

amasty

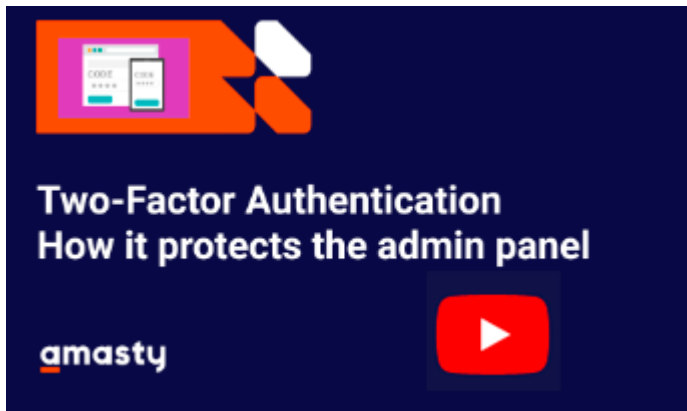
For more details see how the [Two-Factor Authentication for Magento 2](#) extension works.

Ultimate Guide for Magento 2 Two-Factor Authentication

Protect your Magento e-business with simple and efficient Two-Factor Authentication extension for Magento 2. Make sure your account is available to verified users only.

- Apply 2-step verification
- Provide full protection from spyware
- Include the necessary IP addresses in the white list
- Configure flexible settings for each user role
- Set your device as the key to the account


See how Two-Factor Authentication protects your backend and how to configure it:



General Settings

To configure the extension, go to **Admin panel** → **System** → **Configuration** → **Two-Factor Authentication**.

General Settings

| | |
|--|--|
| Enable Two-Factor Authentication <small>[global]</small> | <input type="text" value="Yes"/> |
| Discrepancy <small>[global]</small> | <input type="text" value="1"/>  |
| Please read here how to use this setting. | |
| Ip White List <small>[global]</small> | <input type="text" value="192.168.1.2"/> |
| Specify IP addresses separated by comma. | |

Enable Two-Factor Authentication - Set to *Yes* to enable two-factor authentication extension on your Magento account.

Note, that this will activate the request for additional security code next time you log in.

Discrepancy — modify the allowed time drift in 30 second units (e.g. 8 means 4 minutes before or after) for verification codes generation.

You can modify the interval for verification codes generation when a user faces an error.

IP White List - In this field, you can include reliable IP addresses. Users, who log in from these IP addresses will not be required for verification code (e.g. your staff members). You can add multiple IPs, separating them with coma.

User Roles

Go to **System** → **Permissions** → **Users** to set admins' permissions.

[Add New User](#)

[Search](#) [Reset Filter](#)

2 records found per page [<](#) of 1 [>](#)

| ID | User Name ↓ | First Name | Last Name | Email | Status |
|--------------------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 1 | admin | admin | admin | admin@amasty.com | Active |
| 4 | NY Admin | NY Admin | NY Admin | test@example.com | Active |

Edit any existing role by clicking it or create a new one using **Add New User** button.

Open the **Two-Factor Settings** tab to configure and synchronize the extension with the Google authentication app. The application generates additional security codes.

admin admin

← Back Delete User Reset Force Sign-In **Save User**

USER INFORMATION

User Info

User Role

Two-Factor Settings

General

Enable TFA

Status Not Configured

Secret Key W023444078800007
Insert this secret key into Google Authenticator or scan QR code to generate Security Code



Security Code
Scan QR code above with Google Authenticator application, then enter the security code in this field and click Check Code link

Security Code [Check Code](#)

Enable TFA - Open your [Google Authenticator application](#) and register the login by scanning the QR Code or entering the Secret Key.

Status - the default status is *Not Configured*. It will be switched to *Configured*, once you enter a Secret Key or scan the QR code.

Secret Key - Insert the *Secret Key* into Google Authenticator app to generate additional *Security Code*.

QR code - Scan *QR code* to receive the *Secret Key* and insert it into Google Authenticator app to generate additional *Security Code*.

Security code - Insert your received *Security Code* and click *Check code* to verify it. **Verify** - If *Security Code* is correct, then *Check code* link will be changed to *Verified*.

Once your [Google Authenticator application](#) is properly configured and synchronized, it will show a onetime passcode that changes every 30 seconds.

Press *Save User* button. The user will now be required to enter one-time security code when logging in admin panel.

Troubleshooting

When the verification returns the **Invalid** value, you can fix this by modifying the **Discrepancy** value in the extension [general settings](#).

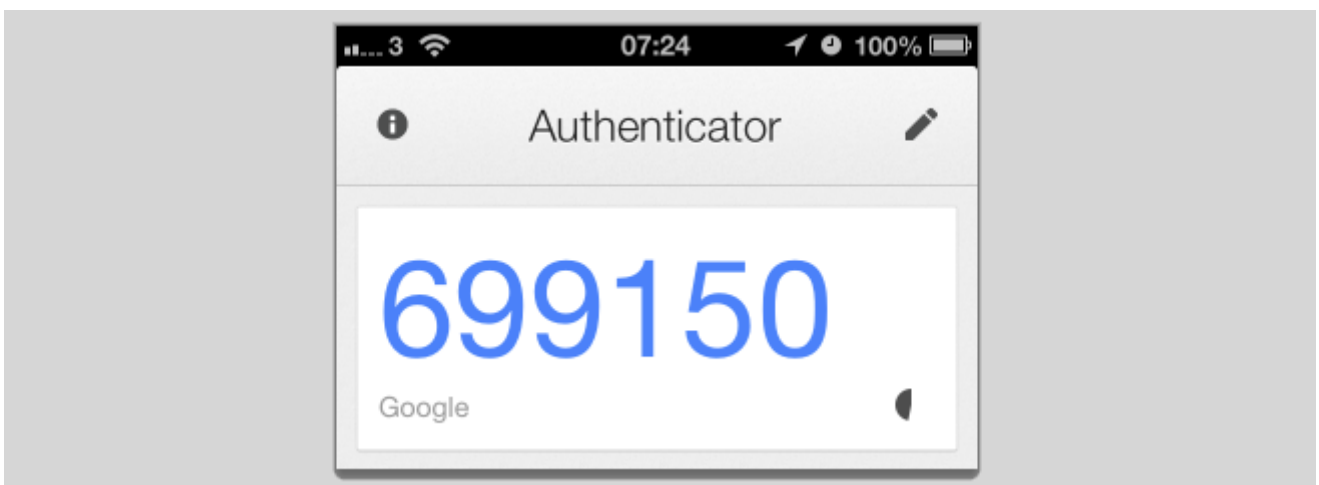
Try increasing the value by 1, save changes, and try the verification procedure once again. If you'll face the Invalid value again, please, try to increase a discrepancy one more time.

Testing two-factor authentication

To test, whether the extension was successfully synchronized with Google Authenticator App and well configured, log out from your current session and try to log in to the account you have configured.



This is how Google Authenticator App generates the security code.



Find out how to install the **Two-Factor Authentication** extension for Magento 2 via [Composer](#).

From:
<https://stg.amasty.net/docs/> - **Amasty Extensions FAQ**

Permanent link:
https://stg.amasty.net/docs/doku.php?id=magento_2:two-step_authentication



Last update: **2020/11/30 12:45**