

eNETS REPORTS & ADMINISTRATION USER GUIDE

COPYRIGHT

The information contained in this manual is proprietary and confidential to eNETS Pte Ltd (“eNETS”). This material may not be duplicated, published or disclosed, in whole or part, without the written permission of eNETS.

CHANGE HISTORY

Periodically, revisions to this Manual will be made as we incorporate enhancements/changes. With each revision, we will list the changes under “Description” below and the date and version of the Manual shall appear in the footer of each page.

Version No.	Revision No.	Description	Approval Date
1	0	Initial release	January 2006
1	1	Update screens / navigations / contacts details	September 2010
1	2	Update contacts details	March 2011

Information about this Manual

This manual contains guidelines on how to use the eNETS Report and Administrative functions. This Manual helps to provide merchant personnel with an understanding of the eNETS Report and Administrative functions.

If you have any questions about this Manual, please give us your comments:

- By Customer Service Hotline: **(65) 6274 1212**

Operating Hours:

8:30am to 6:00pm Mondays - Fridays.

Closed on Saturdays, Sundays and Public Holidays.

- By Email: info@nets.com.sg

Table of Contents

1	Introduction	1
1.1	Overview	1
1.2	Helpdesk	1
2	Access Control by System Administrator	2
2.1	Access Control Management.....	2
2.2	Role Management.....	3
2.2.1	Create Role.....	3
2.2.2	Housekeeping Roles.....	6
2.3	User Management	10
2.3.1	Create User	10
2.3.2	List Users.....	11
3	Getting Around	16
3.1	URL.....	16
3.2	What's needed for login	16
3.3	Login For the First time	17
3.4	Navigation after login	17
3.5	Changing Password.....	18
4	Specific Functions	19
4.1	Merchant Profile Management.....	19
4.1.1	Update Profile	19
4.1.2	View Profile.....	19
4.2	Public Key Management.....	19
4.2.1	Request Public Key Upload.....	19
4.2.2	Upload Public Key	21
4.2.3	View Public Key.....	22
4.3	Transaction Management (valid ONLY for Credit Card transactions)	23
4.3.1	Setup of Blacklist Credit Cards.....	23
4.3.2	Setup of Whitelist Credit Cards	24
5	Virtual Terminal Transactions.....	25
5.1	Credit Card Sale Transaction	25
5.2	Credit Card Authorization Transaction.....	27
5.3	Credit Card Capture Transaction.....	28
5.3.1	Multiple-full Captures	30
5.3.2	Partial Capture.....	31
6	eInvoice	33

6.1	Non-Master Merchant eInvoice.....	33
7	Reports	36
7.1	Reports for ALL eNETS Payment Services	36
7.1.1	Transactions for All Payment Types.....	36
7.1.2	Sales for All Payment Types	37
7.2	Reports Specific to Credit Card Transactions.....	39
7.2.1	Credit Card Authorization Report	39
7.2.2	Transaction Report With Credit Card Numbers.....	40
8	Quick Reference Guide	41

1 Introduction

1.1 Overview

The eNETS Report and Administration is an internet-based portal that allows merchants to monitor and manage their online transactions. To use this facility, a merchant profile is needed. The profile is a record of the merchant's details and permitted functionalities (e.g. ability to perform authorization, view selected reports etc).

1.2 Helpdesk

For problems or queries in using the system, please contact us by:

- Customer Service Hotline: **(65) 6274-1212**
Operating Hours:
8:30am to 6:00pm Mondays - Fridays.
Closed on Saturdays, Sundays and Public Holidays.
- Email: info@nets.com.sg

2 Access Control by System Administrator

Note to Reader:

This Section should be read by the System Administrator (SA) of the company. If you are NOT the SA of the company, please proceed to Section 3 and onwards.

The SA account is the top-level account and is the only account created by NETS for each company. It is advisable that this account is used ONLY for administrative purpose i.e. do not use this account for other transaction or report functions. The SA account is the only account that is not removable and consequently provides the only access should other accounts be locked. It should therefore be the ownership of a Manager/Supervisor of the company.

2.1 Access Control Management

In each organization, eNETS shall assign a “**Group Name**” to the organization e.g. “Ocean Group”, “Astoria Florist” etc. Against each of this Group, the relevant **functions** will be assigned. e.g. “Ocean Group” has been granted the functions “Merchant Reports”, “Merchant Admin” etc.

For each organization, eNETS will only create one account, and this account is typically assigned to the SA of the company. Thereafter, the SA will be responsible for creating the “**Roles**”, and Users. By Roles, the SA can define what functions can be accessed by users under this Role. For example, the Finance department is in charge of billing and the operations department takes care of fulfillment. The SA can create two roles: Finance and Operations. Against the Finance Role, the SA can assign the ability to view eInvoices and Transaction Reports. Likewise, for the Operation Role, the SA can assign the ability to view Transaction Reports, and even the function to authorize a credit card payment.

The diagram in Figure 2.1 illustrates the relation between Group, Roles and Users.

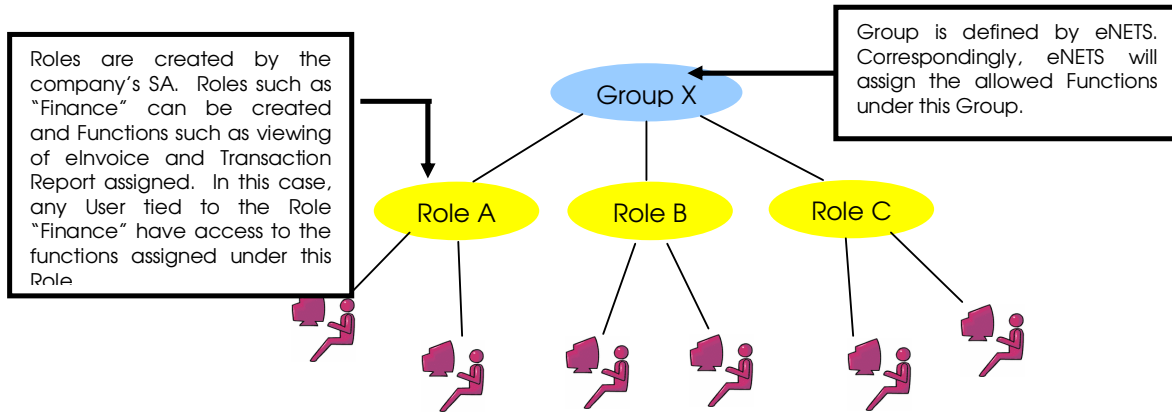


Figure 2.1 - Relationship between Group, Role and Users

2.2 Role Management

2.2.1 Create Role

In each organization, the role of each person or supporting unit may be different. Under eNETS, the SA can assign the relevant functions, reports to each department.

For example, the Finance department is in charge of billing and the operations department takes care of fulfillment. The SA can create two roles: Finance and Operations. Against the Finance Role, the SA can assign the ability to view eInvoices and Transaction Reports. Likewise, for the Operation Role, the SA can assign the ability to view Transaction Reports, and even the function to authorize a credit card payment.

Finally, under each Role, you can assign one or more Users.

For an SA to create a Role:

- Login to the eNETS Administration & Report Portal (refer to Section 3) for details on Login).
- Please ensure that you are assigned the function "Access Control". From this function, you will be able to manage the roles of your users within your company.
- To create a "Role", from **Figure 2.2**, navigate as follows:

[Access Control > Role Management > Create Role](#)

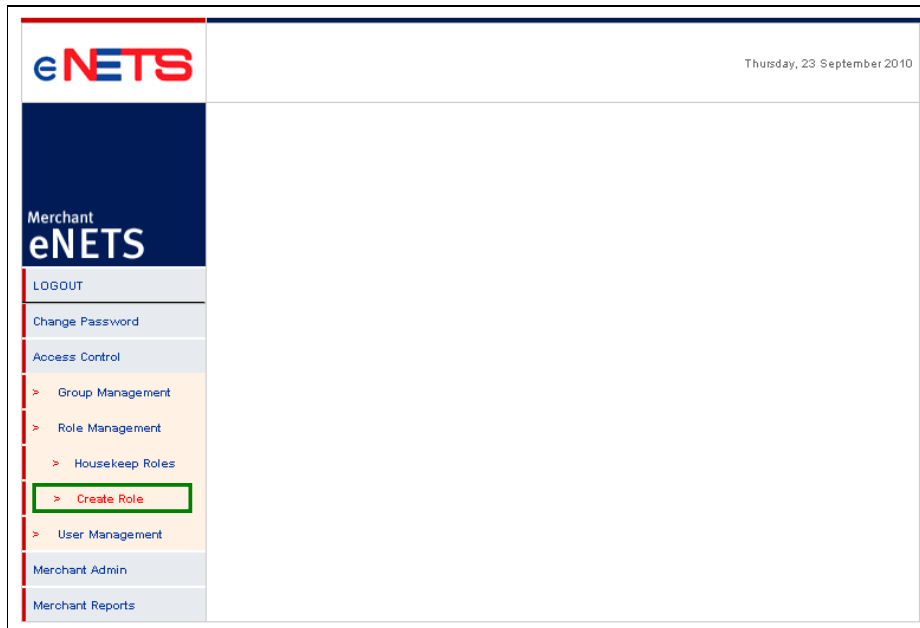


Figure 2.2 - Page showing navigation menu with Create Role highlighted

- Enter the name for the new role in the page that follows (Figure 2.3). As a guideline, the name of a "Role" could describe the main/primary responsibility of a group of personnel in your company. For example, you can create the role "Finance", and subsequently assign the functions such as accessing of salient transaction reports for accounts reconciliation.

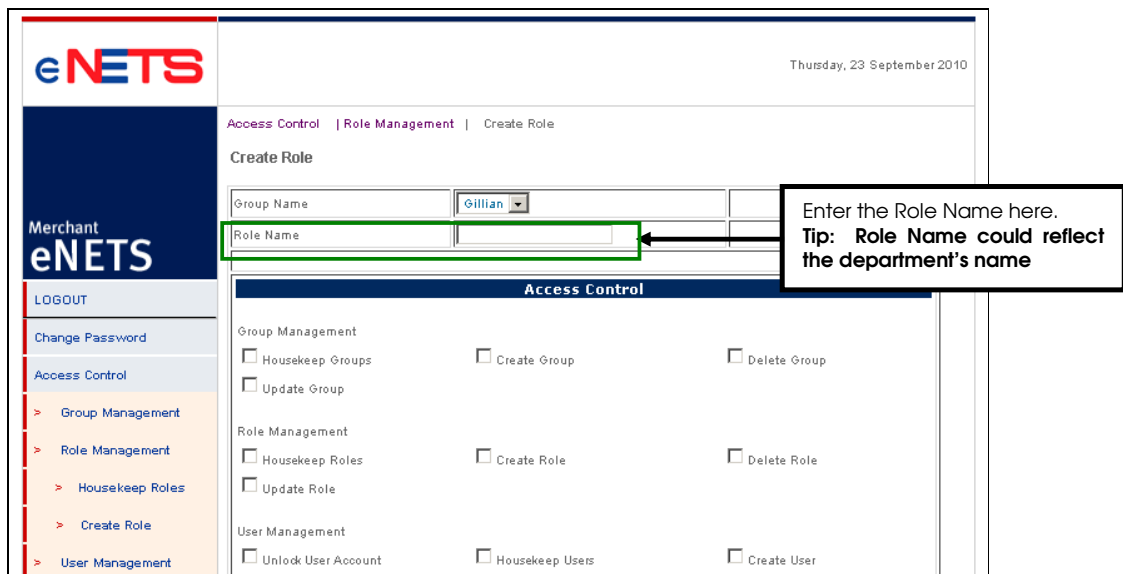


Figure 2.3 – Assigning a Name to a Role to be created under your organization

- To assign the functions against the Role, check the appropriate boxes. (Figure 2.4)
- Click the "Submit" button to save the functions against this role.

