

Digital Receipt Management System (DRMS)

2FA Merchant User Guide

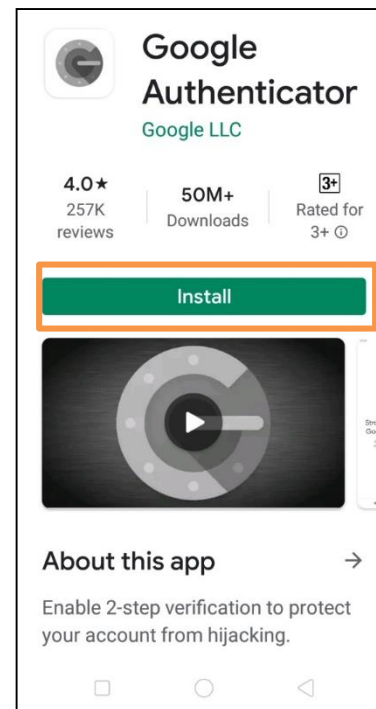
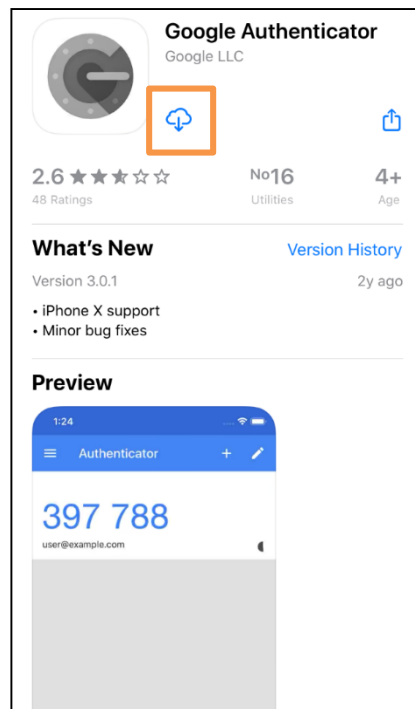
Use cases

- First-time validation on DRMS
- Subsequent access to DRMS
- Creating new user with 2FA
- Revoking 2FA for existing user
- Assigning 2FA to existing user

First time validation on DRMS

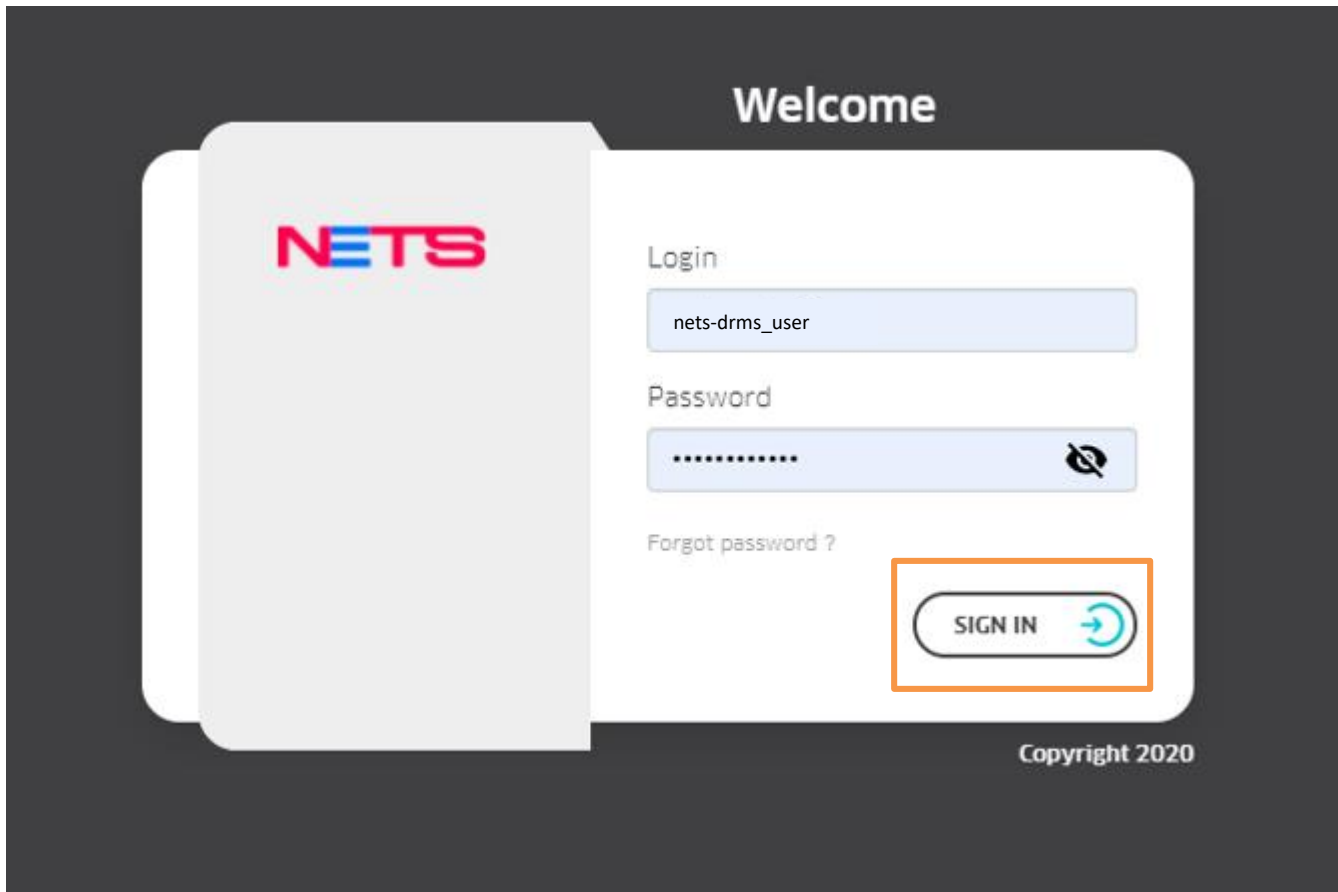
If you are logging into DRMS with 2FA for the first time, please follow the steps below.

