captured.

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

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

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

Viewing an Individual Order - The Order Details Page

The **Order Details** page lists the following information for an order:

- Order Details (Table 7)
- Address Verification Details (Table 10)
- Card Details (Table 8)
- Authorisation Response Data (Table 9)
- Risk Assessment Details (Table 13 Risk Assessment Details)
- Action (Table 11)
- History (Table 12)

Order Details

Table 7 Order Details

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.
IP Address	The IP address of the source of the transaction.
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.
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
Manual Authorisation	Indicates ('Yes' or 'No') whether the order was authorised manually. Manual authorisations require an authorisation code to be specified by the operator.

Field	Description
Merchant Transaction Source	<p>The method by which the merchant received the order. Typical transaction sources include:</p> <ul style="list-style-type: none"> • Default • Internet • Card Present • MOTO • Telephone Order • Mail Order • Voice Response • Auto (Risk) - indicates that the system initiated the transaction due to risk assessment. Orders rejected due to risk assessment after the financial transaction are automatically reversed by the system. <p>Note: If 'Default' is selected, the Payment Server will use the Default Transaction Source specified in the merchant profile for the acquirer processing the order.</p>
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 cardholder's order. • Recurring 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 and 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. <p>Note: The Payment Server does not perform Recurring or Installment payments on behalf of the merchant. If configured, the merchant's integration software will initiate these transactions.</p>
Response Code	<p>A code and brief description summarising the result of attempting to process the order. Example response codes are:</p> <ul style="list-style-type: none"> • 0 - Approved • 3 - Timed Out.

Field	Description
Recurring Response Code	<p>The system response code for recurring transactions. The values are:</p> <ul style="list-style-type: none"> 01 New Account Information Available 02 Try again later 03 Do not try again later for recurring payment transactions. <p>Note: This field may or may not appear, depending on the merchant's configuration.</p>
Wallet Indicator	The identifier returned by MasterPass Online if MasterPass Online digital wallet was used by the customer to provide the card details for this transaction.

Card Details

Table 8 Card Details

Field	Description
Card Type	The type of card used for the transaction.
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.
Account Type	<p>The type of bank account - Savings or Cheque.</p> <p>Note: This field is displayed for Maestro cards only.</p>
Commercial Card	<p>Indicates if the card used is a commercial card. Example codes are:</p> <ul style="list-style-type: none"> N - Not a commercial card Y - Commercial card U - Undetermined.
Commercial Card Indicator	<p>Indicates the type of commercial card as returned by the card issuer. For example,</p> <ul style="list-style-type: none"> 0 (zero) - Decline or not a Commercial Card (Visa only) 1 - Consumer card (MasterCard only) R - Corporate Card (Visa only).
Card Start Date	The start date of the card, if provided.
Issue Number	The issue number, if provided.
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.

Authorisation Response Data

Note: The following fields are additional authorisation data returned by the issuer for authorisation and purchase transactions. This data may vary based on the card scheme.

Table 9 Authorisation Response Details

Field	Description
Return ACI	The ACI (Authorisation Characteristics Indicator) returned by the issuer.
Issuer Transaction Identifier	The unique identifier for the transaction returned by the issuer.
Card Level Indicator	Indicates the card level result returned by the issuer.
Financial Network Code	Indicates the code of the financial network that was used to process the transaction with the issuer.

Address Verification Details

Table 10 Address Verification Details

Field	Description
Card Holder Name	The name of the cardholder.
Address	The street details of the cardholder billing address.
City/Town	The city or town of the cardholder billing address.
State/Province	The state or province of the cardholder billing address.
Zip/Postal Code	The zip or postal code of the cardholder billing address.
Country	The country of the cardholder 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)'.

Action

This section displays tasks that may be performed against the order. The actions available depend on the history of actions previously performed on the order. For example, an order which has only been authorised will allow amounts of the order to be captured. However, an order which has been completed, will no longer display the Capture action button.

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

Table 11 Order Action

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

The History section displays a list of all transactions that have so far been processed for the order.

Table 12 Order History

Field	Description
Response Code	A code and brief description summarising the result of attempting to process the order. Example response codes are: <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	Indicates the type of action performed on the order, e.g: <ul style="list-style-type: none">• Authorisation• Capture• Purchase• Refund• Void Capture• Void Purchase• Void Refund• Credit Payment• Void Credit Payment.
Amount	The amount associated with the transaction in the transaction currency. For example, AUD \$100.00.
Operator ID	The identifier of the merchant operator that performed the action.
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.
Transaction Source	Indicates the integration facility used to generate the transaction. Typical transaction sources include: <ul style="list-style-type: none">• PC — the transaction source is Payment Client.• MOTO — the transaction source is Merchant Administration.• 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 and is automatically attempted for a reversal by the system.

Risk Assessment Details

The **Order Response** and **Order Details** screens may display the Risk Assessment Details for an order, which includes the overall risk result and the individual rules configured for the merchant and the MSO. For further information see *Working with Payment Authentications*.

You can choose to view or hide the system/merchant rules by clicking the [Show](#) or [Hide](#) links as shown below:

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

Risk Assessment Details

Risk Recommendation

Accept

Order Reversal Status

OK

Risk Rules

Rule	Result	Details	Source
Trusted Card List	<div>✓</div> No Action		Merchant Rules
Merchant BIN Range	<div>✓</div> No Action	512345	Merchant Rules
Merchant CSC	<div>✗</div> Reject	U	Merchant Rules
Suspect Card List	<div>✓</div> No Action		Merchant Rules
MSO BIN Range	<div>✓</div> No Action	512345	MSO Rules
MSO CSC	<div>✓</div> No Action	U	MSO Rules

Table 13 Risk Assessment Details

Field	Description
Risk Recommendation	<p>This field indicates the final action taken on the order based on the risk assessment performed. Possible values are:</p> <ul style="list-style-type: none"> Accept — indicates that the order can be processed normally. Not Checked — indicates that the order was NOT assessed for risk. This may occur: <ul style="list-style-type: none"> if the order is processed by activating Bypass Risk Management option. if neither MSO nor merchant risk rules are configured in the system. Review — indicates that the order requires manual review. Reject — indicates that the order was rejected and cannot proceed. 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.

Field	Description
Order Reversal Status	<p>This field indicates the result of an order reversal for each authorisation or purchase that occurred due to risk assessment.</p> <p>This field is displayed only for orders that are rejected due to risk assessment after the financial transaction has been performed. Rejected 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 enable the "May Use Verification Only for AVS/CSC Risk Assessment" merchant privilege. Verification Only allows the system to verify cardholder information without performing a financial transaction.</p>
Risk Rules	<p>This sections displays the following details about risk rules:</p> <p>Rule - The type of risk rule configured by the merchant or MSO. For example, Merchant BIN Range, MSO CSC, Suspect Card List, etc.</p> <p>Result - result for the specific risk rule when performed against this order. 🟢 and 🚫 indicate positive and negative assessment respectively. ⚠️ indicates review.</p> <p>Details - Additional information about the risk rule result. For example, if a BIN Rule was configured at the MSO level, the record displays the BIN range.</p> <p>Source - The source of the risk rule. Valid values are:</p> <ul style="list-style-type: none"> • Merchant Rules: Internal risk rules configured at the merchant level, which include Card BIN Rules, Trusted Cards, Suspect Cards, IP Address Range, IP Country, 3-D Secure, AVS, and CSC Rules. • MSO Rules: Internal risk rules configured at the MSO level, which always override the rules configured at the merchant level.

Implications of Risk Recommendation

This section describes the implications of the risk recommendation when internal risk is enabled.

Note: Only Authorization, Pay, Verification Only, and Standalone Capture transactions are assessed for risk. Risk assessment on other transactions such as Standalone Refunds or Voids is not performed.

The possible values for risk recommendation are:

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

When Risk Recommendation is Set to Accept

A risk recommendation of Accept is displayed in the **Orders - 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

Order Reversal Status

OK

Risk Rules

Rule	Result	Details	Source
Trusted Card List	No Action		Merchant Rules
Merchant BIN Range	No Action	512345	Merchant Rules
Merchant CSC	Reject	U	Merchant Rules
Suspect Card List	No Action		Merchant Rules
MSO BIN Range	No Action	512345	MSO Rules
MSO CSC	No Action	U	MSO Rules

Examples

Case A: 3-DS Rule with Clash Rule Configuration

The cardholder who initiated the transaction is enrolled for 3-DS and the following system and merchant rules apply. Also assume that the 3-DS authentication returns Verification Attempted as the authentication result.

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

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

- Go to the 3-DS Rules Configuration page and configure the Clash Rule to Always Accept to proceed with the order. For more information on Clash Rule, see *Adding 3-D Secure Rule*.
- Go to the 3-DS 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: 3-DS Rule when failed authentication is rejected by the system

The cardholder who initiated the transaction is enrolled for 3-DS and the following system and merchant rules apply.

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

Based on the Overall Risk Result, it seems that this transaction should be accepted; however, if the 3-DS 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 3-DS 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.

An order with the 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.

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. You can retry an order reversal on a failed reversal by clicking **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 for 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.

Case C: IP Country Rule

The cardholder who initiated the transaction is currently present in Country_A and the following system and merchant rules apply.

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

You 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, resubmit the order by enabling the **Bypass Risk Management** option.
- As the cardholder appears trustworthy, add the cardholder to the Trusted Cards list to ensure that any future review decisions on this cardholder can be bypassed. A cardholder added to the trusted cards list is always accepted unless rejected at the MSO level.

Case D: CSC Rule

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

Rule Type	System Rules	Merchant Rules	Overall Risk Result
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 without 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 authorisation 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 for this particular cardholder, resubmit 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 **Orders - 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 reconfigured to accept the transaction.

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 **Orders - 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 authorisation returns an overall risk result of Review, then a subsequent Capture transaction will not be allowed until 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.