Figure 2.4 - Create Role Page after role name input and function allocation

2.2.2 Housekeeping Roles

This function will give the SA a holistic view of the various Roles in the organization, and the functions assigned against each role. From here, you will be able to housekeep the accounts.

- After login, access this functional page, as shown in **Figure 2.5**, via the navigation menu in the following order:

Access Control > Role Management > Housekeep Roles

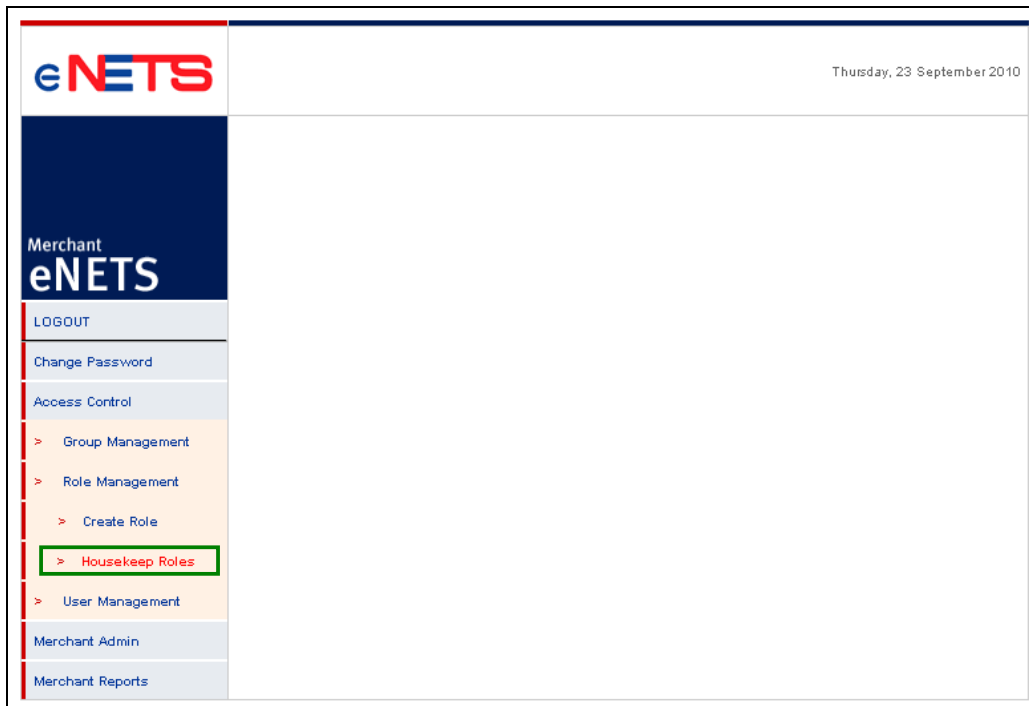


Figure 2.5 – “Access Control” with ability to list Roles assigned to an organization

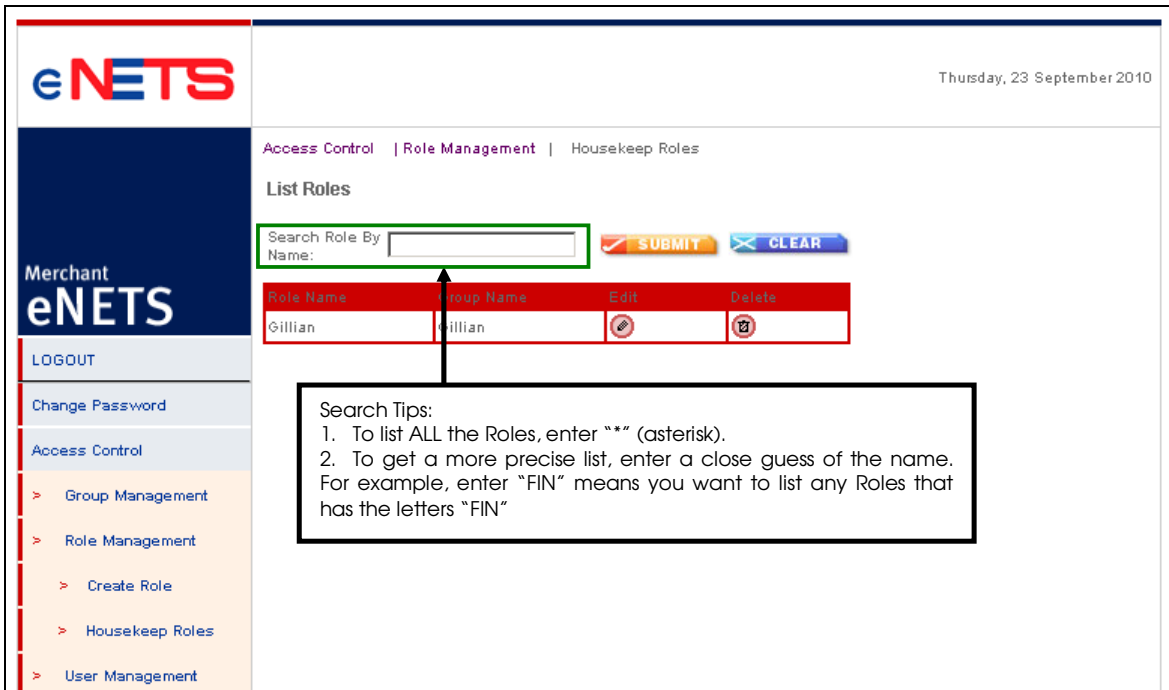


Figure 2.6 – Search for a particular Role

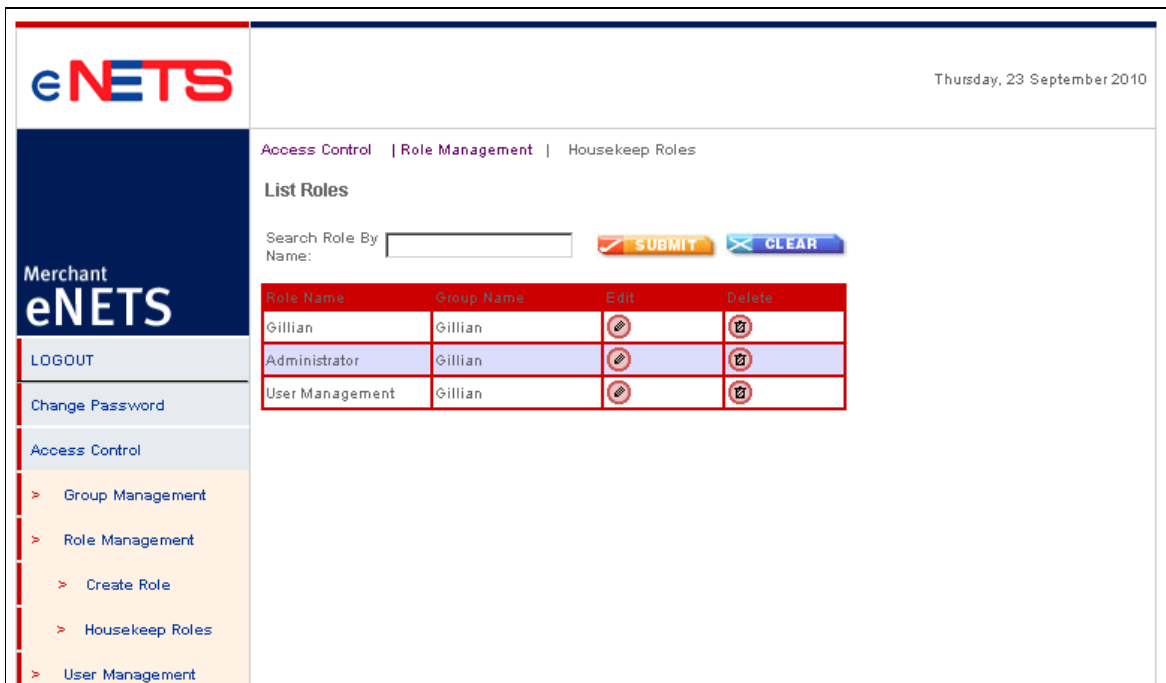



Figure 2.7 – Results presented after a search

- From the results page (**Figure 2.7**), there are two actions which the SA may undertake:

- Edit the functions assigned to a Role.
- Delete the Role.

2.2.2.1 Editing an existing Role

- From **Figure 2.7**, click on the  icon under the "Edit" column of the corresponding Role.
- The following Edit Role page displayed will show the list of functions assigned against the Role.

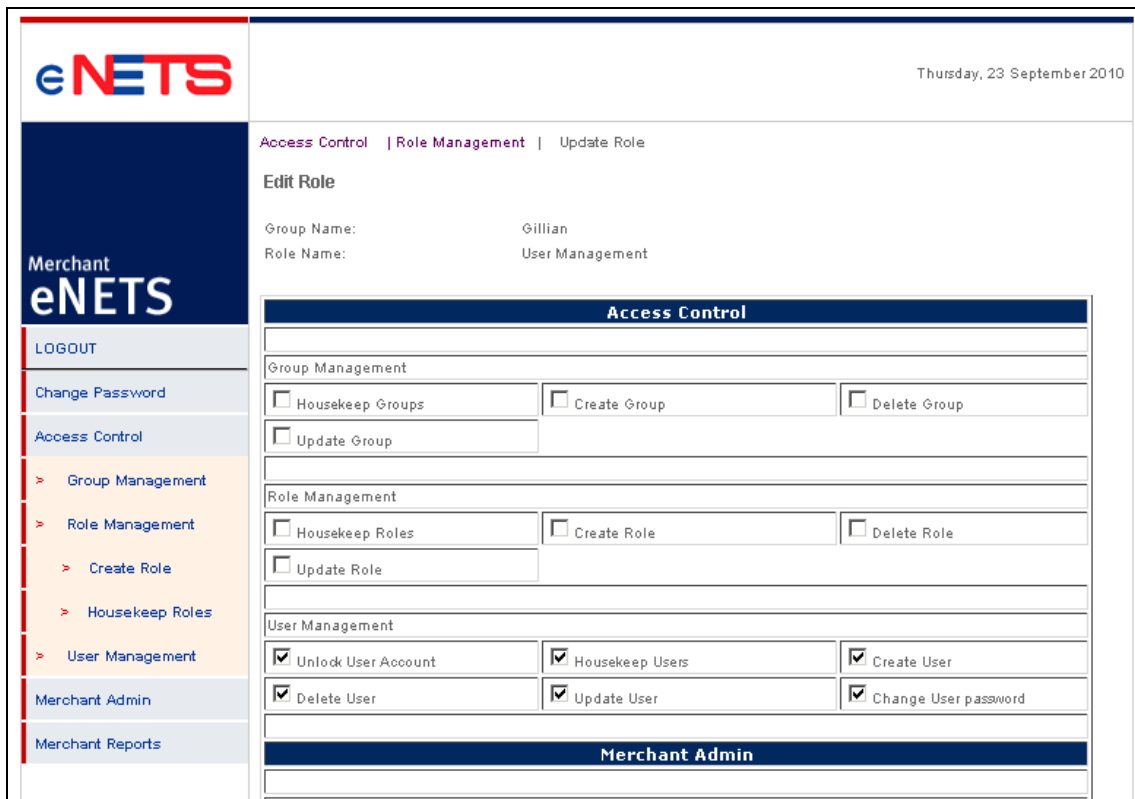



Figure 2.7.1 – Editing a Role

- To add a new function against this Role, check against the box (as illustrated in **Figure 2.4**).
- Similarly, to remove a particular function against the Role, click on the "checked box". You should notice that the "check" against the box would

disappear. This would indicate that the function is no longer available against this Role.