Step 1: Download the Google Authenticator app from the Google Play Store or Apple App Store on your mobile phone



First time validation on DRMS

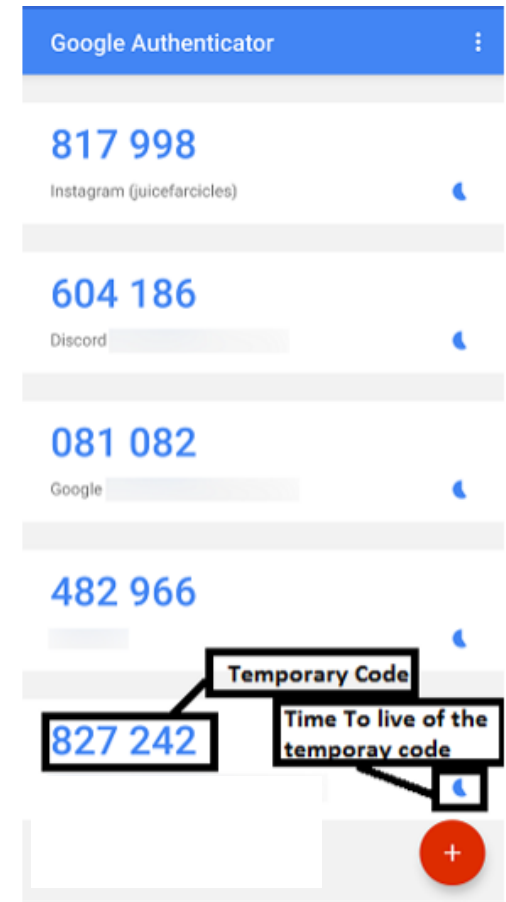
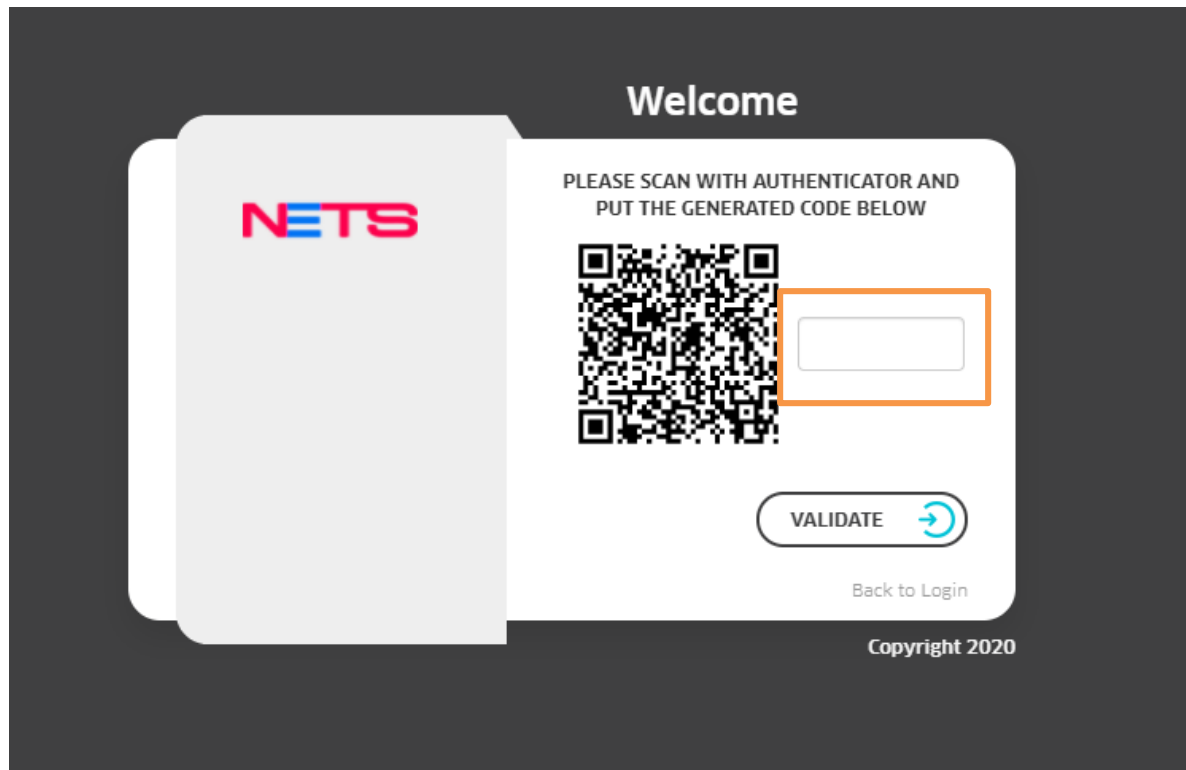
Step 2: Sign into DRMS using your login details