On the Order Details screen, click **Accept Order** to proceed with the order, or else click **Reject Order**.

The reviewed orders will display the risk review resolution under **Risk Assessment Details**.

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

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

- The acquirer supports Void Purchase, and
- The order is in an unreconciled batch.

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 are not allowed to perform bulk capture on orders with the Risk Recommendation of Review.

Case E: IP Country Rule

The cardholder who initiated the transaction is currently present in Country_A and the following system and merchant rules apply.

Rule Type	System Rules	Merchant Rules	Overall Risk Result
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 even 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 any future review decisions on this cardholder can be bypassed.
- Reject the order if the cardholder has a fraudulent transaction history or has no previous records of transaction. As the cardholder appears untrustworthy, add the cardholder to the Suspect Cards list to ensure that any future review decisions on this cardholder can be bypassed.

Case F: Card BIN Rule

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	Overall Risk Result
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 any future review decisions on this cardholder can be bypassed.
- Proceed with the order if the merchant operator identifies the risk rule as false and reconfigure 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 any future review decisions on this cardholder can be bypassed.

Performing Actions on Orders

The **Action** section on the **Orders Details** page allows the Operator to perform actions on an Order. These actions will vary according to the payment type and the stage of the payment cycle. For example, an order which has been partially captured may display as shown in the example.

Card Details	
Card Type	Mastercard
Card Number	531358000000430
Card Expiry	05/13
Action	
Refund Amount	AUD \$ <input type="text" value="60.00"/>
<input type="button" value="Refund"/>	

Note: The only Action available for a Purchase transaction, that is, for a Purchase only merchant, is Refund.

Actions which may be available for a transaction are:

- Capture
- Refund
- Complete
- Void.

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

Note: The merchant acquirer link used to process the order must still be active, however, it need not be configured for the currency and card type associated with the order.

Capturing an Order Amount

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

To capture an amount for an authorised transaction:

1. Enter the amount in the **Capture Amount** field.
2. Click **Capture**.

The refreshed **Order Details** page appears. The Capture Amount is incremented by the amount of the capture.

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.

For example, a book supplier may have authorised an order for three books, but then discovers that only two of the ordered books can be found on the 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 **Complete**.

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 **Incomplete**.

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 an Order Amount

Refunds are performed for many reasons, for example, the return of unwanted, incorrect, or faulty goods. A refund can do either of the following:

- Cancel any purchases performed on a pre-authorised amount
- Cancel any captures performed on a pre-authorised amount.

To refund a shopping transaction:

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

Notes:

Refunds are not supported by all card types.

The Payment Server also supports Stand Alone Refunds, which do not need to be performed against an existing order. Stand Alone Refunds may be performed through Virtual Payment Client.

Excessive Refunds

An excessive refund is one which exceeds the authorised amount of an order. Excessive refunds are permitted if you have the user privilege **Perform Excessive Refunds** selected in the Operator Details page (see *Merchant Administration Operator Details* page). An excessive refund limit for each currency configured for the merchant is also specified in this page. If the refund limit is not specified, you cannot perform an excessive refund against that currency.

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 a refund, purchase, or a capture. The option displayed depends on the action you last performed. You cannot void a nominal authorisation.

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

Card Details	
Card Type	Mastercard
Card Number	531 358xxxxxx430
Card Expiry	

Action	
Refund Amount	AUD \$ 20.00
<button>Refund</button>	
<button>Void Capture</button> Void the most recent successful capture	

To void an Order:

- Click **Void Purchase, Void Refund** or **Void Capture**.

The refreshed **Order Details** page displays and includes the new transaction.

Capture Completed

If you do not expect to completely capture an outstanding authorised amount, you can mark a transaction as **Capture Completed**. This removes it from the Outstanding Authorisations list.

To mark an Order ID transaction (shopping transaction) as Capture Completed:

- Click Complete.

The refreshed **Order Details** page displays and shows the outstanding authorisation as completed.

4 Working with 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, authorising 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 **Search - Financial Transaction Search** page displays.

Search - Financial Transaction Search

Search for Financial Transactions

From	5/6/13 12:00 AM	?
To	5/6/13 11:59 PM	
Transaction Number		
Settlement Batch Number		?
RRN		
Merchant Transaction Reference		
Currency	All Currencies	
Transaction Type	All	
Payment Method	All	
Acquirer ID	All	
Transaction State	All	
Authentication Type	Ignore	
Authentication State	Ignore	
Number Of Results To Display On Each Result Page		

Submit **Download**

2. Enter the search parameters.
If you enter multiple search parameters, the records returned will match all the search criteria.
3. Click **Submit**.
The **Search - Financial Transaction List** page displays.

Search - Financial Transaction List

Financial Transaction List

Acquirer ID	Transaction Number	Merchant Transaction Reference	Transaction Type	Amount	Date	Response Code
MIGS S2I Test Bank	49		Void Purchase	AUD \$100.00	5/6/13 11:47 AM	0 - Approved
MIGS S2I Test Bank	48		Purchase	AUD \$100.00	5/6/13 11:46 AM	B - Fraud Risk Blocked

1

Download Search Results

- Select an individual **Transaction ID** to view its details.
The *Orders - Financial Transaction Details* page displays.

<i>Orders - Financial Transaction Details</i>	
Financial Transaction Details	
Acquirer ID	MIGS S2I Test Bank — 987654321234567
Transaction Number	49
Transaction ID	5R1GPB
Merchant Transaction Reference	
Date	5/6/13 11:47 AM
Transaction Type	Void Purchase
Payment Method	Credit
Amount	AUD \$100.00
Order ID	48
Settlement Batch Number	20130605
Acquirer Batch Reference	
RRN	315611344436
Response Code	0 - Approved
Acquirer Response Code	00
Authorisation Code	
Integration Type	MA (Merchant Administration)
Transaction Source	Risk Auto

Financial Transaction Search Page

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

Table 14 Financial Transactions Search Page

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 user's 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.
Settlement Batch Number	Select transactions belonging to a particular batch.
RRN	The RRN (Reference Retrieval Number) allows the Acquirer to uniquely identify a transaction.

Field	Description
Merchant Transaction Reference	A unique merchant specific identifier.
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. <ul style="list-style-type: none"> • Credit.
Acquirer ID	Search for orders processed by a particular acquirer.
Currency	Search for orders processed by a particular currency or all currencies.
Transaction State	Search for orders having a specific success status (for example, successful, failed, or referred).
Authentication Type	Search for a particular type of 3-DS 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 • MasterCard SecureCode • Verified By Visa • JCB J/Secure • American Express SafeKey • Diners Club ProtectBuy.
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 **Submit** to start the search. The **Search - Financial Transaction List** page displays.

Viewing the Financial Transaction List

To view financial transactions, use the search methods described in *Searching for Financial Transactions* on page 43.

The **Search - Financial Transaction List** page details the following information for each transaction.

Select an individual Financial Transaction ID to view its details.

Table 15 Financial Transactions List

Field	Description
Acquirer ID	The unique identifier of the acquirer or bank who will process the order.
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.
Transaction Type	Indicates the type of action performed on the order, for example: <ul style="list-style-type: none">• Authorisation• Capture• Purchase• Refund• Void Capture• Void Purchase• Void 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 summarising 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 Financial Transaction

After the list of financial transactions displays, you can select an individual financial **Transaction ID** to view its details. The **Orders - Financial Transaction Details** page displays the following details of an individual financial transaction.

Table 16 Individual Financial Transaction Details

Field	Description
Acquirer ID	The unique identifier of the acquirer or bank who will process the order.
Transaction Number	An automatically generated number uniquely identifying the transaction. This identifier is unique within the merchant.
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.
Date	The user-locale date and time at which the order was created.
Transaction Type	Indicates the type of action performed on the order, for example: <ul style="list-style-type: none"> • Authorisation • Capture • Purchase • Refund • Void Capture • Void Purchase • Void Refund.
Payment Method	The category of the card type. <ul style="list-style-type: none"> • Credit.
Amount	The total amount of the order in the transaction currency. For example, AUD \$100.00.
Order ID	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).
Settlement Batch Number	The identifier for the batch to which the transactions belongs.
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 summarising 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.

Field	Description
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. <p>Note: The Payment Client is no longer available for new merchant integrations.</p>
Integration Type Version	<p>The version number of the payment software used to integrate with the Payment Server.</p> <p>Note: This field is displayed only if the Integration Type is PC or VPC.</p>
Transaction Source	<p>Indicates the source of the transaction. Typical transaction sources include:</p> <ul style="list-style-type: none"> • PC • MOTO • 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 and is automatically attempted for a reversal by the system.
Payment Authentication ID	<p>Displays the unique ID of an authentication record, if payment authentication was used in processing the transaction.</p>

Downloading Transaction Files

To use the download transaction information functionality, you must have been set up to do so by your Payment Service Provider.

The Download button on **Search - Financial Transaction Search** or the [Download Search Results](#) link on the **Search - Financial Transaction List** allow 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 Comma Separated Value 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.

