

Suncorp Bank

Virtual POS Merchant Administration Guide



Copyright

Suncorp Bank 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 Suncorp Bank 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

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

Suncorp Bank
GPO Box 1453
Brisbane QLD 4001
Phone 13 11 55
www.suncorp.com.au/banking

Contents

Copyright	2
License Agreement	2
Trademarks	2
About Merchant Administration	5
Introduction	5
Managing Transactions with Payment Server	5
Types of Orders	5
Prerequisites	6
Administrator Account	6
Frequently Asked Questions	7
Getting Started	9
Logging in to Merchant Administration	9
Changing Your Password at Login	10
Selecting Merchant Administration Menu Options	10
Creating New Operators	10
Setting Privileges	12
Configuring details	14
Locked-out users	15
Changing Password	15
Logging Out	15
Working with Orders	16
Creating an Order	16
Searching for Orders	19
Performing Actions on Orders	24
Working with Financial Transactions	26
Searching for Financial Transactions	26
Viewing the Financial Transaction List	29
Viewing an Individual Financial Transaction	29
Downloading Transaction Files	30
Payment Authentications	31
Working with Payment Authentications	31
Payment Authentication Information Flow	31
Payment Authentications Status	32
Searching for Payment Authentications	32
Payment Authentications Search Page	33
Viewing Payment Authentications	33
Viewing an Individual Payment Authentication	34
Downloading Payment Authentication Information	36
Working with Reports	37
Search for a Gateway Report	37
View a Gateway Report	38
Admin Options	39
Configuring Your Settings	39
Managing Merchant Administration Operators	42
Glossary	47
Appendix A	49
Test Environment – Test Cards	49

This page left blank intentionally.

About Merchant Administration

Introduction

Suncorp Bank 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.

Virtual POS—clientless software provided by Suncorp Bank—is required to provide the interface between the MiGS Payment Server and your merchant Shop & Buy application.

For more information on the Virtual POS, ask Suncorp Bank for the Virtual POS 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 Virtual POS 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 POS 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. There are two 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 8).

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 13).

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 15. 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 *Working with 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 15).

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 15).

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 38 to access daily, weekly, monthly or yearly transaction reports.

Getting Started

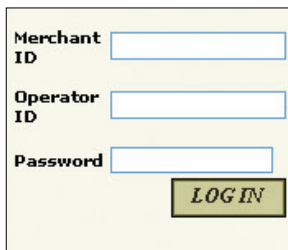
Merchant Administration allows you, as an authorised Operator, to monitor and manage your electronic orders. Authorised Operators can log in from the Login screen and use the various features of Merchant Administration.

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.



The screenshot shows a login form with three text input fields labeled 'Merchant ID', 'Operator ID', and 'Password'. Below these fields is a button labeled 'LOGIN'.

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 44.

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 Suncorp Bank to have Production mode enabled so that you can process transactions in real-time.

Login Field Definitions

The Merchant Administration Login screen requires the following information.

Login Field Definitions

Field Types	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* on page 9.

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 43.

The following menu administration options are available in Merchant Administration.

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

Merchant Administration Menu Options

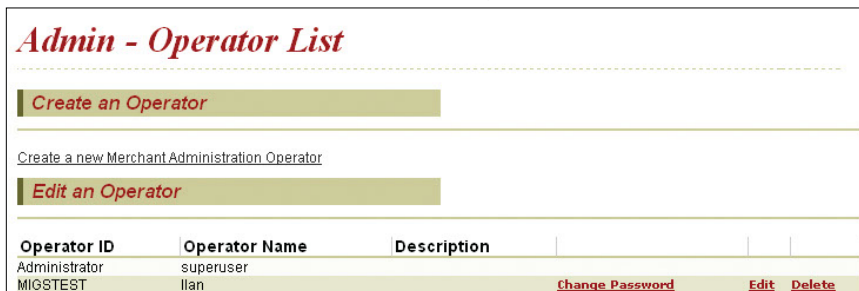
Menu Option	Description
Search	Access orders, financial transactions, and payment authentications.
Orders	Create an initial order manually, or perform an address verification.
Reports	Select and view reports.
Admin	Create new Operators, change and delete existing Operator records and privileges, change passwords and edit merchant configuration details.
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.