The screenshot displays a login interface for DRMS. On the left, there is a grey vertical bar with the 'NETS' logo in red and blue. The main content area is white and titled 'Welcome'. It contains a 'Login' field with the text 'nets-drms_user', a 'Password' field with masked characters and a visibility icon, and a 'Forgot password?' link. A 'SIGN IN' button with a circular arrow icon is highlighted with an orange border. The footer text reads 'Copyright 2020'.

First time validation on DRMS

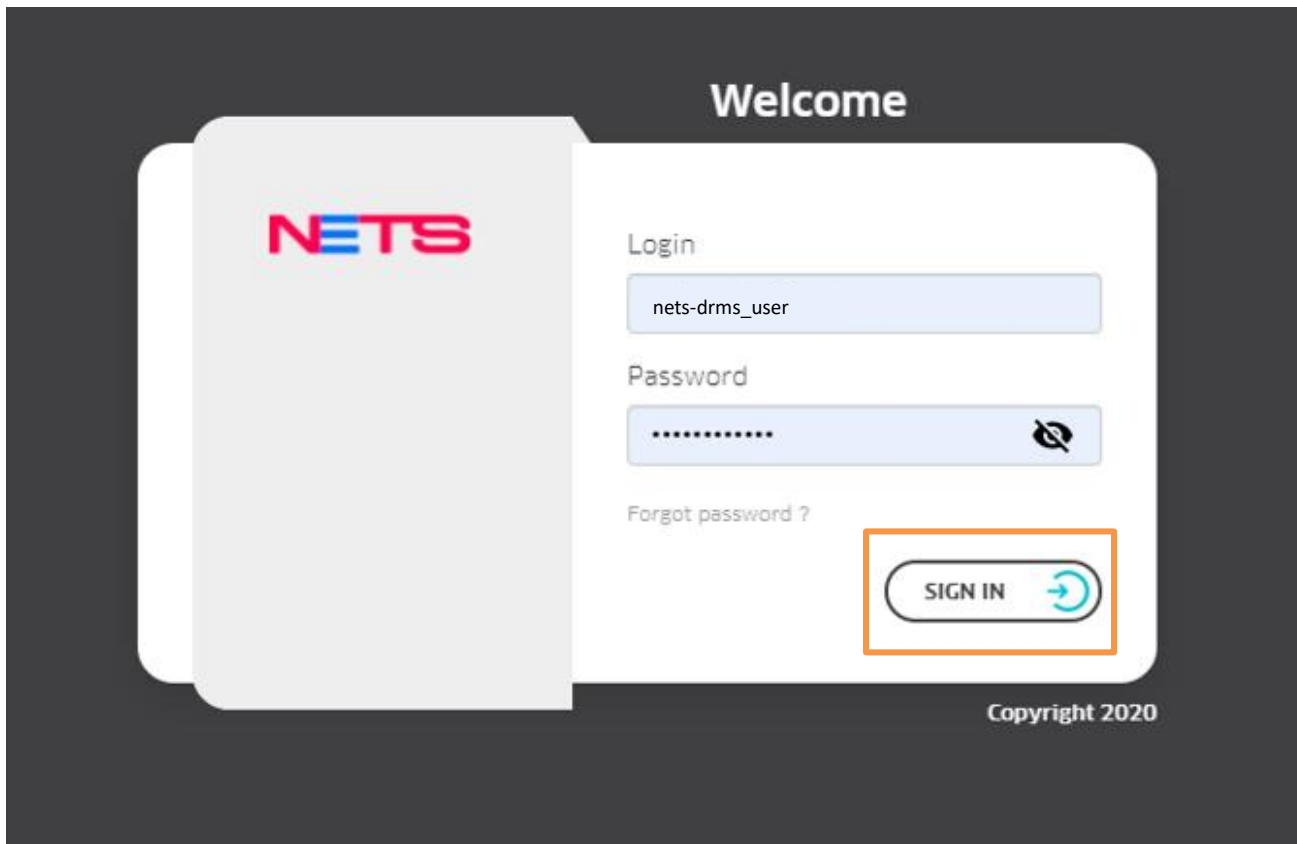
Step 3: On this page, scan the QR code using your Google Authenticator app to generate the temporary code. Type the code into the field next to the QR code to complete the validation



Subsequent access to DRMS

If you are accessing DRMS after your first-time validation, please follow the steps below.

Step 1: Sign into DRMS using your login details as per normal



Welcome

NETS

Login

nets-drms_user

Password

.....