2.2.2.2 Deleting an existing Role

- From **Figure 2.7**, click on the  icon under the “Delete” column of the corresponding Role.
- You will see a pop-up box, asking for your confirmation (**Figure 2.8**).
- When a Role is deleted, this means that any Users who were tied to this Role, will NO longer be able to perform the functions. For example if User1, User2, User3 are all tied to the Role “Finance” (which has the functions of View Invoices and Transaction Reports), and “Finance” is deleted, all of these three users will NOT be able to view Invoices and Transaction Reports.
- **Once a Role is deleted, the system will not be able to “roll-back” the settings.**

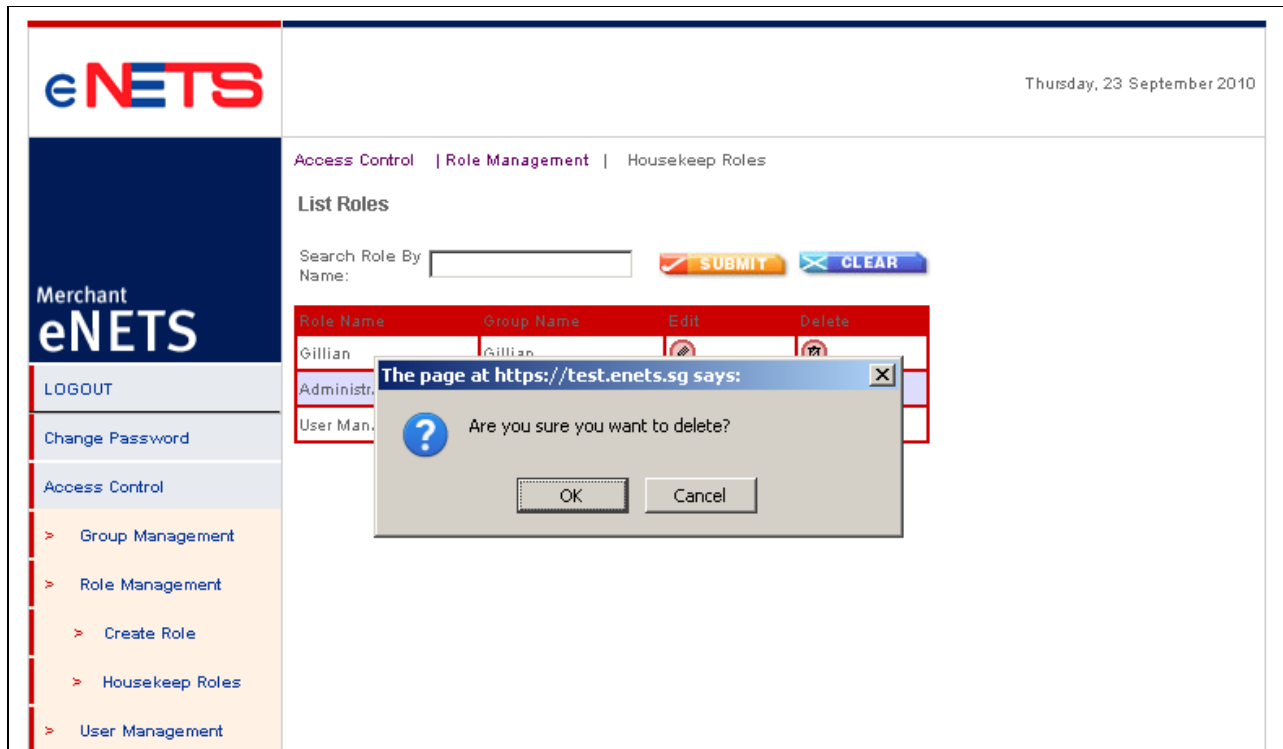


Figure 2.8 – Deleting a Role

2.3 User Management

2.3.1 Create User

After the SA has created the Role, specific users can be assigned to the Roles created.

To create a User (against a Role):

- After login, access this functional page, as shown in **Figure 2.9**, via the navigation menu in the following order:

Access Control > User Management > Create User

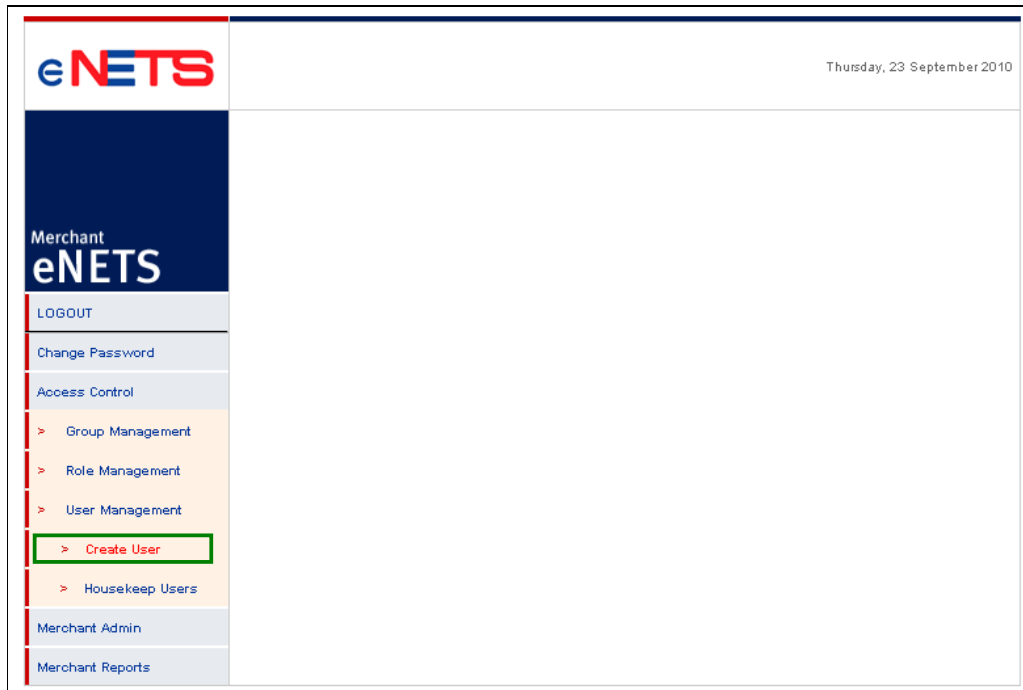


Figure 2.9 - Navigation menu with option to Create User

- To set-up a User account (**Figure 2.10**), the SA must provide the following information:
 - i) Name of User,
 - ii) Email Address,
 - iii) User Login ID,
 - iv) Password. Rules for setting the password:
 - 6 – 20 characters in length.**
 - Must be alphanumeric i.e. combination of numbers and alphabets.**
 - Cannot be the same as the Login ID.**

- Once the User account has been set-up, the SA may email the Login ID and Password to the relevant User. SA should advise the user that upon the first login, the user will be prompted by the system to change the password.

The screenshot shows the 'Create User' form in the eNETS system. The form is titled 'Create User' and is located under the 'User Management' section. The form includes the following fields and options:

- Group Name: Gillian (dropdown menu)
- Choose Role: Gillian (dropdown menu)
- Enter User Name: Andrew Tan
- Enter email: adrevtan@yahoo.com.sg
- Enter Login ID: andrewitan
- Enter Password: (masked with asterisks)
- Re-type Password: (masked with asterisks)

There are two buttons at the bottom of the form: a red 'SUBMIT' button and a blue 'CLEAR' button. A callout box with a black border and white background points to the 'Choose Role' dropdown menu. The text inside the callout box reads: 'Enter the information of the User. Once the set-up is completed, the SA is required to email or inform the User of the assigned Login ID and Password.'

The left sidebar of the page contains the following navigation options:

- LOGOUT
- Change Password
- Access Control
 - > Group Management
 - > Role Management
 - > User Management
 - > Housekeep Users
 - > Create User

Figure 2.10 - Create a new User

2.3.2 List Users

This function will give the SA a holistic view of the various Users in the organization, and the functions assigned against each role. It is advisable that the SA reviews the list of Users accessing the system at least once a year. This will help the SA housekeep the list of Users who should have the rights to access the system.

To view the list of Users that is currently able to access the system

- After login, access this functional page, as shown in **Figure 2.11**, via the navigation menu in the following order:

[Access Control](#) > [User Management](#) > [Housekeep Users](#)