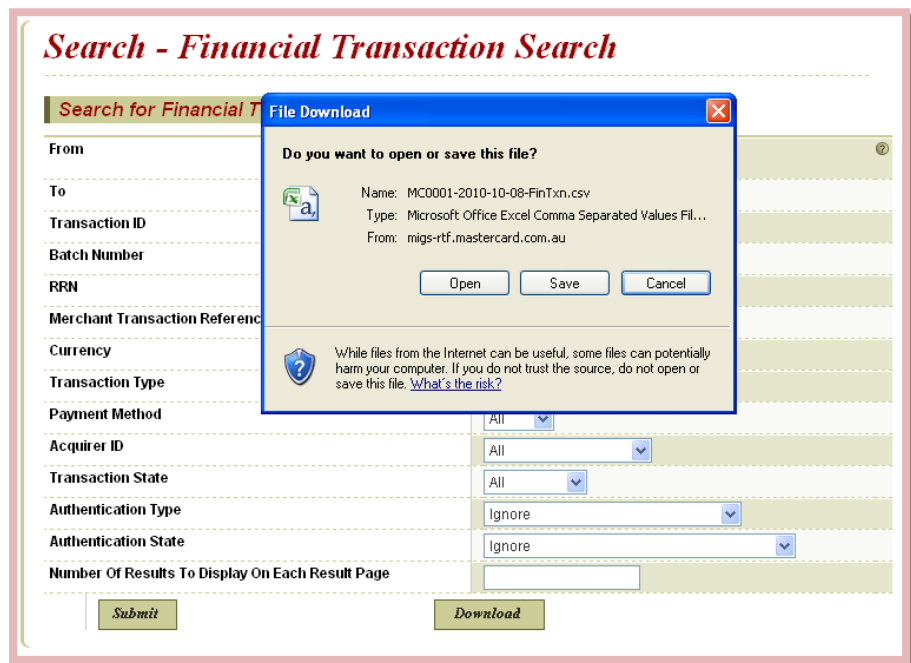
To download transaction information you must first enter your search criteria in the **Search - Financial Transaction Search** page.

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.

The screenshot shows the 'Search - Financial Transaction Search' form. It has a title bar with the text 'Search - Financial Transaction Search' in red. Below the title bar is a section header 'Search for Financial Transactions' in a green box. The form contains several input fields and dropdown menus for search criteria: 'From' (date/time: 5/6/13 12:00 AM), 'To' (date/time: 5/6/13 11:59 PM), 'Transaction Number', 'Settlement Batch Number', 'RRN', 'Merchant Transaction Reference', 'Currency' (dropdown: All Currencies), 'Transaction Type' (dropdown: All), 'Payment Method' (dropdown: All), 'Acquirer ID' (dropdown: All), 'Transaction State' (dropdown: All), 'Authentication Type' (dropdown: Ignore), 'Authentication State' (dropdown: Ignore), and 'Number Of Results To Display On Each Result Page'. At the bottom of the form are two buttons: 'Submit' and 'Download'.

1. From the **Search - Financial Transaction Search** page, enter the search criteria and click **Download**.

A dialog box displays, prompting you to Open or Save the file.



2. Open or save the file.

Select **Open** to open the transaction information file, for example using Excel (the default option).

Select **Save** to save the transaction information in a text or csv file by entering the file name and selecting the location to save the file.

The format of the file is Comma Separated Value and the filename has 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.

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

5 Working with Payment Authentications

The various card schemes 3-D Secure (3DS) programs are payment authentications designed to reduce 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 enters 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 3-DS 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 cardholder 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, and 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 payment authentication:

1. Select **Search** from the Main menu.
2. Select **Payment Authentications Search** from the submenu.
The **Search - 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 **Search - Payment Authentication Search** page to find the required payment authentications.

The search parameters are as follows:

Table 17 Searching for Payment Authentications

Field	Description
Merchant ID	Enter a Merchant ID or click Search 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 user's 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 3-DS 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• MasterCard SecureCode• Verified By Visa• JCB J/Secure• American Express SafeKey.• Diners Club ProtectBuy

Field	Description
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.

Viewing Payment Authentications

To view the results of your search, click **Submit** on the **Search - Payment Authentication Search** page (see *Searching for Payment Authentications* on page 53).

The results display on the **Search - Payment Authentication List** page.

The **Search - Payment Authentication List** page details the following information for each authentication.

Table 18 Viewing Payment Authentications

Field	Description
Authentication ID	The unique payment authentication ID. Click on the ID to view the authentication details.
Authentication Type	The type of 3-DS authentication. The available types of 3-DS 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. • Diners Club ProtectBuy
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.

Field	Description
Response Code	<p>A code and brief description summarising the result of attempting to process the order. Example response codes are:</p> <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 **Search - Payment Authentication Search** page (see *Searching for Payment Authentications* on page 53). The **Search - Payment Authentication Details** page displays.

The **Search - 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.

Table 19 Viewing an Individual Payment Authentication

Field	Description
Authentication ID	A unique payment identifier for the authentication ID. Click on the ID to view the authentication details.
Date	The user-locale date and time at which the action or order was processed or created.
Order Reference	The merchant's reference number for the order.
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 (654321xxxxxx123) • The full card number is displayed • The card number is not displayed.
Amount	The total amount processed for the transaction or order in the transaction currency. For Example, AUD \$100.00.
Authentication Type	<p>The type of 3-DS authentication. The available types of 3-DS authentication are:</p> <ul style="list-style-type: none"> • All Authenticated Transactions • All Non-Authenticated Transactions • Verified by Visa • MasterCard SecureCode • JCB J/Secure • American Express SafeKey • Diners Club ProtectBuy.

Field	Description
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>
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.</p> <p>It is shown for all transactions except those with authentication status "Failure".</p> <p>These values are:</p> <ul style="list-style-type: none"> • 05 – Fully Authenticated • 06 – Not authenticated (cardholder not participating) • 07 – Not authenticated (usually due to a system problem or invalid password).
Verification Token (CAVV)	The Verification Token (CAVV = Cardholder Authentication Verification Value) is a Visa/Diners Club token generated at the card issuer to prove that the Visa/Diners Club cardholder authenticated satisfactorily.
Verification Token (UCAF)	The Verification Token (UCAF = Universal Cardholder Authentication Field) is a MasterCard token generated at the card issuer to prove that the MasterCard cardholder authenticated satisfactorily.
Verification Token (AEVV)	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.

Field	Description
3-D Secure VERes.Enrolled	<p>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:</p> <ul style="list-style-type: none"> Y – Yes N – No U – Undetermined. For example, the payment authentication 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 PARes.Status	<p>Indicates the result of the cardholder authentication. The available values are:</p> <ul style="list-style-type: none"> Y – Yes N – No A – Attempted authentication but failed. For example the cardholder failed to enter their password after five attempts. U – Undetermined. The payment authentication 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.
Enable 3-D Secure Blocking	<p>Allows the merchant to block transactions that fail 3-D Secure verification (a mechanism requiring the cardholder to enter a password that is linked to their credit card). In this context, a transaction is considered to have failed 3-D Secure verification if it results in a Verification Security Level of '07'.</p> <p>Corporate cards that are given a Verification Security Level of '07' for business reasons will also be blocked.</p> <p>A blocked transaction results in a Dialect Response Code of 'B', which is included in the DR and displayed in the Financial Transaction Details page.</p> <p>If you disable this option, a transaction with failed Authentication (eg, wrong password) will still be blocked. Disabling this option allows Merchants to pass transactions with a Verification Security Level of '07' resulting from a system error, or for other business reasons.</p> <p>Note: Transactions that are blocked by 3-D Secure verification are not saved in the database, and cannot be viewed in Merchant Administration.</p>

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).

Field	Description
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.

1. Enter your search criteria in the **Search - Payment Authentication Search** page.
2. Click **Download**, or click the [Download Search Results](#) link on the **Search - Payment Authentication List** page.

A dialog box displays, prompting you to Open or Save the file.

3. Select **Open** to open the transaction information file, for example using Excel (the default option).

Select **Save** to save the transaction information in a text or csv file by entering the file name and selecting the location to save the file.

The format of the file is Comma Separated Value and the filename has 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.

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.

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

6 Working with Reports

A range of reports is available depending on the merchant operator's privileges. The commonly used fields for searching reports are shown below

Searching for a Gateway Report

Gateway reports display the details of all merchants' transactions that have been processed by the Payment Server. The option 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 **Reports - Gateway Reports** page displays.

2. Enter your search parameters.
If you enter more than one parameter the records returned match all your search criteria.
3. Click **Submit**.
The Gateway Report page displays.

Gateway Report Search Page

Use the fields on the **Reports - Gateway Reports** page to enter the search parameters for your order search.

The search parameters are as follows:

Table 20 Gateway Report Search Page

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.

Field	Description
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	Search for orders processed by a particular acquirer.
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 **Reports - Gateway Reports** page.

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

The following table shows fields from the report. Actual fields in a report may vary depending on the merchant's configuration by the acquirer.

Table 21 Viewing a Gateway Report

Field	Description
Date	The start date of the period for which transactions are aggregated.
Acquirer	The name of the acquirer who processed the transactions.
No. Transactions	The number of transactions processed by the acquirer, in a given currency, during the reporting period.
Merchant	The merchant's unique alphanumeric identifier. There is a unique Merchant ID for each merchant account and profile.
No. Settlements	The number of transactions 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.

Field	Description
Total Refunds	The total amount (specified using the currency and the currency symbol) of refunds in the reported transactions.

7 Admin Options

The **Admin** menu allows you to:

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

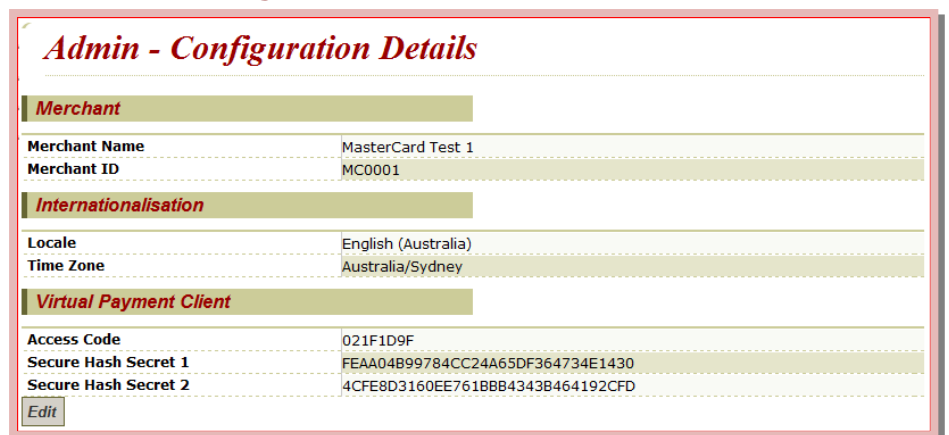
Configuring Your Settings

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

How to configure your merchant settings:

1. Select **Admin** from the Main menu.
2. Select **Configuration Details** from the submenu.

The **Admin – Configuration Details** page displays.



