

One Time Password Via Twilio V5.0.1

OTP (One Time Password) is a string of numeric or alphanumeric characters that generates automatically. And it is the most reliable authentication process.

With the help of this module, the admin can integrate OTP (One Time Password) verification feature on the Adobe Commerce store.

Thus, OTP verification can use for the new customer while they are registering on the store, during sign-in, when they want to reset their password, and during the checkout process.

OTP (One Time Password) Extension Features

Admin can configure to enable/disable the OTP module.

Admin can set OTP Expiry duration.

One Time Password verification of the customers at the time of registration.

Admin can enable/disable OTP verification of the customers at the time of checkout.

The admin can select the payment option, for which the customers will verify OTP.

Admin can set email templates for OTP verification notifications.

This module supports all Payment Methods.

The customer cannot reuse the expire/use OTP.

The customer receives the Mobile OTP (SMS) on the registered mobile if Twilio Mobile Verification enable otherwise customer receives the OTP on the email address.

OTP string supports numeric digits only.

The One Time Password can be resend to the customer.

The customer can't use the OTP for cross-customer accounts.

Need OTP validation on Customer Forget Password

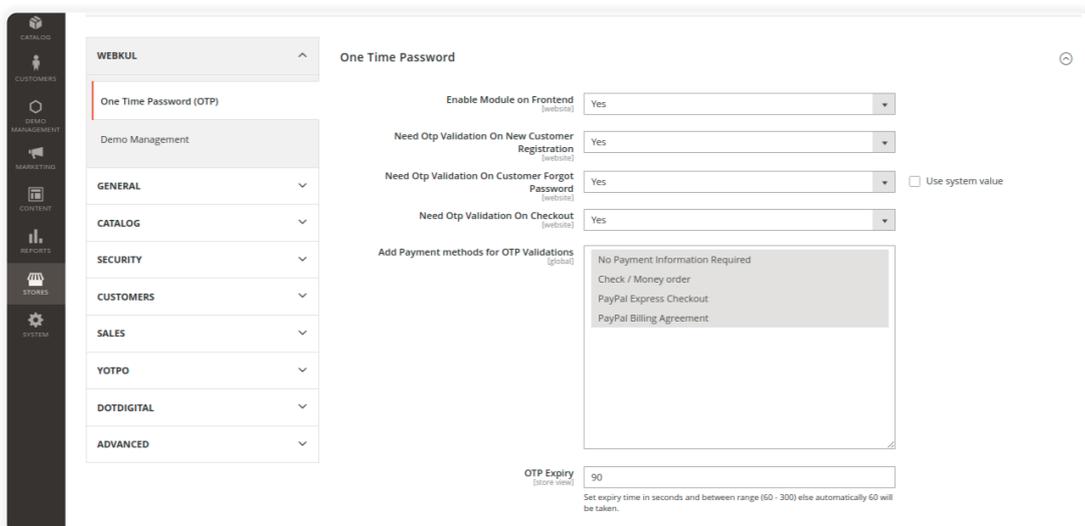
OTP validation while login as a customer

Send OTP in Email in case of mobile OTP failure.

OTP Module Configuration

To do the module configuration in the admin panel, please navigate through **Stores>Configuration>Webkul>One Time Password(OTP)**.

Thus, the following options will appear for doing module configuration:



The screenshot shows the 'One Time Password' configuration page in the admin panel. The left sidebar contains a navigation menu with categories: CATALOG, CUSTOMERS, DEMO MANAGEMENT, MARKETING, CONTENT, REPORTS, STORES, and SYSTEM. The 'STORES' category is expanded, showing sub-menus: WEBKUL, Demo Management, GENERAL, CATALOG, SECURITY, CUSTOMERS, SALES, YOTPO, DOTDIGITAL, and ADVANCED. The main content area is titled 'One Time Password' and contains the following configuration options:

- Enable Module on Frontend** (website): Yes
- Need Otp Validation On New Customer Registration** (website): Yes
- Need Otp Validation On Customer Forgot Password** (website): Yes Use system value
- Need Otp Validation On Checkout** (website): Yes
- Add Payment methods for OTP Validations** (global):
 - No Payment Information Required
 - Check / Money order
 - PayPal Express Checkout
 - PayPal Billing Agreement
- OTP Expiry** (store view): 90
Set expiry time in seconds and between range (60 - 300) else automatically 60 will be taken.

One Time Password

Enable Module on Frontend – Select the “**YES**” option to enable the module on the front end or else select “**NO**”.

OTP Validation On New Customer Registration – Select the “**YES**” option to enable OTP verification for the new customer at the time of registration or else select “**NO**”.

Need OTP Validation On Customer Forget Password – Select the “**YES**” option to enable OTP verification for the customer at the time of the customer forgetting a password or else select “**NO**”.

Need OTP Validation On Checkout – Select the “**YES**” option for enabling OTP validation during the checkout or else select “**NO**”.

Add Payment methods for OTP Validations – Admin can select for which payment method, he/she wants to enable the OTP verification.

OTP Expiry – Admin can set expiry time in seconds and between range [60 – 300] else automatically 60 will be taken.

OTP Email Settings

Select OTP Notification Template – Select the OTP notification template that will be sent to the new customer during **REGISTRATION**.

Select OTP Notification Template – Select the OTP notification template that will be sent to the customer at the time of **CHECKOUT**.

[Save Config](#)

Select Otp Notification Template at time of New Registration [store view]

Select Otp Notification Template at time of Checkout [store view]

Twilio Auth [-]

Enable Mobile Verification [website] Use system value

Send OTP Email In Failure [website] Use system value

Auth Id [store view]

Token [store view]

Message [store view]

Sender Number [store view]

Twilio Auth

“Twilio” is a communications platform for sending and receiving text messages using it’s web service APIs.

The admin can signup for the Twilio services and register to the Twilio. To register, the admin can visit [Twilio](#) then click on the signup button.

SIGNAL 2019 | AUGUST 6 - 7: TWO DAYS OF LEARNING, TALKS, AND NETWORKING
HELP LOG IN

[Products](#)
[Solutions](#)
[Docs & Tools](#)
[Customer Stories](#)
[Partners](#)
[Pricing](#)

[Talk to an expert](#)
[Sign up](#)

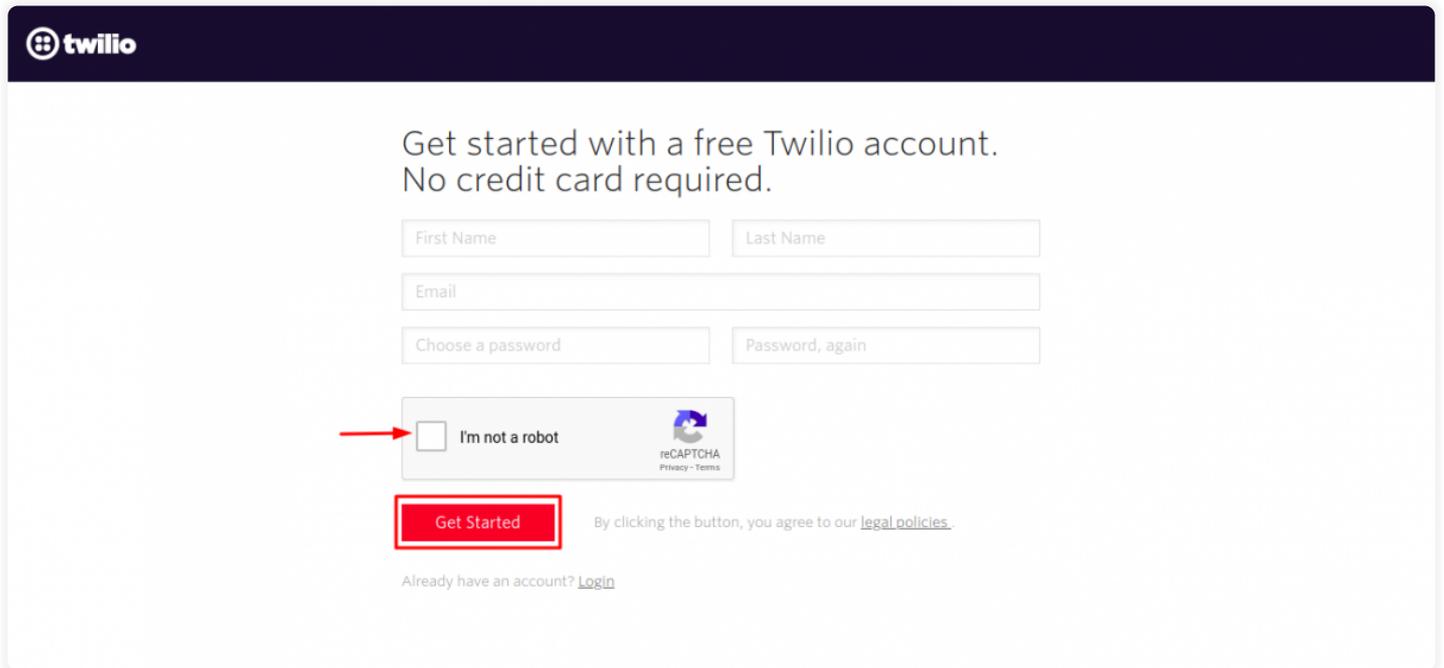
BUILD A BETTER CUSTOMER EXPERIENCE

Connect with customers using Flex, the world’s first fully-programmable contact center platform.