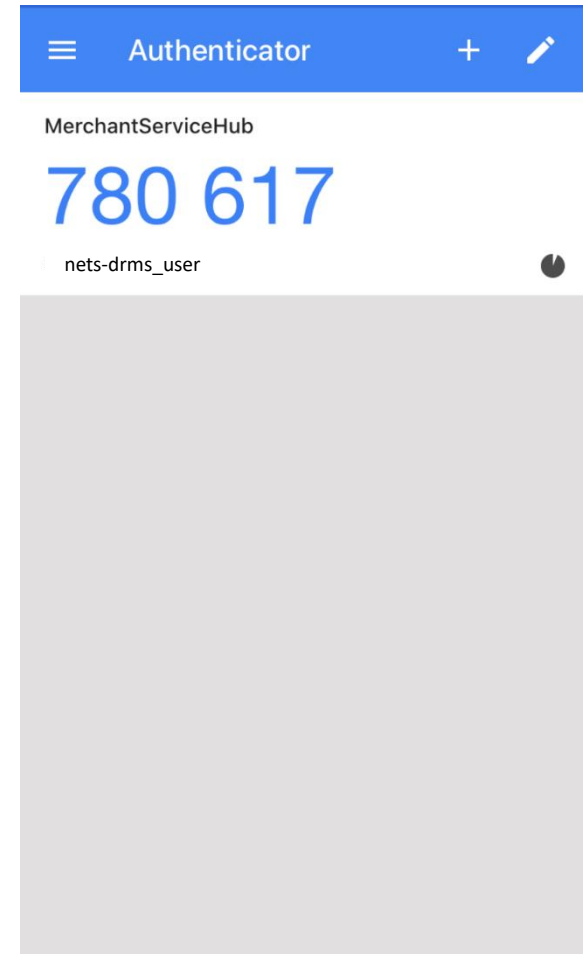
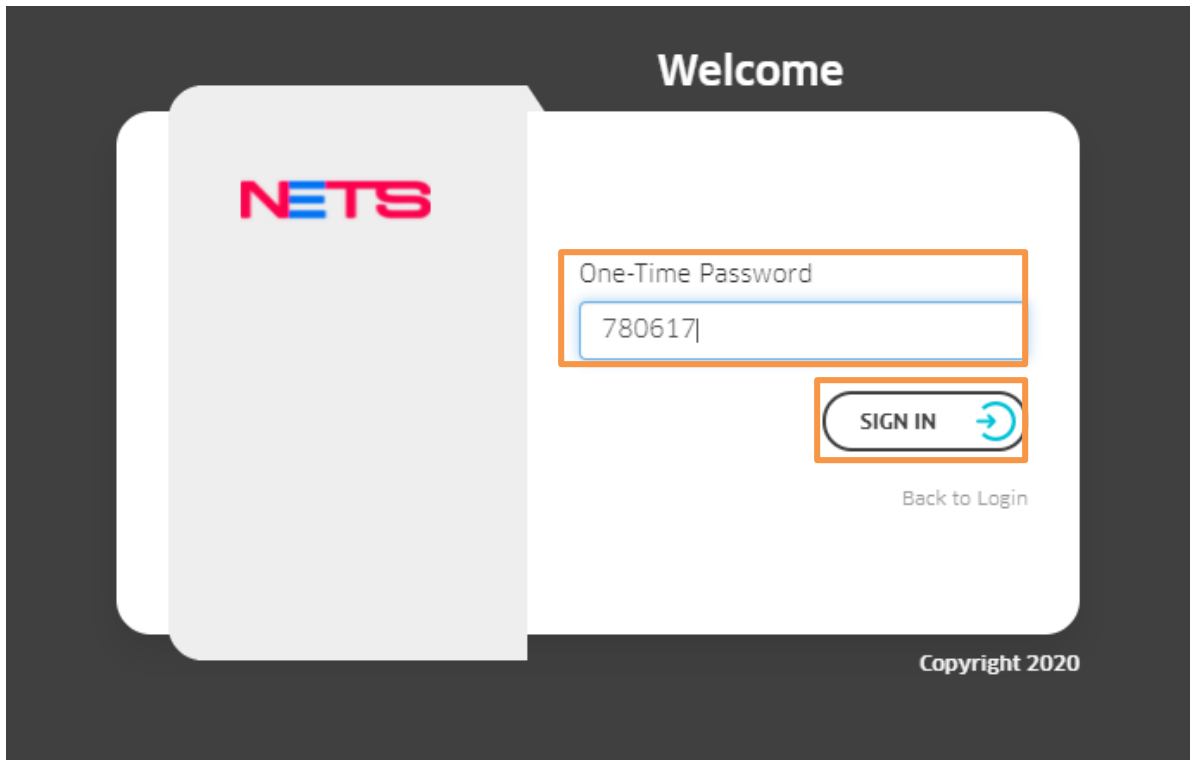
Forgot password ?