The screenshot shows the 'Admin - Configuration Details' page. It is divided into three main sections: Merchant, Internationalisation, and Virtual Payment Client. Each section contains a table of configuration details. The Merchant section shows 'Merchant Name' as 'MasterCard Test 1' and 'Merchant ID' as 'MC0001'. The Internationalisation section shows 'Locale' as 'English (Australia)' and 'Time Zone' as 'Australia/Sydney'. The Virtual Payment Client section shows 'Access Code' as '021F1D9F', 'Secure Hash Secret 1' as 'FEAA04B99784CC24A65DF364734E1430', and 'Secure Hash Secret 2' as '4CFE8D3160EE761BBB4343B464192CFD'. There is an 'Edit' button at the bottom left of the form.

Merchant	
Merchant Name	MasterCard Test 1
Merchant ID	MC0001

Internationalisation	
Locale	English (Australia)
Time Zone	Australia/Sydney

Virtual Payment Client	
Access Code	021F1D9F
Secure Hash Secret 1	FEAA04B99784CC24A65DF364734E1430
Secure Hash Secret 2	4CFE8D3160EE761BBB4343B464192CFD

3. Click **Edit**.
4. Make changes as required and click **Submit**.
5. The message "Configuration Changes Saved" is displayed on the Configuration Details screen and details redisplayed with changed information.

Merchant Details

Table 22 Configuration Details - Merchant

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

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

Internationalisation Details

Table 23 Configuration Details - Internationalisation

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, contact your MSO.

Virtual Payment Client Details

Table 24 Configuration Details - Virtual Payment Client

Field	Description
Access Code	<p>The access code is an identifier that is used to authenticate the merchant for Virtual Payment Client transactions.</p> <p>The access code is generated automatically when the merchant is granted the privilege to use the Virtual Payment Client.</p>

Field	Description
Secure Hash Secret 1 and 2	<p>The secure hash is generated automatically and assigned to you when you were granted the Virtual Payment Client privilege.</p> <p>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.</p> <p>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.</p> <p>The Secure Hash Secret is made up of alphanumeric characters which are appended to the transaction.</p>
3-Party Return URL	<p>The default return web address when using the Virtual Payment Client interface.</p> <p>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.</p> <p>The Return URL must start with either http:// or https://and may be up to 255 characters.</p>

Payment Client Details

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

Table 25 Configuration Details - Payment Client

Field	Description
Client 3-Party Return URL	<p>The default return web address for the Payment Client interface.</p> <p>The cardholder is returned to this URL at the completion of the transaction where the merchant initiated the payment using the Payment Client without specifying a return URL.</p> <p>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 the Merchant Administration component and the ReturnURL component in the digital order.</p> <p>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

To edit your configuration settings:

1. Select **Admin** from the Main menu.
2. Select **Configuration Details** from the submenu.
The **Admin – Configuration Details** page displays.
3. Click **Edit**.

Admin - Configuration Details

Merchant

Merchant Name: MasterCard Test 1
Merchant ID: MC0001

Internationalisation

Locale: English (Australia)
Time Zone: Australia/Sydney

Virtual Payment Client

Access Code: 021F1D9F
Secure Hash Secret 1: FEAA04B99784CC24A65DF364734E1430 [Delete]
Secure Hash Secret 2: 4CFE8D3160EE761BBB4343B464192CFD [Delete]
3-Party Return URL:

Payment Client

Client 3-Party Return URL:

[Submit] [Cancel]

4. Enter changes in the fields that permit changes and click **Submit**.
5. The **Admin – Configuration Details** page redisplay with the changed information (see *Merchant Details*).

Editing Merchant Configuration - Internationalisation

On the **Configuration Editor** page:

1. Select a **Locale** and/or **Time Zone** from the drop down list.
2. Click **Submit**.

The **Admin – Configuration Details** page redisplay, with the updated 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
- 3-Party Return URL.

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 **Add**.

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 for each secret.

Admin - Configuration Details

Merchant

Merchant Name: MasterCard Test 1
Merchant ID: MC0001

Internationalisation

Locale: English (Australia)
Time Zone: Australia/Sydney

Virtual Payment Client

Access Code: 021F1D9F
Secure Hash Secret 1: FEA04B99784CC24A65DF364734E1430 [Delete]
Secure Hash Secret 2: 4CFE8D3160EE761BBB4343B464192CFD [Delete]
3-Party Return URL:

Payment Client

Client 3-Party Return URL:

[Submit] [Cancel]

2. Click **Submit**.

The **Admin - Configuration Details** page redisplay, with the updated information.

To Delete a Secure Secret Hash

On the **Configuration Editor** page:

1. Click **Delete** for the Secure Secret Hash that you want to permanently remove.

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 the first secret.

2. Click **Submit**.

The **Admin - Configuration Details** page redisplay with the updated information.

To Edit a Return URL

On the **Configuration Editor** page:

1. Enter a URL in the **3-Party Return URL** field.
2. Click **Submit**.

The **Admin - Configuration Details** page redisplay with the updated information.

Editing Merchant Configuration - Payment Client

On the **Configuration Editor** page:

1. Enter a URL in the **Client 3-Party Return URL** field.
2. Click **Submit**.

The **Configuration Details** page redisplay with the updated information.

Managing Merchant Administration Operators

Merchant Administration allows you to create, modify, enable and delete an Operator's details. To perform these functions you must have the user privilege **Perform Operator Administration**. These functions are performed from the Operator Details page from the **Admin** menu.

To create and edit Merchant Administration Operators:

1. From the Main menu, select **Admin > Operators**.
The **Admin – Operator List** displays.
2. You can choose to create an Operator, or edit, delete or change a password of an existing Operator.

Operator ID	Operator Name	Description
Administrator	superuser	
MIGSTEST	Ilan	

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.
- **AMA User Operators** - these are Operators who perform administration functions (any requests other than normal payment, such as Refund, Capture, QueryDR, etc.) using the Virtual Payment Client or Payment Client.

This Operator must have the user privilege **Advanced Merchant Administration**. Advanced Merchant Administration uses the Virtual Payment Client or Payment Client to directly access the MiGS 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 Virtual Payment Client Integration Guide or Payment Client Integration Guide.

If you do not have the privilege **Enable Advanced Merchant Administration Features** available, it means your merchant account has not been assigned for this feature. Contact your Payment Service Provider.

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 **Admin - Operator List** page displays.

Operator ID	Operator Name	Description	Change Password	Edit	Delete
Administrator	superuser				
MIGSTEST	Ilan				

2. Select **Create a new Merchant Administration Operator**.

The **Admin - Operator Details** page displays. It has sections for recording operator details, security privileges and transactions for new Operators.

Admin - Operator Details

Operator Details

Merchant	<input type="text" value="VIC0001"/>
Operator ID	<input type="text"/>
Operator Name	<input type="text"/>
Description	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
Email Address	<input type="text"/>
Locale	<input type="text" value="English (Australia)"/>
TimeZone	<input type="text" value="Australia/Sydney"/>

Security

Lock Operator Account	<input type="checkbox"/>
Change Their Own Password	<input type="checkbox"/>
Must Change Password At Next Login	<input type="checkbox"/>
Password Reset Required	<input type="checkbox" value="No"/>

Transactions

Perform MOTO Transactions	<input type="checkbox"/>
Perform Purchases	<input type="checkbox"/>
Perform Voids	<input type="checkbox"/>
Perform Stand Alone Captures	<input type="checkbox"/>
Perform Refunds	<input type="checkbox"/>
Perform Stand Alone Refunds	<input type="checkbox"/>

Merchant Maintenance

Modify The Merchant Configuration	<input type="checkbox"/>
Perform Operator Administration	<input type="checkbox"/>

General

View Report Pages	<input type="checkbox"/>
Enable Advanced Merchant Administration Features	<input type="checkbox"/>
Download Order Search Results	<input type="checkbox"/>
Download Transaction Search Results	<input type="checkbox"/>
Allow Software Download	<input type="checkbox"/>
Allow Payment Client Download	<input type="checkbox"/>
Allow Merchant Admin Documentation Download	<input type="checkbox"/>
May Configure Risk Rules	<input type="checkbox"/>
May Perform Risk Assessment Review	<input type="checkbox"/>
May Bypass Risk Management	<input type="checkbox"/>

3. Enter the details as required.

4. Click **Submit**.

The **Admin - Operator List** redisplay and includes the new Operator.

Merchant Administration Operator Details page

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

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

Operator Details

Table 26 Operator Details

Field	Description
Merchant ID	The merchant's unique alphanumeric identifier. There is a unique Merchant ID for each merchant account and 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).
Password	The password must be at least eight characters long and contain at least one alphabetical character and one number. 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.
Email Address	The Operator's email address.
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 Privileges

Table 27 Security Privileges

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.
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, the next time an Operator logs in they are required to change their password.
Change Their Own Password	Operator is allowed to change their own password.

