



Google Authenticator Plugin for nopCommerce

Plugin Documentation

Contents

Features	3
Customer Account Setup	4
Error Codes	5
Force Authentication	6
Force MFA Customer Role	6
Installing the Plugin	8
Configure Settings	8
Contact Us	9

Google Authenticator Plugin Documentation


This plugin provides stronger security by requiring a second step of verification when you log in. The plugin uses Google Authenticator App to allow a customer to setup two-factor authentication for registration and login.

Features

- Does not require any Google Configuration
- Customer Setup using QR Code
- Allow the use of a backup code for which is emailed in case Authenticator App not available
- Customer can disable use at anytime, or
- Force Authentication for Customers in a specific Role (also works with Google Authenticator)
- Trust Authentication for X number of Days

MULTI-FACTOR
AUTHENTICATION

Please download the Google/Microsoft Authenticator App to scan this QR code. If you cannot scan the QR code then you can manually input the key beside it



Key: 6GO5KR7A6HMPGHAUT3SQGOSGPKJPE6L4

Please enter the code you received from authenticator app.

Authenticator Code:

CONFIRM

Welcome, Please Sign In!

Please Enter the code from your authenticator app

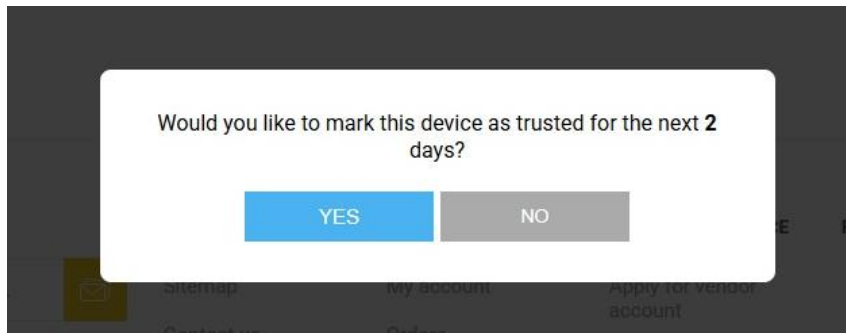
Authenticator Code:

Can't access your authenticator app? [Use a backup code](#)

CONFIRM

Trust Authentication

The customer can decide to trust Authentication for X number of days



Customer Account Setup

My account

- Customer info
- Addresses
- Orders
- Downloadable products
- Back in stock subscriptions
- Reward points
- Change password
- My product reviews
- [Multi-factor authentication](#)

My account - Multi-factor authentication

To activate multi-factor authentication for your account, you need to:

1. Activate the 'Is enabled' setting.
2. Choose one of the multi-factor authentication providers.
3. Save.
4. Configure the selected multi-factor authentication provider by following the instructions on the individual settings page of the selected provider.



Changing Providers: To change the provider, first uncheck 'Is enabled' then click **Save** then follow the instructions above.

WARNING: After saving the selected provider, be sure to configure it, otherwise you will be denied access the next time you try to enter your account.

Settings

Is enabled: ☒

Authentication providers

	
<p><input checked="" type="radio"/> Google Authenticator Google Authenticator is a software-based authenticator that implements two-step verification services for authenticating users. To configure the authenticator app, please click the Config button below.</p>	<p><input type="radio"/> Microsoft Authenticator Microsoft Authenticator is a software-based authenticator that implements two-step verification services for authenticating users. To configure the authenticator app, please click the Config button below.</p>
CONFIG	CONFIG

Welcome, Please Sign In!

Please Enter the code from your authenticator app

Authenticator Code:

Can't access your authenticator app? [Use a backup code](#)

CONFIRM

Invalid token or its lifetime has expired.



Force Authentication

The plugin has an option to Force Authentication for specific customers. This option is provided by the Microsoft Authenticator Plugin so you need to have this plugin installed to enable this option.