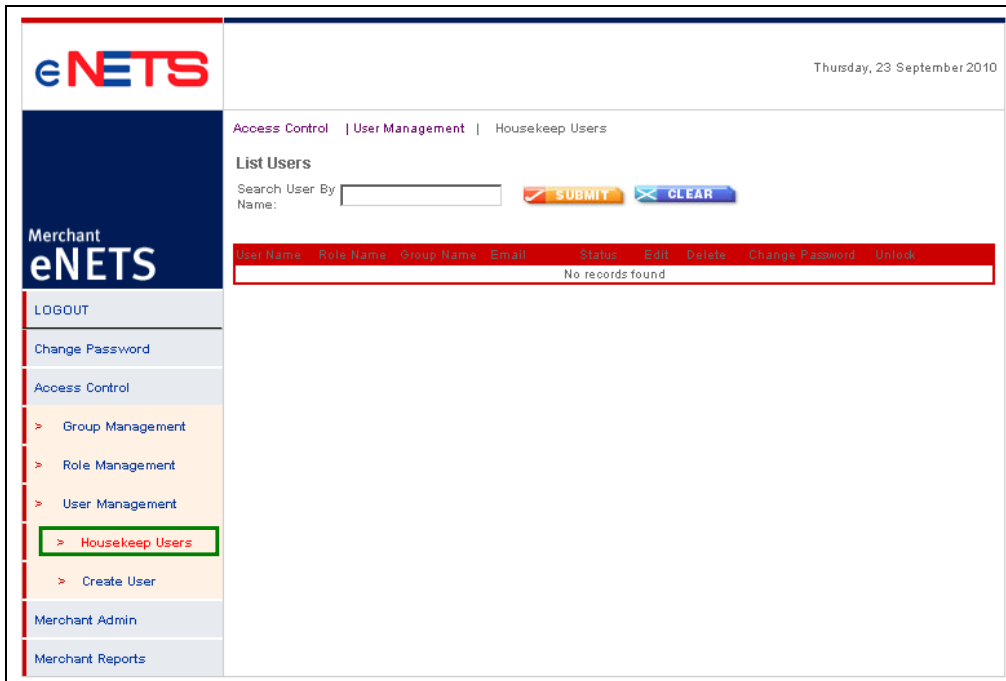


Figure 2.11 - Navigation menu to view list of Users

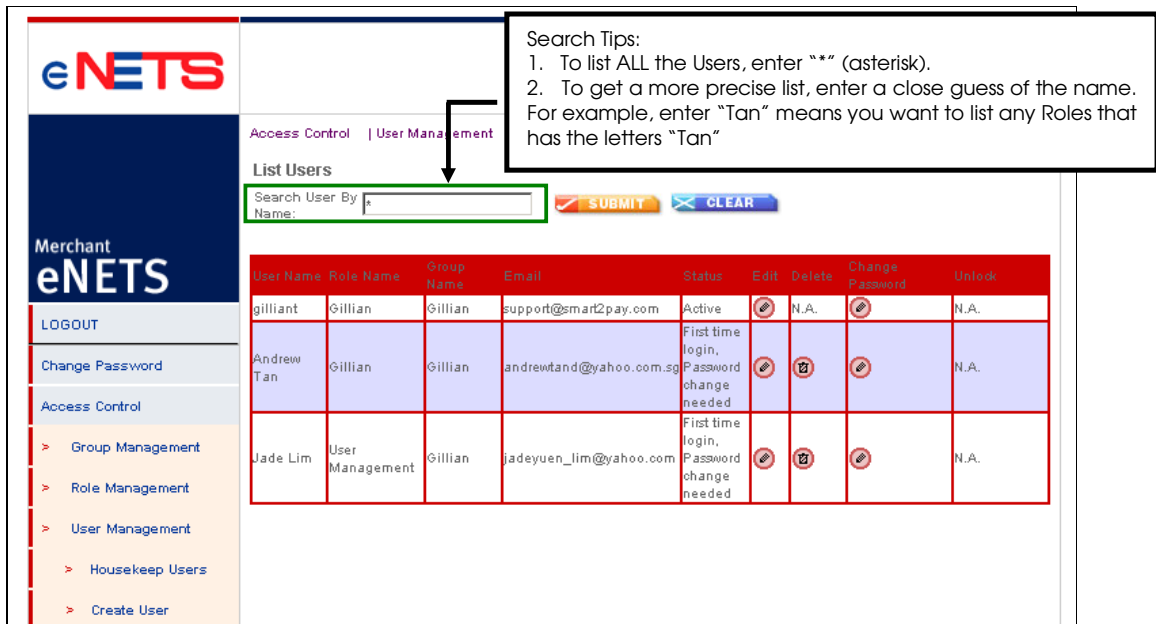



Figure 2.12 - List of Users to the system currently

- From the results page (**Figure 2.12**), the status of the User accounts are indicated. The possible status are:
 - Active: Accounts that are able to access the eNETS Administration and Report System.
 - First time login, Password change needed: These accounts reflect those where the user has yet to login, and upon first login, they will be prompted to change their password. It also indicates the status for users whose password has been reset, but have yet to login to change.
- The other tasks that the SA is able to perform against each User account here includes:
 - i) Editing of the User's account
 - ii) Deleting the User's account from further use of the system.
 - iii) Changing of Password.
 - iv) Unlocking of the User's account

2.3.2.1 Editing of a User's account

- From the results page (**Figure 2.12**), click on the  icon under the "Edit" column of the corresponding User's account.
- At the following page (**Figure 2.13**), only two set of information can be edited:
 - Name of the User
 - Email Address.
- Information such as the Login ID cannot be amended.

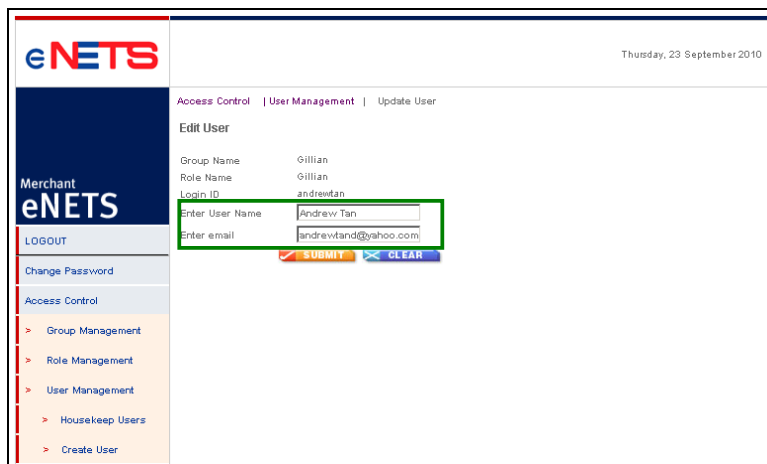




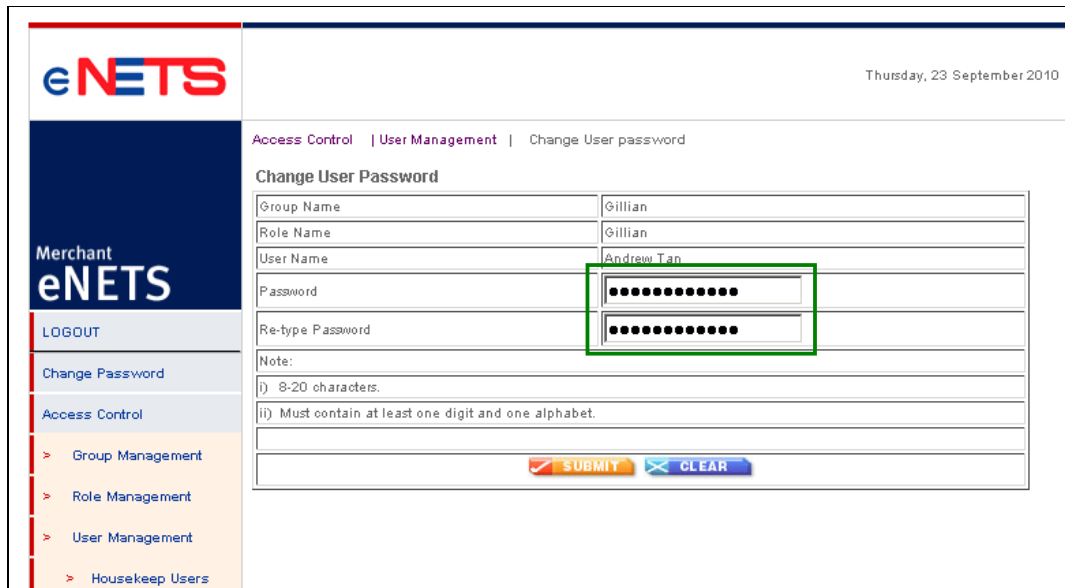
Figure 2.13 - Edit User's information

2.3.2.2 Delete a User's account

- From the results page (**Figure 2.12**), click on the  icon under the "Delete" column of the corresponding User's account.
- You will see a pop-up box, asking for your confirmation on the deletion of the User's account.
- When an account is deleted, this means that the selected user will NO longer be able to perform the functions.
- **Once a User account is deleted, the system will not be able to "roll-back" the settings.**

2.3.2.3 Change Password for a User's account

- From the results page (**Figure 2.12**), click on the  icon under the "Change Password" column of the corresponding User's account.
- In the following screen (**Figure 2.14**), you will be required to enter the new password of the User.
- **Important password rules to note:**
 - i) **6 – 20 characters in length.**
 - ii) **Must be alphanumeric i.e. combination of numbers and alphabets.**
 - iii) **Cannot be the same as the Login ID.**



Thursday, 23 September 2010

Access Control | User Management | Change User password

Change User Password

Group Name	Gillian
Role Name	Gillian
User Name	Andrew Tan
Password
Re-type Password

Note:


- i) 8-20 characters.
- ii) Must contain at least one digit and one alphabet.

Figure 2.14 - Change User Password

2.3.2.4 Unlocking of a User's account

A User's account will be locked if there was **three consecutive failed logins**. In such a case, the User may request for the SA to assist in "unlocking" the account. In most cases, users are unable to login due to the fact that they may have forgotten their password. In this case, after unlocking, the SA may select to change the password of the affected account. The steps for changing password for the user are covered in Section 2.2.2.3.

To unlock a user's account,

- From the results page (**Figure 2.12**), click on the  icon under the "Unlock" column of the corresponding User's account.
- Once the account has been unlocked, the confirmation page shown in **Figure 2.15** is displayed.

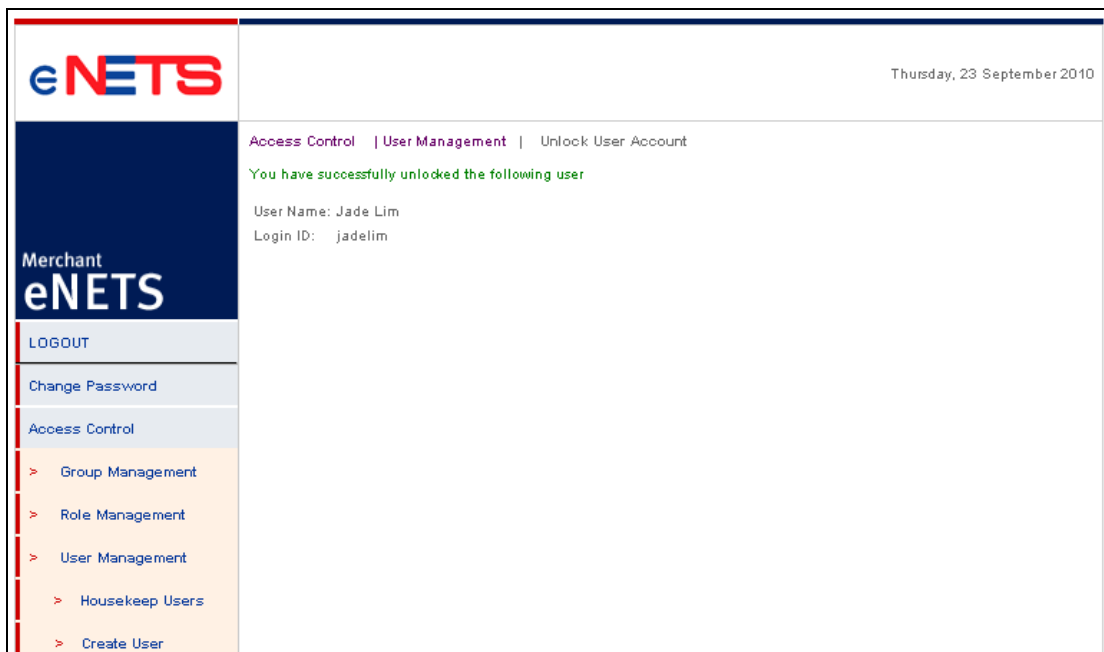


Figure 2.15 – Confirmation page after unlocking a user account

3 Getting Around

3.1 URL

The eNETS Administration and Report System is accessible from:

<https://admin.enets.sg>

3.2 What's needed for login

To access any of the functions in the system, a User must have:

- Login ID
- Password

The Login ID and Password may be obtained from your company's System Administrator (SA). Please note the Login ID and Password are both case sensitive.

If you are unable to recall your Password, please inform your SA who will be able to reset your password.

In the event that you enter your Password incorrectly, you will be locked out from the system automatically after **three consecutive failed attempts**. In this case, please request for your company's SA to reset your account.

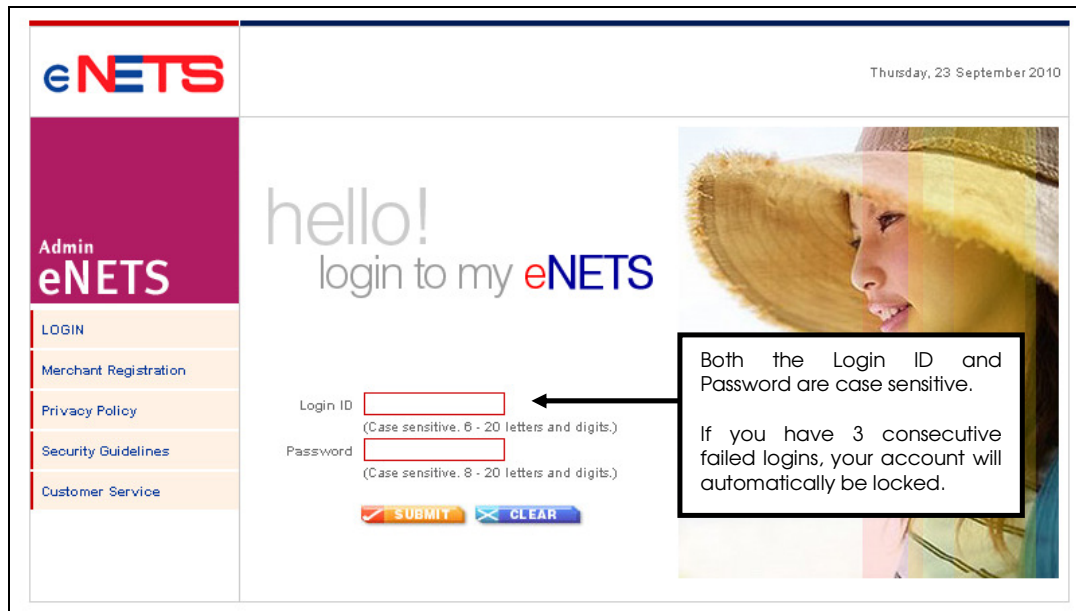


Figure 3.1 – Login Page to eNETS Administration & Report portal

3.3 Login For the First time

When you login for the first time, you will be required to change your password (**Figure 3.2**). After you have changed your password, you will be required to login again, this time, using the password that you have specified.