Password Reset Required	<p>Indicates if password reset is required. This field is set to "Yes" after five failed login attempts, otherwise it is set to "No".</p> <p>If the field is set to "Yes", the administrator will need to reset the Operator's password. For information on how to reset an Operator's password, see <i>Changing an Operator's Password</i>.</p>
-------------------------	--

Transactions

Table 28 Transactions

Field	Description
Perform MOTO Transactions	Allows the operator to create orders in Merchant Administration and allows user to mark orders as complete.
Verification Only	Allows the operator to perform address verifications on cardholders.
Perform Voids	<p>Allows the operator to void transactions.</p> <p>A void is the cancellation of a previous transaction. Voids can only be performed if the transaction is in an unreconciled batch.</p> <p>Note: A void is only possible if voids are supported by the acquirer.</p>
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 cardholder.
Perform Stand Alone Refunds	Allows a refund to be performed through the Payment Client or Virtual Payment Client without first creating a capture or purchase.
Allow Excessive Refunds	Allows the operator to perform refunds for amounts greater than the authorised amount.
Excessive Refunds Limit	<p>The maximum limit allowed for an excessive refund, in excess of the authorised amount.</p> <p>You must set a refund limit for each currency configured for the merchant.</p>

Merchant Maintenance

Table 29 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.

General Privileges

Table 30 General Privileges

Field	Description
View Report Pages	Authorised to view Reports.
Allow Advanced Merchant Administration Features	<p>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.</p> <p>Note: If this privilege is selected for a Merchant Administration Operator, the operator will not be able to use Merchant Administration.</p>
Download Order Search Results	<p>Allows the Operator to download order information in a text file.</p> <p>The file contains the orders with all the associated financial transactions data.</p> <p>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.</p>
Download Transaction Search Results	<p>Allows the Operator to download transaction information in a text file.</p> <p>The file contains the orders with all the associated Financial Transactions and Payment Authentication Transaction data.</p> <p>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.</p>
Allow Software Download	<p>Allows the merchant to download software and documentation from the Payment Server.</p> <p>Note: This privilege is a pre-requisite to the Payment Client Download and Documentation Download privileges.</p>

Field	Description
Allow Payment Client Download	Allows the merchant to download the Payment Client software. Note: Payment Client is no longer available for new merchant integrations.
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 MSO Group Resource Bundle Translation	Allows the merchant to use the translation portal for an MSO group.
Permit MSO Resource Bundle Translation	Allows the merchant to use the translation portal for an MSO.
Permit Merchant Group Resource Bundle Translation	Allows the merchant to use the translation portal for a merchant group.
Perform Credit Payment	Allows the merchant to perform credit payment transactions.
May Configure Risk Rules	Allows the Operator to configure risk rules for a merchant using the Risk Management module.
May Perform Risk Assessment Review	Allows the Operator to take a decision on whether to approve or cancel an order based on the risk assessment results.
May Bypass Risk Management	Allows the Operator to process orders without performing risk checks and assessment of orders.

Editing Operators

To edit a currently configured Operator:

1. Select **Admin > Operators**.

The **Merchant Administration – Operator List** displays.

The **Edit an Operator** section shows all existing Operators.

Admin - Operator List

Create an Operator

Create a new Merchant Administration Operator

Edit an Operator

Operator ID	Operator Name	Description			
Administrator	superuser				
MIGSTEST	Ilan		Change Password	Edit	Delete

2. You can do any of the following:
 - To edit a particular Operator, click **Edit**. The **Operator Detail** 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**. The **Change Password** page appears.

Note: The Change Password link does not display for the logged in user. Use *Admin > Change Password* (see *Changing Your Password at Login*) 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 **Admin - 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 **Submit** 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 clear the Lock Operator Account check box (see steps 1-4 above).

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 the **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 1 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.

If given the required privileges, Operators can change their password at any time.

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:

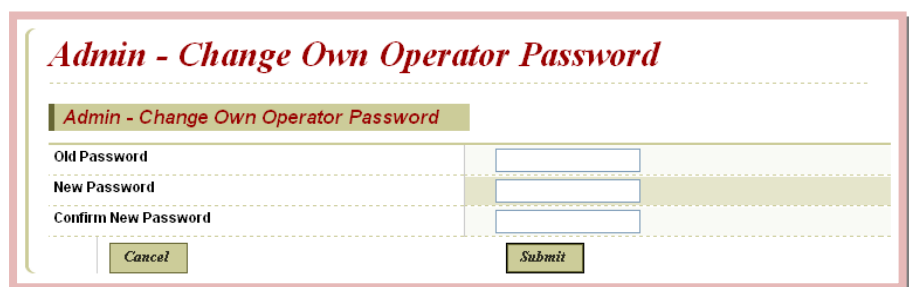
1. From the Main menu select **Admin > Operators**.
The **Admin - Operator List** page displays.
2. Identify the Operator in the **Edit an Operator** section, and click **Change Password**.
The **Admin - Change Operator Password** page displays.
3. Enter the new password in the **New Password** field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

Changing Your Own Operator Password

Note: To change your own password, you must have the **Change Own Password** Operator privilege.

To change your password:

1. From the Main menu select **Admin > Change Password**.
The **Admin - Change Own Operator Password** page displays.



The screenshot shows a web form titled "Admin - Change Own Operator Password". Below the title is a sub-header "Admin - Change Own Operator Password". The form contains three input fields: "Old Password", "New Password", and "Confirm New Password". At the bottom of the form are two buttons: "Cancel" and "Submit".

2. Enter the **Old Password**, the **New Password**, and re-enter the new password in the **Confirm New Password** field.
3. Click **Submit**.

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

8 Managing Risk

Introduction to the Risk Management Module

Risk Management is a module used for Card-Not-Present (CNP) transactions, which enables MSOs and merchants to use a set range of business risk screening rules. These risk rules are configured to screen transactions of perceived high or low risk thereby enabling merchants to accept, reject, or mark transactions for review based on their risk assessment.

Typically, merchants adopt a combination of fraud prevention tools, for example 3-D Secure, AVS, CSC (Card Security Code), manual screening of orders, etc., to combat fraud. With the introduction of the Risk Module, merchants can now automate the process of accepting, rejecting, or reviewing the order based on preset risk rules. The risk rules are evaluated to determine the action taken on the order, thereby requiring 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 cardholder 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 where each rule contributes differently to the risk profile. IP Address Range and Card BIN rules enable blocking 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 suspect card numbers respectively. 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.

MSOs have the added privilege of defining rules that merchants cannot bypass — MSO rules always override merchant rules. Also, an MSO rule configured to reject a transaction has the ability to not only block the transaction but also block merchant configured rules from being processed. MSOs, however, cannot configure rules for review, unlike merchants who can configure rules for reject, review, or normal processing of a transaction.

Risk Management is available for both 2-Party and 3-Party transactions. Though risk rules can be configured only through the Merchant Administration or Merchant Manager portals, transactions processed through the Virtual Payment Client will be assessed for risk, and the overall risk result for each authorisation and purchase will be returned in the Transaction Response. However, merchants using the Virtual Payment Client will not be able to make a review decision on the order — orders can be reviewed for processing or cancellation only through the Merchant Administration portal. You can view the overall risk result details in the search results of an Order Search using the Merchant Administration or Merchant Manager portals on the Payment Server.

Note: Merchants must have the **May Use Risk Management** privilege enabled to use Risk Management. To enable this feature contact your MSO.

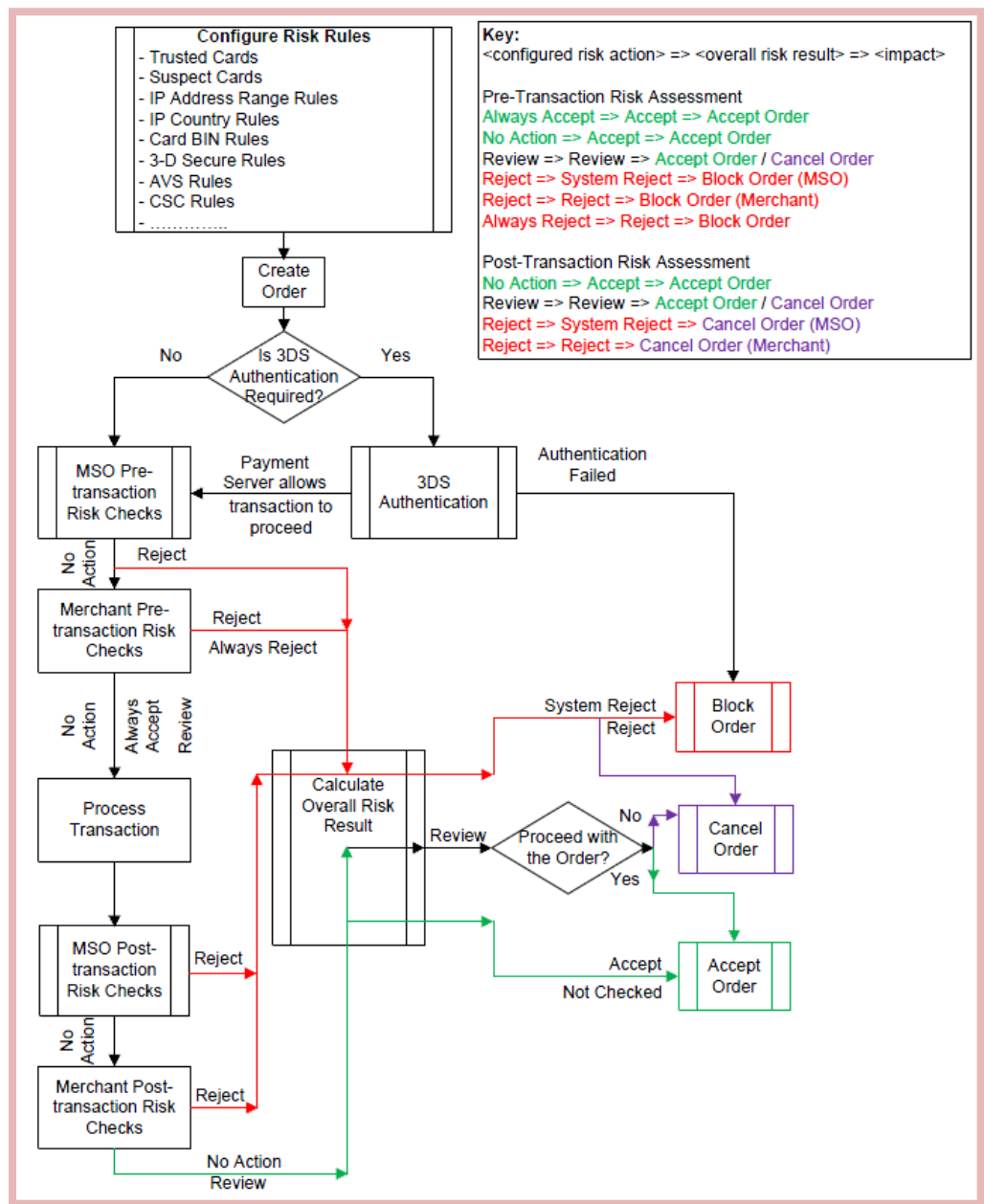
Note: Risk Management is applicable only to **Auth Then Capture** and **Purchase** transaction modes. Standalone Captures, Standalone Refunds, etc., will not be assessed for risk.