Try Flex for free >_

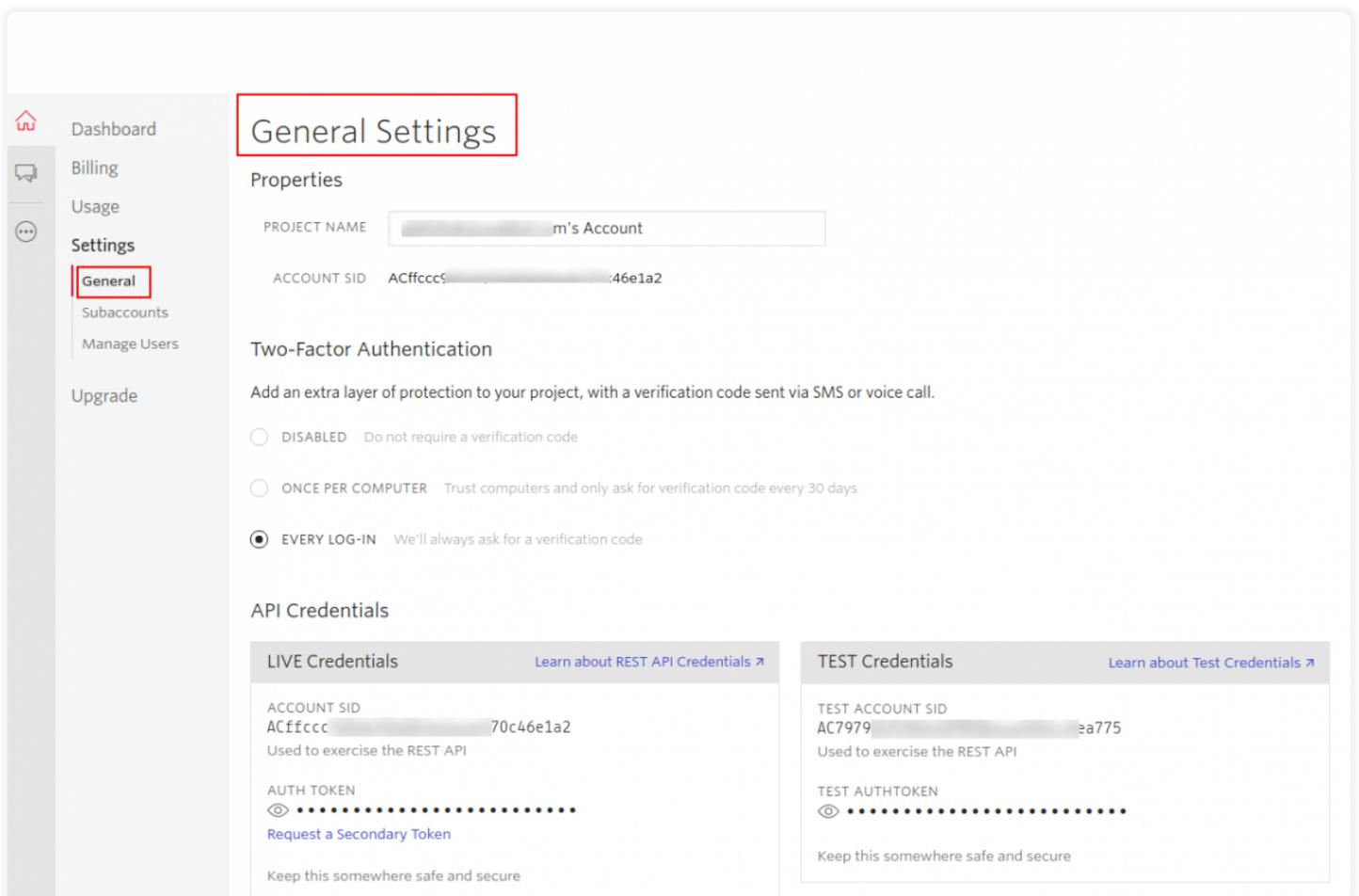
Questions? [Talk to an expert.](#)

Here, the admin can fill the required feild as shown in the image below-



The image shows the Twilio account creation page. At the top left is the Twilio logo. The main heading reads "Get started with a free Twilio account. No credit card required." Below this are several input fields: "First Name", "Last Name", "Email", "Choose a password", and "Password, again". A reCAPTCHA widget is present with the text "I'm not a robot" and a red arrow pointing to the checkbox. Below the reCAPTCHA is a red "Get Started" button. To the right of the button, it says "By clicking the button, you agree to our [legal policies](#)." At the bottom, there is a link: "Already have an account? [Login](#)".

Now, from the Twilio account, the admin can access the information which will be required in the admin dashboard.



The image shows the Twilio account settings page. On the left is a sidebar with navigation options: Dashboard, Billing, Usage, Settings, Upgrade, Subaccounts, and Manage Users. The "Settings" section is expanded, and "General" is selected. The main content area is titled "General Settings" and is enclosed in a red box. It contains several sections: "Properties" with fields for "PROJECT NAME" (containing "m's Account") and "ACCOUNT SID" (containing "ACffccc...46e1a2"); "Two-Factor Authentication" with three radio button options: "DISABLED" (selected), "ONCE PER COMPUTER", and "EVERY LOG-IN"; and "API Credentials" which is divided into two panels: "LIVE Credentials" and "TEST Credentials". Each panel shows "ACCOUNT SID" and "AUTH TOKEN" fields, with the tokens masked with dots. Links to "Learn about REST API Credentials" and "Learn about Test Credentials" are provided for each panel. A note at the bottom of each panel says "Keep this somewhere safe and secure".

So, using the Twilio, the admin can enable the Mobile OTP. To enable this, the admin has to enter the Auth Id, Token, and message. The store owner can generate these login credentials from [Twilio](#).

Enable Mobile Verification – Select the “**YES**” option to send the Mobile OTP (SMS) or else select “**NO**” to send the OTP through the email.

Send OTP Email in Failure – When selected “**Yes**” OTP will be sent via email in the failure of the SMS.

Auth ID – The admin has to enter Auth ID from Twilio

Token – The admin has to enter the Token generated from the Twilio.

Message – In the message section the admin can enter the message format for the OTP

Sender number – Here admin has to enter his Twilio auth registration number.

Send OTP Via– Here admin can select the means of sending OTP.

The screenshot displays the 'Configuration' page for 'Twilio Auth' in a Magento 2.4.1 admin interface. The page includes a sidebar with navigation options like Dashboard, Sales, Catalog, Customers, Order Management, Marketing, Content, Reports, Stores, and System. The main content area is titled 'Twilio Auth' and contains several configuration fields:

- Enable Mobile Verification**: A dropdown menu set to 'Yes' with a 'Use system value' checkbox.
- Send OTP Email in Failure**: A dropdown menu set to 'Yes' with a 'Use system value' checkbox.
- Auth Id**: A text input field with a masked value '.....'.
- Token**: A text input field with a masked value '.....'.
- Message**: A text area containing the text 'Your One Time Password is (otp)'.
- Sender Number**: A text input field containing '+1 970 414 4827'.
- Send Otp Via**: A dropdown menu with options 'Mobile', 'Email', and 'Both', currently set to 'Mobile'. It also has a 'Use system value' checkbox.

