SiamPay

Merchant User Guide v3.5

(Leave Blank Intentionally)

Copyright Information

AsiaPay Limited

121/49 R.S.Tower Level 11, Ratchadapisek Road,

Dindeang, Bangkok Thailand 10400

Telephone :(662) 642 3272 auto

Fax: (662) 642 3279

Web site: http://www.asiapay.co.th/

Confidentiality and Usage

The information contained in this document (and any attachments) is confidential information provided by AsiaPay Limited. This document is intended only for use by merchants, customers, partners and other parties approved by AsiaPay Limited. Any copying, distribution or dissemination of this document by any other parties is prohibited.

Revision History

Revision	Date	Revision Description
1.0	Mar 10, 2003	First issue
2.0	Dec 12, 2004	New functions & order status and documentation list update
2.1	Sep 20, 2005	Revised password policies
3.0	May 12, 2009	Overall Revision of Content

TABLE OF CONTENTS

Overview

Introduction

SiamPay is a powerful web-based online payment services platform, which provides secure, multi-channel, multi-lingual and multi-currency payment services. It is used by many renowned companies and organizations in the region.

This document will help you get the most from the SiamPay payment services. With this document, SiamPay merchants will be able to understand the various features of SiamPay services. It is suggested that you read this document prior to using SiamPay services. It contains valuable information that helps you to learn faster and enhance your experience.

Thank you for using SiamPay services!

Getting Started

There are several steps that must be completed prior to accept payments through SiamPay payment services.

Step 1 – Apply for a Merchant Account

Before any integration is being carried out, it is presumed that the merchant has already applied a merchant account with AsiaPay (Thailand) Limited. If you do not have a merchant account, please contact us for application.

Step 2 – Integrate SiamPay payment services

This step should be completed after reading our Integration Guide. SiamPay payment service supports different types of channels' integration. Make sure that you have the right version of Integration Guide for your application.

Step 3 – Application Test

When steps 1 and 2 are completed, you may apply a testing account with us to test your application before the official launch of your online business. In the testing environment, only testing credit cards and account numbers work. During testing process, please enter some transactions and check to see that those transactions are authorized. Check the details of each transaction, such as Merchant name, currency, amount and etc. are correct. To check the details, you have to login your merchant admin tools which at SiamPay testing environment provides detail information for transaction of your account. If your testing does not give you the expected result, please contact us for assistance.

Step 4 – Official Launch

At the moment after satisfactory testing result, it is ready for your web application launch. Make sure necessary modifications are made for production environment. If everything is ready, you can start enjoying the benefits of real-time payment process with SiamPay.

How does SiamPay Payment Services work?

Merchants using SiamPay

Payment Services can automatically authorize and settle credit card payments either on their web site or on standard payment interface on SiamPay.com with 128-bits SSL encryption. Transactions history is recorded in our database and merchants can access the information by logging into merchant administration tools at www.siampay.com.

Usually, a transaction starts when a consumer makes a purchase at a merchant's website. The required purchase information is sent securely to SiamPay Payment Services platform. Upon the transaction reaches SiamPay, our database records the information and requests the acquiring bank to authorize the transaction. The result is returned through our payment platform to client browser within seconds.

With SiamPay Administration Tools, the merchant can query the transactions' status via their web browser. They can also perform actions like void, request refund, download report and etc. In the following sections, there contains detailed information on the features of SiamPay Administration Tools.

Administration Tools

SiamPay Merchant Administration Login

Merchant can access the Administration Tools, the user must set the correct URL or use the shortcut link at www.siampay.com homepage by selecting "Merchant Login" or

(https://www.siampay.com/b2c2/eng/merchant or https://www.siampay.com/b2c2/tha/merchant) and then enters **Merchant ID**, **Login name** and **Password** in the form as shown below. Click the "Submit" button to submit the form. All fields are case sensitive. i.e. 'ABC' is not the same as 'abc'.
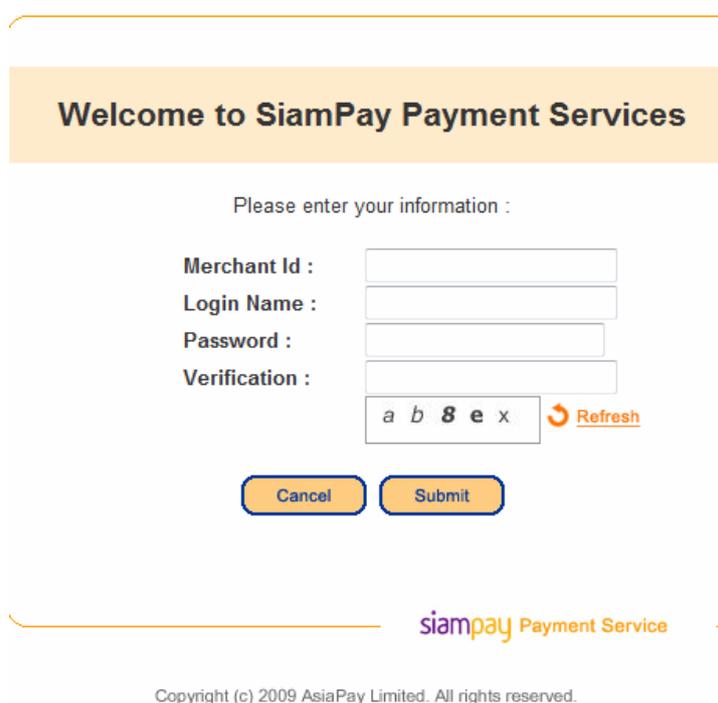
Welcome to SiamPay Payment Services

Please enter your information :

Merchant Id :
Login Name :
Password :
Verification :

a b 8 e x   ↻ Refresh

Cancel   Submit

siampay Payment Service

Copyright (c) 2009 AsiaPay Limited. All rights reserved.

Figure 1: Merchant Admin Login Screen

In the production environment, the data transmitted via browser will be encrypted. Please make sure there is lock-liked icon 🔒 shown at the lower-right corner of your browser. This means the browser is protected and server connected is authenticated. To authenticate the identity of the server ID certificate, double click the icon to read the details. Contact SiamPay or the certificate issuer if there is any doubt.

The user will be temporarily locked when the system records more than 6 consecutive login failures due to incorrect password. Users are required to change password periodically. When a user's password is expired, the system will prompt the user to change the password automatically.

After a successful login, the first page presented is the **Merchant Admin Homepage** as shown below.

Figure 2: Merchant admin home page

At the top of this home page, it contains account information, including:

- **Merchant ID**
- **Merchant Name**
- **Last Logon,** it shows the date and time last time you logon for security purpose.

Merchant MTD Transaction Summary

The Merchant MTD (Month to date) Transaction Summary shows transactions of the account in the current month by payment method.

Merchant's Bulletin Board

Just below the Merchant MTD Transaction Summary, there is a **Bulletin Board** which covers the update news and benefits for merchants. You are recommended to view the contents regularly.

Hot Tips

"Your business is our business". SiamPay always aims at providing comprehensive information to help our business partners and merchants like you to develop a profitable and healthy e-commerce business. This **Hot Tips** area contains useful information and business tips for e-business such as reference on fraud prevention and chargeback prevention.

Online Help

Simply click the 'Help' button on the right upper corner, you can get more information or explanation of items on the merchant admin tools usage.

In order to protect the user account, the login session will be expired automatically when the browser is idle for too long. You are highly recommended to logout the account when you are using a public terminal computer or leaving your seat.

At the left-hand-side of the screen are tags to other section: *1) **Profile**; 2) **Operations**; 3) **Risk Control**; 4) **Analysis**; 5) **Services**; 6) **Support*** and these will be discussed in more detail.

Merchant's Profile

When the **Profile** tag is selected, the menu of **Merchant's Profile** section is shown as below.
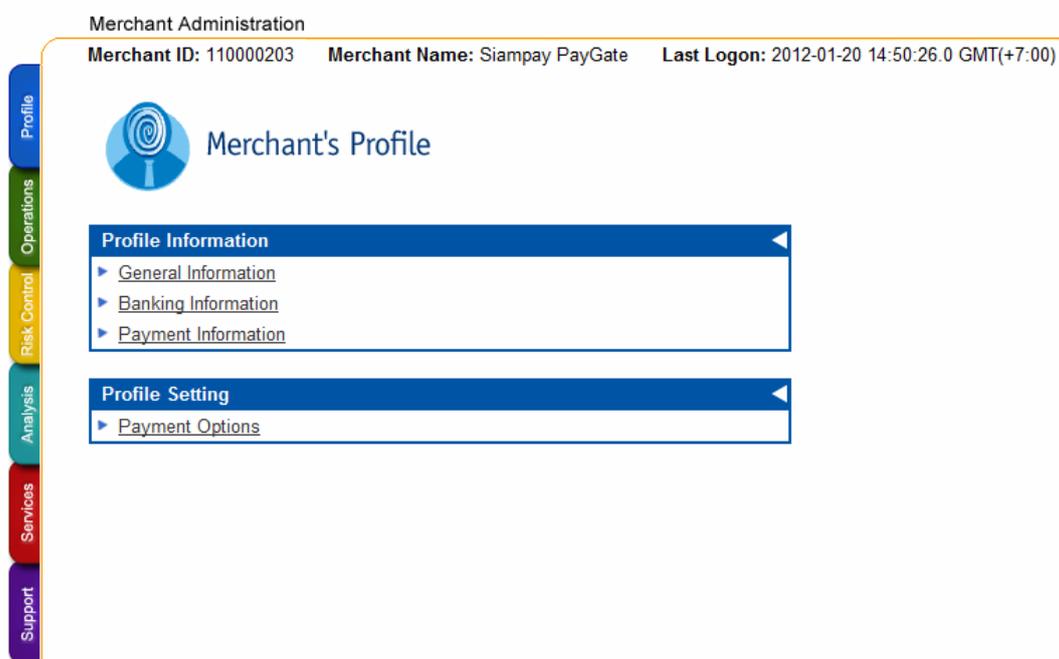

Figure 3: Menu of Merchant's Profile

This Merchant's Profile section is divided into 2 parts:

    i)   Profile's Information – records the Merchant Information: -

- General information
- Banking information
- Payment information

    ii)   Profile Setting – shows existing payment options: -

- Datafeed failure alert by email to contact email (depends on Datafeed setting)

General Information

Figure 4: General Information Screen

Merchants have the responsibility to ensure the company information is up-to-date and accurate. The descriptions of the form as follow:

General Information

Field name	Description
Merchant ID	Unique ID number of the merchant account
Company Name	Merchant's registered company name
Merchant Class	The plan applied for the merchant
Merchant Type	Business type of merchant
Payment Type	Type of payment to be accepted with this merchant account. **Sale** means the amount is debit from the credit card account, while **Authorize** only holds the request amount from the account without debit at instant.
Short Name	Company name in short
Business Registration No.	The certificate number of the company

URL	Registered URL for online business
Mailing Address	Corresponding address of the merchant
Business Address	Registered address of the merchant's company
Country / Region	Country / Region of business registration
Country Domicile	Country domicile of the registered company
Fax Number	Corresponding fax number
Enquiry Hotline	Telephone number for general enquiry about the merchant's business. (e.g. Customer Service Hotline)

Contact Information (Name, Telephone No. & Email)

Field name	Description
Project Contact	Person who is in charge of the SiamPay merchant account set-up
Operations Contact	Person who is in charge of the daily operations of the online transactions
Technical Contact	Person who is in charge of the technical issue related to this account

SiamPay will send email to your operation contact email address(es) for the followings:

1) real-time email notification of successful/unsuccessful transactions

2) chargeback and retrieval request notification

3) accounts related issue e.g. refund, payment invoice

To update the company profile information (e.g. business and mailing address, contact number, website URL), please submit the 'Merchant Account Maintenance Form'. You can download this form at the Support session.