SIGN IN →

Copyright 2020

Subsequent access to DRMS

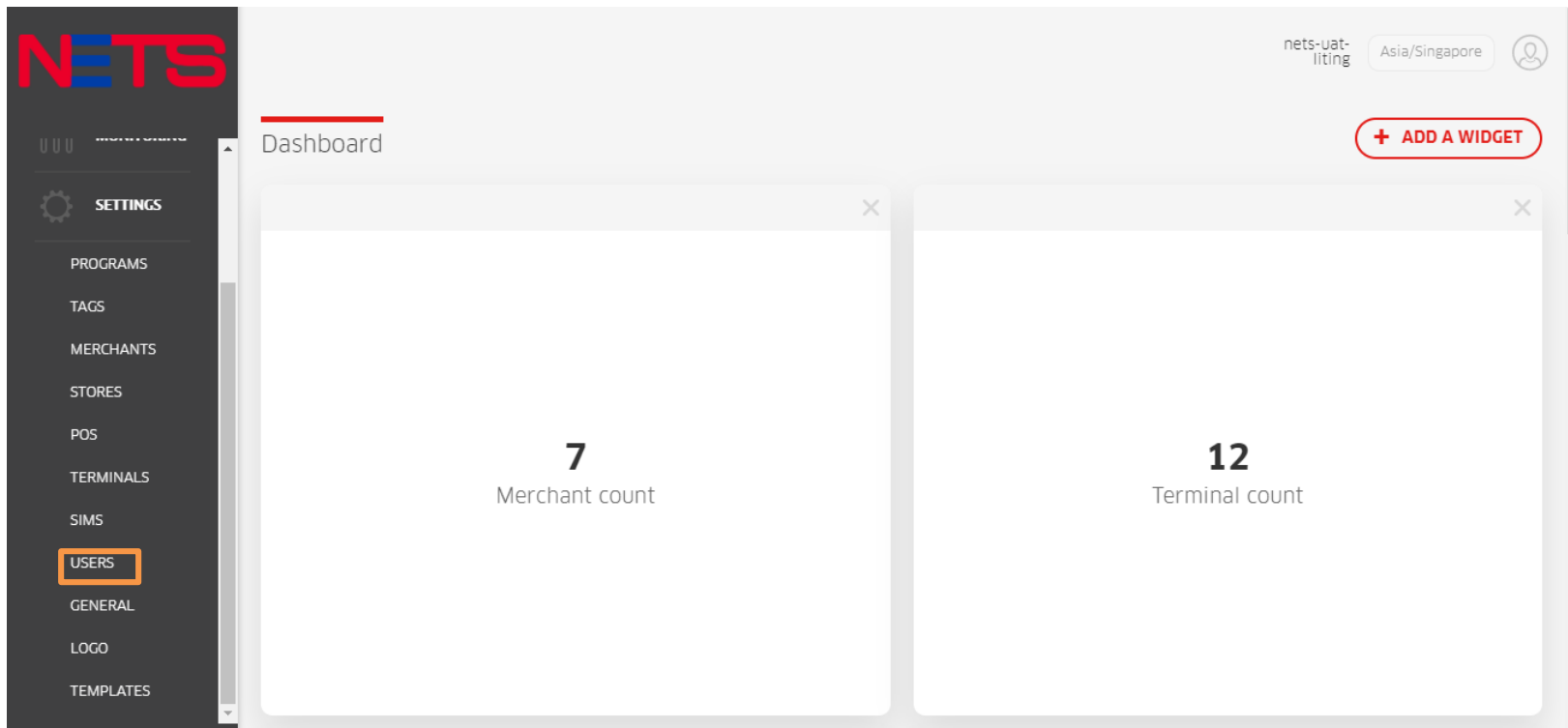
Step 2: When you get to this page, open your Google Authenticator app and key in the OTP generated into the OTP field to sign in



Creating a new 2FA user

If you want to create a new user with 2FA, please follow the steps below.

Step 1: On the left side panel, click 'Users' to go to the users management page



Creating a new 2FA user

Step 2: On the users management page, click on the 'Create A User' button to create a new user.

+ CREATE A USER

Step 3: Key in the details of the user that you want to create, then click 'Save'

Users > Create a User

Login*

Email*

Permissions

Single session

Restricted by services

Without restriction
 Restricted to Merchants
 Restricted by Transaction fields

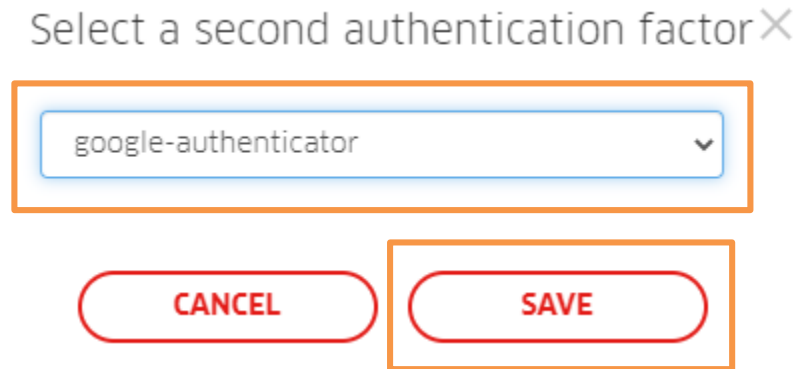
Creating a new 2FA user

Step 4: A pop-up will appear for the second authentication factor selection. Ensure that google-authenticator is selected before clicking 'Save'. Upon clicking 'Save', creation of user with 2FA is completed.