At the bottom right, there is a 'Save Config' button. The footer includes the copyright notice 'Copyright © 2020 Magento Commerce Inc. All rights reserved.' and links for 'Privacy Policy', 'Account Activity', and 'Report an Issue'.

Now, Admin can click **Save Config** to apply your changes.

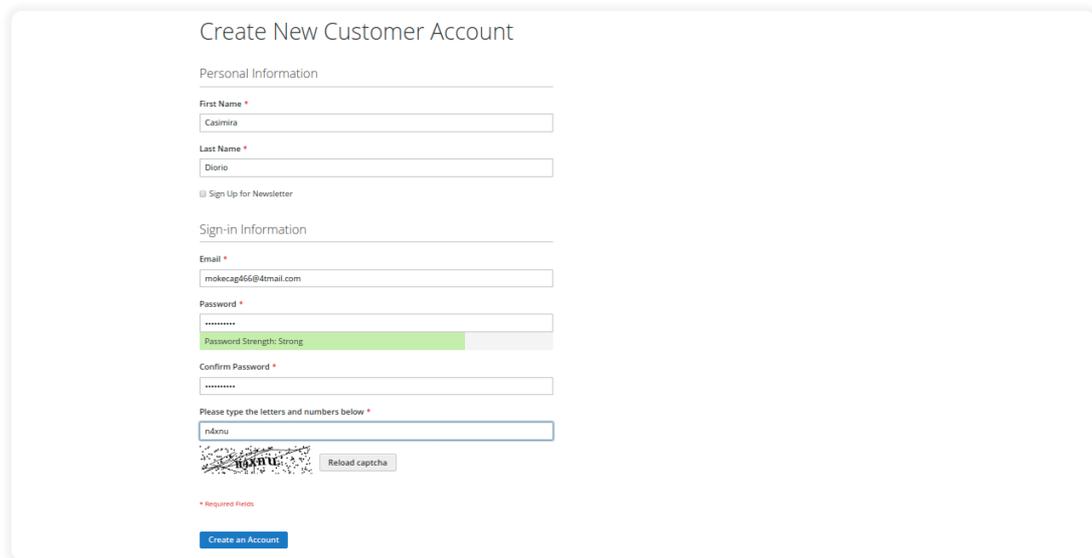
Thus, there are three scenarios to receive OTP-

1. Through E-mail
2. On Mobile Number (SMS)
3. Both

One Time Password Generation (New Registration)- Through E-Mail

OTP will be sent via email only if, In the Twilio auth section in the OTP module, the admin disables the Mobile Verification.

So, if the admin enables the module and “**Need OTP Validation On New Customer Registration**” is set to “**YES**”, the customer will receive the OTP in the email.

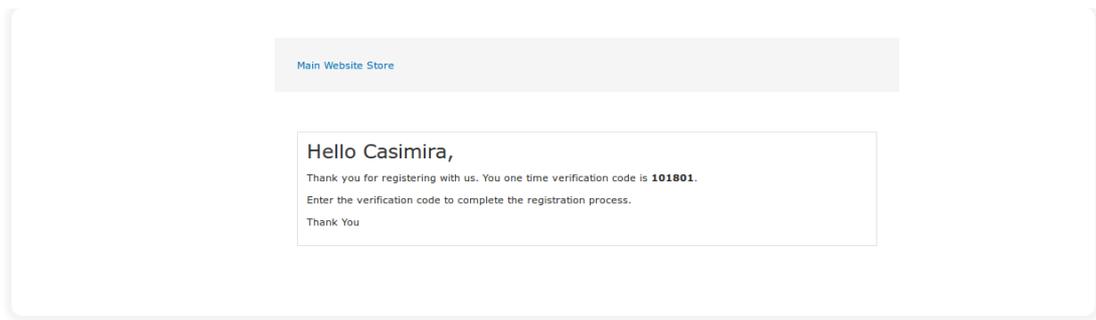


The image shows a registration form titled "Create New Customer Account". It is divided into two main sections: "Personal Information" and "Sign-in Information".

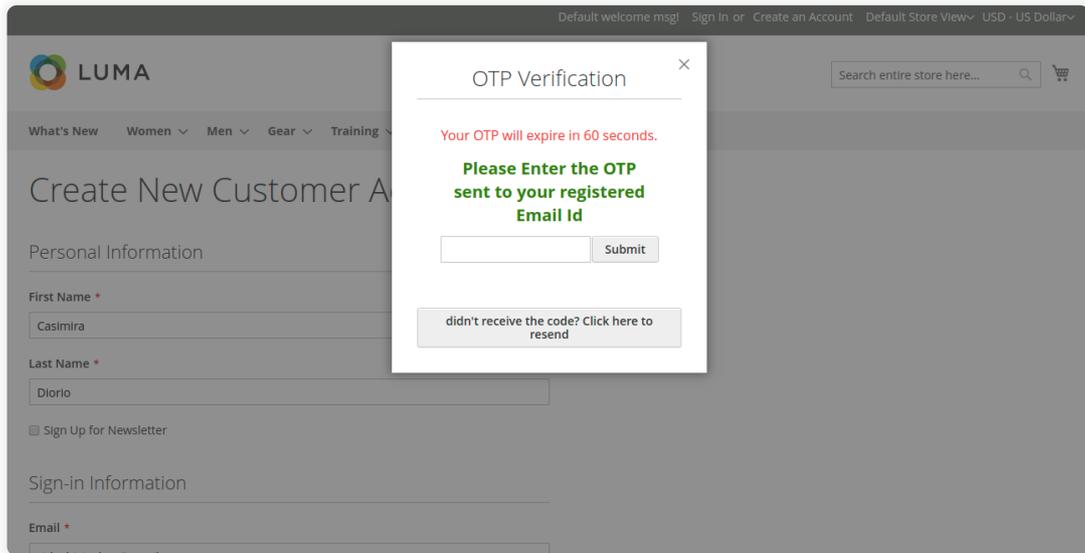
- Personal Information:**
 - First Name * (Text input: Casimira)
 - Last Name * (Text input: Diorie)
 - Sign Up for Newsletter (Checkbox: unchecked)
- Sign-in Information:**
 - Email * (Text input: mokecag66@gmail.com)
 - Password * (Text input: masked with dots; Password Strength: Strong, indicated by a green bar)
 - Confirm Password * (Text input: masked with dots)
 - Please type the letters and numbers below * (Text input: n4enu)
 - Captcha (Image: n4enu; Reload captcha button)

At the bottom, there is a red asterisk indicating required fields and a blue "Create an Account" button.

The customer's email id receives the OTP, as shown in the image below.

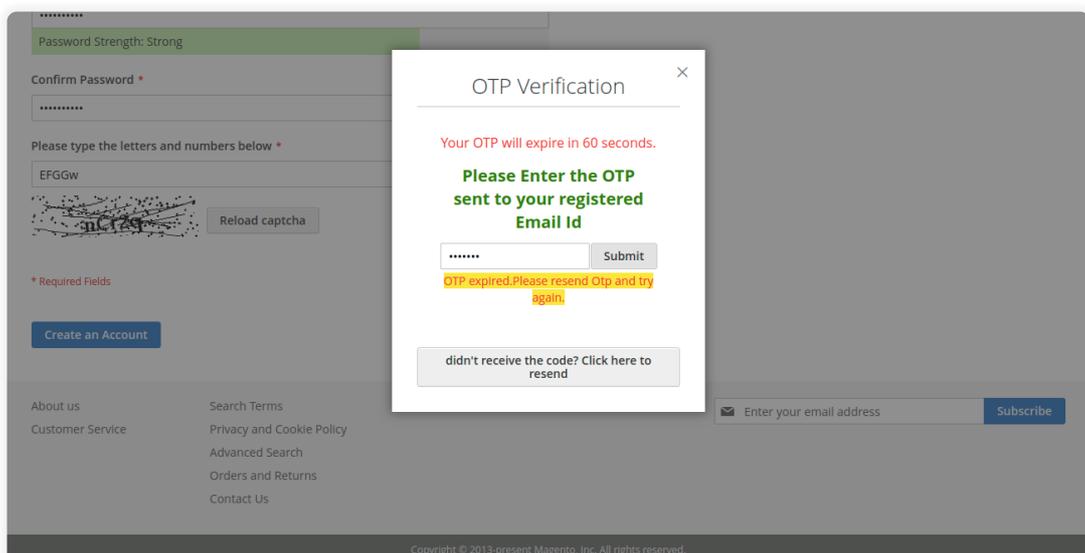


However, the OTP pop box appears, as shown in the image below.