For merchants who are using our SiamPay standard payment page, you may now enjoy personalized payment page. After the simple setup, your Company logo can be shown on every page throughout the payment process, so as to provide a more company-specific image to your customers. To register, please fill in the 'Merchant Account Maintenance Form' and prepare your company logo in .jpg, .png or .gif format (The suggested file size is: 150 x 60 pixels). Please kindly submit the form and logo by email to our Service Department.

Banking Information

Figure 5: Banking Information Screen

Banking Information

Field name	Description
Bank	Name of settlement bank
Bank Account Title	Registered name for the account
Bank Account Number	Registered account number
Bank Account Currency	Currency of settlement for the account

For merchant accounts, you may register with our auto settlement service. For details, please contact our Account Department.

Payment Information

Figure 6: Payment Information Screen

Payment Information

Field name	Description
Currency	Currency setting for the merchant account.
Return Value Link (Data Feed)	This is the location where merchant's application accepts the return value of the payment transaction.
Secure Hash	This function is to enhance the transaction message communication security between merchant site and SiamPay. By employing this technology, the integrity of the information and the identity of the signatory can be authenticated with industry standard.

To enable the Secure Hash function, please submit the 'Merchant Account Maintenance Form'. You can download this form at the Support session. For the details of integration, please refer to the "SiamPay PayGate Integration Guide" which can be downloaded at the Support session.

Each Secure Hash Secret key is valid for two years, please contact our Service department to renew the Secure Hash Secret key before it is expired

Payment Options

Figure 7: Payment Options Screen

For each payment option, you can enable or disable at anytime by simply selecting the options and click the button UPDATE to confirm the changes.

| Option	Description
Return Value Link (Datafeed)	This is the location where merchant's application accepts the return value of the payment transaction (**Warning:** Please consult with your development/IT team before update as it may seriously affects the location of return value)
Datafeed failure alert email to contact email	When there is problem in returning you with the registered datafeed, we will send an email notification to your technical contact email (for merchants who registered the datafeed function)
Payment method selection in payment page	SiamPay provides two different payment pages: Payment method selection by logo [Default value] and Payment method selection by Text. Merchant may choose the payment page according to the own preference (for merchants who are using "Client Post Through Browser" connection method, please consult with your development/IT team for more information)

Two SiamPay payment page interfaces as below:
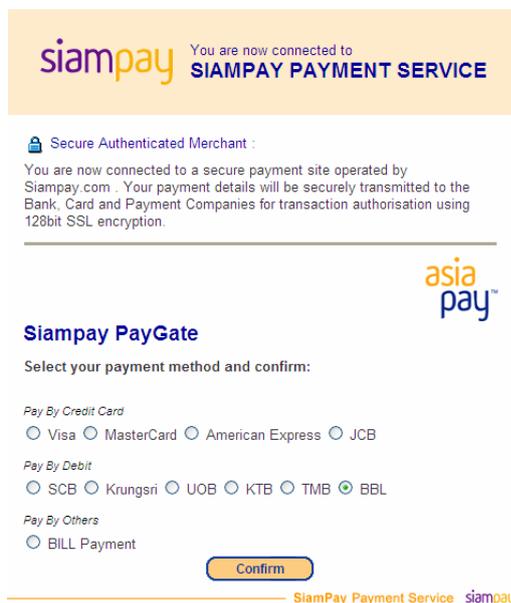
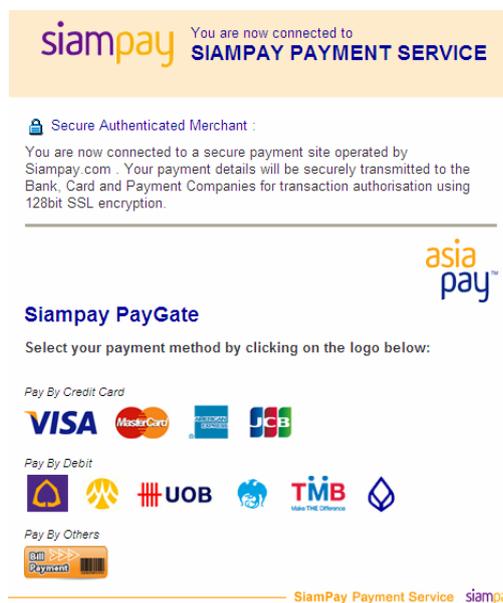Figure 7a: Payment method selection by Text

Figure 7b: Payment method selection by Logo

Operations & Reports

When the **Operations** tag is selected, the menu of **Operations & Reports** section is shown as below.

Figure 8: Menu of Operations & Reports

What administrator can do in this section is mainly checking the transaction details and generating reports. The menu is divided into 2 parts: *i) Operations;* and *ii) Reports*.

Sub-menu	Contents
Operations	- Transaction Details
	- eStatement (for standard merchants)
	- MemberPay
	- Online Shop Management
	- eStatement
	- Hotel Reservation management System
Reports	- Sales Report
	- Refund Report (for standard merchants)
	- ChargeBack Report (for standard merchants)
	- Transaction Summary Report
	- Bank Settlement Report (for premier merchants)

To streamline your daily operation flow, you can now perform i) Sales, ii) Authorize, iii) Capture and iv) Refund in a batch request. Just simply prepare a text file consisting all the required transactions details, and then upload to our system. You may also set the target processing date at your convenience. Please contact our Sales Department for further details of this function.
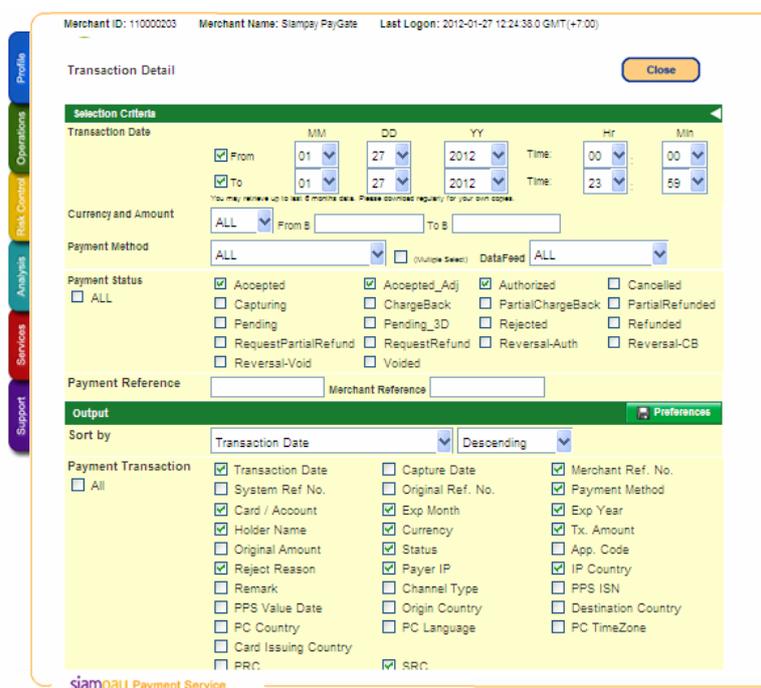
Transaction Detail

Figure 9: Transaction Detail screen

This function provides SiamPay merchants a powerful and flexible transaction searching and reporting based on the specified selection and sorting criteria. And, the selected details can also be downloaded to CSV format for recording and other processing reference. The first page of the Transactions Detail is to define selection criteria and output. Steps for transactions retrieval:

Steps	Description
Step 1 – Define Searching Criteria	There are a number of selection criteria for searching. The logic of search is 'AND', i.e. Combination of all the fields. Leaving the field blank and selection to ALL will return all records. By default, **only today's transaction** will be shown.
Step 2 – Output Sorting and fields to display	Output can be sorted by any of the criteria, ascending order or descending order. By default, the returned records are sorted by the field selected, such as Transaction Date, in descending order.
Step 3 – Submit Search	Click View button to start searching and view online. Click Download button to download the extracted data.

Please note that the searching date range is set at 7 days and you may retrieve up to previous 6 months data. You are recommended to download the reports monthly for your own reference.

In order to provide a detail picture to Transaction Detail, there are descriptions of each selection criterion and output field in the following tables.

Selection Criteria of Transaction Detail

Field name	Parameter / Type	Description
Transaction Date	**From** Date and **To** Date (MM: Month; DD: Day; YY: Year; Hr: Hour; Min: Minutes)	Default value is **today**. Check **From** only to define the start date of search and Check **To** only to define the end date of search. **Uncheck** both **From** and **To** returns all transactions.
Currency and Amount	Currency (Selection) and range of amount (Float)	Currency of transaction and amount or range of amount
Payment Method	List of payment method	Payment Method (e.g. Visa and MasterCard)
Datafeed	Datafeed Indicator	Available for merchants who have registered the datafeed link All: all statuses **T**: Successfully get response from merchant's defined datafeed page **F**: Fail to get response from merchant's defined datafeed page or error occurs **R**: Datafeed retry succeeds **U**: Datafeed retry fails (**R** & **U**: only available for merchants who have registered the datafeed retry service)
Order Status	Check box: - Accepted - Accepted_Adj - Authorized - Cancelled - Capturing - Chargeback - PartialChargeback - PartialRefunded - Pending - Pending_3D - Rejected - Refunded - RequestPartialRefunded - RequestRefund - Reversal-Auth	**Accepted:** Successful sale transaction **Accepted_Adj:** Transaction is accepted but there is a partial chargeback or partial refund involved **Authorized**: Hold request transaction limit only; awaiting for capture **Cancelled**: Payment cancelled by customer **Capturing:** Transaction waiting for the completion of a capture process **Chargeback**: Cardholder raises a dispute to the card issuer (full amount) **PartialChargeack**: Cardholder raises a dispute to the card issuer (partial amount) **PartialRefunded**: Requisition of partial amount refund is processed by SiamPay **Pending**: Incomplete transaction **Pending_3D**: Transaction waiting for completion of

	- Reversal-CB - Voided - Reversal-Void	3D authentication process **Rejected:** Unsuccessful sale transaction **Refunded:** Requisition of full amount refund is processed by SiamPay **RequestPartialRefunded:** Requisition of partial amount refund by merchant is submitted **RequestlRefunded:** Requisition of full amount refund by merchant is submitted **Reversal-Auth**: Cancellation of successful authorized transaction by merchant **Reversal-CB**: Chargeback transaction is successfully appealed by merchant **Voided:** Cancellation of successful transaction before daily bank settlement by merchant **Reversal-Void**: Withdraw the cancel request by merchant
Payment Reference No.	Number	Payment Reference No. is a unique number generated by SiamPay platform. Separate by "," (comma) for more than one entry.
Merchant Reference No.	Text	Reference No. submitted by merchant

Searching Output of Transaction Detail – Payment Transaction

Field name	Description
Transaction Date	Date of transaction
Capture Date	Date of Capture process (for authorized transaction only)
Merchant Ref. No.	Reference No. submitted by merchant
System Ref. No.	SiamPay generated unique number for each payment transaction
Original Ref. No.	A System Ref. No. of the original parent transaction of a transaction
Payment Method	Method of payment, e.g. VISA or MasterCard
Card/Account	Credit Card account number
Exp Month	Expiry month of the card
Exp Year	Expiry year of the card
Holder Name	Credit Card's Holder name
Currency	Currency of transaction
Tx. Amount	Amount of transaction
Original Amount	Original amount of transaction when there is a modification during capture process
Status	Payment status (e.g. Accepted and Rejected)
App. Code	The return value code sent by bank or card company for successful payment
Reject Reason	Reason for unsuccessful transaction
Payer IP	IP address of transaction
IP Country	Country origination of the transaction (Country code will be shown)
Remark	Remark submitted by merchant
Channel Type	The source channel of payment Transaction. Refer to 'Online Help' for details.
PPS ISN	Payment reference number for PPS
PPS Value Date	Payment date for PPS
Origin Country	Country of Physical Address (Information provided from the merchant)
Destination Country	Country of Delivery address (Information provided from the merchant)
PC Country	Payer's computer setting on PC country
PC Language	Payer's computer setting on PC Language
PC TimeZone	Payer's computer setting on PC Time Zone
Card Issuing Country	Country of the card issuing bank (Information provided from acquiring bank; for reference only)