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

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="MC0001"/>
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 Privileges

Operator Locked Out	<input type="checkbox"/>
Change Their Own Password	<input type="checkbox"/>
Must Change Password At Next Login	<input type="checkbox"/>

Transactions

Perform MOTO Transactions	<input type="checkbox"/>
Perform Voids	<input type="checkbox"/>
Perform Captures	<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 "Operator Locked Out" 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 on next page.

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 Virtual POS 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.

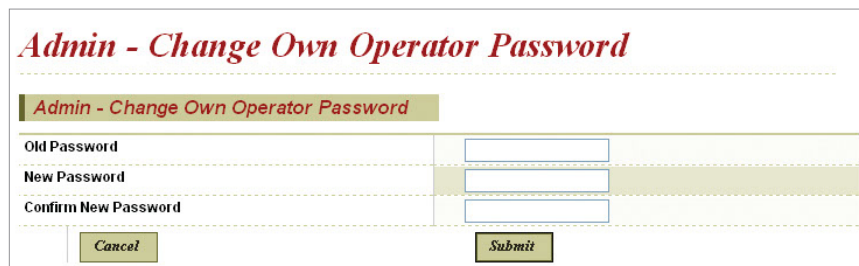
Security Privileges

— Operator Locked Out

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". It contains three text input fields labeled "Old Password", "New Password", and "Confirm New Password". Below the fields are two buttons: "Cancel" and "Submit". The form is styled with a light green header and a white body.

— 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 Suncorp 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.

The screenshot shows a web form titled "Reports - Gateway Reports". The form is divided into sections by dashed lines. The first section is "Gateway Reports" with a green header. Below this, there are several input fields: "From" and "To" both containing "01/01/10"; "Time Interval" with a dropdown menu set to "Daily"; "Acquirer" with a dropdown menu showing "Daily", "Weekly", "Monthly", and "Yearly"; and "Currency" with a dropdown menu showing "es". A "Submit" button is located at the bottom left of the form.

- 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 Virtual POS software, 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.

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, Suncorp Bank should be contacted first.

<i>Admin - Configuration Details</i>	
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
<input type="button" value="Edit"/>	

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

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

<i>Admin - Configuration Details</i>	
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
<input type="button" value="Add"/>	
3-Party Return URL	<input type="text"/>
Payment Client	
Client 3-Party Return URL	<input type="text"/>
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

You can amend the following fields for Virtual POS.

Virtual POS

- Secure Hash Secret 1

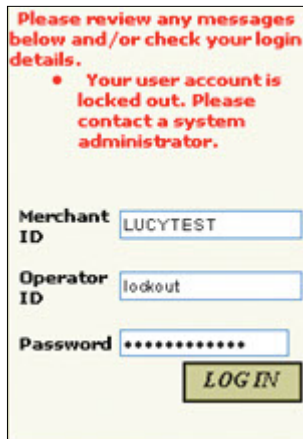
This allows you to add another Secure Hash Secret value if desired.

- 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.

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:



Please review any messages below and/or check your login details.

- Your user account is locked out. Please contact a system administrator.

Merchant ID: LUCYTEST

Operator ID: lockout

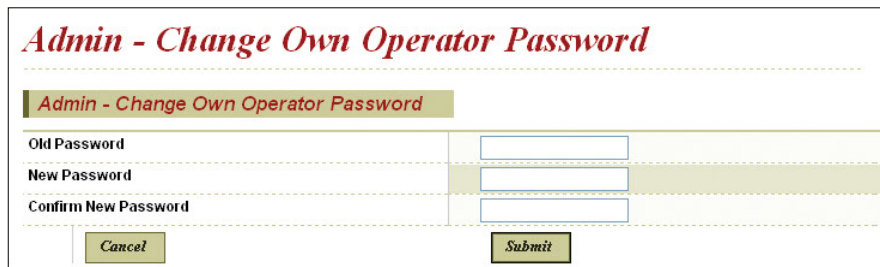
Password: *****

LOGIN

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 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:

Cancel Submit

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.

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.