After entering the correct OTP, the customer needs to click on the submit button for the completion of the process.

So, in case the OTP is filled incorrectly, the following image will be displayed.

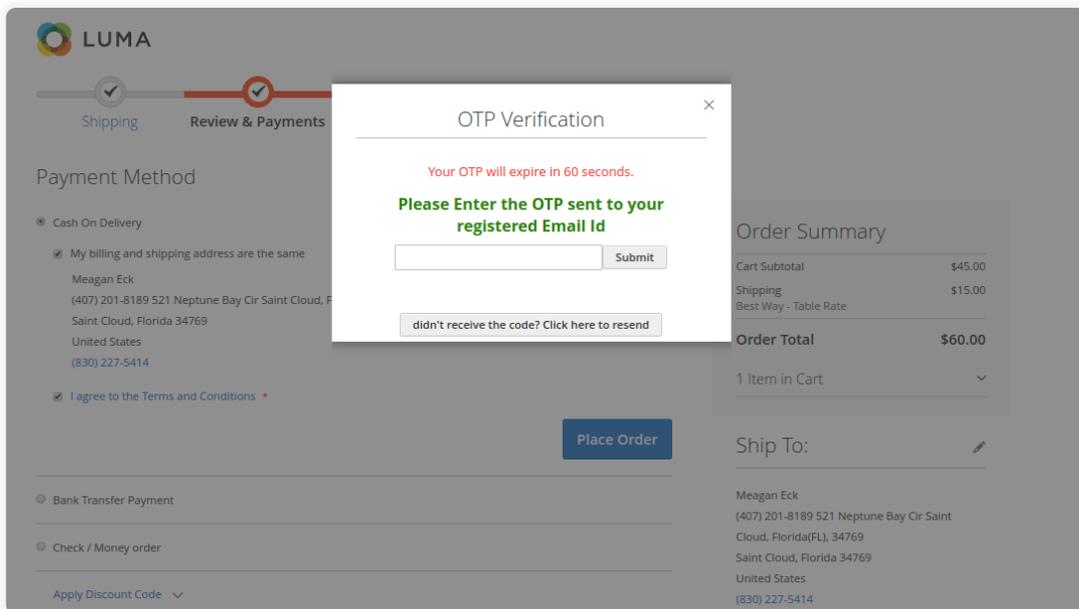


One Time Password Generation (During Checkout)- Through E-Mail

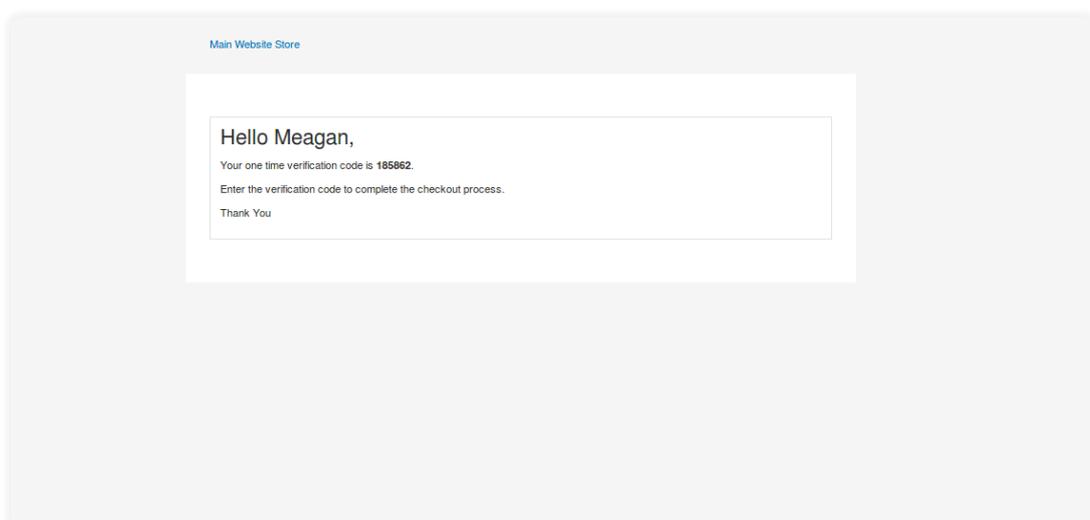
The customer will receive the OTP via E-mail only if in the Twilio auth section admin disables the **Mobile Verification**.

Hence, the “**Need OTP Validation On Checkout**” is set to “**YES**”.

When a customer adds the product to the cart and desired payment method selected and the “**Place Order**” button click the OTP pop-up box will appear on the store, as shown below.



Thus, the registered mail id will get the OTP, as shown in the image below.



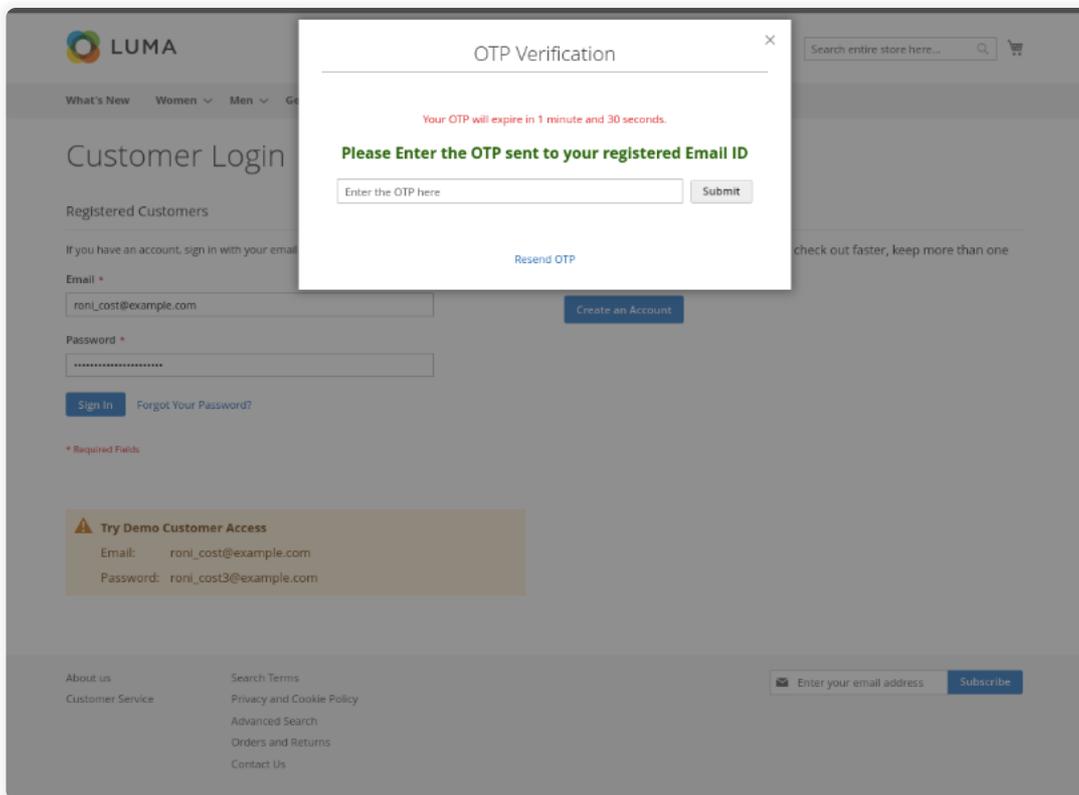
After the entering correct OTP, the submit button should be clicked for the completion of the process.

However, entering the invalid OTP will generate an error message.

NOTE: The customer can use the OTP for a single time only.