Risk Management Architecture

Risk Management primarily comprises 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).

Notes: MSO level risk rules always override merchant level risk rules. You cannot bypass MSO level risk rules.

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



3DS 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 (i.e. Authorisation or Purchase transactions that received a "Refer to Issuer" acquirer response).

Basic Risk Management 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. 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.

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. System 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 cardholders the merchant considers trustworthy to transact with.

Suspect Cards

A set of credit card numbers owned by those cardholders 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.

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 Risk Management

To use the Risk Management module, the MSO must enable the **May Use Risk Management** 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 overall risk result
- **May Bypass Risk Management** — enables the merchant operator to process orders without performing risk checks.


For more information on privileges, see *Setting Privileges* on page 11.


Viewing Risk Management Summary

The Risk Management Summary page introduces the Risk Management module and provides various options for risk mitigation on the submenu. You can choose to configure risk rules for IP Country, IP Address Range, Card BIN, Trusted Cards and Suspect Cards, AVS, or CSC by clicking the rule type, which takes you to the corresponding configuration page.

Action Items

(x) the number "x" represents 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
This link appears only if the merchant operator has May Perform Risk Assessment Review privilege.
- Failed Risk Reversals.

Risk Assessments for Review

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 is 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

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 When Risk Recommendation is Set to Reject in Implications of Risk Recommendation.

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

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 offline 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:

- **Trusted Cards** — enables you to always accept transactions from the card numbers identified as Trusted Cards.
- **Suspect Cards** — enables you to always reject transactions from the card numbers identified as Suspect Cards.
- **IP Address Range Rules** — enables you to block transactions based on IP addresses of transactions.
- **IP Country Rules** — enables you to block transactions based on IP addresses of countries.
- **Card BIN Rules** — enables you to block transactions based on BINs (Bank Identification Numbers).
- **3-D Secure Rules** — enables you to block transactions based on 3-DS authentication states.
- **AVS Rules** — enables you to block transactions based on AVS (Address Verification Status) response codes. Available only in limited countries – check with your acquiring bank.
- **CSC Rules** — enables you to block transactions based on CSC (Card Security Code) response codes.

Trusted Cards

The trusted cards list is a set of credit card numbers owned by those cardholders the merchant considers trustworthy to transact with. Typically, a cardholder 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 add trusted cards, you must be aware of the prerequisites.

Prerequisite

To add trusted cards, you must have the **May Configure Risk Rules** operator privilege.

Adding Trusted Card Numbers

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

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

3. Click **Add**. The **Risk Management - Trusted Cards** page redisplay with the updated current trusted card numbers list sorted by card numbers.

Current Trusted Card Numbers

Select: [All](#) | [None](#) Filter By Card Number: [Go](#) [Clear](#)

[Remove Trusted Card Numbers](#)

Select	Card Number	Card Holder Name	Reason	
<input type="checkbox"/>	531365xxxxxx4258	John Citizen		Edit

The card numbers are displayed in the 6.4 card masking format irrespective of the card masking format configured for the merchant.

Reviewing Current Trusted Card Numbers

1. From the Main menu, select **Risk Management > Trusted Cards**. The **Risk Management - 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 allows you to navigate between multiple pages.

2. 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.
3. To edit a card number:
 - Click **Edit** next to the card number record.
 - Make changes to the required fields.
When you modify the card number, ensure 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 **Update** to process the changes, or **Cancel** to cancel the changes.

Deleting Trusted Card Numbers

1. From the Main menu, select **Risk Management > Trusted Cards**. The **Risk Management - 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 allows you to navigate between multiple pages.
2. Use **Filter By Card Number** to find card numbers you want to delete. See *Reviewing Current Trusted Card Numbers* on page 88.
3. Select the check boxes under the **Select** column for the card numbers you want to delete. You may use **Select All** or **None** to select or clear all card numbers.

Current Trusted Card Numbers

Select: [All](#) | [None](#) Filter By Card Number: [Go](#) [Clear](#)

[Remove Trusted Card Numbers](#)

Select	Card Number	Card Holder Name	Reason	
<input checked="" type="checkbox"/>	531365xxxxxx4258	John Citizen		Edit

1

4. Click **Remove Trusted Card Numbers** to delete the selected card numbers.

Suspect Cards

The suspect cards list is a set of credit card numbers owned by those cardholders the merchant considers untrustworthy to transact with. Typically, a cardholder with fraudulent transaction history has a high potential of being added to the suspect card list. Configuring suspect card rules enables you to block transactions from suspect cards.

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

Prerequisite

To add suspect cards, you must have the **May Configure Risk Rules** operator privilege.

Adding Suspect Card Numbers

1. From the Main menu, select **Risk Management > Suspect Cards**. The **Risk Management - Suspect Cards** page displays.

2. In the **Add New Card Number** section, enter the following information.

Term	Description
Card Number	The credit card number of the cardholder.
Card Holder Name	The name of the cardholder. This is an optional field. Note: The cardholder 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 **Add**. The **Risk Management - Suspect Cards** page redisplay 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.

Reviewing Current Suspect Card Numbers

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

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

2. 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.
3. To edit a card number:
 - Click **Edit** 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 **Update** to process the changes, or click **Cancel** to cancel the changes.

Deleting Suspect Card Numbers

1. From the Main menu, select **Risk Management > Suspect Cards**. The **Risk Management - Suspect Cards** page displays. The **Current Suspect Card Numbers** section displays a list of all currently added suspect card numbers and their corresponding details.
If the list of suspect cards exceeds 20 entries, pagination 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 Suspect Card Numbers* on page 90.
3. Select the check boxes under the **Select** column for the card numbers you want to delete. You can use **Select All** or **None** to select or clear all card numbers.

4. Click **Remove Suspect 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 cardholder. Configuring IP Address Range rules enables 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 two categories:

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

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

Prerequisite

To configure IP Address Range rules, you must have the **May Configure Risk Rules** operator privilege.

Adding an IP Address Range Rule - Merchant

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

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

Risk Management - IP Address Range Rules

You can configure a single IP Address or an IP Address range. For example, if you want to configure a rule for IP Address 111.112.113.0, simply type 111.112.113.0 as the IP Address Range Start entry. If the defined IP Address ranges overlap to belong to both the categories, the action Reject overrides Review.

Add IP Address Range Rule

IP Address Range Start	IP Address Range End	Action
<input type="text"/>	<input type="text"/>	<input type="radio"/> Review <input type="radio"/> Reject <input type="button" value="Add"/>

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.

Select: [All](#) | [None](#) Filter Ranges by IP Address:

Select	Start	End	Action
There are no Merchant IP Address Range Rules configured.			

- In the **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.

To block a single IP Address, for example 192.0.2.255, enter 192.0.2.255 as the **IP Address Range Start** entry and choose the required action.

To block an IP address range, for example, 192.0.2.222 to 192.0.2.255, enter 192.0.2.222 and 192.0.2.255 as the **IP Address Range Start** and **IP Address Range End** respectively.

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

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

Term	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	The action you want to perform on the IP range. Valid options are: <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, or else click **Cancel**.

- Click **Add**. The **Risk Management - IP Address Range Rules** page redisplay with the updated current IP address range rules list.

Risk Management - IP Address Range Rules

You can configure a single IP Address or an IP Address range. For example, if you want to configure a rule for IP Address 111.112.113.0, simply type 111.112.113.0 as the IP Address Range Start entry. If the defined IP Address ranges overlap to belong to both the categories, the action Reject overrides Review.

Add IP Address Range Rule

IP Address Range Start	IP Address Range End	Action	
<input type="text"/>	<input type="text"/>	<input type="radio"/> Review [?] <input type="radio"/> Reject [?]	<input type="button" value="Add"/> [?]

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: Off

Select: [All](#) | [None](#) Filter Ranges by IP Address: [?]

Select	Start	End	Action
<input type="checkbox"/>	192.0.2.222	192.0.2.255	Review

1

Reviewing Current IP Address Range Rules

1. From the Main menu, select **Risk Management > IP Address Range Rules**. The **Risk Management - 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 allows you to navigate between multiple pages.

2. 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.

Deleting 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 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 94.

Risk Management - IP Address Range Rules

You can configure a single IP Address or an IP Address range. For example, if you want to configure a rule for IP Address 111.112.113.0, simply type 111.112.113.0 as the IP Address Range Start entry. If the defined IP Address ranges overlap to belong to both the categories, the action Reject overrides Review.

Add IP Address Range Rule

IP Address Range Start	IP Address Range End	Action	
<input type="text"/>	<input type="text"/>	<input type="radio"/> Review <input type="radio"/> Reject	<input type="button" value="Add"/>

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.