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	<input type="text"/>
Amount *	<input type="text"/> AUD - Australian Dollar
Card Holder Name	<input type="text"/>
Card Number *	<input type="text"/>
Card Expiry *	<input type="text"/> / <input type="text"/> (mm / yy)
Card Security Code	<input type="text"/>
Airline Ticket Number	<input type="text"/>
Address	<input type="text"/>
City/Town	<input type="text"/>
State/Province	<input type="text"/>
Zip/Postal Code	<input type="text"/>
Country	Australia
Merchant Transaction Source	Default
Transaction Frequency	Default
<input type="button" value="Reset To Default Values"/>	<input type="button" value="Submit"/>

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.

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	The currencies supported by the merchant acquirer relationships, displayed with the currency code and the full name. E.g: – AUD - Australian Dollar
Card Holder Name	The name of the cardholder.
Card Number	The card number used in the order. Depending on your profile, the format used for displaying card numbers is one of the following: – 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 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.
Card Security Code	This is a security feature used for card not present transactions. 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. – 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.
Airline Ticket Number	Originally used for the airline industry, this is an optional field where extra information about the transaction can be stored.

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>
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 <ul style="list-style-type: none"> The Payment Server will use the Default Transaction Frequency specified in the merchant profile for the acquirer processing the order. – Single Transaction <ul style="list-style-type: none"> This indicates to the acquirer that a single payment is used to complete the cardholder’s order. – Recurring <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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.

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

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.

Field	Description
Card Number	The card number used in the order. Depending on your profile, the format used for displaying card numbers is one of the following: <ul style="list-style-type: none"> – 0.4 Format, for example (xxxxxxxxxxx1234) – 6.3 Format, for example (654321xxxxxxxx123) – The full card number is displayed – The card number is not displayed.
Card Expiry	The expiry date of the card, in mm/yy format.
Account Type	The type of bank account – Savings or Cheque. <div style="border: 1px solid black; padding: 2px; margin-top: 5px;">Note: This field is displayed for Maestro cards only.</div>
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	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.
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.

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.

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.

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.
Outstanding Authorisations	Search for orders that have authorised amounts against them which have not yet been captured. Note: The orders returned will exclude outstanding authorisations marked as complete.
Acquirer ID	Search for orders processed by a particular acquirer.
Currency	Search for orders processed by currency.
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).
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.

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: – 0 - Approved – 3 - Timed Out.
Status	The result of the most recent action performed on the order. Example values are: – 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: This field is displayed for Maestro cards only.

Viewing an Individual Order - The Order Details Page

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

- Order Details
- Card Details
- Authorisation Response Data
- Address Verification Details
- Action
- History

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.
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 <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <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> </div>
Merchant Transaction Frequency	<p>Indicates whether the transaction was a single, recurring or part of an instalment payment. Depending on your configuration the available frequencies can include:</p> <ul style="list-style-type: none"> – Single Transaction <ul style="list-style-type: none"> This indicates to the acquirer that a single payment is used to complete the cardholder's order. – Recurring <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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.
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.
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. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: This field may or may not appear, depending on the merchant's configuration.</p> </div>

Card Details

Field	Description
Card Type	The type of card used for the transaction.
Card Number	The card number used in the order. Depending on your profile, the format used for displaying card numbers is one of the following: <ul style="list-style-type: none"> – 0.4 Format, for example (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	The type of bank account - Savings or Cheque. <div style="border: 1px solid black; padding: 2px; margin-top: 5px;">Note: This field is displayed for Maestro cards only.</div>
Commercial Card	Indicates if the card used is a commercial card. Example codes are: <ul style="list-style-type: none"> – N - Not a commercial card – Y - Commercial card – U - Undetermined.
Commercial Card Indicator	Indicates the type of commercial card as returned by the card issuer. For example, <ul style="list-style-type: none"> – O - 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.
Acquirer CSC Result Code	Card security code validation result code as provided from the acquirer.
Dialect CSC Result Code	Card security code validation result code in standard payment server result format.

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.

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

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 will 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 on page 23).

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.

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.
Merchant Transaction Source	The method by which the merchant received the order. Typical transaction sources include: <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. <div style="border: 1px solid black; padding: 5px;">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.</div>

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	531358XXXXXXXX430
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-authorized amount
- Cancel any captures performed on a pre-authorized 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.