Searching Output of Transaction Detail - Security

Field name	Description
ECI	Electronic Commerce Indicator (ECI) is a value that is returned from the Directory Server (Visa, MasterCard, and JCB) to indicate the authentication results of your customer's credit card payment on 3D Secure. Refer to 'Online Help' for details.
CVV Check	CVV2/CVC2 checking is an indicator to explain if the cardholder enters the verification number at the time of payment. Y - CVV2/CVC2 is entered by cardholder during payment N - CVV2/CVC2 is NOT entered by cardholder during payment (Applicable for merchants who have enabled CVV2/CVC2 checking function only)
Enabled Screening	Merchant can selectively block a particular IP address or card number
Payer Auth. Ref	3D Payer Authentication Reference Data
Payer Auth Status	3D Payer Authentication Status Y – Card is 3D-secure enrolled and authentication succeeds N – Card is 3D-secure enrolled but authentication fails P – 3D secure check is pending A – Card is not 3D-secure enrolled yet U – 3D-sercure check is not processed
Payer Response Code	Response code of authentication process
Payer Response Detail	Response code 's description

Searching Output of Transaction Detail – System/Operations

Field name	Description
DataFeed	Result of Datafeed process: T – Successfully get response from merchant's defined datafeed page F – Fail to get response from merchant's defined datafeed page or error occurs R – Resend successfully U – Resend unsuccessfully (R & U: only available for merchants who have registered the datafeed retry service)
DataFeed Return	Acknowledged print out received from the merchant's defined datafeed page

SiamPay provides a special function called the 'unique merchant reference number checking'. You may enable/disable this function according to your business needs. For more details, please contact our Service Department.

When the searching is finished, the result will be generated as the screen below.

Figure 10: Transaction Detail searching result

There is an **Action** column at the leftmost of the page which MAY contain any of these 5 buttons: i) **Void**, ii) **Refund**, iii) **Capture**, iv) **Reverse** and v) **Resend Datafeed**.   The **Void** and **Refund** actions are cancellation of success sales payment while **Reverse** action is cancellation of successfully authorized payment. And **Capture** action is confirmation of the payment and the amount will be debit from the credit card account once the **Capture** action is taken.

Hints: To achieve quicker results.   For authorized transactions, if you wish to cancel the order at real time, you are suggested to first capture the transaction and void it, instead of doing reversal.

Action Type	Description
Success Payment WITH DEBIT (Accepted)	
Void	**Void** is available before daily bank settlement.
Refund	**Refund** is available within 14 days from the transaction
Successfully Authorized Payment WITHOUT DEBIT (Authorized)	
Capture	**Capture** is available within 14 from the transaction. (exceptions subjected to payment bank)
Reverse	**Reverse** is available within 14 from the transaction. (exceptions subjected to payment bank)
Datefeed Retry	
Resend Datafeed	**Resend Datafeed** is available within 14 from the transaction.

CAPTURE of Authorized Transactions

SiamPay recommends our Merchants to perform the CAPTURE action as soon as the transaction is confirmed as valid.   Once captured, the customer's credit card will be debited and merchants can receive the payment as per the scheduled pay date.   If the merchant does not capture/reverse the authorized transaction over 14 days, the credit limit will be released to the cardholder after a time period which is subjected to card issuing bank.

Full Amount Refund (for standard plan merchants)

Full Refund is available both online and offline.   If the transaction has occurred within the 14 days after-sale period, merchants can perform online refund, by visiting the **Transaction Detail** Report, and clicking the **REFUND** Action button.   If the transaction has occurred for more than 14 days, merchants can download a Merchant Refund Request form, from the **Account Service in the Support Centre**.

Partial Amount Refund (for standard plan merchants)

Partial refund is only available through offline application.   Merchant can download the same form as mentioned above.   Simply fill in the necessary details and send it back to AsiaPay for manual processing.

After receiving a refund request, AsiaPay will gather all the necessary information and send them to the bank for processing.   The refund request will then be processed by the bank, and will take up to 4 to 6 weeks to credit into the customer's credit card account.

Please note that different payment method has its own refund processing period.   You have to send us the refund request latest as follows:

Payment Method	Max. refund period
Visa / MasterCard / JCB / PPS/Amex	180 Days
AliPay	90 Days
China UnionPay	30 Days
99Bill	180 Days

The merchant should directly settle the refund request with the customer after the above said period.

For Premier merchants and AE merchants, you have to contact the bank or card company directly to process refund.

Void, Refund, Reverse and Capture Transaction

Figure 11: Void/Refund/Reverse Transaction

The above screen is opened when the **Void**, **Refund** or **Reverse** button is clicked. In this page, the detail transaction information is shown. To confirm the action, click the **Confirm** button to continue. If decided not to proceed, click the **Cancel** button.

To capture a transaction, the below screen is opened when the **Capture** button is clicked. You may choose to capture the original authorized amount or a smaller amount.
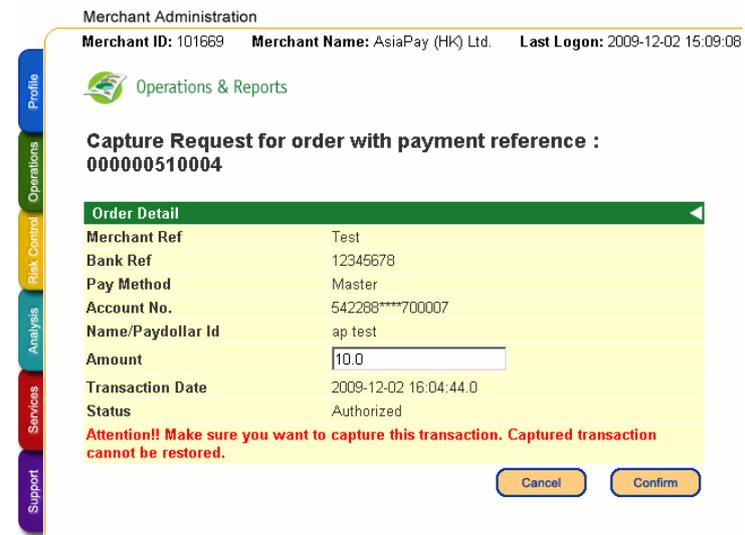
Figure 12: Capture Transaction

To learn more about the action log of a particular payment status for the transactions, simply click on the Status for that transaction; an **Action History** window will pop up, to show you more information. Action History lists all the actions performed for a particular transaction.
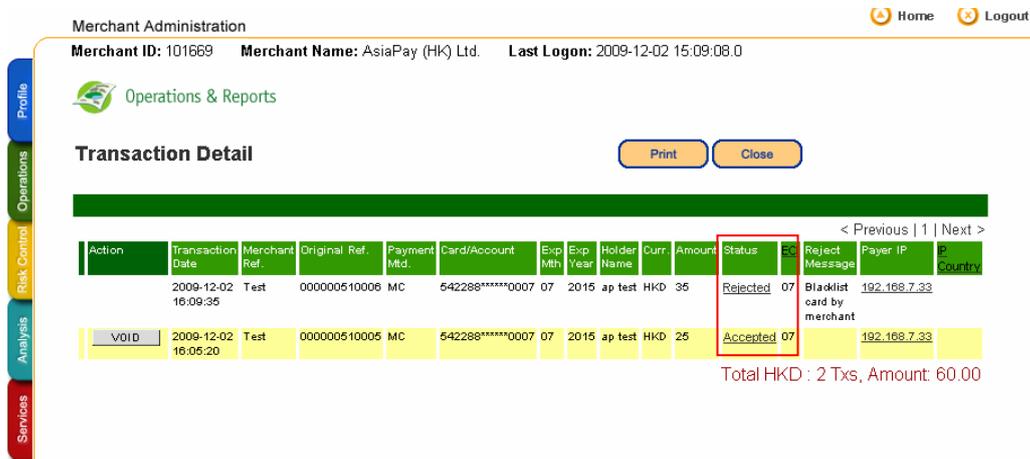
Figure 13: Payment Status

The Action History provides information on when a specific action is performed. The **Action Date** shows the date and time that lead to the present payment status.   You can also find out the operator that is in charge of such action from the **Operator** column.
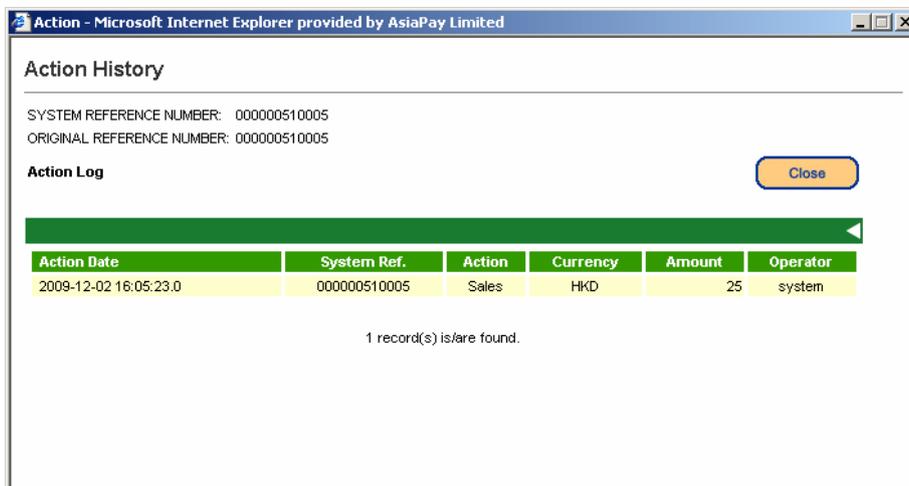
Figure 14: Action History Log

Additional Information on Rejected and Pending Transactions

A.   Rejected Transactions

To learn more about why a transaction is being rejected, before viewing the Transaction Detail Report, please select the **Reject Reason** in the Output section, this will enable the Reject Reason to be displayed on the report as **Reject Message**.

Figure 15: Transaction Detail Report Options

Figure 16: Transaction Detail Report (Rejected Message)

The most common rejected reasons are:

1) Do not honour / Bank Decline: When the card under some account conditions that card issuers disapprove the transactions. Reasons behind includes marginally credit record, abnormal purchase amount or frequency, credit card not allowed for online payment, etc.   Please invite your customers to contact the card issuing bank for the account status.

2) Payer Authentication Fail: Transaction authentication is very important in online payment process; authentication process can ensure the identity of the customers, and again to a large extent can lower the chance of chargeback cases. The 3D-secure check is enforced and the customer fails to confirm his/her identity. If the cardholder fails to pay with their VISA/MasterCard, please kindly invite the cardholder to contact the card issuing bank and register the Verified by VISA (VBV) / MasterCard SecureCode (MSC). If he has already registered the password, there may be input error during the payment, please check with the bank and try to process the transaction once again.

3) High Risk Country: A list of countries with a high reported incident of suspected fraud.   By default, transactions originated from these countries will be blocked by system (Please go to Profile > Payment Options to change the checking status if necessary).   Once you have disabled the checking, you are suggested to perform order confirmation with the customers whenever there is suspicion.

4) Expired Card: The cardholder inputs the expiry date wrongly, the transaction will be rejected with the reason of 'Expired Card'. Please invite your customers to contact the card issuing bank for the account status.

5) Invalid card number: The transaction may be rejected due to the customer entered the wrong card number. Please kindly invite your customers to perform the payment again and ensure that they are entering the correct card numbers.

6) Lost card: The card is reported as a lost card (by the cardholder) at the bank.

7) Stolen card, pickup card: The card is reported as a stolen card / being picked up by a third party.

8) Not sufficient funds: The credit limit of the card is not enough to process a transaction. Please invite your customers to contact the card issuing bank for the account status.