Select a second authentication factor ✕

google-authenticator ▼

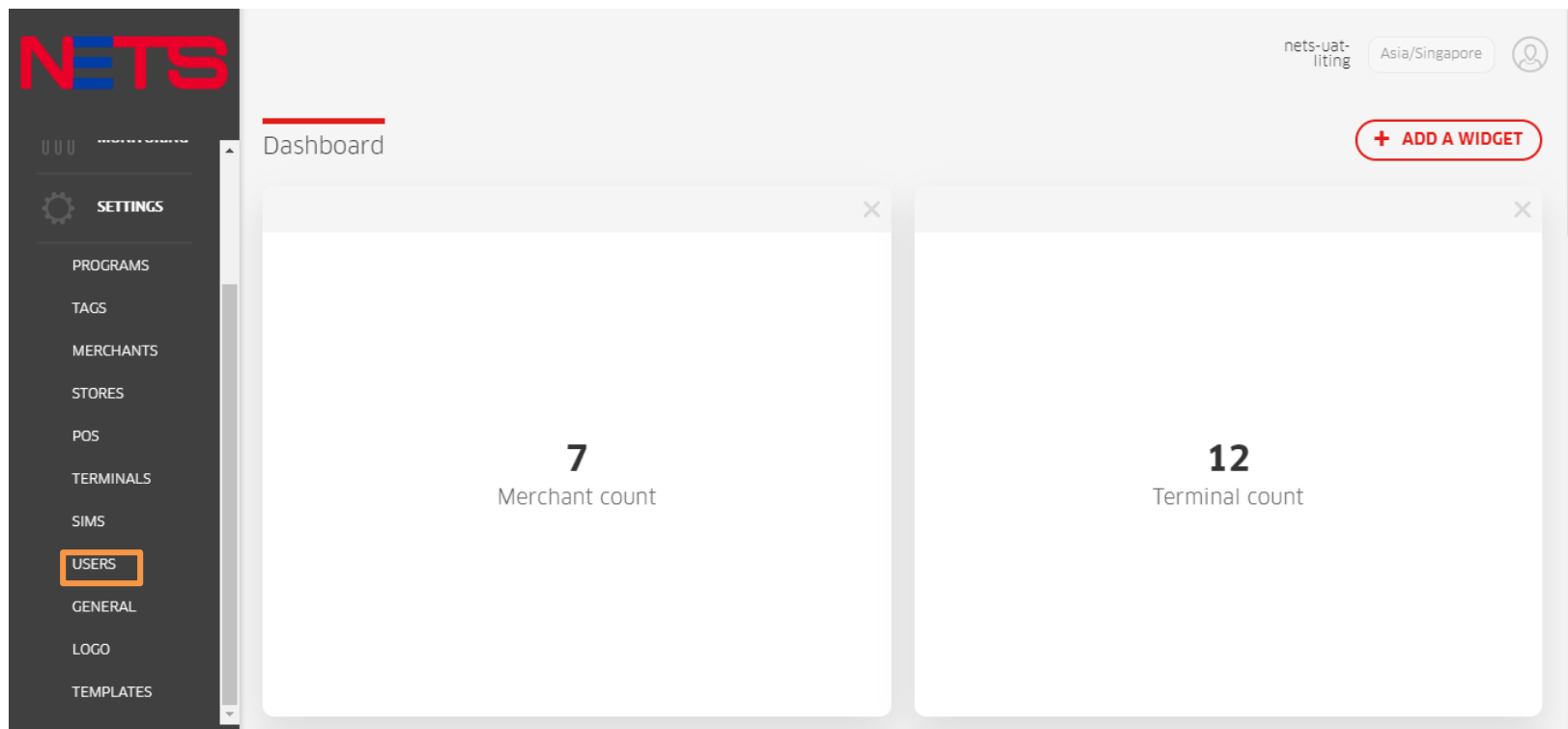
CANCEL SAVE



Revoking 2FA for existing user

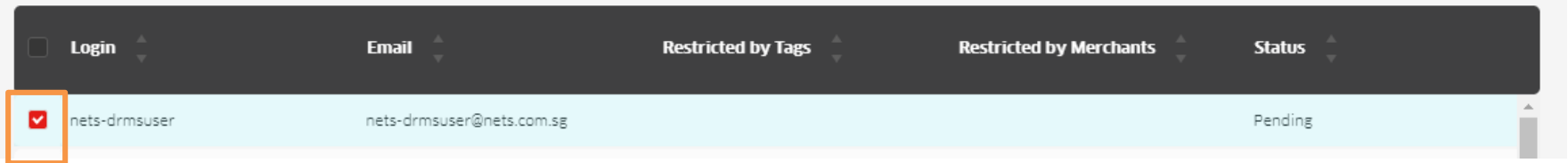
If you need to revoke 2FA for a user who lost his/her mobile or has left the company, please follow the steps below.