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	531358XXXXXXXX430
Card Expiry	

Action	
Refund Amount	AUD \$ <input type="text" value="20.00"/>
Refund	
Void Capture	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.

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 for Financial Transactions	
From	8/10/10 12:00 AM
To	8/10/10 11:59 PM
Transaction ID	
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	
<input type="button" value="Submit"/> <input type="button" value="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.

<i>Search - Financial Transaction List</i>						
Financial Transaction List						
Acquirer ID	Transaction ID	Merchant Transaction Reference	Transaction Type	Amount	Date	Response Code
MIGS S2I Test Bank	35		Void Refund	AUD \$800.00	8/10/10 6:47 PM	0 - Approved
MIGS S2I Test Bank	34		Refund	AUD \$800.00	8/10/10 6:46 PM	0 - Approved
MIGS S2I Test Bank	33		Capture	AUD \$800.00	8/10/10 6:44 PM	0 - Approved
MIGS S2I Test Bank	32		Authorisation	AUD \$321.11	8/10/10 6:39 PM	3 - Timed Out
MIGS S2I Test Bank	31		Authorisation	AUD \$321.11	8/10/10 6:38 PM	3 - Timed Out
MIGS S2I Test Bank	30		Authorisation	AUD \$9,999,991.11	8/10/10 5:41 PM	0 - Approved
MIGS S2I Test Bank	29		Authorisation	AUD \$9,999,991.11	8/10/10 5:38 PM	0 - Approved
MIGS S2I Test Bank	28		Authorisation	AUD \$0.01	8/10/10 5:36 PM	0 - Approved
MIGS S2I Test Bank	27		Authorisation	AUD \$132.00	8/10/10 5:33 PM	0 - Approved

4. 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 ID	30
Merchant Transaction Reference	
Date	8/10/10 5:41 PM
Transaction Type	Authorisation
Payment Method	Credit
Amount	AUD \$9,999,991.11
Order ID	30
Batch Number	20101009
RRN	028116003106
Response Code	0 - Approved
Acquirer Response Code	00
Authorisation Code	005481
Integration Type	MA (Merchant Administration)
Transaction Source	MOTO

Financial Transaction Search Page

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

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.
Batch Number	Select transactions belonging to a particular batch.
RRN	The RRN (Reference Retrieval Number) allows the Acquirer to uniquely identify a transaction.
Merchant Transaction Reference	A unique merchant specific identifier.
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.
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 51.

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

Select an individual Financial Transaction ID to view its 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.
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.

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).
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.

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.
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.
Integration Type	The means by which the merchant accesses the Payment Server. The available integration types are: <ul style="list-style-type: none"> - VPC - Virtual POS - MA - Merchant Administration.
Integration Type Version	The version number of the payment software used to integrate with the Payment Server. <div style="border: 1px solid black; padding: 2px; margin-top: 5px;">Note: This field is displayed only if the Integration Type is VPC.</div>
Transaction Source	Indicates the source of the transaction. Typical transaction sources include: <ul style="list-style-type: none"> - Default - PC - MOTO - Auto (Risk). <div style="border: 1px solid black; padding: 2px; margin-top: 5px;">Note: 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 attempted for a reversal by the system.</div>
Payment Authentication ID	Displays the unique ID of an authentication record, if payment authentication was used in processing the transaction.

Downloading Transaction Files

To use the download transaction information functionality, you must have been set up to do so by Suncorp Bank.

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.

Search - Financial Transaction Search

Search for Financial Transactions

From	<input type="text" value="7/9/10 12:00 AM"/>
To	<input type="text" value="8/10/10 11:59 PM"/>
Transaction ID	<input type="text"/>
Batch Number	<input type="text"/>
RRN	<input type="text"/>
Merchant Transaction Reference	<input type="text"/>
Currency	<input type="text" value="All Currencies"/>
Transaction Type	<input type="text" value="All"/>
Payment Method	<input type="text" value="All"/>
Acquirer ID	<input type="text" value="All"/>
Transaction State	<input type="text" value="All"/>
Authentication Type	<input type="text" value="Ignore"/>
Authentication State	<input type="text" value="Ignore"/>
Number Of Results To Display On Each Result Page	<input type="text"/>

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.