9) Blacklisted IP and card by merchant/system: After the merchant has applied a screening management, to block the IP address or credit card number of a particular transaction. That transaction will be rejected due to this blacklisted record.

10) Others: Please contact us for further details.

B.   Pending Transactions

This may due to either the transaction is under processing or the Banking System does not respond to the transaction request. Please contact our Service Department for details.

Resend Datafeed

Datafeed Retry Function

(Applicable for merchants who have registered the datafeed link and retry function)

Sometimes, you may not be able to receive the datafeed response due to reasons like internet connection issue, incorrect datafeed URL being used, etc.

a) After enabling the "Auto retry failed data feed",

Datafeed will be resent:

(1) Immediately after the original attempt is failed, and

(2) 15 minutes after if (1) is also failed

b) After enabling the "Receive data feed alert email"

an email notification (Retry unsuccessful) will be sent to the technical contact email address if retry (2) fails.

(To receive email notification for (1), please enable the function at Payment Options > Datafeed failure alert email to contact email)

At Transaction Detail Page, you can resend datafeed manually by pressing the '**resend datafeed**' button on the action column within 14 days after the transaction (for transactions with the datafeed indicator of "F" and "U").

To register the datafeed retry function (a and b), please submit the 'Merchant Account Maintenance Form'. You can download this form at the Support session.

Screening Function

If the "Screening Function" box is checked as one of the Searching Output field in the report, a **Screening** column is added to the 2nd leftmost column of the page and a **Screen** button will be shown as below.
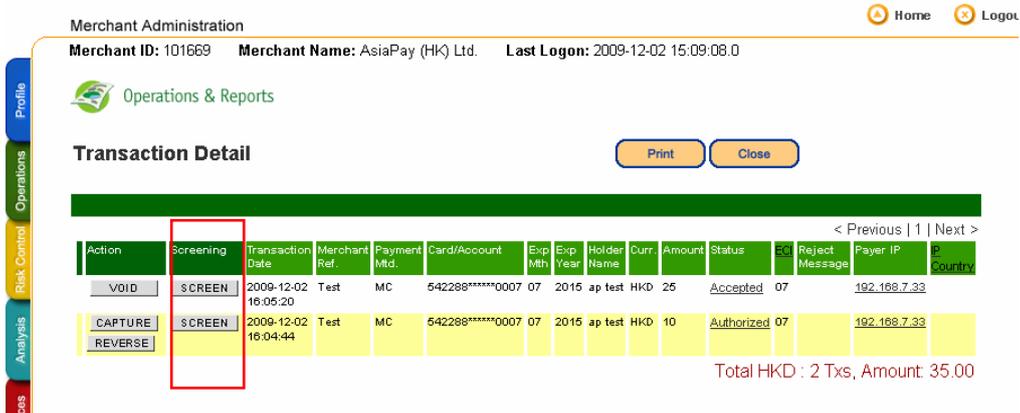
Figure 17: Transaction Detail Report with Screening Function
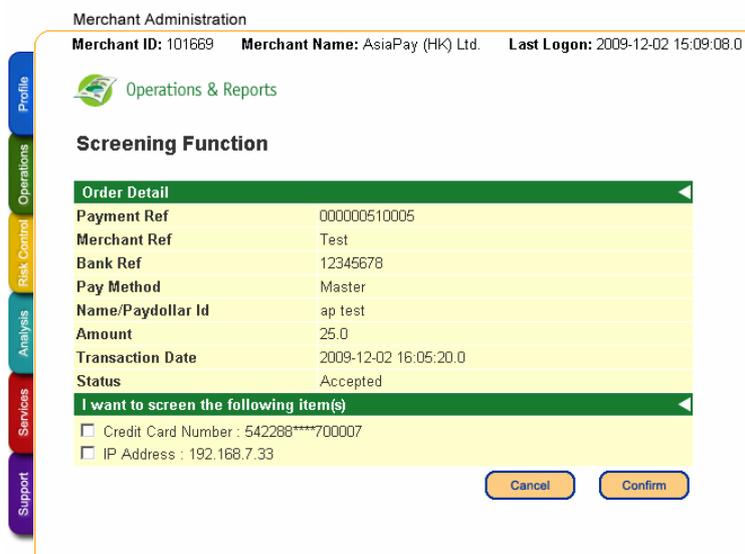
Figure 18: Screening Function Screen

Once the **Screen** button is clicked, the above page is opened to facilitate the screening function. It allows the following screening effects:

Item	Description
Screen the Credit Card Number	Further transaction with that credit card number will be blocked
Screen the IP Address	Further transaction from that IP address will be blocked
Both of the above items	Further transaction either with that credit card number or from that IP address will be blocked

To confirm the action, click the **Confirm** button to continue. If decided not to proceed, click the **Cancel** button.

A **Screening Management** function is available under the **Risk Control** tag to review or delete the current screening rules. Details of this function will be described in the later **Risk Control** section.

eStatement (for standard plan merchants)

(For premier merchants, please contact your acquiring bank for the settlement issue.)

This is an online statement which shows the settlement detail in either by group of payment method or one-by-one transaction listing. In addition, merchant can view their coming settlement schedule and current transaction fee settings.

Three functions are available in the eStatement's menu:
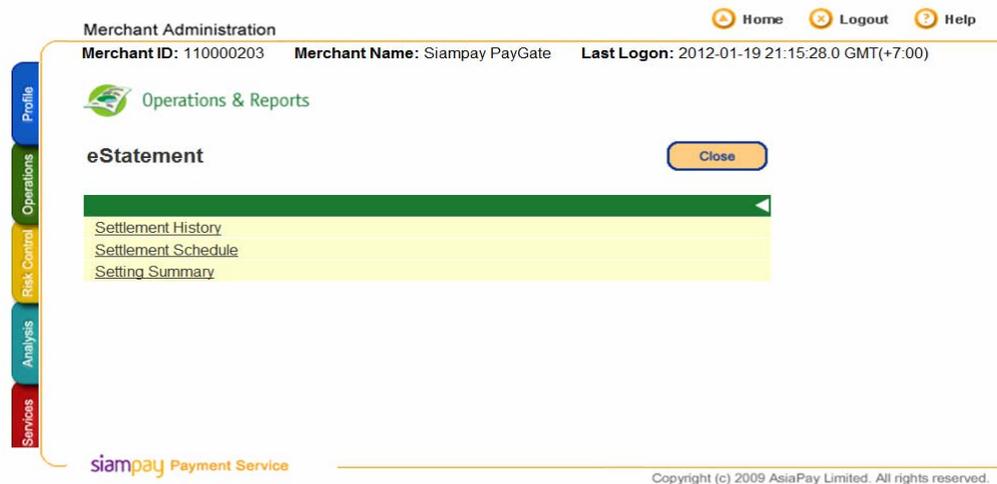
Figure 19: eStatement Menu Screen

1) Settlement History

In this function, merchants are allowed to search the past settlement records by settlement number, paid date or settlement balance.
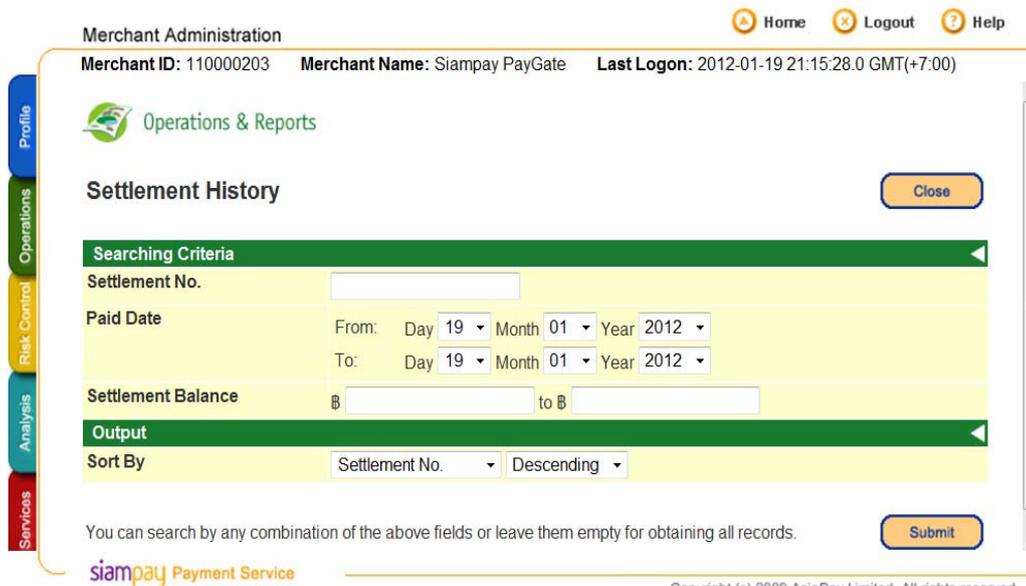
Figure 20: Settlement History Search

After clicking the SUBMIT button, available records will be shown as below:
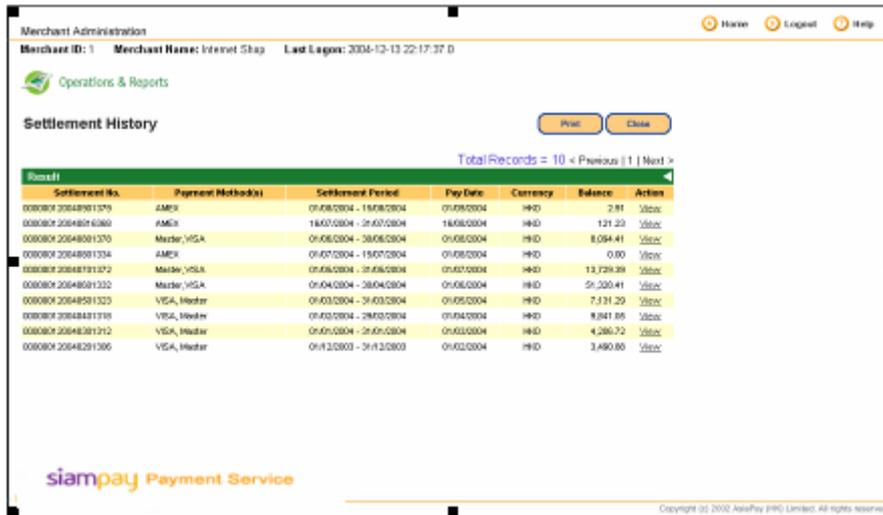
Figure 21: Searching Result Screen

In the above screen, there is an action column with a "View" hyperlink provided for every record. Once it is pressed, the settlement detail will be shown in statement format. Below is one of the statement samples.
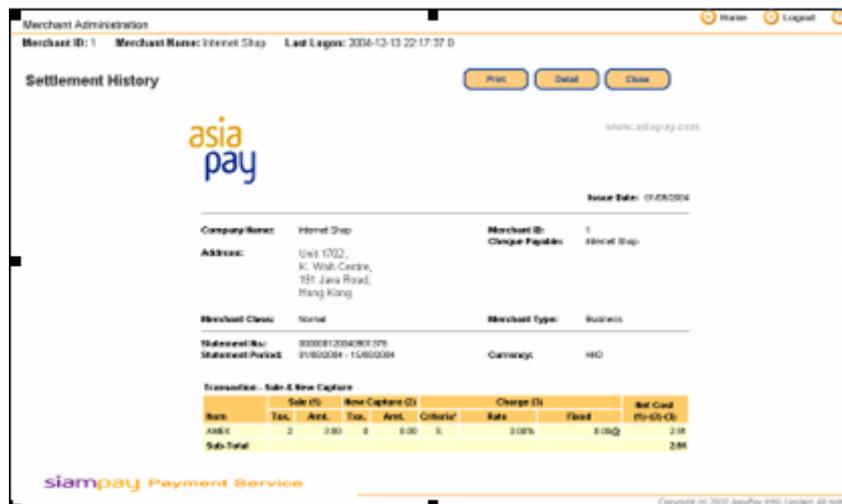
Figure 22: Sample Statement Screen (By payment method grouping)