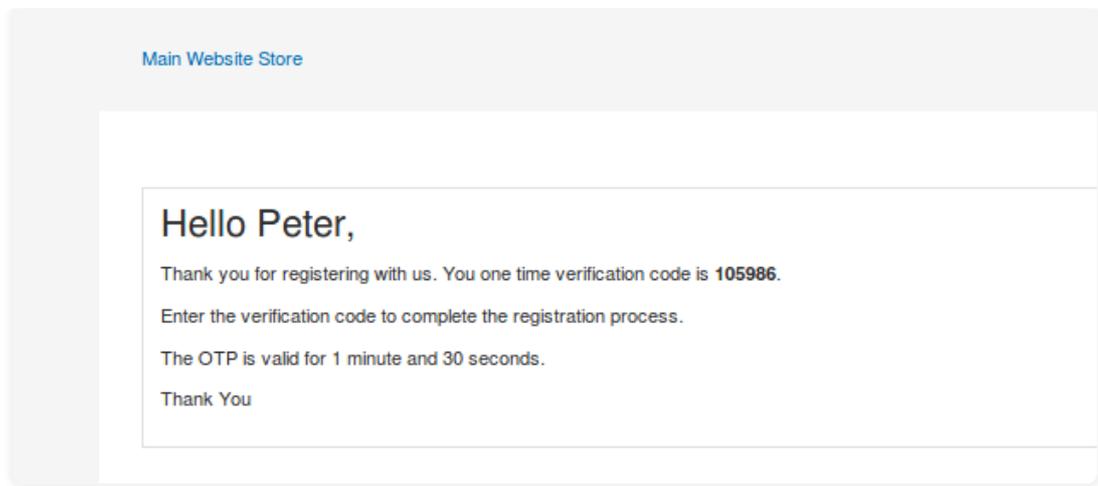
One Time Password Generation (During Sign-In)-Through E-Mail

OTP will also be sent when signing in to the account.



It will ask the customer to enter the OTP to sign-in. The customer will receive the OTP to their registered email id or mobile number configures by the admin.

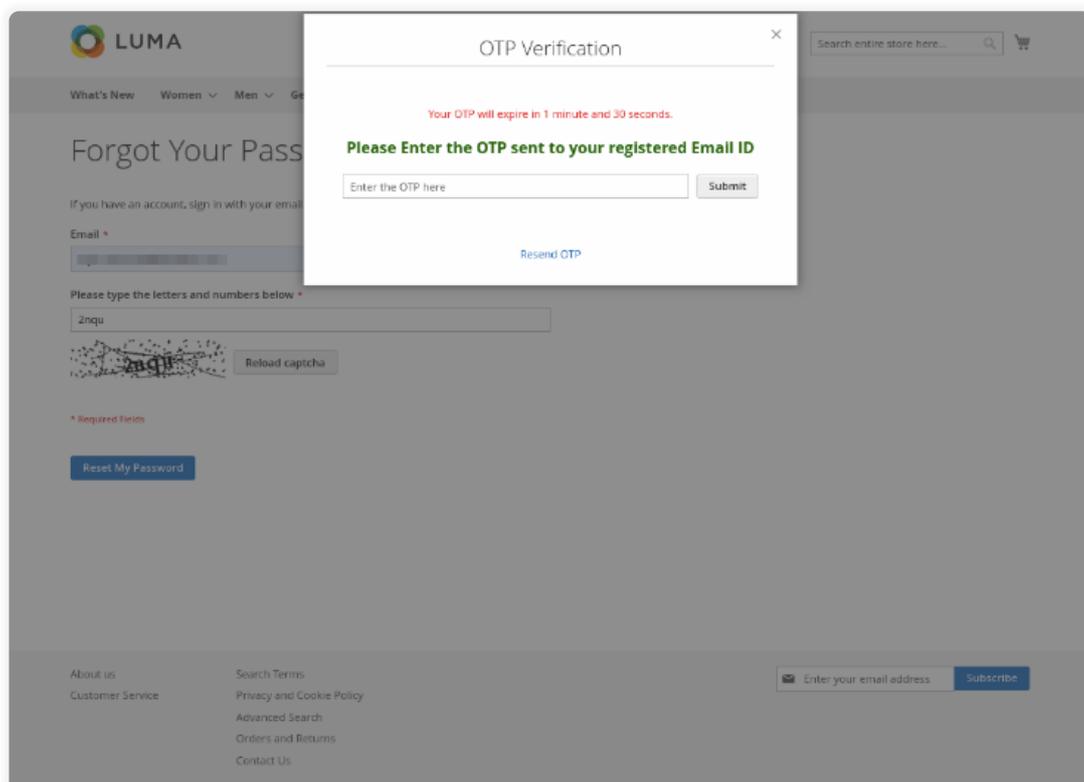
The customer will receive the OTP in their mail and that can use to login to their account.



One Time Password Generation (If Forget The Password)-Through E-Mail

To recover the password using the “forget password” option, the customer can reset the password by verifying the OTP.

The customer will receive the OTP to their registered email or mobile number as per the configuration of the module.



After filling the details like email, captcha code, the customer can click on the “Reset My Password.”

Now the customer will receive the OTP that will be used to verify and get the link to change the password.

Now the customer will receive the OTP in their email address and it can be used to validate and process further to receive the password reset link.

After successfully validating the link the customer will receive the link to reset their password.

One Time Password Generation(New Registration)- Through Mobile

The customer will receive the OTP in form of SMS on Mobile only if in the Twilio auth section the Mobile Verification enables by the admin.

So, if the admin enables the module and “**Need OTP Validation On New Customer Registration**” is set to “**YES**”, the customer will receive the OTP (SMS) in the mobile.