Select: [All](#) | [None](#)
 Filter Ranges by IP Address:

Select	Start	End	Action
<input checked="" type="checkbox"/>	192.0.2.222	192.0.2.255	Reject

1

3. Select the check boxes under the **Select** column for the IP Address range you want to delete. You can use **Select All** or **None** to select or clear all the records.
4. Click **Delete**. A warning message displays to alert you about deleting IP Addresses that occur in multiple IP ranges if overlapping IP ranges have been defined.
5. Click **OK** to delete the selected IP ranges, or click **Cancel** to cancel the deletion.

Configuring IP Country Rules

IP addresses can help in identifying the location of the cardholder. Configuring IP Country Rules enables 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 block countries, you must be aware of the prerequisites.

Prerequisite

To configure IP Country Rules, you must have **May Configure Risk Rules** operator privilege.

Adding 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.

Risk Management - IP Country Rules

Add an IP Country Rule

Unknown Country ☒ No Action ☐ Review ☐ Reject ?

Anonymous Proxy ☒ No Action ☐ Review ☐ Reject ?

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

No Action ? **Select:** All | None

Afghanistan
 Åland Islands
 Albania
 Algeria
 American Samoa
 Andorra
 Angola
 Anguilla
 Antarctica
 Antigua and Barbuda
 Argentina
 Armenia
 Aruba
 Australia
 Austria
 Azerbaijan
 Bahamas
 Bahrain
 Bangladesh
 Barbados
 Belarus
 Belgium
 Belize
 Benin

Move Selected Countries To:

Review ? **Select:** All | None

Move Selected Countries To:

Reject ? **Select:** All | None

Move Selected Countries To:

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

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

Term	Description
Unknown Country	<p>A country that's not listed in Risk Manager or an IP address that does not correspond with a valid country in Risk Manager.</p> <p>For example, if "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.</p> <p>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.

Term	Description
Anonymous Proxy	<p>IP address of a known anonymous proxy server. These addresses have been identified to mask the true origin of the request.</p> <p>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.</p> <p>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.

3. To mark a country for review:

- Select the country from either the **No Action** or the **Reject** list box.
- Click **Review** 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 No Action or Reject.

Note: Press Ctrl and click to select multiple items.

4. To **reject a country**:

- Select the country from **the No Action** or the **Review** list box.
- Click **Reject** 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 **No Action** or **Review**.

5. Click **Save** to save the IP Country Rule, or click **Cancel** to exit the IP Country Rules page without saving any changes.

Reviewing Currently Rejected IP Countries

From the Main menu, select **Risk Management > IP Country Rules**. The **Risk Management - 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.

Risk Management - IP Country Rules

Add an IP Country Rule

Unknown Country ☐ No Action ☐ Review ☒ Reject

Anonymous Proxy ☐ No Action ☐ Review ☒ Reject

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

No Action <small>Select: All None</small>	Review <small>Select: All None</small>	Reject <small>Select: All None</small>
<div style="border: 1px solid #ccc; padding: 5px; min-height: 200px;"> Åland Islands Albania Algeria American Samoa Andorra Angola Anguilla Antarctica Antigua and Barbuda Argentina Armenia Aruba Australia Austria Azerbaijan Bahrain Bangladesh Barbados Belarus Belgium Belize Benin Bermuda Bhutan </div>	<div style="border: 1px solid #ccc; padding: 5px; min-height: 200px;"> Bahamas Nigeria </div>	<div style="border: 1px solid #ccc; padding: 5px; min-height: 200px;"> Afghanistan </div>
<p>Move Selected Countries To:</p> <p><input type="button" value="Review"/> <input type="button" value="Reject"/></p>	<p>Move Selected Countries To:</p> <p><input type="button" value="No Action"/> <input type="button" value="Reject"/></p>	<p>Move Selected Countries To:</p> <p><input type="button" value="No Action"/> <input type="button" value="Review"/></p>

Deleting an IP Country Rule

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

Note: Press Ctrl and click to select multiple items.

2. Click **No Action** to move the country to the **No Action** list box.
3. Click **Save** 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 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 enables 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 two categories:

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

Before you 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.

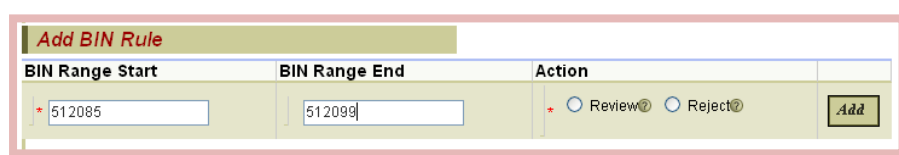
Adding Card BIN Rules

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

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

2. In the **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, enter 123456 as the **BIN Range Start** entry. To block a BIN range, for example 111111 to 222222, type 111111 and 222222 as the **BIN Range Start** and **BIN Range End** respectively.

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



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.</p> <p>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 categories (Review and Reject), the action Reject overrides Review.

- Click **Add**. The **Risk Management - Card BIN Rules** page redisplay with the updated **Current BIN Rules** list.

Current BIN Rules			
Select: All None			
Delete			
Select	Start	End	Action
<input type="checkbox"/>	512085	512099	Review

Reviewing Current Card BIN Rules

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

Current BIN Rules			
Select: All None			
Delete			
Select	Start	End	Action
<input type="checkbox"/>	512085	512099	Review

Deleting a Card BIN Rule

- From the Main menu, select **Risk Management > Card BIN Rules**. The **Risk Management - Card BIN Rules** page displays. The **Current BIN Rules** section displays a list of all currently blocked BIN ranges and their corresponding action status.
- Select the check boxes under the **Select** column for the BIN range you want to delete. Use **Select All** or **None** to select or clear all the records.

Current BIN Rules			
Select: All None			
Delete			
Select	Start	End	Action
<input checked="" type="checkbox"/>	512085	512099	Review

- Click **Delete**. A warning message displays to alert you about deleting BIN ranges that occur in multiple BIN ranges if overlapping BIN ranges have been defined.
- Click **OK** to delete the selected BIN ranges, or click **Cancel** to cancel the deletion.

Configuring 3-D Secure Rules

3-Domain Secure™ (3-D Secure or 3DS) is a protocol for authenticating cardholders. 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, 3-DS 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
- 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 enables merchants to either accept or block any transaction based on the 3-DS authentication states. The authentication states are uniform across all authentication schemes and acquirers.

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

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

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

Prerequisites

To configure 3-DS Rules, you must have:

- The **May Configure Risk Rules** operator privilege. See *General Privileges* on page 75
- The privilege to at least one 3-DS authentication scheme, namely MasterCard SecureCode, Verified by Visa, JCB J/Secure, American Express SafeKey, or Diners Club ProtectBuy. See Cardholder Verification in Merchant Privileges. If you do not have this privilege, the 3-DS Rules option does not appear in the Risk Management submenu
- The card type that supports the 3-DS authentication scheme
- The merchant acquirer link that has authentication details configured for the 3-DS authentication scheme
- The 3-Party gateways privilege.

Adding 3-D Secure Rules

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

Risk Management - 3-D Secure Rules

Not all 3DS authentication states can be configured using this page - the authentication states that indicate a failed authentication block transactions at the system level itself. The configured rules apply to all authentication schemes - Verified By Visa, MasterCard SecureCode, American Express SafeKey and J/Secure. "Always Accept" overrides all other actions except "Always Reject". As a processing guideline, "Always Accept" and "Always Reject" have the highest priority followed by "Reject", "Review" and "No Action".

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"/>

Cancel Save

2. In the **Configure 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. An overall risk result 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* on page 33.

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 3-DS 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 3-DS authentication states. The following table lists the authentication states and their descriptions.

Field	Description
Cardholder 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.
Cardholder not enrolled (E)	Indicates that the cardholder is not enrolled in an authentication scheme, namely MasterCard SecureCode, Verified by Visa, JCB J/Secure, American Express SafeKey, or Diners Club ProtectBuy.
Undetermined (U)	Indicates that the issuer ACS (Access Control Server) is not responding and/or is 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 cardholder enrollment check.
Internal Error - Enrollment (A)	Indicates an internal system error during cardholder 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)	The Access Control Server returned an Enrolment Status of "U".
Invalid Enrollment Request (Z)	The Directory Server returned an Enrolment 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)	The Directory Server returned an Enrolment Status of "U" WITH an Invalid Request element.
Enrollment Undetermined (B)	The Directory Server returned an Enrolment Status of "U" WITHOUT an Invalid Request element
Enrollment Parse Error (W)	The system was unable to parse VERes received from the Directory Server

4. For an authentication state, select:
 - **No Action** if you want a transaction returning the selected authentication state to be processed normally
 - **Reject** if you want a transaction returning the selected authentication state to be blocked automatically
 - **Always Accept** if you want a transaction returning the selected authentication state to be always processed normally
 - **Review** if you want a transaction returning the selected authentication state to be marked for manual review.
- Click **Save** to save the 3-DS rule including the clash rule configuration, or, click **Cancel** to exit the 3-DS Rules configuration page without saving any changes.

Note: A 3-DS risk result of **Always Accept** returns an Overall Risk Result of **Accept**.

Reviewing Currently Rejected 3-D Secure Authentication States

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

Risk Management - 3-D Secure Rules

Not all 3DS authentication states can be configured using this page - the authentication states that indicate a failed authentication block transactions at the system level itself. The configured rules apply to all authentication schemes - Verified By Visa, MasterCard SecureCode, American Express SafeKey and J/Secure. "Always Accept" overrides all other actions except "Always Reject". As a processing guideline, "Always Accept" and "Always Reject" have the highest priority followed by "Reject", "Review" and "No Action".

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"/>

Cancel
Save

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

1. From the **Authentication State** column, select an authentication state for which you want to delete the 3-DS Rule.
2. Select **No Action** to allow a transaction with the selected authentication state to be processed normally.
3. Click **Save** to save the 3-DS Rule, or click **Cancel** to exit the CSC Rules configuration page without saving any changes.