For every statement, it is divided into 5 sections:

Section	Description
Statement Information	Includes merchant information and the statement no. and period
Sale & New Capture Transaction	Net balance of Sale transaction and New Capture transaction
	* Net balance = Total Sale/New Capture transaction amount - transaction fee
Refund Transaction	Net balance of Refund Transaction
	* Net balance = Total Refund amount + Return charge
	(Return charge means the transaction fee charged in the past/current statement)
Chargeback Transaction	Net balance of Chargeback transaction
	* Net balance = Total Chargeback amount + Return charge – Handling fee
	(Return charge means the transaction fee charged in the past/current statement)
Adjustment	Adjustment details

Merchant can use the DETAIL button to view all the transactions that are included in the corresponding statement. Below is the sample layout:
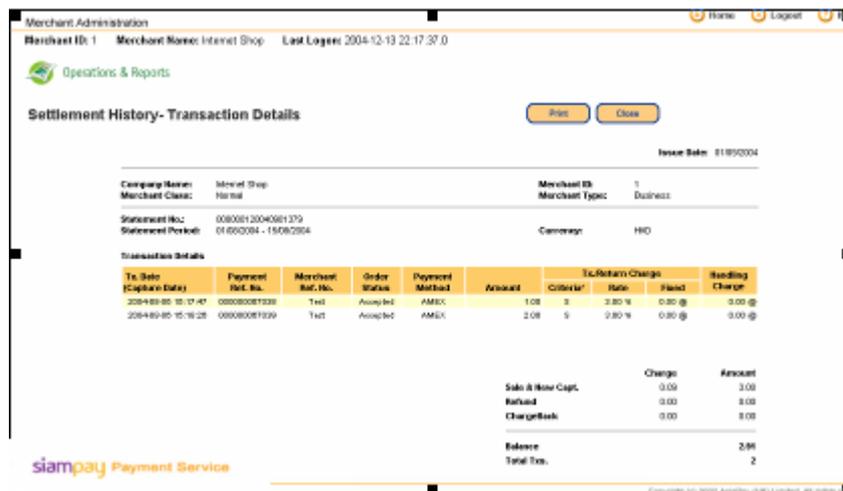
Figure 23: Statement Detail Screen

2) Settlement Schedule

Merchant can view their coming settlement schedule by selecting their desired period. Any change on the settlement schedule will also be reflected in this function.
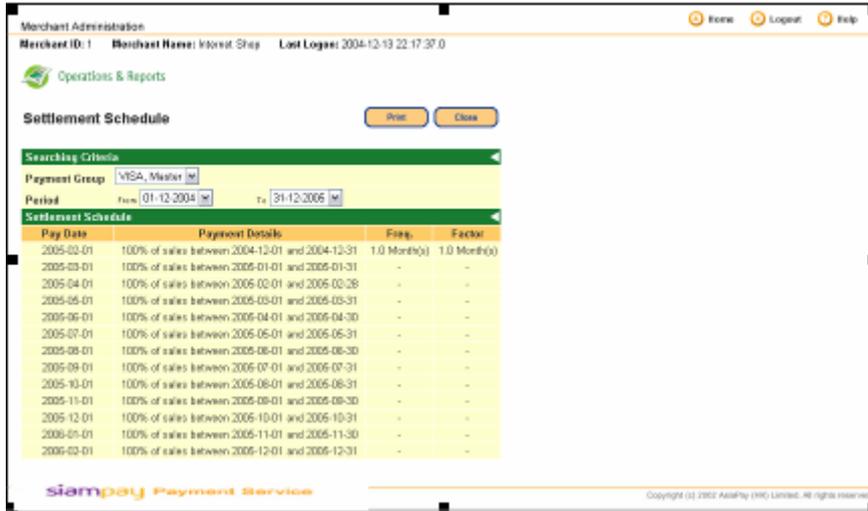
Figure 24: Settlement Schedule Screen

3) Setting Summary

It shows the current transaction fee setting for each payment method.
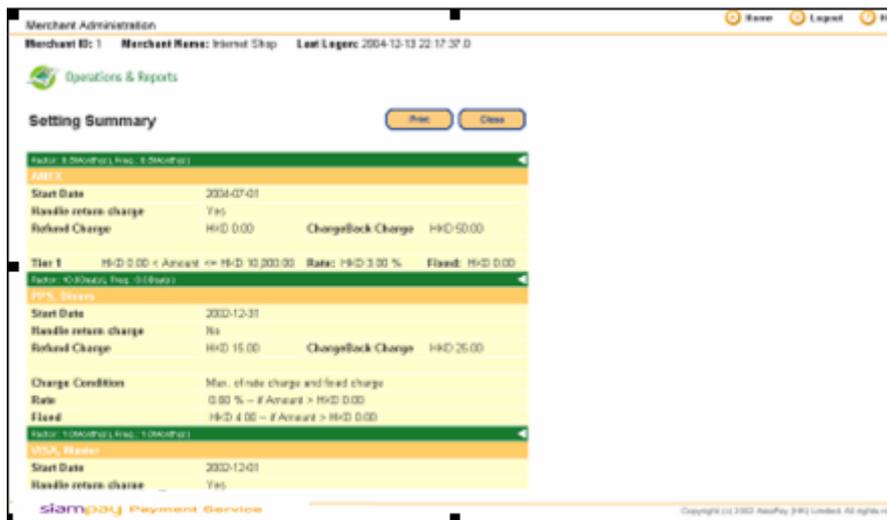
Figure 25: Setting Summary Screen

Sales Report

This online report provides a powerful reporting of **Sales** transactions based on the specified selection criteria including day range and currency. SiamPay merchant can choose to view, print or download (in CSV format) the report.

By default, the total sales within past 2 days will be shown.

Figure 26: Sales Report

You are recommended to download the sales report monthly for your own reference.

Refund Report (for standard plan merchants)

Refund report, is similar to Sales report, which provides reporting of **Refund** transactions based on the specified selection criteria including day range and currency. SiamPay merchant can choose to view, print or download (in CSV format) the report.

By default, the total refund within past 2 days will be shown.

Figure 27: Refund Report

For premier merchants, please contact your acquiring bank for refund details.

Chargeback Report (for standard plan merchants)

Chargeback report is an online report that provides a reporting of **Chargeback** transactions based on the specified selection criteria including day range and currency. SiamPay merchant can choose to view, print or download (in CSV format) the report.

By default, the total chargeback transaction within past 2 days will be shown.
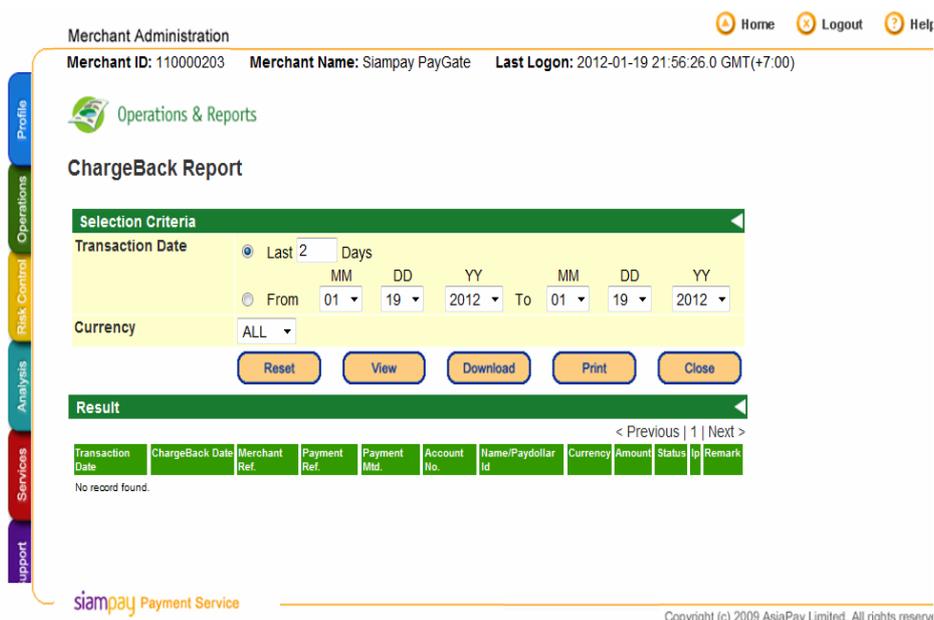
Figure 28: Chargeback Report

For premier merchant, please contact your acquiring bank for chargeback details.

Transaction Summary Report

Figure 29: Transaction Summary Report main screen

Transaction summary report is a concise report that provides a summary of total amount and number of transactions within the specified date range. Total amounts of all transactions breakdown by payment method are available. The following is a sample result page of the summary report.

Figure 30: Transaction Summary Report search result

Bank Settlement Report (for premier merchants)

After daily settlement, premier merchants can work on accounts reconciliation based on the bank settlement report and payment advice received from bank.

You can view the settlement by payment bank and settlement date.

Figure 31: Bank Settlement Report – Payment Bank and Settlement Date searching

Figure 32: Bank Settlement Result

You can choose to view or download the settlement report (in csv or txt format) for your own record.

Figure 33: Settle Detail Report (view)

Risk Control

When the **Risk Control** tag is selected, the menu of **Risk Control** section is shown as below.
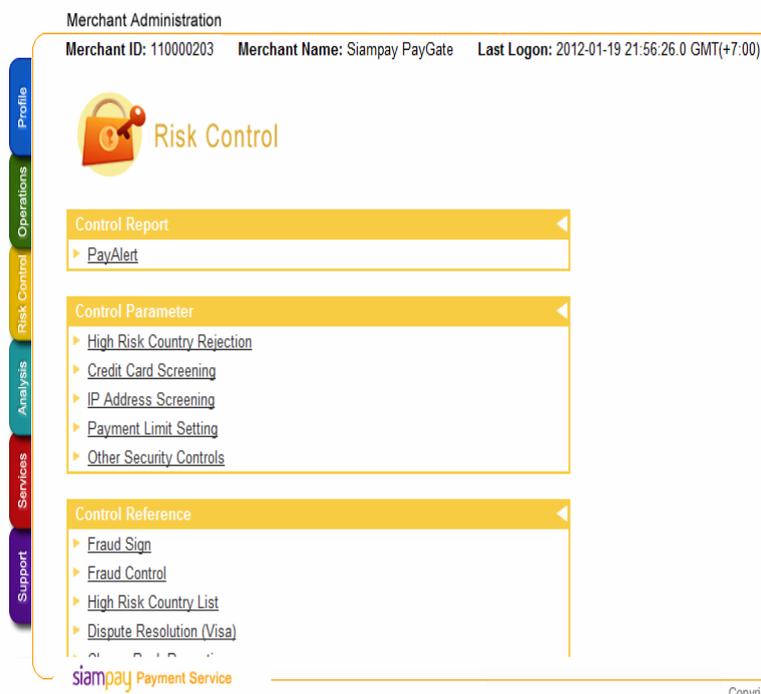
Figure 34: Menu of Risk Control

This menu is divided into 3 parts: *i) Control Report ii) Control Parameter;* and *iii) Control Reference*.

Sub-menu	Contents
Control Report	- PayAlert
Control Parameter	- High Risk Country Rejection
	- Card Screening
	- IP Screening
	- Payment Limit Setting
	- Other Security Controls
Control Reference	- Fraud Sign
	- Fraud Control
	- High Risk Country List
	- Dispute Resolution (Visa)
	- Charge Back Prevention
	- Chargeback Cycle (Visa)
	- Verified by Visa Transaction Process
	- Visa eCommerce Merchant Guide to risk Management

PayAlert Report

PayAlert is a power fraud management tool designed by SiamPay to assist merchants closely monitoring the transactions. It displays a **PayAlert alert symbol** to indicate the merchants if there is suspicious transaction.