Sign-in Information

Email *

Country *

India

Mobile *

Password *

Password Strength: Strong

Confirm Password *

Please type the letters and numbers below *

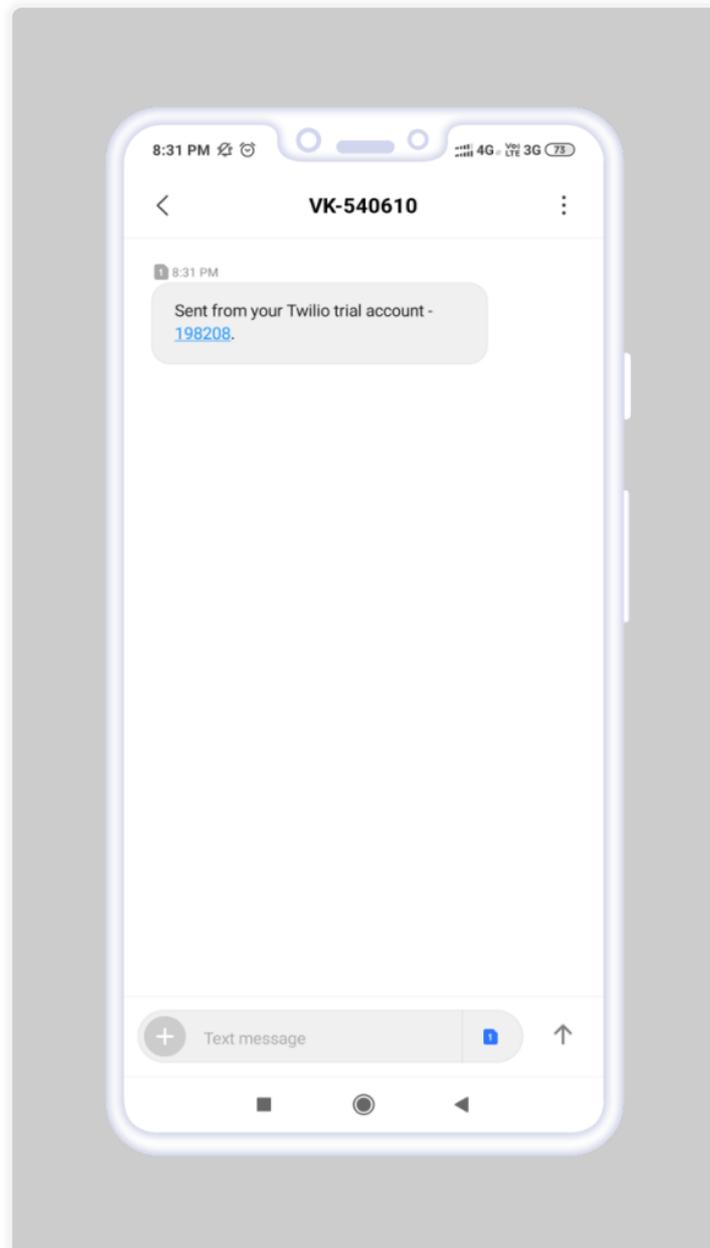
6ASW

Reload captcha

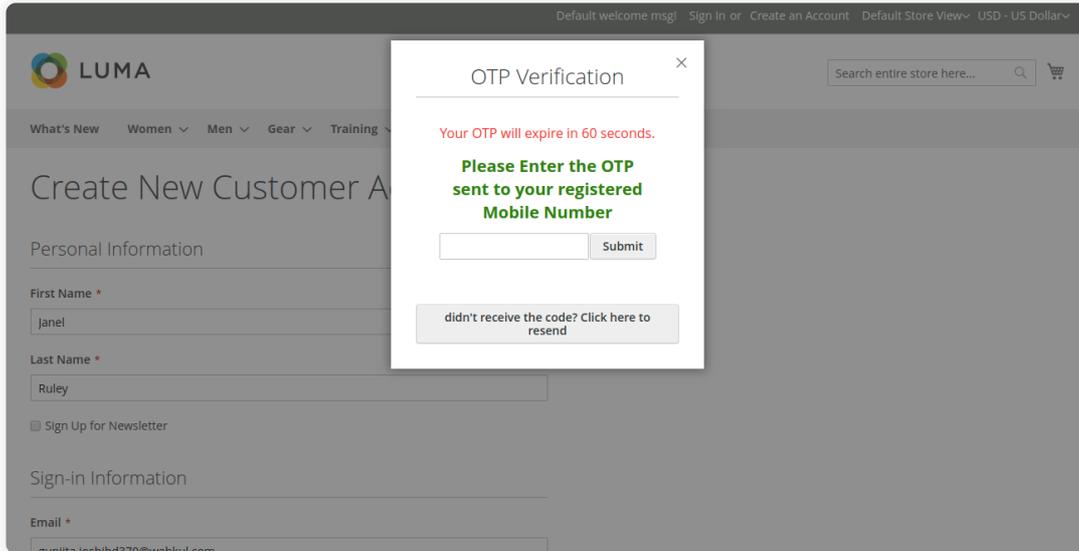
* Required Fields

Create an Account

Thus, the customer receives the OTP (SMS) on the mobile, as shown in the image below.

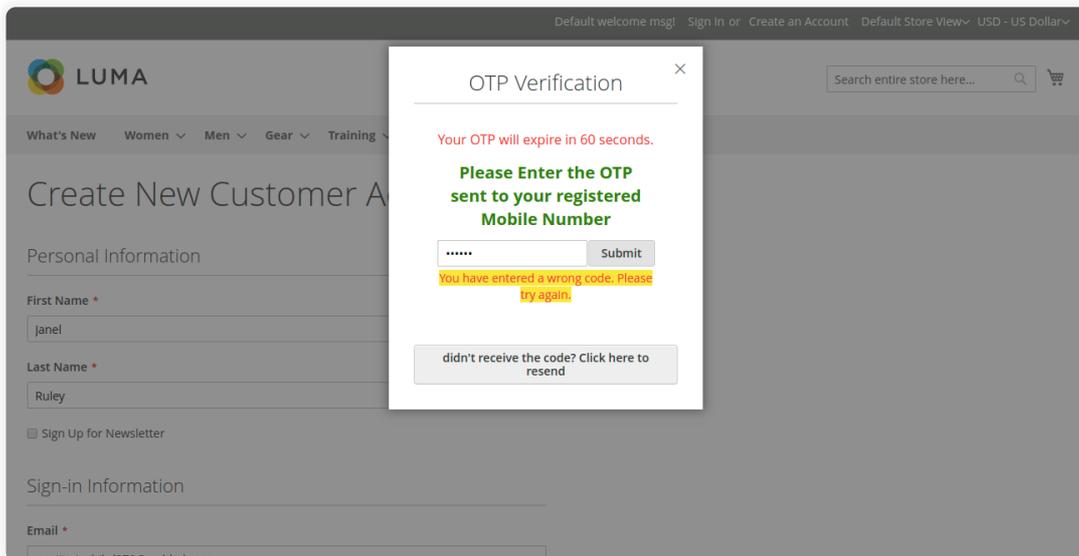


And OTP pop box appears, as shown in the image below.



After entering the correct OTP, the customer needs to click on the submit button for the completion of the process.

So, if in case the OTP is filled incorrectly, the following image will be displayed.



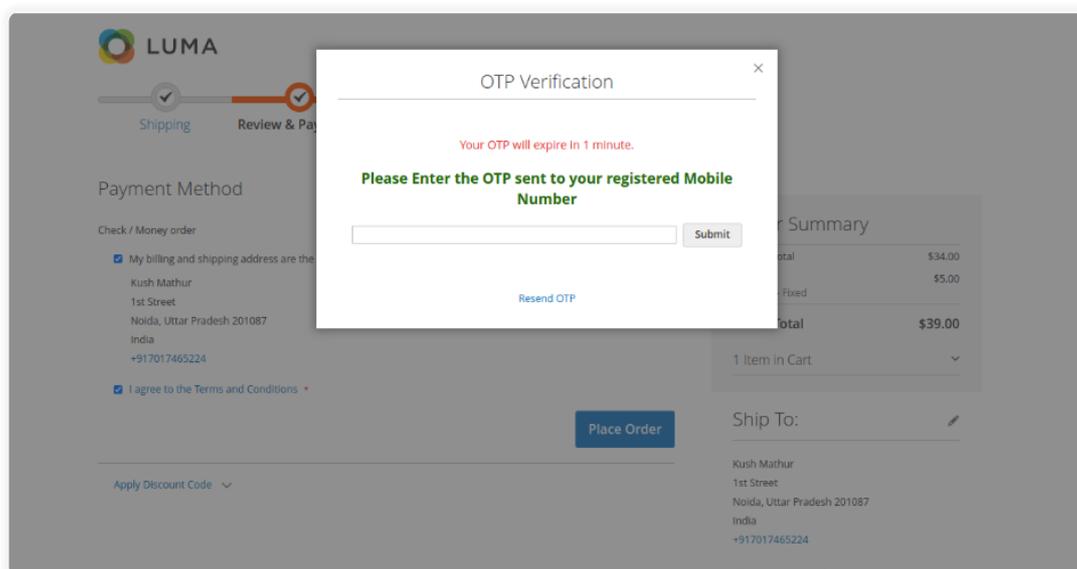
One Time Password Generation (During Checkout)- Through Mobile

If- In the Twilio auth section in the OTP module, the admin enables the **Mobile Verification** option, the customer will receive the OTP in mobile-only.

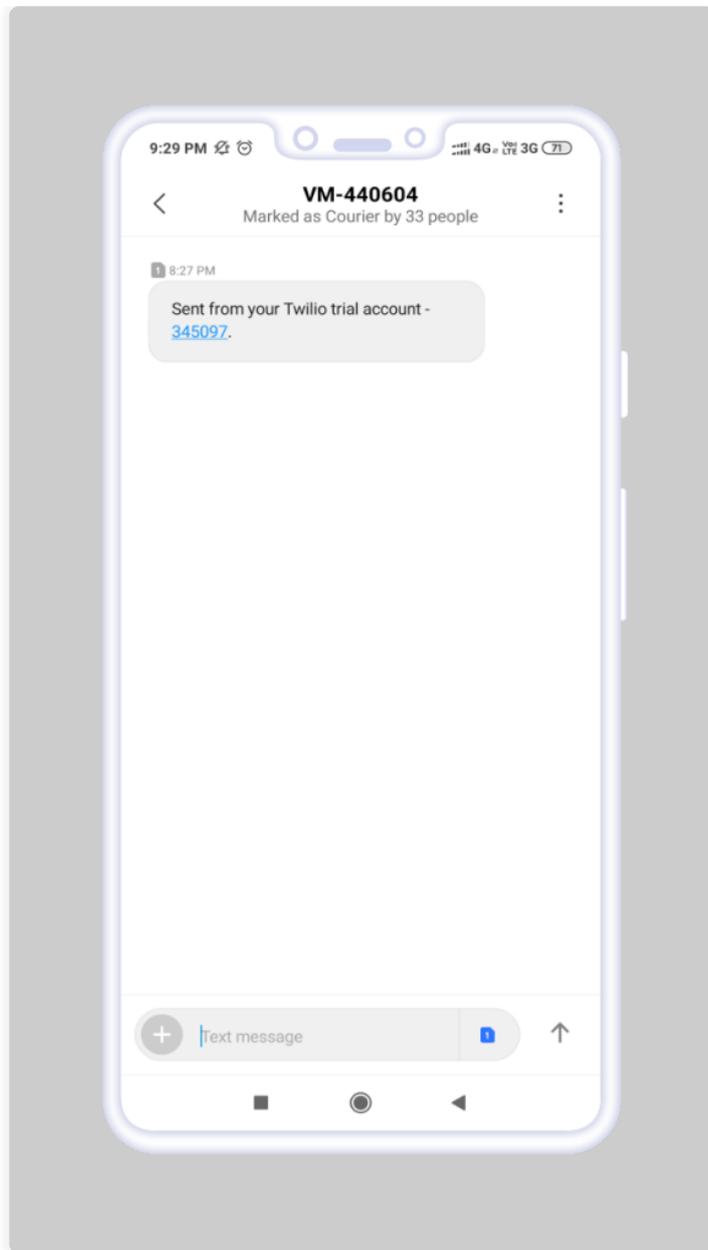
Hence, if the “**Need OTP Validation On Checkout**” is set to “**YES**”.