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.

Note: AVS is only available in limited countries. Contact your acquiring bank to determine if AVS is applicable in your country.

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 cardholder 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
- 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 enables merchants to either accept or block any transaction based on the AVS response codes. You can configure AVS response codes to belong to one of three categories:

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

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.

Prerequisites

To configure AVS Rules, you must have:

- The **May Configure Risk Rules** operator privilege. See *General Privileges* on page 75.
- 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 cardholder 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 cardholder successfully.

Adding AVS Rules

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

Risk Management - AVS Rules

If the merchant privilege to perform Verification Only for AVS/CSC Risk Assessment is enabled, then AVS Rules are processed after a Verification Only transaction but before the financial transaction. If not, then AVS Rules are processed after the financial transaction, and any order rejected by the AVS rule is automatically attempted for a reversal by the system.

Configure AVS Response Codes

AVS Response Code	No Action ^②	Review ^②	Reject ^②
(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"/>

Cancel
Save

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:
 - **No Action** if you want a transaction returning the selected response code to be processed normally.
 - **Reject** if you want a transaction returning the selected response code to be blocked automatically.
 - **Review** if you want a transaction returning the selected response code to be marked for manual review.
4. Click **Save** to save the AVS Rule, or click **Cancel** to exit the AVS Rules configuration page without saving any changes.

Reviewing Currently Rejected AVS Response Codes

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

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

Resetting an AVS Rule

1. From the **AVS Response Code** column, select a response code for which you want to reset the AVS Rule.
2. Select **No Action** to allow a transaction with the selected response code to be processed normally.
3. Click **Save** 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 CVV (Visa), CVC2 (MasterCard), 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. The result code verifies the CSC level of accuracy used to match the card security code.

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

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

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.

Prerequisites

To configure CSC Rules, you must have:

- The **May Configure Risk Rules** operator privilege. See *General Privileges* on page 75.
- 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 cardholder 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 cardholder successfully.

Adding CSC Rules

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

Risk Management - CSC Rules

If the merchant privilege to perform Verification Only for AVS/CSC Risk Assessment is enabled, then CSC Rules are processed after a Verification Only transaction but before the financial transaction. If not, then CSC Rules are processed after the financial transaction, and any order rejected by the CSC rule is automatically attempted for a reversal by the system.

Configure CSC Response Codes

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"/>

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

Table 31 CSC Response Codes

Term	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.

3. For a response code, select:
 - **No Action** if you want a transaction returning the selected response code to be processed normally.
 - **Reject** if you want a transaction returning the selected response code to be blocked automatically.
 - **Review** if you want a transaction returning the selected response code to be marked for manual review.

Click **Save** to save the CSC Rule, or click **Cancel** to exit the **Risk Management - CSC Rules** configuration page without saving any changes.

Reviewing Currently Rejected CSC Response Codes

From the Main menu, select **Risk Management > CSC Rules**. The **Risk Management - 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 type="radio"/>	<input checked="" type="radio"/>
(N) No CSC match	<input type="radio"/>	<input checked="" type="radio"/>	<input 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.

Resetting CSC Rules

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

Searching for Orders Based on Risk Assessment

The Risk Management module enables you to search for orders based on the risk assessment results. See *Order Search Page* on page 24.

You can also view the Risk Assessment Details for individual orders in *The Create Order Response Page* on page 21), and *Order Details* on page 27).

9 Glossary

This chapter defines various terms, concepts, acronyms, and abbreviations used in this document. These definitions appear for convenience only and are not to be used or otherwise relied on for any legal or technical purpose. MasterCard specifically reserves the right to amend any definition appearing herein and to interpret and apply all such definitions in its sole discretion as MasterCard deems fit.

In addition, the descriptions of terms in this section are in the context of what they mean within the MiGS service, rather than any more generic meaning.

Term	Description
Acquirer	The financial institution or bank that maintains the merchant relationship and the processing of payments on behalf of the merchant.
Advanced Merchant Administration (AMA)	A special privilege which can be granted to a MiGS Merchant Administration user, allowing a merchant to perform administrative functions (such as captures, refunds, and voids) using their host system, as an alternative to performing these functions via the Merchant Administration Portal.
American Express SafeKey®	A program designed to provide online retailers the added security of having issuing banks authenticate their SafeKey enabled American Express cardholders and qualify their online transactions for protection against "cardholder unauthorised" chargebacks.
Authorisation	The processing of a transaction by or on behalf of the cardholder's bank (the issuer) according to defined operations regulations. MiGS will return the response to the authorisation request to indicate approval or reason for decline.
Batch	The grouping of transactions by MiGS into payment groups. MiGS stops each day's processing batch at a set time, opening a new batch for the next day's transactions. It should be noted that the cut-over time of the batch may not be in line with the merchant's business hours. Contact MasterCard for details of the cut-over time.
Capture Transaction	<p>A capture is only relevant to merchants who perform split Authorisation/Capture combinations. Most merchants will not use this function as capture of funds is performed automatically with a cardholder's authorisation on MiGS.</p> <p>If Authorisation/Capture is used, a separate request by the merchant is performed to capture the funds from the cardholder.</p>
Cardholder	The customer to whom a card has been issued or the individual authorised to use the card. This is the customer of the merchant or somebody purchasing goods on behalf of the customer.

Term	Description
Diners Club ProtectBuy SM	A program designed to provide online retailers the added security of having issuing banks authenticate their ProtectBuy enabled Diners Club cardholders and qualify their online transactions for protection against "cardholder unauthorised" chargebacks.
Issuer	The bank or institution which issues the card to the cardholder. In MiGS, the issuer or their agent decides on approval or decline of a cardholder request for payment of goods or services from the merchant. If a transaction is declined by the issuer, the cardholder generally needs to contact their issuing bank.
JCB J/Secure TM	A program designed to provide online retailers the added security of having issuing banks authenticate their J/Secure enabled JCB cardholders and qualify their online transactions for protection against "cardholder unauthorised" chargebacks.
Mail Order/Telephone Order (MOTO)	A generic term referring to any 'Card Not Present' transaction. When the cardholder's card is not present, the merchant may be allowed to accept the card details from the cardholder by mail or telephone. In this type of transaction, the merchant collects the card details and supplies all of this information to MiGS in the request.
MasterCard Internet Gateway Service (MiGS)	MasterCard's outsourced, multi-channel payment gateway solution for financial institutions to provide to their merchants for card present and card not present transaction processing.
MasterCard [®] SecureCode TM	A program designed to provide online retailers the added security of having issuing banks authenticate their MasterCard SecureCode enabled cardholders and qualify their online transactions for protection against "cardholder unauthorised" chargebacks.
Merchant	A retailer or any other person, firm or corporation that (pursuant to a merchant agreement) agrees to accept credit cards. Merchants should only operate on MiGS if they have signed agreements with an acquiring bank.
Merchant Administration (MA)	An Internet Web browser-based portal which allows merchants to monitor and manage their online processing. It also provides access to administrative functions on payments.
MiGS	See MasterCard Internet Gateway Service
MOTO	See Mail Order/Telephone Order
MSO	Merchant Services Organisation. This is the organisation who has access to Merchant Manager and is managing the merchant, including performing the initial setup. The function of the MSO may be performed by a bank, Payment Service Provider or other organisation.

Term	Description
Payment Authentication	A process whereby the cardholder authenticates their identity with the issuing bank during the online transaction process. This is made possible by a MasterCard® SecureCode™, Verified by Visa™ or JCB J/Secure™ password which is requested for each transaction. It is a similar concept to the use of a Personal Identification Number (PIN) on Automated Teller Machines (ATMs).
Payment Client	A back-end processing tool integrated into the merchant's Website which allows the real-time sending of secure transactions (digital orders) to MiGS and the receipt of transaction results (digital receipts).
Payment Server	The MiGS payment gateway service hosted by MasterCard International which provides an interface into the authorisation and authentication networks. The Payment Server accepts incoming secure transactions from the Payment Client and Virtual Payment Client, and processes transactions in real-time.
Purchasing Transaction	The most common MiGS payment. Transactions of this type both authorise the payment request (via the issuer) and facilitate payment to the merchant (via the acquirer) in a single message.
Refund	A transfer of funds from the merchant back to the cardholder, for example when goods are returned or unable to be delivered. On MiGS, refunds must be matched to a purchase or capture transaction and must not exceed the original value of the transaction.
SSL	Secure Socket Layer (SSL) developed by Netscape Communications Company, is a standard that encrypts data between a web browser and a web server. SSL does not specify what data is sent or encrypted. In an SSL session, all data sent is encrypted. MiGS only supports SSL connections with a minimum of 128 bit encryption from the cardholder or merchant browser.
Verified by Visa™	A program designed to provide online retailers the added security of having issuing banks authenticate their Verified by Visa enabled Visa cardholders and qualify their online transactions for protection against "cardholder unauthorised" chargebacks.
Void	A cancellation of the payment portion of the transaction, so that no funds are transferred between the cardholder and the merchant. The transaction is cancelled and is not recorded on the cardholder's statement. Voids can only be performed on transactions that have not yet been sent to the acquirer by MiGS for processing at the end of day (see Batch). Once a transaction has been sent by MiGS to the acquirer for processing, the merchant must perform a refund instead of a void.

10 Appendix A

Test Environment – Test Cards

The following table shows the test card numbers and associated expiry dates configured for each card scheme on the MiGS Payment Server.

Table 31 Test Cards

Card Type	PAN	Expiry Date (mm/yy)
MasterCard	5123456789012346	05/17
MasterCard	5313581000123430	05/17
VISA	4005550000000001	05/17
VISA	4557012345678902	05/17
AMEX	371449635311004	05/17
Diners	30123456789019	05/17
JCB	3528123456789012	05/17