Step 1: Click 'Users' on the left side panel to go to the users management page

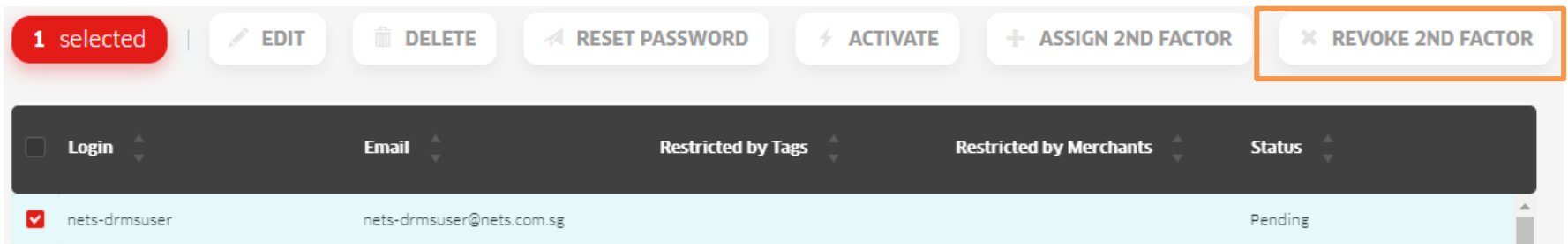


Revoking 2FA for existing user

Step 2: On the users management page, select the user whose 2FA you want to revoke



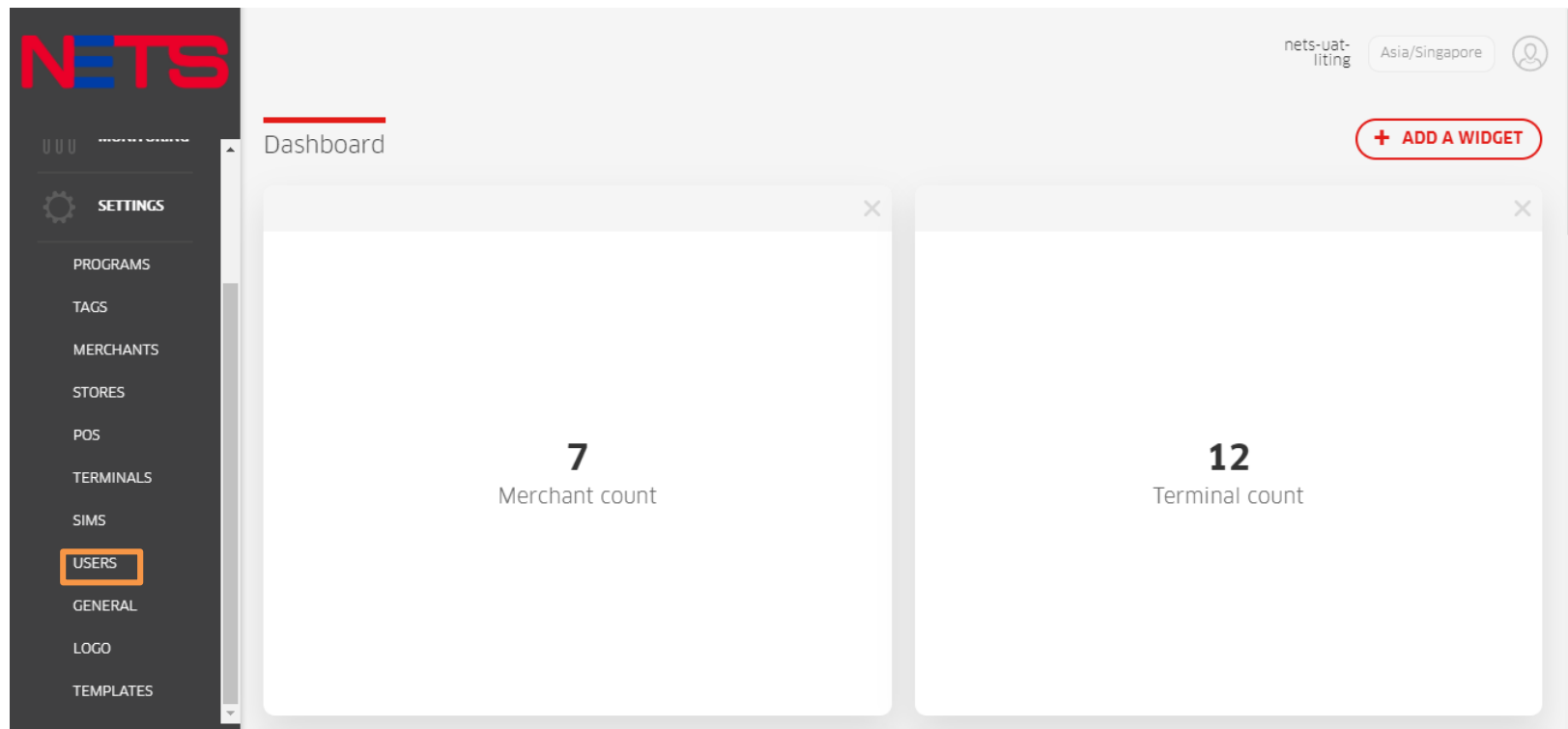
Step 3: Once user is selected, a 'Revoke 2nd Factor' button will appear. Click on the button to revoke the 2FA for the user.