So, the customer will receive the OTP (SMS) when the product is added to the cart and the customer selects the payment method. Now, click the “**Place Order**” button.

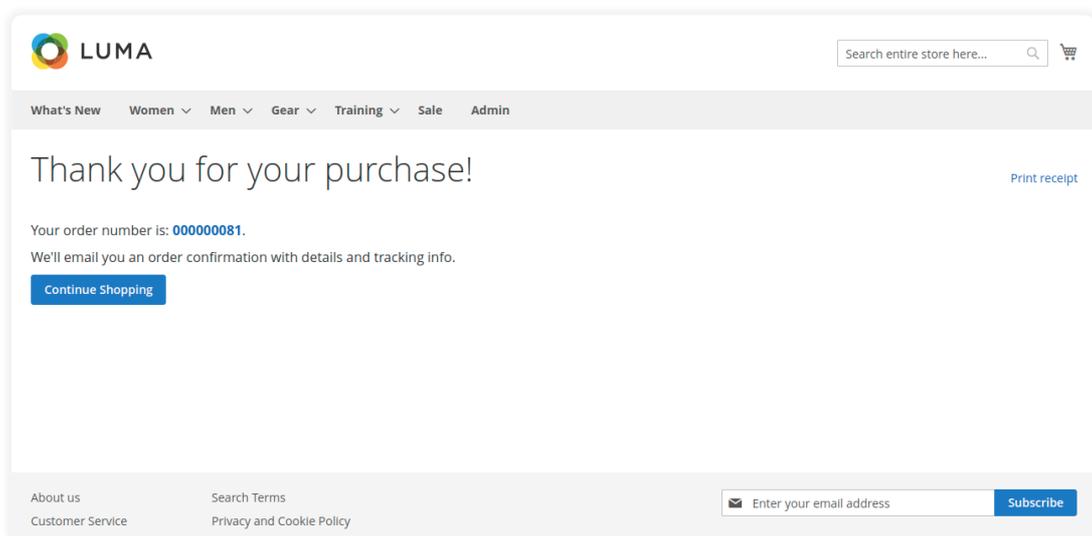
Hence, the OTP pop-up box will appear in the store, as shown below.



The registered mobile will receive the OTP via SMS, as shown in the image below.



After entering the correct OTP, the submit button should be clicked for the completion of the process. However, the customer will be redirected to the thank you page.



Thus, entering the invalid OTP will generate the error message.

This Module offers the store owner an additional layer of security to prevent false order placement and prevents false customer registration over the online store.

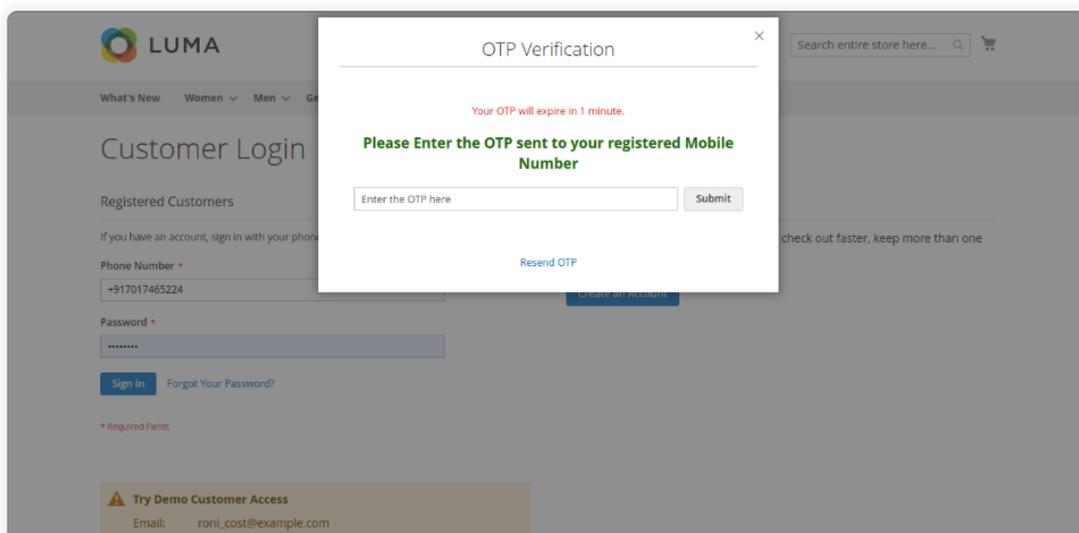
Hence, it offers a unique OTP code for a specific duration for each validation process.

The OTP strings are auto-generated and mailed to the customers over the registered mail address or send through the SMS on their mobile.

NOTE: The customer can use the OTP for a single time only.

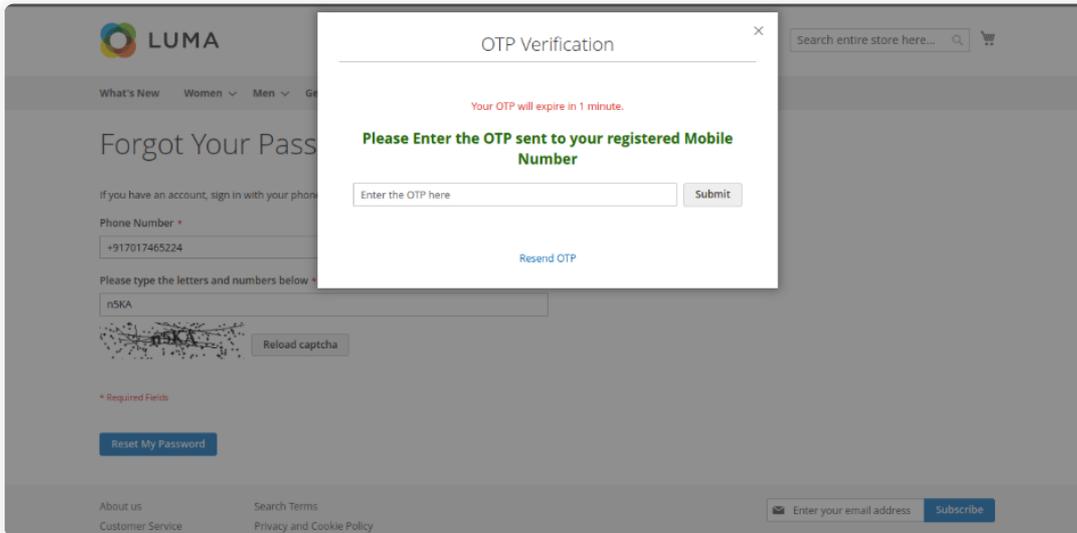
One Time Password Generation (During Sign-In)-Through Mobile

The customer can generate the One Time Password through mobile during the sign-in process and can sign in after entering the OTP as shown in the image.