Search - Financial Transaction Search

Search for Financial T

File Download

Do you want to open or save this file?

Name: MC0001-2010-10-08-FinTxn.csv
Type: Microsoft Office Excel Comma Separated Values Fil...
From: migs-rtf.mastercard.com.au

Open Save Cancel

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. [What's the risk?](#)

From
To
Transaction ID
Batch Number
RRN
Merchant Transaction Reference
Currency
Transaction Type
Payment Method
Acquirer ID
Transaction State
Authentication Type
Authentication State
Number Of Results To Display On Each Result Page

Submit Download

2. 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.

Payment Authentications

Working with Payment Authentications

MasterCard® SecureCode™ (MasterCard 3-Domain Secure), Verified by Visa™ (Visa 3-Domain Secure), and J/Secure™ (JCB 3-Domain Secure) 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: Ensure that you take necessary security measures to protect the data downloaded on to your computer.

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:

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.
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.
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 33).

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

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

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.
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.

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 33). 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.

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	The card number used in the order. Depending on your profile, the format used for displaying card numbers is one of the following: <ul style="list-style-type: none">– 0.4 Format, for example (xxxxxxxxxxx1234)– 6.3 Format, for example (654321xxxxxxxx123)– The full card number is displayed– The card number is not displayed.
Amount	The total amount processed for the transaction or order in the transaction currency. For Example, AUD \$100.00.
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– J/Secure– American Express SafeKey.

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. M – Success - The cardholder is not enrolled, but their card issuer attempted processing. E – Not Enrolled - The cardholder is not enrolled. F – Failed - An error exists in the request format from the Merchant. N – Failed - Verification Failed. U – Undetermined - The verification was unable to be completed. This can be caused by network or system failures. T – Undetermined - The cardholder session timed out and the cardholder’s browser never returned from the Issuer site. A – Undetermined - Authentication of Merchant ID and Password to the Directory Failed. D – Undetermined - Error communicating with the Directory Server. C – Undetermined - Card brand not supported. S – Failed - The signature on the response received from the Issuer could not be validated. This should be considered a failure. P – Failed - Error receiving input from Issuer. I – Failed - Internal Error.</p>
Verification Token (CAVV)	The Verification Token (CAVV = Cardholder Authentication Verification Value) is a Visa token generated at the card issuer to prove that the Visa cardholder authenticated satisfactorily.
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.
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).
3-D Secure VRes.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 PRes.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.

Field	Description
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'. 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.

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

Search 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:

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.
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.

View 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.

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

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

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.
3. Click **Edit**.
4. Make changes as required and click **Submit**.

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
	<input type="button" value="Add"/>
3-Party Return URL	<input type="text"/>

Payment Client

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

5. The message “Configuration Changes Saved” is displayed on the Configuration Details screen and details redisplayed with changed information.

Configuration Details

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

Configuration Details Definitions

Field	Description
Merchant Name	The merchant’s registered business, trading or 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 Suncorp Bank.

International Definitions

The **Internationalisation** section on the **Admin - Configuration Details** screen contains the following information:

International Definitions

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 Suncorp Bank.

Configuration Details - Virtual POS

The **Virtual POS** section on the **Admin - Configuration Details** screen contains the following information:

Configuration Details - Virtual POS

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

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:

The screenshot shows the 'Admin - Configuration Details' page. It is divided into three sections: 'Merchant', 'Internationalisation', and 'Virtual Payment Client'. Each section has a header bar and a table of configuration items. 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' and 'Secure Hash Secret 1' as 'FEAA04B99784CC24A65DF364734E1430'. There is an 'Edit' button at the bottom left of the form.

3. Click **Edit**.
4. Enter changes in the fields that permit changes and click **Submit**.
5. The **Admin - Configuration Details** page redisplay with the changed information.

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 POS

On the **Configuration Editor** page, you can edit the following for the Virtual POS:

- 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.