Figure 35a: PayAlert Report

The 3 different levels of PayAlert are High, Medium and Low, and each is represented with a different alert symbol:

- High PayAlert Level   - Medium PayAlert Level   - Low PayAlert Level.

Figure 35b: PayAlert Report Screen

PayAlert Level

The table below shows the description and suggested actions to be taken for each PayAlert level. SiamPay recommends merchants when identifying suspicious transactions, to: 1). **VOID** or 2). **REFUND** the transactions, and even apply the screening management rule whenever necessary.

PayAlert Level	Description	Suggested Actions
High	High PayAlert Level signifies a high level of doubt and uncertainty about the transaction being checked. They are potentially caused by: - Using stolen credit cards - Shoppers from high risk countries - Unusual shopping patterns, such as repeated orders, or transaction attempts using invalid information - Credit card with a series of chargeback records	SiamPay highly recommends you to take active actions to ensure the buyer and the transaction are legitimate, to prevent fraudulent transactions. For example: - Send email or call up to ensure the shopper is valid and knows about the transaction - Check shopper's shipping address, billing address, IP address and card issuer to see if it is suspicious - Look through transactions carried out by this particular shopper to study his/her spending history
Medium	Medium PayAlert Level signifies inconsistencies in the transaction being processed. It is less risky compared to High PayAlert Level, and potentially caused by: - Unusual shopping patterns, such as repeated orders, or transaction attempts using invalid information - Credit card with chargeback records	You may wish to carry out further checks before fulfilling the order. Refer to the above actions listed for High PayAlert.
Low	Low PayAlert Level indicates there is a slight chance of fraud in the transaction. Potentially caused by: - Repeated purchase within a short period of time - Credit cards with a chargeback record	You may closely monitor the customer to early detect any undesirable or fraudulent behaviour.

High Risk Country Rejection

This checking is enabled by default, i.e. all transactions originated from high risk countries will be blocked.   You can unclick a particular country on the list to accept payment.   Once click 'Enable', the high risk country list will be shown.

Figure 36: Payment Options Screen – High Risk Country Rejection

Screening Management – Credit Card Screening, IP Address Screening

Screening Management covers **TWO** main areas:

- **Credit Card Screening**
- **IP Address Screening**

This function shows all the currently filtered card number and IP addresses and allows deletion on specific record.
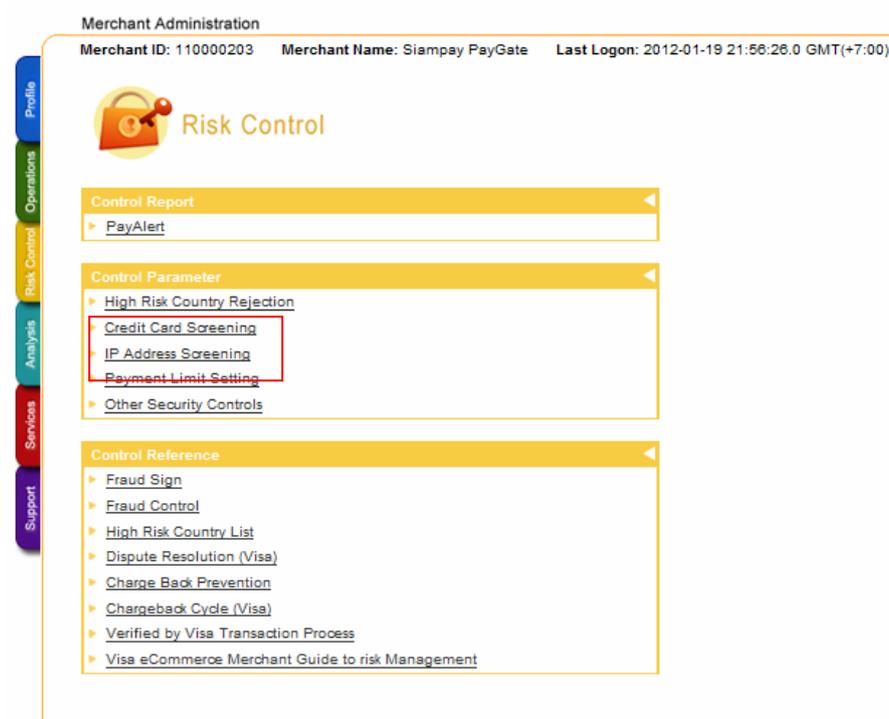
Figure 37a: Screening Management in Risk Control
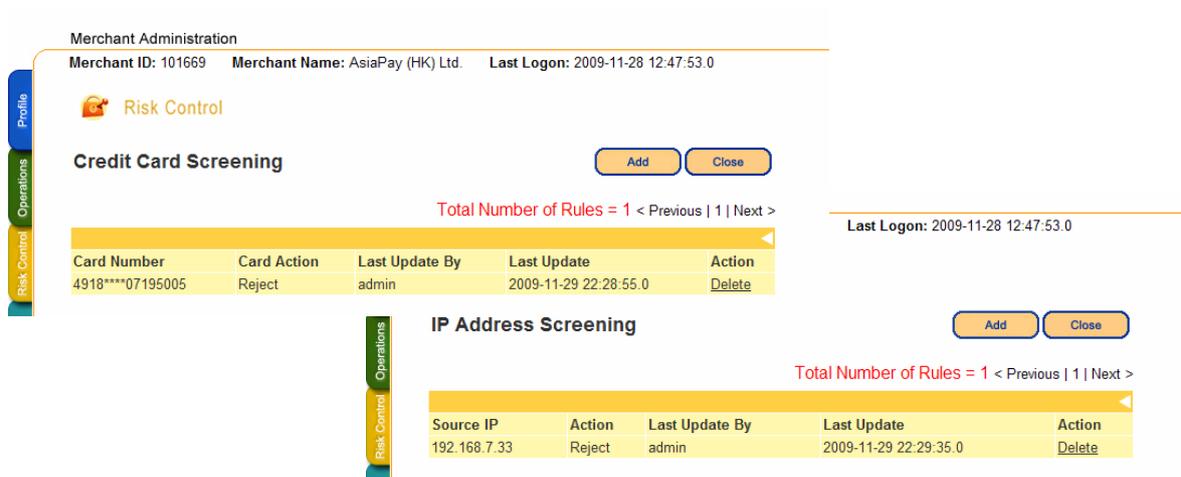
Figure 37b: Card Number & IP Address Screening

Payment Limit

Figure 38: Payment Limit Information

Payment Information

Field name	Description
Transaction Limit	Maximum limit for each single transaction
Daily Limit	Maximum total transaction amount per day
Monthly Limit	Maximum total transaction amount per month

To request for a payment limit upgrade, please submit the 'Merchant Account Maintenance Form'.   You can download this form at the Support session.   You have to provide supporting documents such as the new pricing plan, sales receipts and invoice for the bank's approval.   The application process will take around 7-10 working days.

To closely monitor the sales performance on daily and monthly basis and to prevent payment limits to be exceeded which affects your online business, we will notify you by email (notification will be sent to your registered operation contact email) once the daily and monthly payment limits have reached 80% of the pre-set limits. As such, you will have an adequate preparation time to request for a payment limit upgrade when necessary.

Other Security Controls

Figure 39: Other Security Controls Screen

For each option, you can enable or disable at anytime by simply selecting the options and click the button UPDATE to confirm the changes.

Option	Description
CVV2/CVC2 Checking	**Card Verification Number** is a 3-digit code imprinted on the back of the card. By enabling this function, your customer will be required to enter the credit card number, expiry date and together with the Card Verification Number printed on the card before starting the online payment process. It is an add-on security function to avoid business loss due to the fraudulent use of card. For more details, please refer to the brief description about "What is CVC2/CVV2?" next to this function.
Cardholder name checking	This checking is subject to the card issuing bank
Decline transaction from the same IP	If you set the no. of transactions originated from the same IP to be N. Transaction N+1 onwards will be blocked by the system.
Domain or IP address checking	The domain and/or IP address of the page will be checked while the transaction is posting to SiamPay's site

Control Reference

In this section, merchant can find useful information on the risk management, such as description on charge back process, guidelines to risk and fraud management, etc.
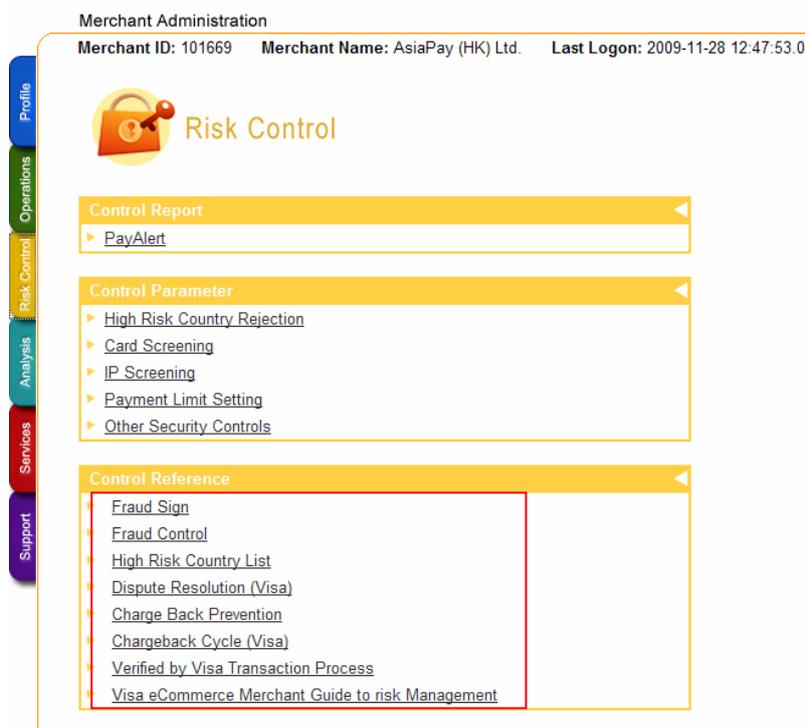
Figure 40: Control Reference Screen

SiamPay Analyzer

When the **Analysis** tag is selected, the menu of **SiamPay Analyzer** section is shown as below.

Figure 41: Menu of SiamPay Analyzer

Advanced chart and analysis tool suite helps the merchant to better managing the sales performance and payment transaction trend in visualizations.

Sub-menu	Contents
SiamPay Analyzer (*All the information showed in this section is for reference only*)	- Peak Hours Traffic Analysis - Weekday vs Weekend Distribution Analysis - Seasonal Analysis - Payer Country Distribution - Business Trend Analysis - Sales Performance Analysis - Reject Distribution Analysis

Peak Hours Traffic Analysis

It is useful for merchants to compare the peak and non-peak hours of the business. It will count the transactions with **ALL** status.

Figure 42a: Peak Hours Traffic Analysis
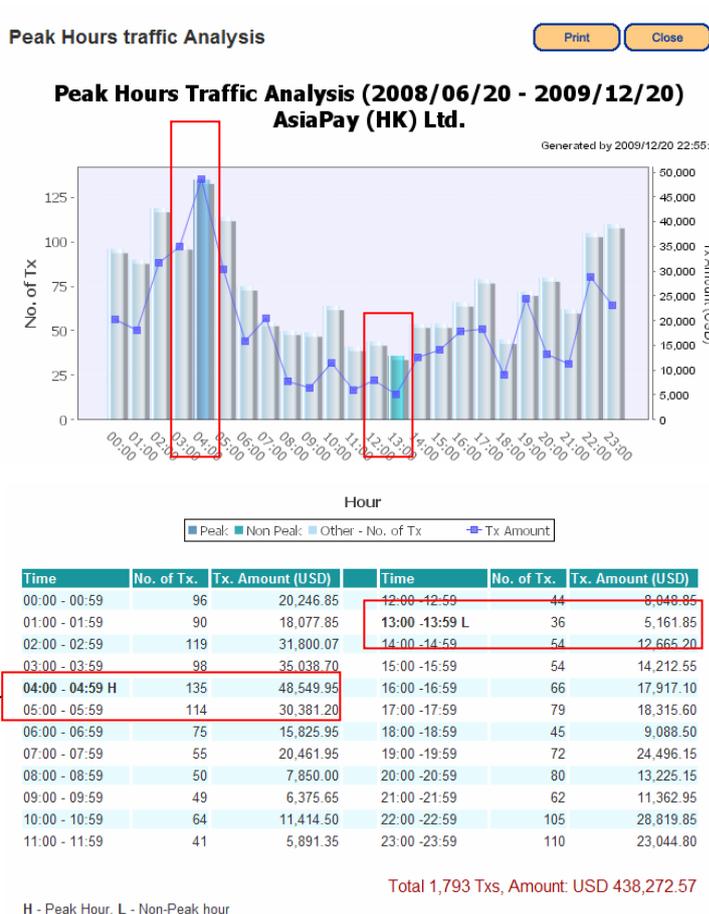
Figure 42b: Peak Hours Traffic Analysis – Chart and Statistic

According to the number of transaction within the chosen period, it will use '**H**' to indicate the Peak hour and '**L**' to indicate the Non-Peak hour.