One Time Password Generation(If Forget The Password)-Through Mobile

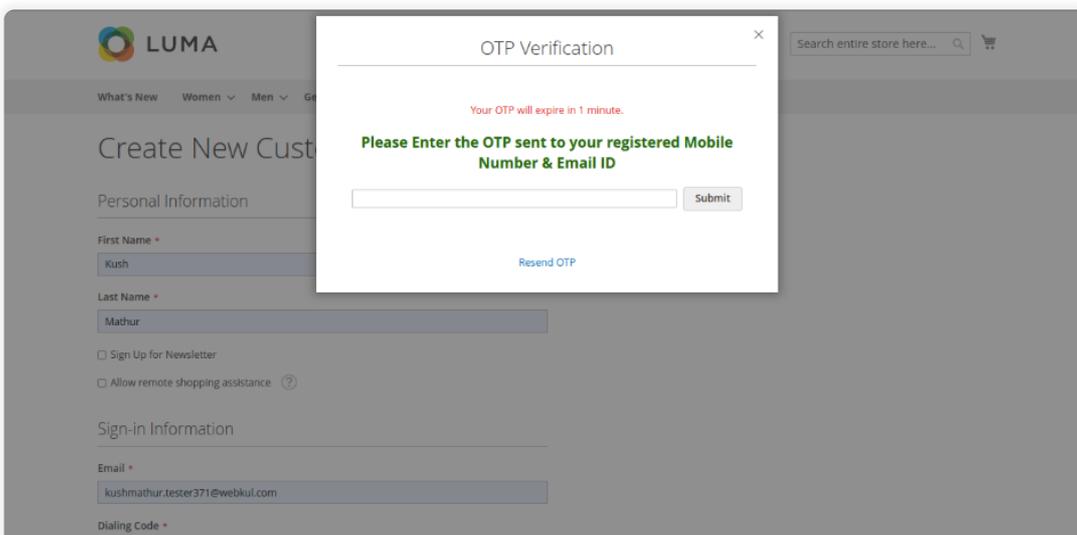
As per the configuration, customers can now reset their password after entering the One Time Password that is sent to their mobile.



after entering the OTP customer can reset the password easily.

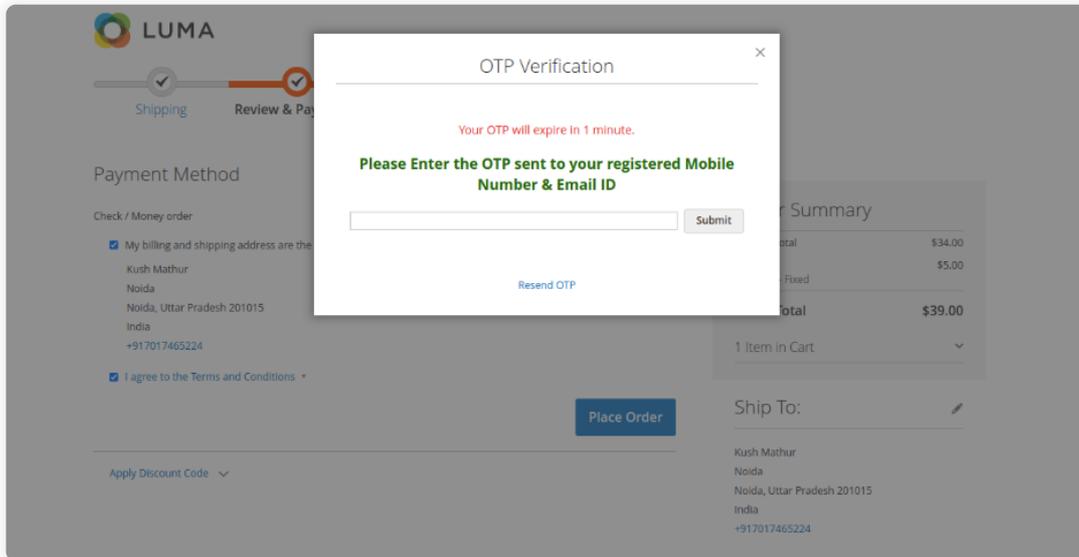
One Time Password Generation(New-Registration)-Through Both

In this scenario, the customer will receive the OTP to their registered email as well as through SMS on their mobile number at the time of their registration.



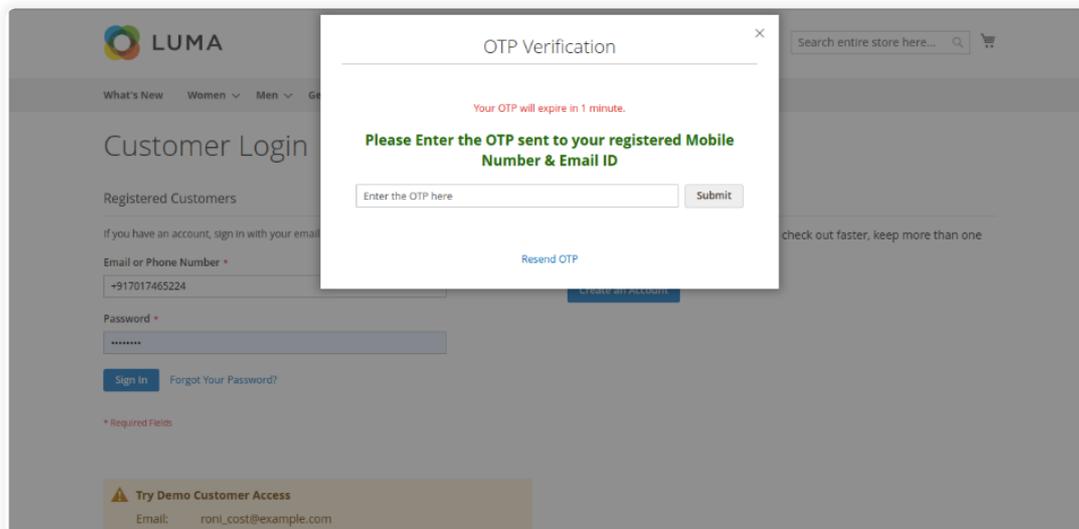
One Time Password Generation (During Checkout)-Through Both

The customer will receive the OTP during checkout to their registered email address and through SMS on their registered mobile number.



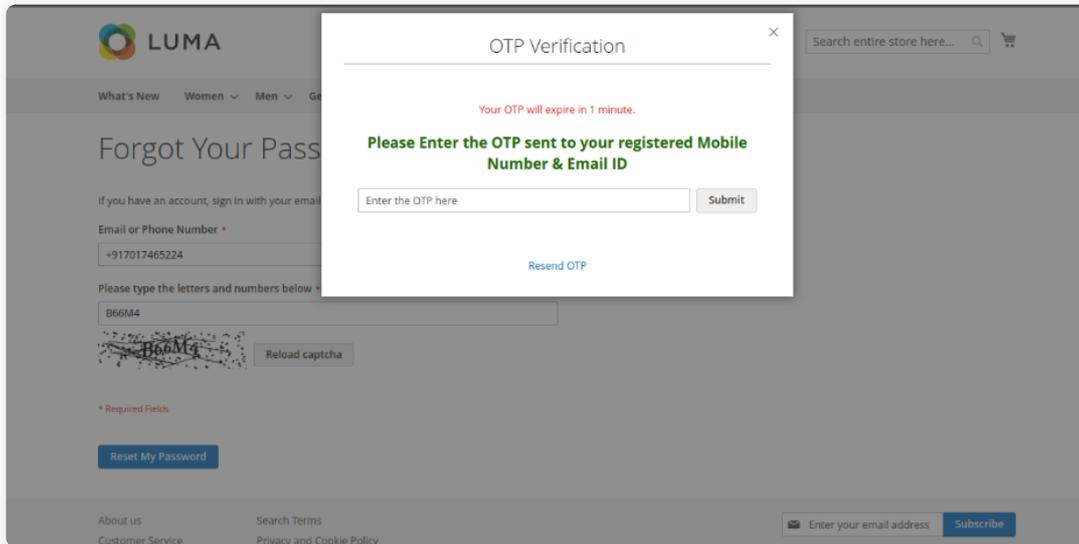
One Time Password Generation (During Sign-In)-Through Both

At the time of login, customers will receive the OTP through SMS on their mobile number and their registered email address also.



One Time Password Generation (If Forget The Password)-Through Both

In this case, the customer will receive the OTP to their registered email address as well as on their mobile number through SMS if they forget their password.



So, that's all for the **One Time Password(OTP) Module**. Still, if you have any issues, feel free to add a ticket at webkul.uvdesk.com.

Current Product Version - 5.0.1

Supported Framework Version - Magento 2.4.x