Assigning 2FA to existing user

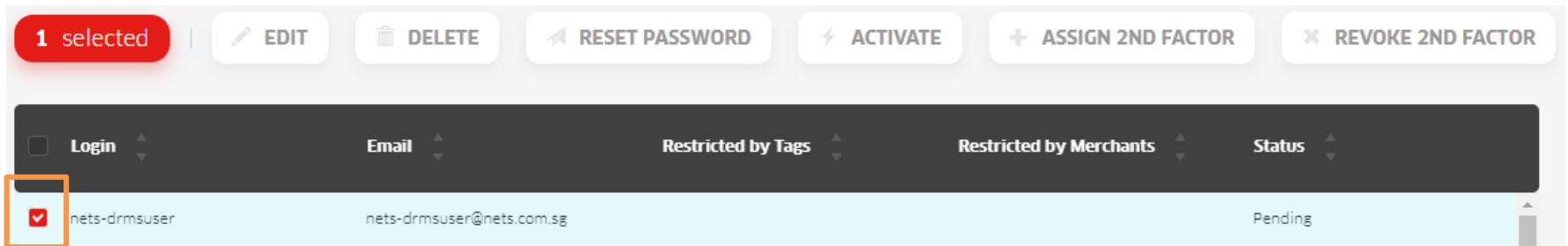
If you need to assign an existing user with 2FA, please follow the steps below.

Step 1: Click 'Users' on the left side panel to go to the users management page



Assigning 2FA to existing user

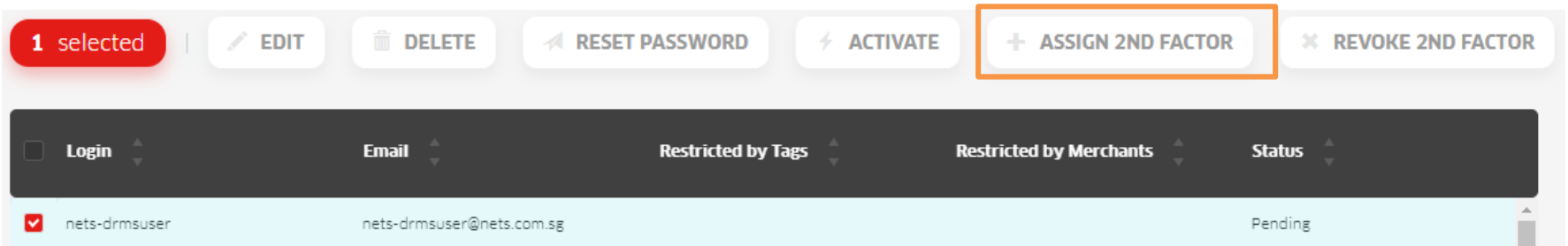
Step 2: On the users management page, select the user to whom you want to assign 2FA



The screenshot shows a user management interface. At the top, there is a toolbar with a red button indicating '1 selected' and several action buttons: 'EDIT', 'DELETE', 'RESET PASSWORD', 'ACTIVATE', 'ASSIGN 2ND FACTOR', and 'REVOKE 2ND FACTOR'. Below the toolbar is a table with columns for 'Login', 'Email', 'Restricted by Tags', 'Restricted by Merchants', and 'Status'. The first row of the table is highlighted in light blue, and a red checkmark in the 'Login' column is enclosed in an orange box. The user's name is 'nets-drmsuser' and their email is 'nets-drmsuser@nets.com.sg'. The status is 'Pending'.

Login	Email	Restricted by Tags	Restricted by Merchants	Status
<input checked="" type="checkbox"/>	nets-drmsuser			Pending

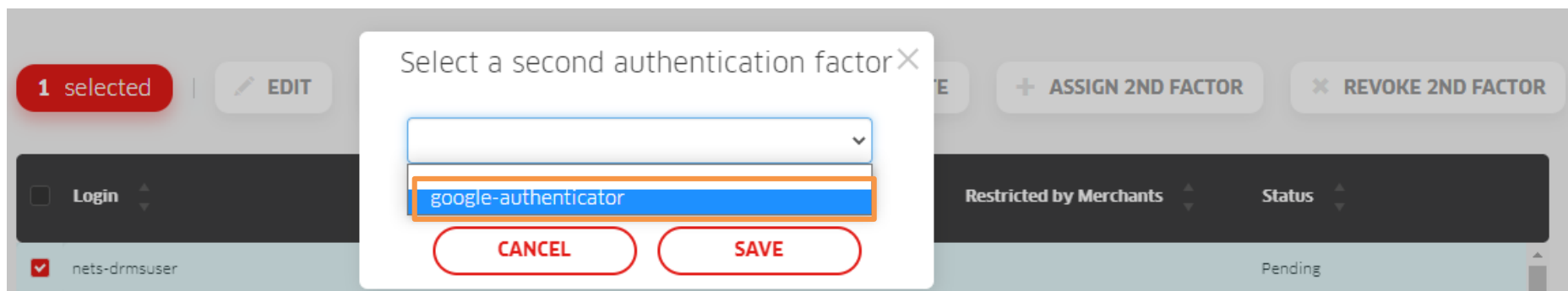
Step 3: Once user is selected, a 'Assign 2nd Factor' button will appear. Click on the button to assign the 2FA to the user.



This screenshot is identical to the previous one, but the 'ASSIGN 2ND FACTOR' button in the toolbar is now highlighted with an orange box, indicating it is the next step in the process.

Assigning 2FA to existing user

Step 4: Upon clicking the 'Assign 2nd Factor' button, a pop-up will appear for selection of the second authentication factor. Ensure that 'google-authenticator' is selected before clicking 'Save'. Upon clicking 'Save', assignment of 2FA to user is completed.



Thank You