Weekday vs Weekend Distribution Analysis

It is useful for merchant to show the transaction distribution between weekday (Mon to Fri) and weekend (Sat and Sun). It will count the transactions with status including: **Accepted, Accepted_Adj, Rejected and Cancelled**.

Figure 43a: Weekday vs Weekend Distribution Analysis

Figure 43b: Weekday vs Weekend Distribution Analysis – Chart and Statistic

Seasonal Analysis

It is useful for merchants to analyze the transactions on quarterly basis in a year and provide an insight of seasonal effect. It will count the transactions with status including: **Accepted, Accepted_Adj**.

Figure 44a: Seasonal Analysis

Quarter	Month	No. of Tx.	Percentage	Tx. Amount (USD)	Percentage
	January	39		6,536.45	
Q1	Feburary	90	16.50%	11,119.30	15.23%
	March	124		15,539.95	
	April	91		12,438.10	
Q2	May	134	23.42%	17,869.55	22.75%
	June	134		19,303.25	
	July	144		21,989.25	
Q3	August	190	29.48%	27,362.30	31.57%
	September	118		19,471.77	
	October	133		20,262.55	
Q4	November	125	30.59%	16,860.70	30.45%
	December	211		29,271.10	

Total 1,533 Txs, Amount: USD 218,024.27

*The analysis records are for reference only

Figure 44b: Seasonal Analysis – Chart and Statistic

Payer Country Distribution

It is useful for merchants to show which country the customers are originated from. Merchant can select the specific date range and the payment method to display the result. Three are three options for choosing payment method:

i)   **All**   – Including all payment methods

ii)   **Credit Payment**   – Including Visa, MasterCard, JCB, AMEX, Diners

iii)   **Debit Payment**   – Including ChinaPay, CUPS, PPS, AliPay, 99Bill, PayPal

Figure 45a: Payer Country Distribution

And, there are six report types for merchant to choose:

i)   Successful Payment Only

ii)   Rejected Payment Only

iii)   Both Successful and Rejected Payment

iv)   Success Ratio

v)   Reject Ratio

Payer IP information is obtained from the third party - MaxMind, Inc., in which the result is based on the browser your customer used when processing the payment. It is for reference only.

An example of searching result:

Figure 45b: Payer Country Distribution – Chart and Statistic (Report Type: Successful Payment Only)

Business Trend Analysis

It is useful for merchants to show the business trend according to the no of transaction and the transaction volume. It will count the transactions with status including: **Accepted, Accepted_Adj**.
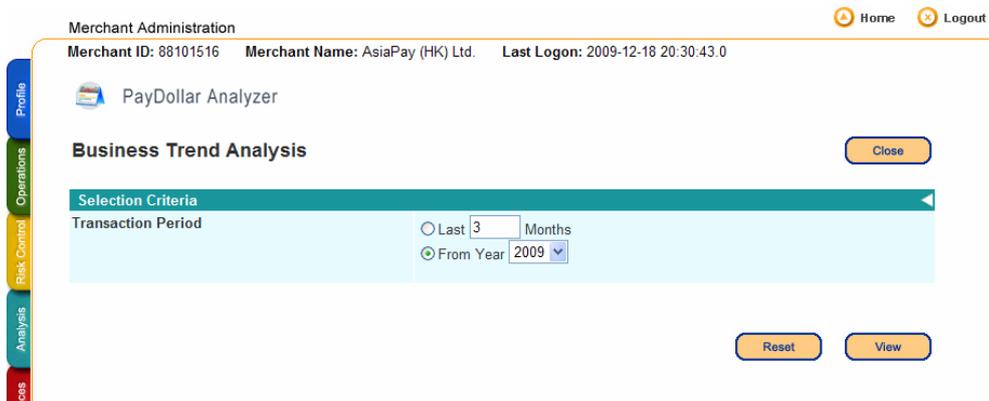
Figure 46a: Business Trend Analysis
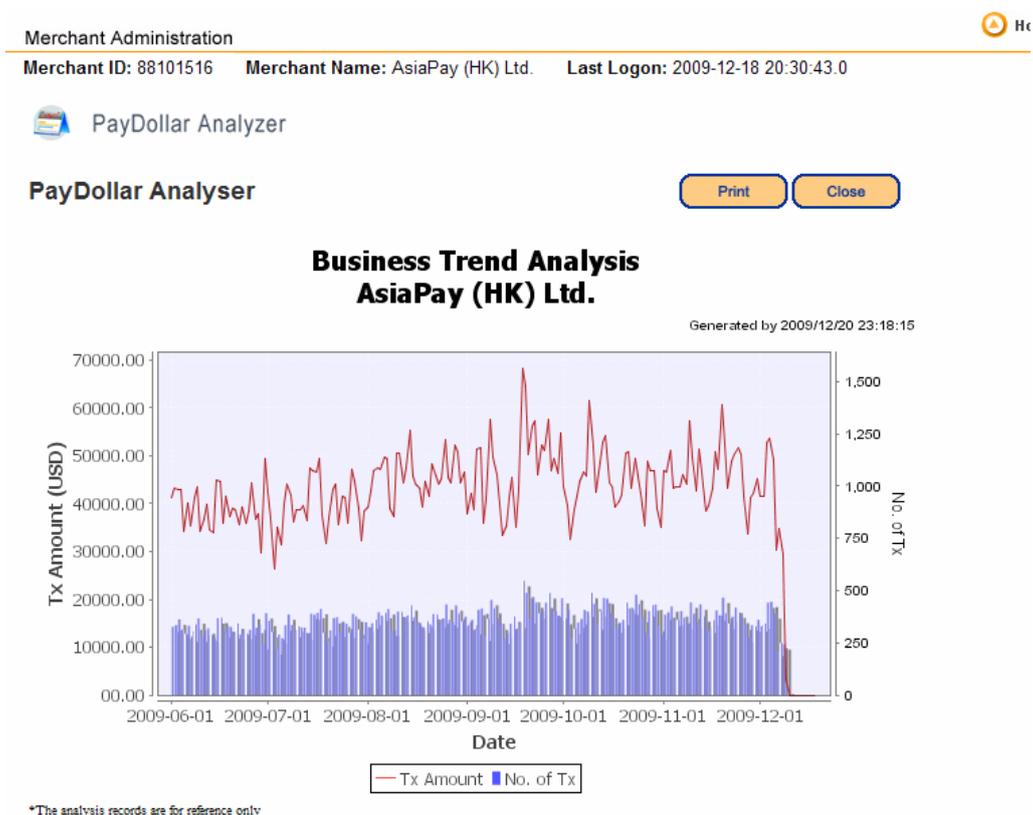
Figure 46b: Business Trend Analysis – Chart

Sales Performance Analysis

It is useful for merchants to calculate their transaction success rate and chargeback rate. Merchant can select the specific date range and the payment method to display the result. Three are three options for choosing payment method:

i)   **All**   – Including all payment methods

ii)   **Credit Payment**   – Including Visa, MasterCard, JCB, AMEX, Diners

iii)   **Debit Payment**   – Including ChinaPay, CUPS, PPS, AliPay, 99Bill, PayPal

Figure 47a: Sales Performance Analysis

There are four report types for merchant to choose:

i)   Success Ratio

ii)   Chargeback Ratio (Chargeback case reported from acquiring bank; Not available for Premier merchants)

iii)   Refund Ratio

iv)   Void Ratio

An example of searching result:

PayDollar Analyzer

Sales Performance Analysis   Print   Close

Sales Performance Analysis - Success Ratio
AsiaPay (HK) Ltd.

Generated by 2009/12/20 23:21:04

-■- Transaction Amount   -●- Volume   —— Threshold

Date	No. of Tx.			Tx. Amount (USD)		
	Success	Total	Percentage	Success	Total	Percentage
2008-10	133	221	60.18%	20,262.55	76,063.05	26.64%
2008-11	125	409	30.56%	16,860.70	142,148.90	11.86%
2008-12	211	317	66.56%	29,271.10	57,256.20	51.12%
2009-01	88	162	54.32%	14,253.85	26,438.15	53.91%

*The analysis records are for reference only

Figure 47b: Sales Performance Analysis – Chart and Statistic (Report Type: Success Ratio)

Reject Reason Distribution

It is useful for merchants to have an overview of rejected payments. As such, merchant can gain a better understanding of the rejected payments classification over a specific period of time.
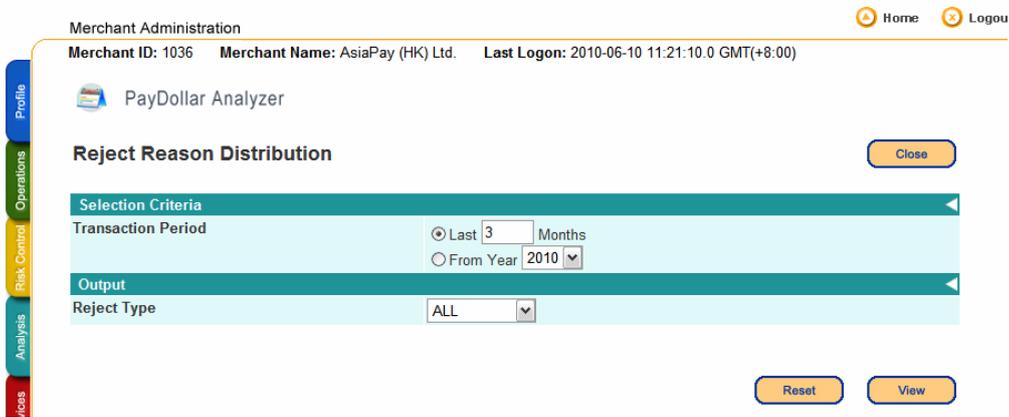
Figure 48a: Reject Reason Distribution