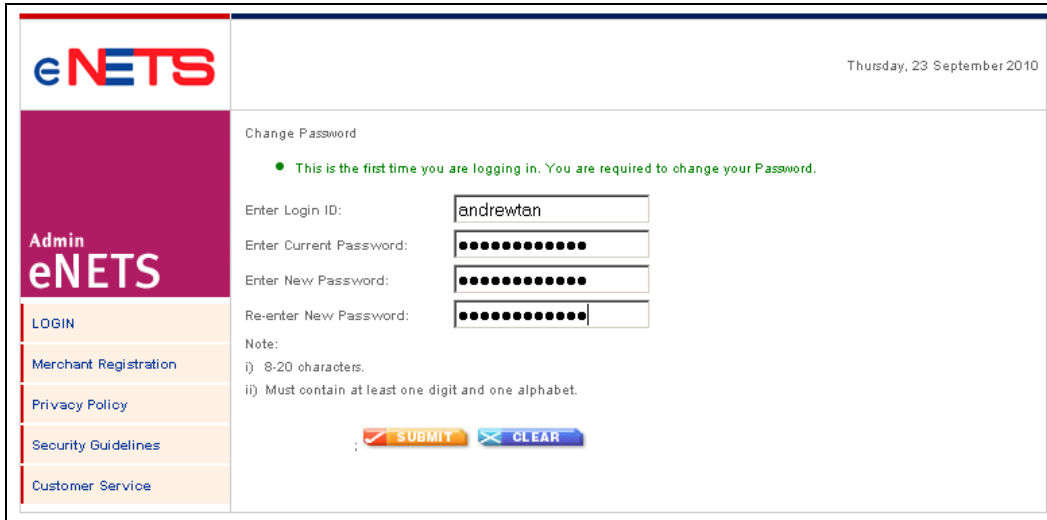


Figure 3.2 – Change password after first login

3.4 Navigation after login

The navigational menu is located on the left-hand side of the page.

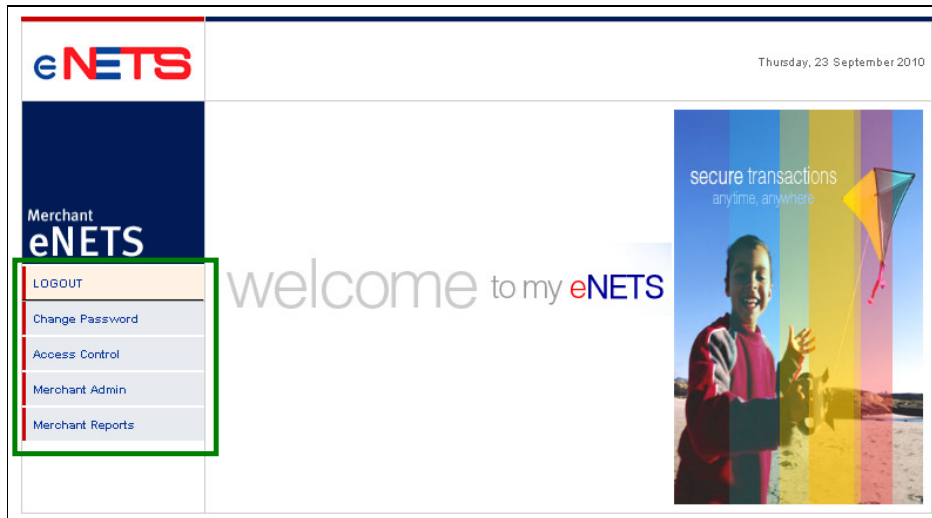


Figure 3.3 – Functions assigned to each user is displayed on the left

Each user may see a different set of options on the left menu. This is due to the functions assigned to each user.

3.5 Changing Password

Users can voluntarily change their password by accessing the “Change Password” option (**Figure 3.4**) on the left of the navigation menu. Also, they may be forced to change password upon login under the following conditions:

- Password is not changed for a configurable of time (e.g. default after 90 days)
- Login for the first time

Some rules to the password that can be used:

- 6 – 20 characters in length.
- Must be alphanumeric i.e. combination of numbers and alphabets.
- Cannot be the same as the Login ID.

The screenshot shows the eNETS user interface for changing a password. On the left is a navigation menu with the eNETS logo and 'Merchant eNETS' text. The menu items are LOGOUT, Change Password (highlighted), Access Control, Merchant Admin, and Merchant Reports. The main content area is titled 'Change Password' and includes three password input fields: 'Enter Current Password:', 'Enter New Password:', and 'Re-enter New Password:'. Below these fields are 'Password Guidelines' with three rules: i) 8-20 characters, ii) Must contain at least one digit and alphabet, and iii) Must NOT be the same as your LoginID. At the bottom of the form are two buttons: 'SUBMIT' and 'CLEAR'. The date 'Thursday, 23 September 2010' is shown in the top right corner.

Figure 3.4 – Subsequent Change password

4 Specific Functions

4.1 Merchant Profile Management

4.1.1 Update Profile

This function allows you to update your company's information including the salient contact people or mailing address. To update your company's information, the navigation menu is as follows:

[Merchant Admin > Merchant Profile > Update Profile](#)

4.1.2 View Profile

This function allows you to view the details of your company's profile. To view the company's profile, access this functional page, the navigation menu is as follows:

[Merchant Admin > Merchant Profile > View Profile](#)

4.2 Public Key Management

4.2.1 Request Public Key Upload

All transactions made between your webstore and eNETS system are digitally signed with a digital certificate. Any payment request originating from your webstore will be signed using the private key accepted to the eNETS system. When the payment request is received at eNETS system, it will be verified with the public key that you have uploaded with the eNETS system. It is recommended that this function is assigned to a person with technical background.

This function allows you to upload the public key that is used to sign your transaction.

- Before you can upload a public key, you would have to submit a request. To request for a public key upload, the navigation menu is as follows:

[Merchant Admin > Public Key Upload > Request Public Key Upload](#)

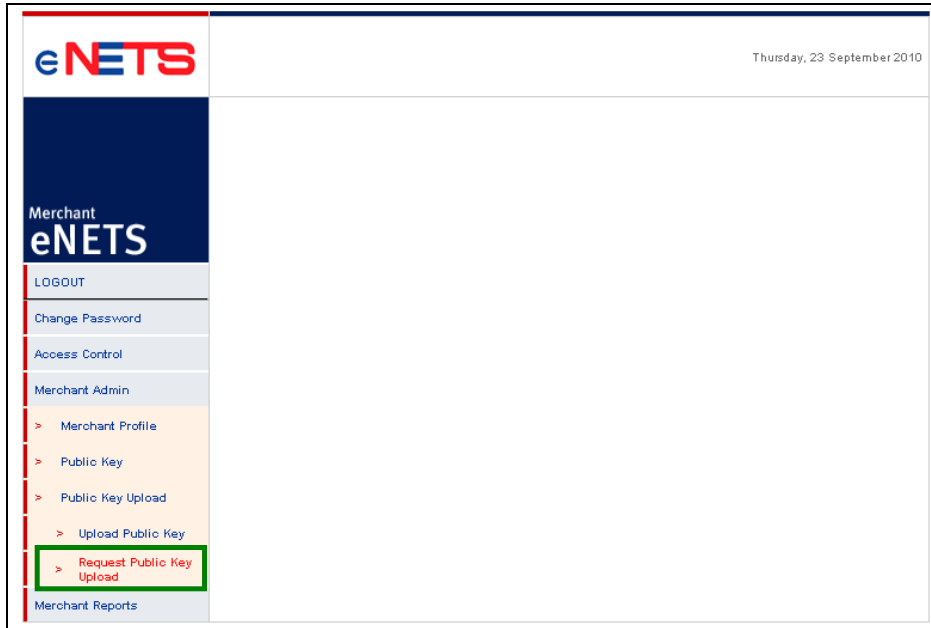


Figure 4.1 - Navigation menu with Request Public Key Upload highlighted

- In the page that follows, click on the “Submit” button to trigger an email containing the password to be sent to the specified company’s email address (this is set to the Main Contact’s email address). Refer to **Figure 4.2** for an illustration.

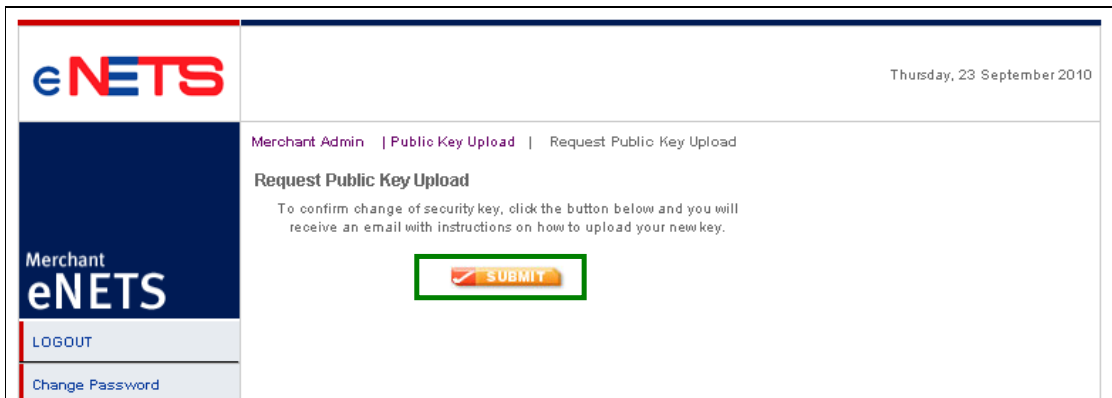


Figure 4.2 - Request for Public Key Upload

- Another page will be shown with the successful message as in **Figure 4.2**.