Force MFA Customer Role

You can define a particular Customer Role and then add customers for whom you want to force authentication to this role.

For example, a role called Member

Edit customer role details - Member [← back to customer role list](#)

Name ?	<input type="text" value="Member"/>
Active ?	<input checked="" type="checkbox"/>
Free shipping ?	<input type="checkbox"/>
Tax exempt ?	<input type="checkbox"/>
Override default tax display type ?	<input type="checkbox"/>
Enable password lifetime ?	<input type="checkbox"/>
Purchased with product ?	<button>Choose a product</button>
Is system role ?	<input checked="" type="checkbox"/> Yes
System name ?	<input type="text" value="Member"/>

Then in the Access Control List add the role to the Permission

Security. Enable multi-factor authentication

Access control list is a list of permissions attached to customer roles. This list specifies the access rights of users to objects. Learn more about [access control list](#)

	Category of permissions
▶	Security
Permission name	Customer roles
Access admin area	Administrators, Vendors, System Manager, Manager
Security. Enable Multi-factor authentication	Member

Previous 1 Next

Customers will then be forced to Setup Multifactor Authentication for their account

My account

Customer info

Addresses

Orders

Downloadable products

Back in stock subscriptions

Reward points

Change password

My product reviews

Multi-factor authentication

My account - Multi-factor authentication

To activate multi-factor authentication for your account, you need to:

1. Activate the 'Is enabled' setting.

2. Choose one of the multi-factor authentication providers.

3. Save.

4. Configure the selected multi-factor authentication provider by following the instructions on the individual settings page of the selected provider.

Changing Providers:

To change the provider, first uncheck 'Is enabled' then click **Save** then follow the instructions above.


WARNING:

After saving the selected provider, be sure to configure it, otherwise you will be denied access the next time you try to enter your account.

Settings

Is enabled: ☒


Authentication providers



☒ **Google Authenticator**

Google Authenticator is a software-based authenticator that implements two-step verification services for authenticating users. To configure the authenticator app, please click the Config button below.

CONFIG



☐ **Microsoft Authenticator**

Microsoft Authenticator is a software-based authenticator that implements two-step verification services for authenticating users. To configure the authenticator app, please click the Config button below.

CONFIG

From this view the Customer must setup MFA using one of the options

Select Systems International

Page | 7

Installing the Plugin

The zip package supplied can be uploaded and installed using the “Upload plugin or theme” button on the Configuration > plugins page.

Refer to Then the installation of the plugin follows the standard nopCommerce procedure.

See <https://docs.nopcommerce.com/user-guide/configuring/system/plugins.html>

Alternatively, you can manually install the plugin:

1. Copy the Plugin to the correct directory
2. Restart the Application – Click the Icon in the top

Once installed the you can configure the plugin.

Configure Settings

Configure - Authenticator

[back to multi-factor authentication method list](#)

To use Microsoft Authenticator, the app is first installed on a smartphone. The plugin provides a shared secret key to the user over a secure channel, to be stored in the Microsoft Authenticator app. This secret key will be used for all future logins to the site.

Business prefix ?

Select Systems v48 Demo Store

QRPixelsPerModule ?

3

Trusted Device Days ?

2

Save

Q Search

Search

Email ?

Q Search

Customer	Delete
steve_gates@nopCommerce.com	<div>Delete</div>
james_pan@nopCommerce.com	<div>Delete</div>

Previous

1

Next

1-2 of 2 items

The settings for the plugin can be set using the configure page.

Business prefix

Enter the Identification Information for the login to be stored in a customer’s Google Authenticator

QRPixelsPerModule

Sets the number of pixels per unit. The module is one square in the QR code. By default, the value is set to 3 for a 171x171 pixel image.

Trusted Device Days

Specify the number of days to trust this device so the authentication code is not required during that period.

Contact Us

If you have any more questions or would like to make suggestions on how to make the plugin operations more functional please email: sales@selectsystems.com.au