An example of searching result:
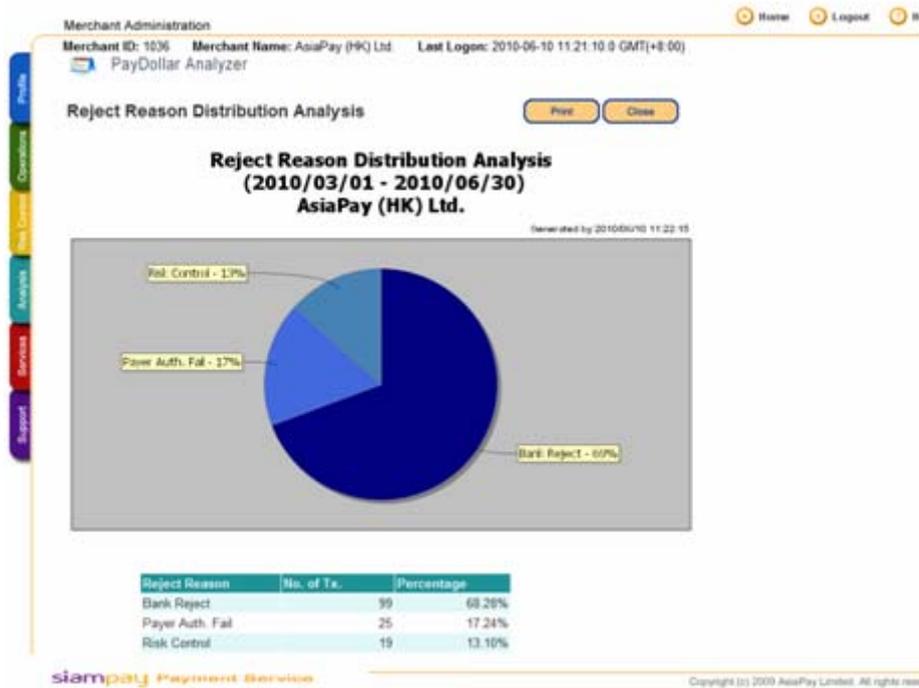
Figure 48b: Reject Reason Distribution – Chart and Statistic

Services Centre

When the **Service** tag is selected, the menu of **Service Centre** section is shown as below.
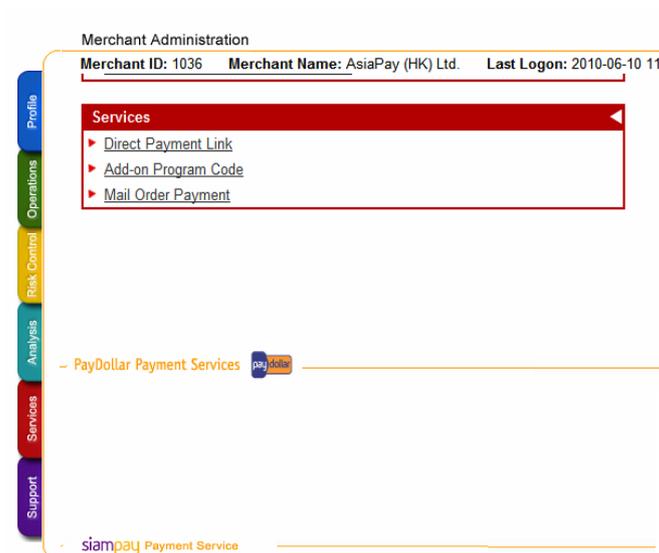
Figure 49: Services Centre main screen

This section provides a collection of functions for account configuration, user control and value-added services. Choose from the submenu, Account Configuration or Services, the merchant can select one of the following options:

Function	Description
Account Configuration	
Change Password	To change admin login password of super admin
User Access Control	To control / amend user and group access rights
Services	
Direct Payment Link	To generate and manage static payment link

Change Password

Figure 50: Change Password screen

To change password, simply enter the old password, then the new password twice to confirm. Press the Submit button to change the password of your given login ID.

It is recommended to use a highly secure password with 7-15 characters. A good password should contain alphanumeric, and should be meaningless to most of the people and CANNOT be found dictionary. The new password chosen could not be the same as the previous 4 password being used before.

If you forget your login password, please contact us to reset the password.

User Access Control

Figure 51: User Account Maintenance main screen

SiamPay Merchant Administration Tools allows different users to access the system. Super Admin may grant different access rights to different users or groups. This is useful, for instance that you may want a user or a group of users to have limited range of control over some aspects, while granting others on some other aspects.

Sub-menu	Functions
User Group Maintenance	- Define new group - Group's access right control - Edit access right
User Maintenance	- Add new user - User search - Group assignment - User's status control - Change password

User Group Maintenance

Figure 52: User Group Maintenance screen

In SiamPay system, a user must be assigned to a group in order to gain access rights. In the diagram at the right-hand-side, it illustrates the procedure of creating groups and assigning users. Since the 'rights' are assigned to a group level, instead of user level, a user must be grouped into a right group to gain the rights.
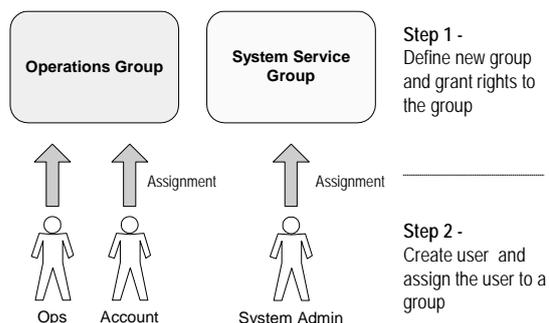
The screen above is the User Group Maintenance section in which list of groups will be shown. To view / update a group, click on the group name to open the group detail screen. To add a new group, click [Add New Group] to open the **Add User Group** form as shown below.

Add User Group

Figure 53: Add User Group screen

Create a new user group by completing the information, then selecting the access rights. Access right are divided in 3 levels:

- **None** means no access right
- **Read only** restricts user to edit / update any information
- **Full** means user is allowed to read and update information

Types and **Functions** are corresponding to the tag-menu (at the left-hand-side) and submenu of each section. When the access right of a function to a user is set as *None*, that menu item will not be seen by that user.

The following is the group detail screen of a sample user group. Update the group information and access right, then Confirm to complete and submit updated information.

Figure 54: User Group Detail screen

User Maintenance

User Maintenance is the second function of User Account Maintenance, in which administrator can add new user by clicking [Add New User] button. To search for a user, enter search criteria, such as **Login ID**, **Name**, **Group** and/or **Status**. Click Submit button to start searching. By default, i.e. click the Submit button without entering any criteria, all active user will be listed as the result screen shown below.

Update User

Figure 57: User Update screen

To update an existing user, click the **Update** link of that user under Action column of User Searching screen. It will present an Update User screen as above. When finish, click Submit button to complete the update process.

If a user forgets the login password, the super admin should set a new password for that user.

Add User

Figure 58: Add User screen

To add a user, click the ⬭Add New User⬭ button to open the add user form as shown above. Complete the information and then press Submit button when finish.

Direct Payment Link
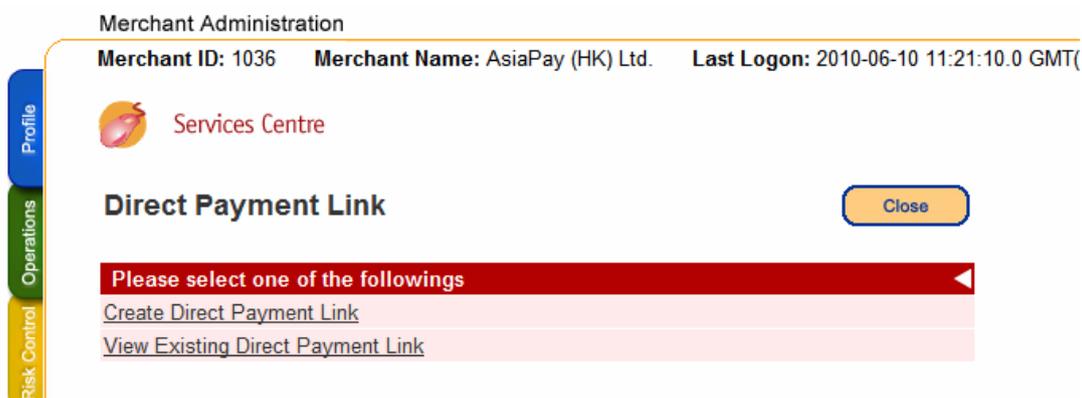
Figure 59: Direct Payment Link main screen

Direct payment link function helps merchants to create hyperlink with necessary payment parameters and manage the existing payment link.

Sub-menu	Functions
Create Direct Payment Link	- Ad a new direct payment link
View Existing Direct Payment Link	- View the history record for the valid direct payment link

Create Direct Payment Link

Create Direct Payment Link is a function that helps merchants to create hyperlink with necessary payment parameters. Merchant can set the valid date up to one year. Within the valid period, customer can make payment via the hyperlink until it's expired.

For example, after you have received an order by e-mail, you can input the necessary information on the page below, then send the hyperlink to the customer for payment.

Figure 60: Create Direct Payment Link screen

View Existing Direct Payment Link

Merchant can keep a history of the direct payment links (up to one year) created at an earlier stage for operational control and review.

Figure 61a: View Existing Direct Payment Link screen
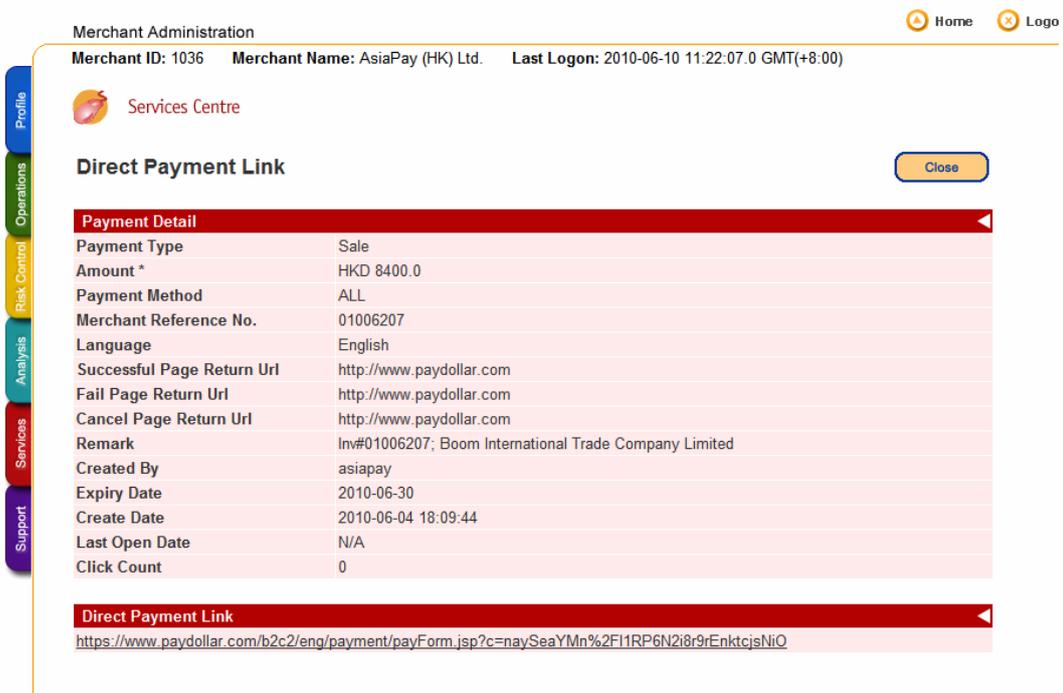
Figure 61b: Details of Direct Payment Link screen

Support Centre

When the **Support** tag is selected, the menu of **Support Centre** section is shown as below.

Figure 62: Support Centre

In Support Centre, merchant can find useful information, such as vendor's contact information, merchant account maintenance form, refund request form, merchant user guide and the Developer Corner etc.

Figure 63: Support Centre – Guide lines of Use of Standard Logos, Multi-Card Logos and 3 D Secure Cards

Under "Support" section, there is a "Guidelines of Use of Standard Logos, Multi- Card Logos and 3 D-Secure Cards" which helps the merchant to use logo on merchant website, please contact our IT Department.

Contact Information

AsiaPay (Thailand) Limited.

121/49 RS Tower, Level 11,

Ratchadapisek Road,

Dindeang, Bangkok

Thailand 10400

Opening Hours

Mon. - Fri. 9:00a.m - 6:00p.m

(except public holidays)

Service and Operation Hotline

Tel: (662) 642 3272

Fax: (662) 642 3272

Email: service@siampay.com

Accounts Hotline

Tel: (662) 642 3272 # 21

Fax: (662) 642 3272

Email: account@siampay.com

Technical Support Hotline

Tel: (662) 642 3272 # 27

Fax: (662) 642 3272

Email: it@siampay.com

~ END ~