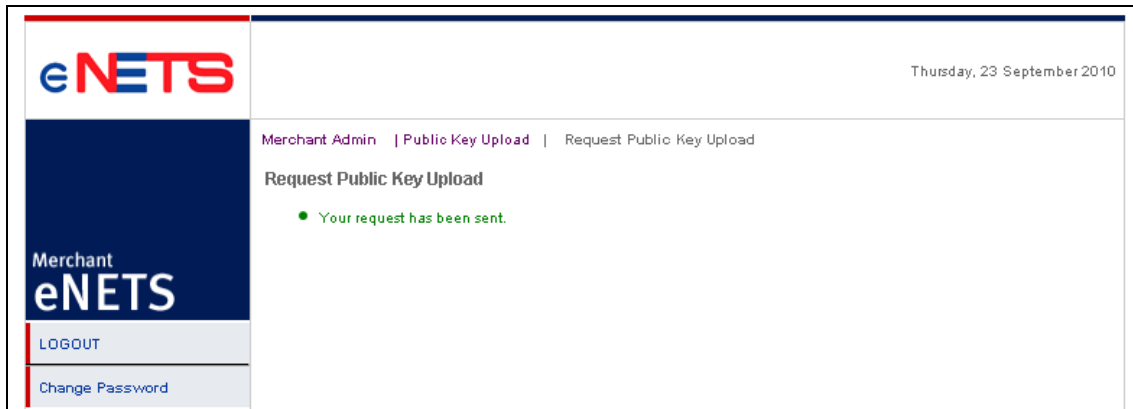


Figure 4.3 - Successful request for Public Key Upload

4.2.2 Upload Public Key

After you have requested to upload the public key (as depicted in Section 4.2.1), you are ready to upload your public key.

- To do this, access the functional page via the navigation menu in the following order:
Merchant Admin > Public Key Upload > Upload Public Key
- In this page as shown in **Figure 4.4**, enter the password that was received in the email and click on "Submit" button.

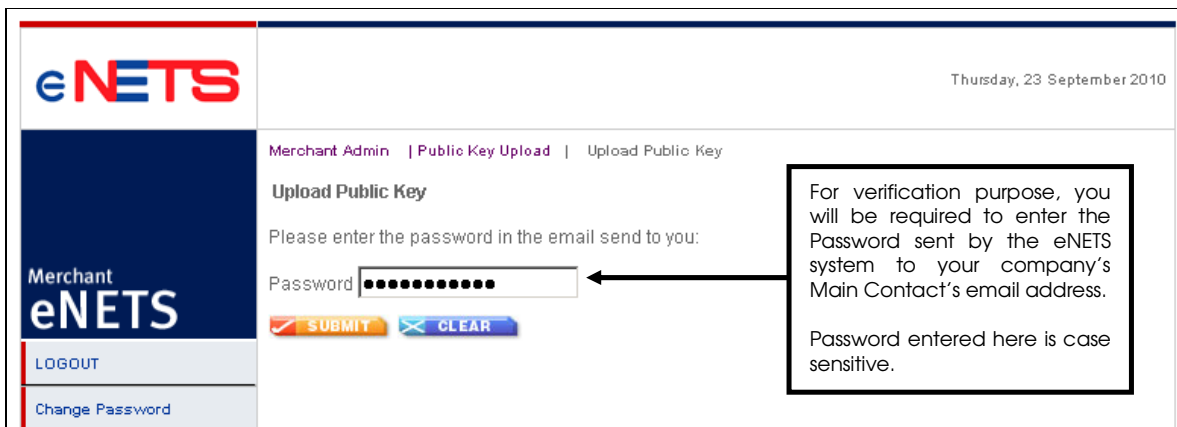


Figure 4.4 - Enter the received password to verify that you have sent a request to upload the certificate

- In the following page (**Figure 4.5**) you will be required to specify the path of your public key. Use the "Browse" function to search for the location of your key.

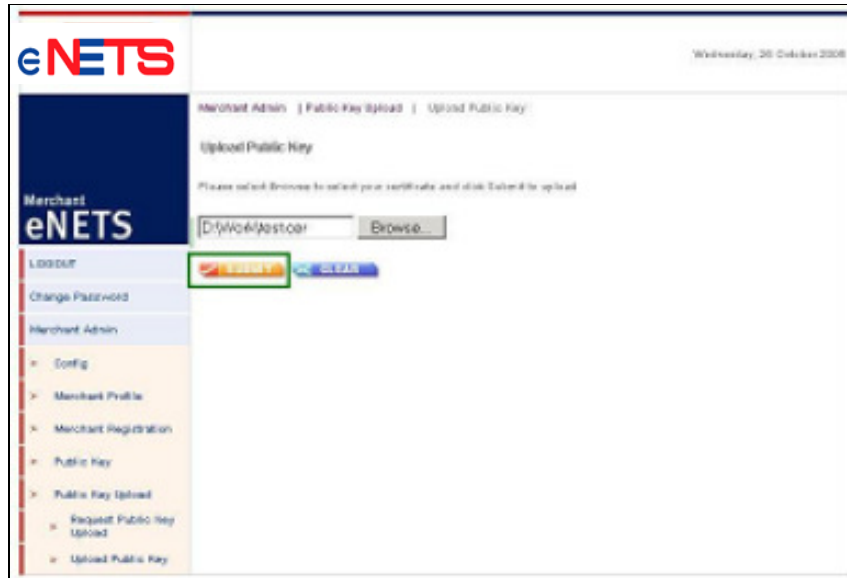


Figure 4.5 - Specify the location of the key for upload

4.2.3 View Public Key

After uploading a key, you are able to view the keys by accessing this function.

- Access this functional page via the navigation menu in the following order:

[Merchant Admin](#) > [Public Key](#) > [View Public Key](#)

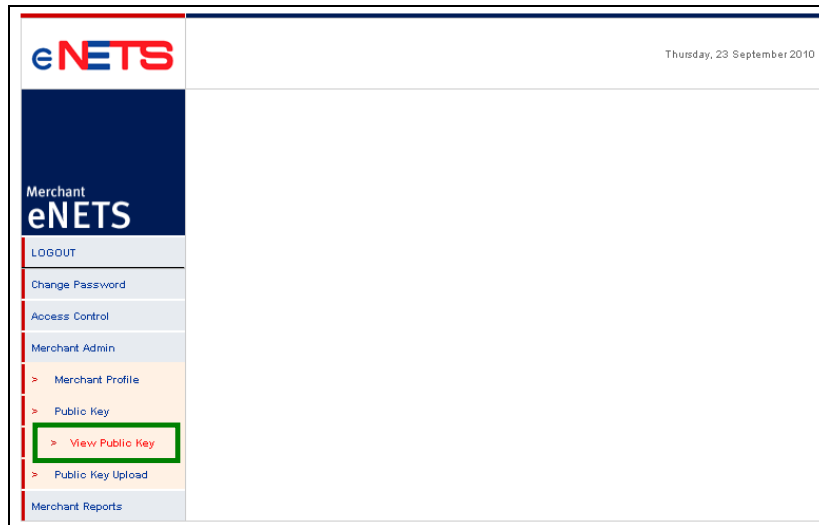
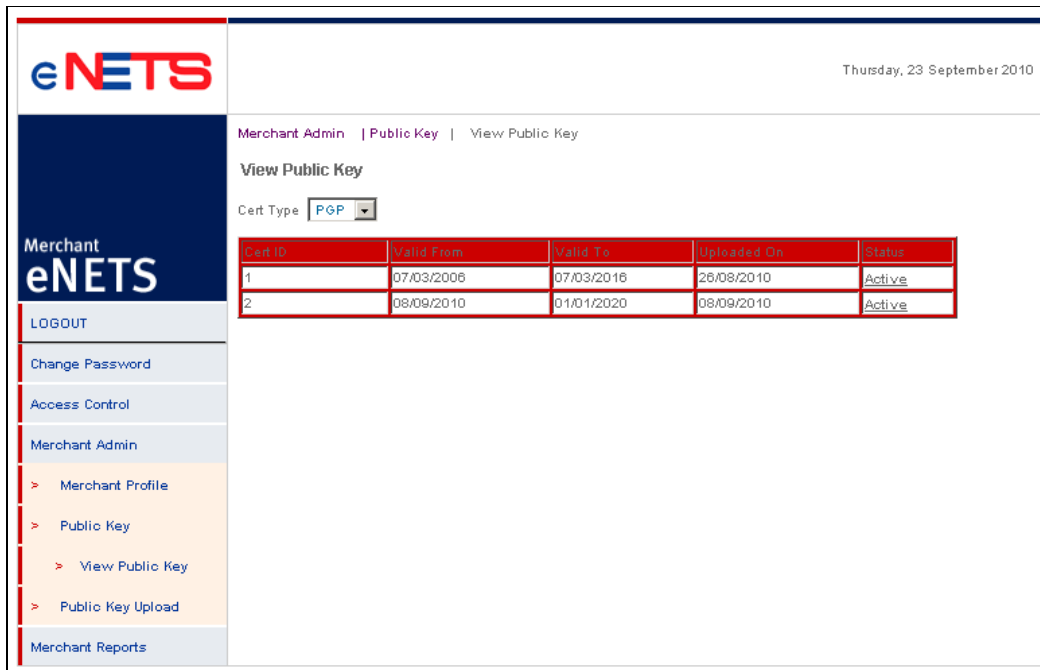


Figure 4.5 - Menu option to view the public key

- The page that follows will display the public key uploaded by your company. In addition, it also gives the validity period of the keys.



Thursday, 23 September 2010

Merchant Admin | Public Key | View Public Key

View Public Key

Cert Type:

Cert ID	Valid From	Valid To	Uploaded On	Status
1	07/03/2006	07/03/2016	26/08/2010	Active
2	08/09/2010	01/01/2020	08/09/2010	Active

Merchant eNETS

LOGOUT

Change Password

Access Control

Merchant Admin

- > Merchant Profile
- > Public Key
 - > View Public Key
 - > Public Key Upload
- Merchant Reports

Figure 4.6 – Information on public key uploaded by your company

4.3 Transaction Management (valid ONLY for Credit Card transactions)

This function allows you to have greater control on the credit cards that you want to allow at your webstore. You can set up a list of:

- Blacklisted credit card: This means that if a credit card number used at your website matches the blacklisted card number set-up at under your account, the card cannot be used for purchasing.
- Whitelisted credit card: This means that you want to accept ONLY a specific set of cards.

4.3.1 Setup of Blacklist Credit Cards

- To set-up credit cards to be blacklisted from your webstore, access the function via the following navigation:

[Merchant Admin > Transaction Management > Setup Merchant Blacklist](#)

- You can add specific card numbers to be blacklisted, or prefixes of cards.
- To do so, enter the first 6 digits of the credit card number.

4.3.2 Setup of Whitelist Credit Cards

- To set-up credit cards to be whitelisted at your webstore, access the function via the following navigation:
[*Merchant Admin > Transaction Management > Setup Merchant Whitelist*](#)
- You can add specific card numbers to be whitelisted.
- To do so, enter the first 6 digits of the credit card number.

5 Virtual Terminal Transactions

5.1 Credit Card Sale Transaction

This facility allows you to perform a credit card sale transaction.

- To perform a credit card Sale transaction, from **Figure 5.1**, navigate as follows:
[Merchant Transaction](#) > [Sales/Authorization](#) > [Perform Sales/Authorization](#)

The screenshot shows the eNETS Merchant Virtual Terminal interface. The top left features the eNETS logo and a navigation menu with options like LOGOUT, Change Password, Access Control, Merchant Admin, Merchant Reports, and Merchant Transaction. The 'Merchant Transaction' section is expanded to show 'Perform Sales/Authorization' highlighted with a green box. The main content area displays the 'Merchant Virtual Terminal' page with the following fields and controls:

- Merchant ID:** 947773000
- Merchant Name:** TEST: Elva
- Merchant Transaction Ref:**
- Currency:** SGD (dropdown menu)
- Amount:** (up to 2 decimal places, e.g. 12.34)
- Transaction Type:**
- Card Number:** (Note: Please note that the Credit Card Number should be 13 or 16 digits. Please input your card number without space or dash.)
- Expiry Date:** Month: Jan (dropdown), Year: 2005 (dropdown)
- Name on card:**
- CVV / CVC2:** (What is CVV/CVC2)

At the bottom of the form are two buttons: a red 'SUBMIT' button and a blue 'CLEAR' button.