The screenshot shows the 'Admin - Configuration Details' page with the following sections:

- Merchant**
 - Merchant Name: MasterCard Test 1
 - Merchant ID: MCD001
- Internationalisation**
 - Locale: English (Australia)
 - Time Zone: Australia/Sydney
- Virtual Payment Client**
 - Access Code: 021F1D9F
 - Secure Hash Secret 1: FEAA04B99784CC24A65DF364734E1430 (with a Delete button)
 - Secure Hash Secret 2: 4CFE8D3160EE761BBB4343B464192CFD (with a Delete button)
 - 3-Party Return URL: (empty text box)
- Payment Client**
 - Client 3-Party Return URL: (empty text box)

At the bottom of the form are **Submit** and **Cancel** buttons.

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 redispays 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 redispays with the updated information.

Managing Merchant Administration Operators

Merchant Administration allows you to create, modify, enable, and delete an Operator's details. To be able 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		Change Password	Edit	Delete

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 POS. This Operator must have the user privilege **Advanced Merchant Administration**. Advanced Merchant Administration uses the Virtual POS 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 POS 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 Suncorp Bank.

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			
Administrator	superuser				
MIGSTEST	Ilan		Change Password	Edit	Delete

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.

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

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

Field	Description
Operator Locked Out	If checked, the Operator has failed to correctly log in five times and hence has been locked out. Clear the check box to re-enable the Operator if you have the required privileges.
Must change password at next login	If selected, the next time an Operator logs in they are required to change their password.
Change Own Password	Operator is allowed to change their own password.

Transactions

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

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

Field	Description
View Report Pages	Authorised to view Reports.
Advanced Merchant Administration	Allows the merchant to perform administration functions through an interface. The merchant can access the Payment Gateway to directly perform all transaction-related actions (for example, voids, purchases and refunds) integrated with merchants' software interfaces, rather than using the portal. Note: If this privilege is selected for a Merchant Administration Operator, the operator will not be able to use Merchant Administration.
Download Order Search Results	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 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.
Download Transaction Search Results	Allows the Operator to download transaction information in a text file. The file contains the orders with all the associated Financial Transactions and Payment Authentication Transaction data. The format of the file is a Comma Separated Value file and ends with the extension .csv. This format is used to transfer data from one application to another. Most database systems can import and export comma-separated value files, which can be used in any spreadsheet program.
Allow 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.

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* on page 8) to change the password of the currently logged in Operator.

Reactivating an Operator When Locked Out

If a Merchant Administration Operator enters their password incorrectly five times, they are locked out.

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

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

1. From the Main menu select **Admin > Operators**.

The **Merchant Administration - Operator List** page displays.

2. Select **Operators** in the submenu.

The **Operator List** page displays.

3. To view the Operator's details click on the Operator in the list.

The **Operator Detail** page displays.

4. Clear the check box of the Operator who has been locked out due to repeated login failure.

5. Enter a new temporary password in the **Password** field and retype that password in the **Repeat Password** field.

6. Provide this new password to the Operator.

7. Click the **Must change password at next** login check box.

This forces the Operator to choose a new password at the next login.

8. Click **Submit** to commit the changes.

The Operator's record has now been unlocked and a new password has been created.

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 **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 Password

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

To change an Operator's password:

1. From the Main menu select **Admin > Change Password**.

The **Admin - Change Own Operator Password** page displays.

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.

Password Requirements

The password must consist of at least eight characters, and include at least one alphabetic character and one number. It must not be one of user's last five passwords. To confirm your password you are required to enter it twice.

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.

The password will automatically expire every 90 days.

Operators can change their password at any time (if given the user privilege), but they cannot re-use that password for the next five password changes.

Operators can also reset their own password if the existing password has been forgotten.

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.

Suncorp Bank specifically reserves the right to amend any definition appearing herein and to interpret and apply all such definitions in its sole discretion as Suncorp Bank 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.
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. Cut-off time for processing is 6pm Sydney time.

Term	Description
Capture Transaction	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. If Authorisation/Capture is used, a separate request by the merchant is performed to capture the funds from the cardholder.
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.
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™	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™	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.
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 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 Virtual POS, 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.

Appendix A

Test Environment – Test Cards

Please refer to the below link for test card information.

https://suncorp.gateway.mastercard.com/api/documentation/integrationGuidelines/supportedFeatures/testAndGoLive.html?locale=en_US

Contact us



Call **13 11 55**



Online
suncorp.com.au/banking



Local branch



Write to
GPO Box 1453, Brisbane QLD 4001



Fax **07 3031 2250**