Figure 5.1 – Virtual terminal option to perform credit card Sales/Authorization

- To process the Sales, enter all information needed for sale transaction as in **Figure 5.2**.

Thursday, 23 September 2010

Merchant Transaction | Sales/Authorization | Perform Sales/Authorization

Merchant Virtual Terminal

Merchant ID: 947773000

Merchant Name: TEST: Elva

Merchant Transaction Ref: 1234567

Currency: SGD

Amount: 100.50
(up to 2 decimal places, e.g.12.34)

Transaction Type: SALE

Card Number: 4551234567890000
Please note that the Credit Card Numbers should be 13 or 16 digits. Please input your card number without space or dash.

Expiry Date: Month: Jan Year: 2016

Name on card: Andrew Tan

CVV / CVC2: 335
(What is CYY/CYY2)

[SUBMIT] [CLEAR]

The Merchant Transaction Reference Number **MUST** be unique.

Ensure that if you are performing a sale, the option under "Transaction Type" **MUST** be set to "SALE".

For better fraud management, CVV/CVC2 may be required. These are the additional 3-4 digits found on the back of the credit card, beside the signature line

Figure 5.2 – Sales transaction page

- Following a submission, the eNETS system will reply with the status of the transaction. **Figure 5.3** gives an example of a successful sales transaction.

Merchant Virtual Terminal

MID: 957374010

Merchant Txn Ref: 123

NETS Txn Ref: 20100324175241870

NETS Txn Time: 20100324 17:52:41.000

NETS Txn Msg: Approval

NETS Amt Deducted: 1.00

Bank Auth ID: 005053

Figure 5.3 – Successful transaction confirmation from eNETS system

5.2 Credit Card Authorization Transaction

The difference between an “Authorization” and “Sale” is that in the former, the funds are earmarked from the cardholder’s credit limit, but at the end of the day, such transactions are not sent for settlement i.e. authorization does NOT lead to actual billing to the cardholder. Sectors that use the “authorization” function widely are hotels, car rentals.

- To perform an authorization, from **Figure 5.1**, navigate as follows:
Merchant Transaction > Sales/Authorization > Perform Sales/Authorization
- Enter all information needed for the authorization as in **Figure 5.4**

The screenshot shows the eNETS Merchant Transaction page. The left sidebar contains navigation links: LOGOUT, Change Password, Access Control, Merchant Admin, Merchant Reports, Merchant Transaction, Capture, Refund, Sales/Authorization, and Perform Sales/Authorization. The main content area displays the following information:

- Merchant Virtual Terminal
- Merchant ID: 947773000
- Merchant Name: TEST: Elva
- Merchant Transaction Ref: 3242342342
- Currency: SGD
- Amount: 1.00 (up to 2 decimal places, e.g.12.34)
- Transaction Type: AUTH
- Card Number: 455699009991111
- Expiry Date: Month Mar, Year 2018
- Name on card: Andrew Tan
- CVV / CVC2: 3344
- Distra Payment Listener: Distra SIT, Distra UAT

Buttons for SUBMIT and CLEAR are at the bottom. A callout box on the right states: "The Merchant Transaction Reference Number **MUST** be unique. Ensure that if you are performing an authorization, the option under "Transaction Type" **MUST** be set to "AUTH". For better fraud management, CVV/CVC2 may be required. These are the additional 3-4 digits found on the back of the credit card."

Figure 5.4 – Authorization Transaction Page

- Following a submission, the eNETS system will reply with the status of the transaction. **Figure 5.3** gives an example of a successful authorization transaction.
- Please refer to Section 6.2 on how to retrieve reports on “Authorized Credit Card Transactions”.

5.3 Credit Card Capture Transaction

This facility allows you to perform capture of a credit card authorization transaction previously performed. By executing a capture, the transaction will be sent to the bank for settlement at the end of the day, and the cardholder will be billed accordingly for the transaction.

- To perform an authorization, from **Figure 5.5**, navigate as follows:

Merchant Transaction > Capture > Perform Capture

The screenshot displays the eNETS Merchant interface. On the left is a navigation sidebar with the eNETS logo and 'Merchant eNETS' text. The sidebar menu includes: LOGOUT, Change Password, Access Control, Merchant Admin, Merchant Reports, Merchant Transaction, > Capture, and > Perform Capture (highlighted with a green box). The main content area has a breadcrumb trail: Merchant Transaction | Capture | Perform Capture. Below this is a 'Capture' section with the following fields: Transaction Period (two date pickers), Merchant ID (957374002), and Currency (SGD). An 'Advanced Options' section contains three checkboxes: Merchant Ref No, Approval Code, and Distracted Payment Listener (Distracted SIT). At the bottom of the form are two buttons: 'Retrieve Authorization Transaction Details' and 'Clear'.

Figure 5.5 – Menu option to perform a Capture

- Thereafter you can define the criteria in retrieving the relevant authorized transaction. You can retrieve by:
 - Specific transaction period
 - Merchant Reference Number
 - Approval Code

Figure 5.6 gives an example, where the search is done by using a specified transaction period. Click on the “Retrieve Authorization Transaction Details” button to display the information.

Figure 5.6 – Define criteria to retrieve list of authorized transactions

Txn Date (dd/mm/yyyy)	Txn Time (hh:mm:ss)	Merchant ID	Merchant Name	Merchant Ref No.	Txn Type	Approval Code	Amount (\$)	Authorized By	Txn Status	System Response of Capture	Full Capture
10/03/2010	15:17:00	957374002	UOB DISTRA BC-VT	20100310018	AUTH	T20045	1.00	distran00114	To be captured	-	<input type="checkbox"/>

Figure 5.7 – Result list of authorization transactions retrieved

- Thereafter you can perform a capture. The system allows you perform a full or partial capture. You can also submit multiple captures.

5.3.1 Multiple-full Captures

- **Figure 5.8** shows an example of multiple-full captures performed. To do this, check on the box under "Full Capture" against the relevant authorized transactions.

Thursday, 05 January 2006

Capture

Transaction Period: 01/01/2006 To 06/01/2006

Merchant ID: OT_M1

Currency: USD

Advanced Options

Merchant Ref No

Approval Code

Retrieve Authorization Transaction Details Clear

Goto Page 1

Tin Date (dd/mm/yyyy)	Tin Time (hh:mm:ss)	Merchant ID	Merchant Name	Merchant Ref No.	Tin Type	Approval Code	Amount (\$)	Authorized By	Tin Status	System Response of Capture	Full Capture
05/01/2006	20:34:47	OT_M1	OneTouch Test Merchant	ref005	AUTH	666999	200.00	-	To be captured		<input type="checkbox"/>
05/01/2006	20:32:32	OT_M1	OneTouch Test Merchant	ref005	AUTH	666999	100.00	-	To be captured		<input checked="" type="checkbox"/>
05/01/2006	20:28:32	OT_M1	OneTouch Test Merchant	ref206010500136	AUTH	666999	100.00	-	To be captured		<input checked="" type="checkbox"/>

Goto Page 1

Capture Selected

Figure 5.8 – Illustration of multiple-full capture transactions

- **Figure 5.9** shows the confirmation page returned by the eNETS system.
- After you have captured the transactions successfully, these transactions will be reflected in the "Credit Card Sales Report".



Figure 5.9 – Successful page for Multiple Capture

5.3.2 Partial Capture

- To perform a partial capture, click on the “Merchant Reference No.”.

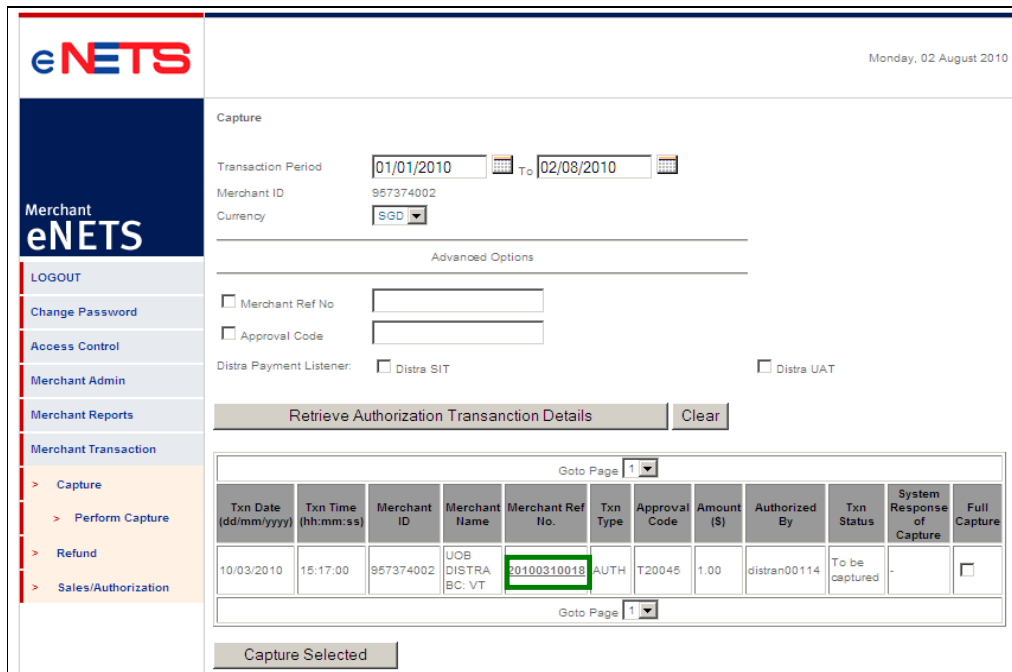


Figure 5.10 – Performing a single capture

The screenshot shows the eNETS interface for a 'Capture' operation. On the left is a navigation menu with 'Merchant eNETS' and options like 'LOGOUT', 'Change Password', 'Merchant Reports', and 'Merchant Transaction' (with sub-options for 'Capture', 'Perform Capture', 'Refund', and 'Sales/Authorization'). The main content area displays transaction information: Transaction ID (20000105203447100), Merchant Reference No. (ref008), Authorized Amount (SGD 200.00), and Capture Amount (SGD 100). There are 'Submit' and 'Clear' buttons. A callout box with an arrow pointing to the '100' in the capture amount field contains the following text:

Rules for partial capture:
 1. You can capture a lower amount, from the original authorized amount.
 2. You may perform only ONE partial capture.

Figure 5.11 – Single partial capture

- A new page will be displayed with a successful message saying that capture has been done successfully.

The screenshot shows the 'Result Page for Single Capture' in the eNETS interface. The left navigation menu is identical to Figure 5.11. The main content area displays the message: 'Capture Captures submitted successfully.'

Figure 5.12 – Result Page for Single Capture

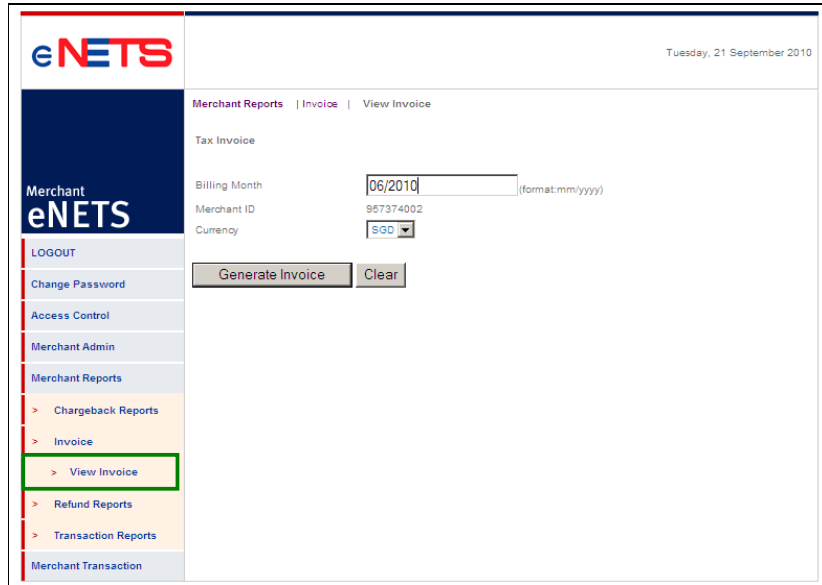


Figure 6.1 – Selection Criteria Page

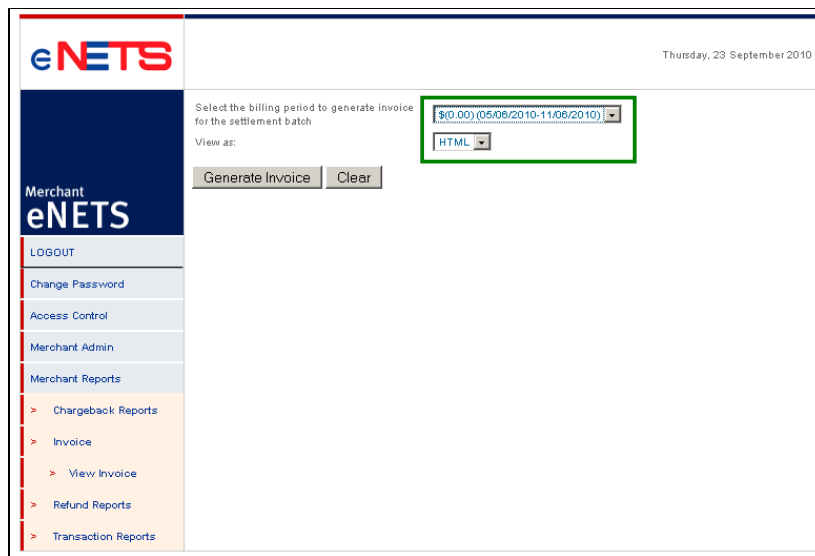


Figure 6.2 – Selection of type of Invoice

Tax Invoice						
Invoice Date:	12/06/2010					
Invoice No:	M-10082010-279					
Account No:	N01234					
Due Date of Invoice:	12/06/2010					
Merchant Name:	TEST: Ally					
Merchant ID:	947773009					
Address:	,Street 298 Tiong Bahru Road #04-01/06 Central Plaza					
Transaction Period:	05/06/2010-11/06/2010					
<u>Transaction Type</u>	<u>Txn Count</u>	<u>Txn Sales(\$)</u>	<u>Refund(\$)</u>	<u>Chargeback(\$)</u>	<u>Net Sales(\$)</u>	<u>Txn Fee(\$)</u>
Credit Service SGD	0	0.00	0.00	0.00	0.00	0.00
(a) Net Sales Value						\$(0.00)
Total Transaction Fee						\$0.00
Other Fees						\$0.00
Total Other Fees						\$0.00
Total Fees						\$0.00
GST @ 7.00%						\$0.00
(b) Total Fees (inclusive of GST)						\$0.00
(c) Outstanding Invoices						\$0.00

Overview of fees payable to eNETS for processing of transactions. Banks would settle with non-master merchant on a daily basis on sales proceeds.

Figure 6.3 – Invoice in HTML format (Section 1)

Adjustments					
(d) Total Adjustments					\$ (0.00)
<u>Movements in Collateral</u>					
	Parent Company Guarantee(\$)	Bank Guarantee(\$)	Cash Deposit(\$)	Funds Withheld(\$)	Total(\$)
(e) Balance B/F	0.00	0.00	0.00	0.00	0.00
Movements during current billing cycle	0.00	0.00	0.00	0.00	0.00
(f) Balance C/F	0.00	0.00	0.00	0.00	0.00
Computation of Collateral Required					
Last 6 months net sales					0.00
Applicable percentage					12,300.00%
Contingent Exposure					0.00
Pending Chargeback from Sales older than 6 months					0.00
Total Collaterals Required					0.00
Net amount payable : a+b+c+d+(f-e)					SGD\$0.00
Net amount payable:					SGD\$0.00
Billing Plan					
GST SGD equivalent = \$0.00					
Batch Number : null					
<p>This is computer-generated invoice. No signature is required. The above Net Amount Payable will be credited into your bank account four working days from the date of this invoice.</p>					

Figure 6.4 – Invoice in HTML format (Section 2)

7 Reports

The Report function provides you with the ability to generate reports of a specified period. The report can be viewed in 3 formats:

- i) HTML
- ii) PDF
- iii) CSV

7.1 Reports for ALL eNETS Payment Services

7.1.1 Transactions for All Payment Types

- This report gives you a list of transactions that have been “settled” by eNETS for a defined period.
- To view this report, navigate as follows:

[Merchant Reports](#) > [Transaction Reports](#) > [Settled Transactions for All Payment Types](#)

The screenshot shows the eNETS web interface for generating a report. The left sidebar contains a navigation menu with 'Settled Transactions For All Payment Types' highlighted. The main content area has the following fields:

- Transaction Period: 01/05/2010 To 31/08/2010
- Merchant ID: 947773009
- Currency: SGD
- View as: HTML

Below these fields are 'Advanced Options' with checkboxes for:

- Product
- Transaction Type
- Merchant Ref No
- Approval Code

Buttons for 'Generate Report' and 'Clear' are located below the filters. A callout box on the right states: "You have a set of filters to select from to streamline the results presented in a report. For example, you can select to view transaction in a specified period. Use the 'Advanced Option' to generate a more specific list of transactions. If you are using more than one payment service from eNETS, use the option 'Product' to search for transactions against a specific product (e.g. credit card, direct debit, virtual account)."

Figure 7.1 - Page to define criteria of report

Merchant - Transactions for All Payment Types Report

Report date: 03/01/2006

Transaction Period: 01/01/2006 to 30/12/2006 Product: Credit Card
 Merchant ID: TEST_A
 Merchant Name: MERCHANT A
 Currency: SGD

All the filter criteria defined in Figure 7.1 is repeated in this section of the report.

Trn Date (dd/mm/yyyy)	Trn Time	Merchant Refno.	EZProtect Score	Trn Type	Product	Approval Code	Transaction Amt (\$)	Transaction Fee (\$)	Settlement Date (dd/mm/yyyy)	User ID
03/01/2006	12:00	rv000	50.00	SALES	CREDIT CARD	-	5,000.00	50	03/01/2006	-

SALES SUMMARY	
Count	1
Value (\$)	0.00
Transaction Fee (\$)	50.00

REFUND SUMMARY	
Count	0
Value (\$)	0.00
Transaction Fee (\$)	0.00

NET SALES TOTAL	
Count	1
Value (\$)	0.00
Transaction Fee (\$)	50.00

List of transaction information will be displayed in this table. In this example, there is ONLY one record that met the filter criteria, and the transaction was settled by eNETS based on the date indicated in "Settled Date".

Summary table at the end of each report presents the total transaction count and value.

Figure 7.2 – Transactions for All Payment Types Report

7.1.2 Sales for All Payment Types

- This report gives you consolidated monthly sales of the current year.
- For example, if you viewed this report on 15-June, the report will give you the consolidated sales from January to May of the current year.
- To view this report, navigate as follows:

[Merchant Reports > Transaction Reports > Sales for All Payment Types](#)

Merchant - Sales for All Payment Types Report

View Sale Up to: 08/2005
(format: MM/YYYY)

Merchant ID: CC_M_V_05

Product: Credit Card

Currency: SGD

View as: HTML

Generate Report Clear

Merchant - Monthly Sales for All Payment Types

Report date: 03/01/2006

Merchant ID: TEST_A
Merchant Name: Merchant A
Month: 12 / 2005
Currency: SGD
Product: DD

Total (YTD)	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
1,000.00	1,000.00											

Figure 7.3 – Define criteria for the report

Merchant - Monthly Sales for All Payment Types

Report date: 03/01/2006

Merchant ID: TEST_A
Merchant Name: Merchant A
Month: 12 / 2005
Currency: SGD
Product: DD

Total (YTD)	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
1,000.00	1,000.00											

Figure 7.4 – Year to date Sales processed through eNETS payment services

7.2 Reports Specific to Credit Card Transactions

7.2.1 Credit Card Authorization Report

- This function allows you to process transactions with a credit cardholder's details. This report assumes that you have a function to allow the authorization of credit card details.
- To view the list of transactions that have been authorized, navigate as follows:

[Merchant Reports > Transaction Reports > Credit Card Authorization](#)

Figure 7.5 - Define criteria of the Authorization report

Important Note:
If a transaction has been captured i.e. no longer the status of "Authorized", it will NOT be reflected in this report. This report is ONLY for transactions that still carry the status of "Authorized".

Credit Card - Authorization Report

Report date: 03/01/2016

Transaction Period: 01/01/2016 to 30/12/2016 Credit Card Type: -

Merchant ID: TEST_A

Merchant Name: MERCHANT A

Trn Date (ddmm/yyyy)	Trn Time (hh:mm:ss)	Merchant Ref No.	ETProtect Score	Approval Code	Currency	Amount(\$)	UserID
03/01/2016	12:00	ref00	100	APP00	SGD	5000.00	-

Figure 7.6 – Credit Card Authorization Report

7.2.2 Transaction Report With Credit Card Numbers

- This report is akin to “Transactions for All Payment Types” report with the exception that this report is only reflects credit card transactions, and you can view the masked credit card number.
- To view this report, navigate as follows:
[Merchant Admins Reports > Transaction Reports > Transaction with Credit Card No.](#)

Figure 7.7 - Define criteria

Ten Date (Month/yy)	Ten Time (mm:ss)	Merchant Ref No.	Ten Type	Approval Code	Amount (\$)	Credit Card No.	EXP. DATE (yy/mm)	Batch ID
01/10/2005	00:00:00	ROBOT'S-1-2005001	SALES	121212	100.00	4512300000001212	07/12	0
01/10/2005	00:00:00	ROBOT'S-2-2005001	SALES	121212	100.00	4512300000001212	07/12	0

Figure 7.8 – Transaction Report with (masked) Credit Card Numbers

8 Quick Reference Guide

Question	Answer
1. Who should use the eNETS Report and Administration facility?	This facility is used by merchant personnel to monitor and manage their online processing and administration of payments
2. How do I access the eNETS Report and Administration facility?	i) You will need to access the URL: https://admin.enets.sg . ii) You will also need a Login ID and Password assigned by your company's System Administrator. iii) While the eNETS Report and Administration facility is compatible with all browsers, it is best viewed using Netscape 6+ and Internet Explorer 5+, with resolution set to 800x600 or above.
3. How can I create addition Login IDs to access eNETS Report and Administration?	You will need to be given "System Administration" rights to create new Login IDs. This is a privilege assigned by NETS. If you have been assigned this privilege, please refer to Section 2 for a systematic approach on managing the users' access within your company.
4. If I am the System Administrator, and I have been locked out of the system, how can I re-enable my account	Your account will be locked after three failed attempts to login in. To re-enable your account, please use the "eNETS Merchant Request Form". You may request for a copy of the form by sending your to: info@nets.com.sg .
5. I am not the System Administrator, but my account has been locked.	Please inform your organization System Administrator, who will be able to "unlock" your account.
6. Why do I have a different set of functionalities from my colleague?	All functions are assigned by the company's System Administrator, and this is assigned based on the roles that need to be undertaken by specific staff. Therefore, if you see a different set of functions, it is likely that your role is different from the other users within your company.