
amasty

For more details see the Two-Factor Authentication extension page.

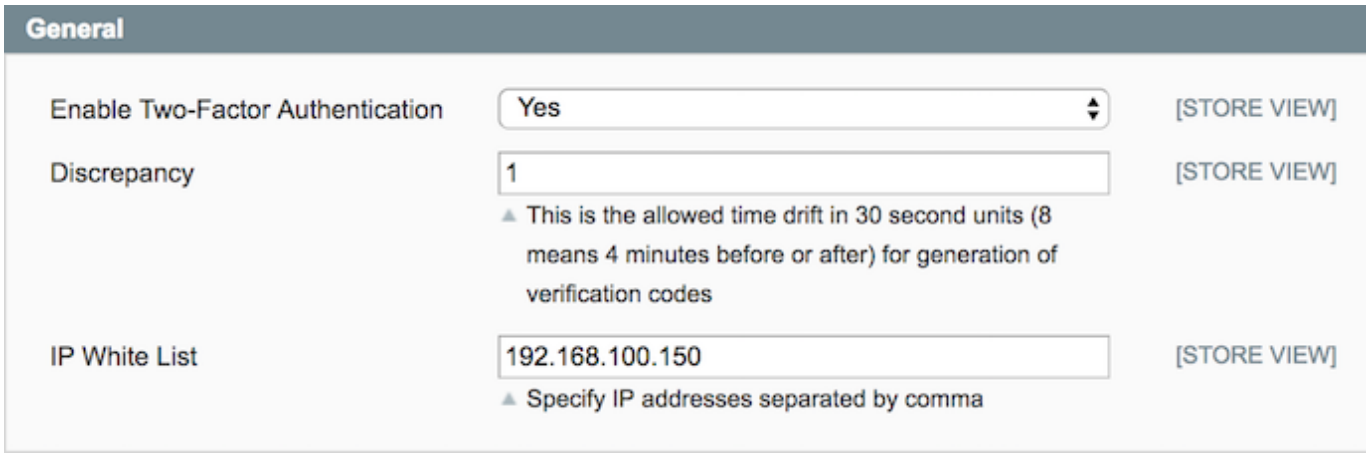
Two-Factor Authentication

Keep your Magento store protected from key loggers, network data sniffers, unsecured Wi-Fi connections, and other possible threats. Use security code in addition to your password to increase the security level.

- Login to Magento admin panel securely
- Avoid connection sniffing
- Stay protected from spyware
- Utilize white list for trusted IP addresses

Extension Configuration

To configure the extension general settings please go to **System → Configuration → Amasty Extensions → Two-Factor Authentication**.



Enable Two-Factor Authentication — use this option to enable or disable two-factor authentication;

Discrepancy — specify the allowed time drift in 30 second units (8 means 4 minutes before or after) for verification codes generation;

IP White List — specify IP addresses separated by commas that will be granted access without two-factor authentication.

Troubleshooting

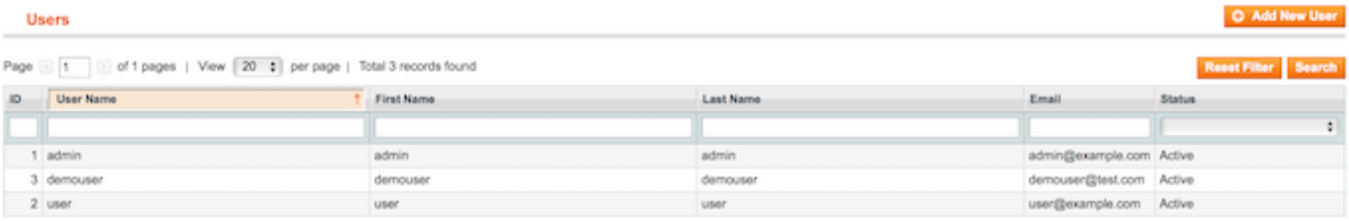
If you are using the old Magento version, you need to replace the **login.phtml** file (Magento_root/app/design/adminhtml/default/default/template/login.phtml) with the attached one.

Please, unzip it before replacing:

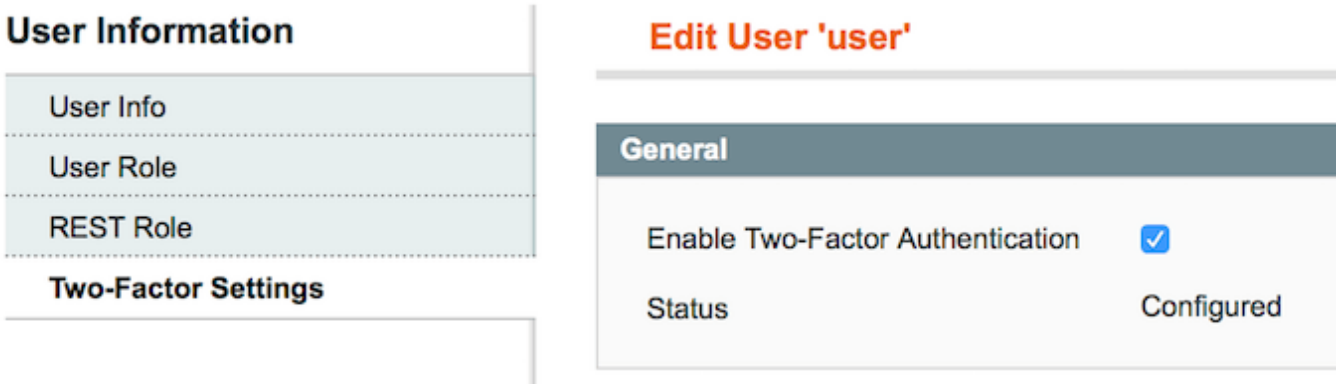
login.phtml

Configuring Two-Factor Authentication per User

Please go to **System → Permissions → Users** and select a user you want to add two-factor authentication to.

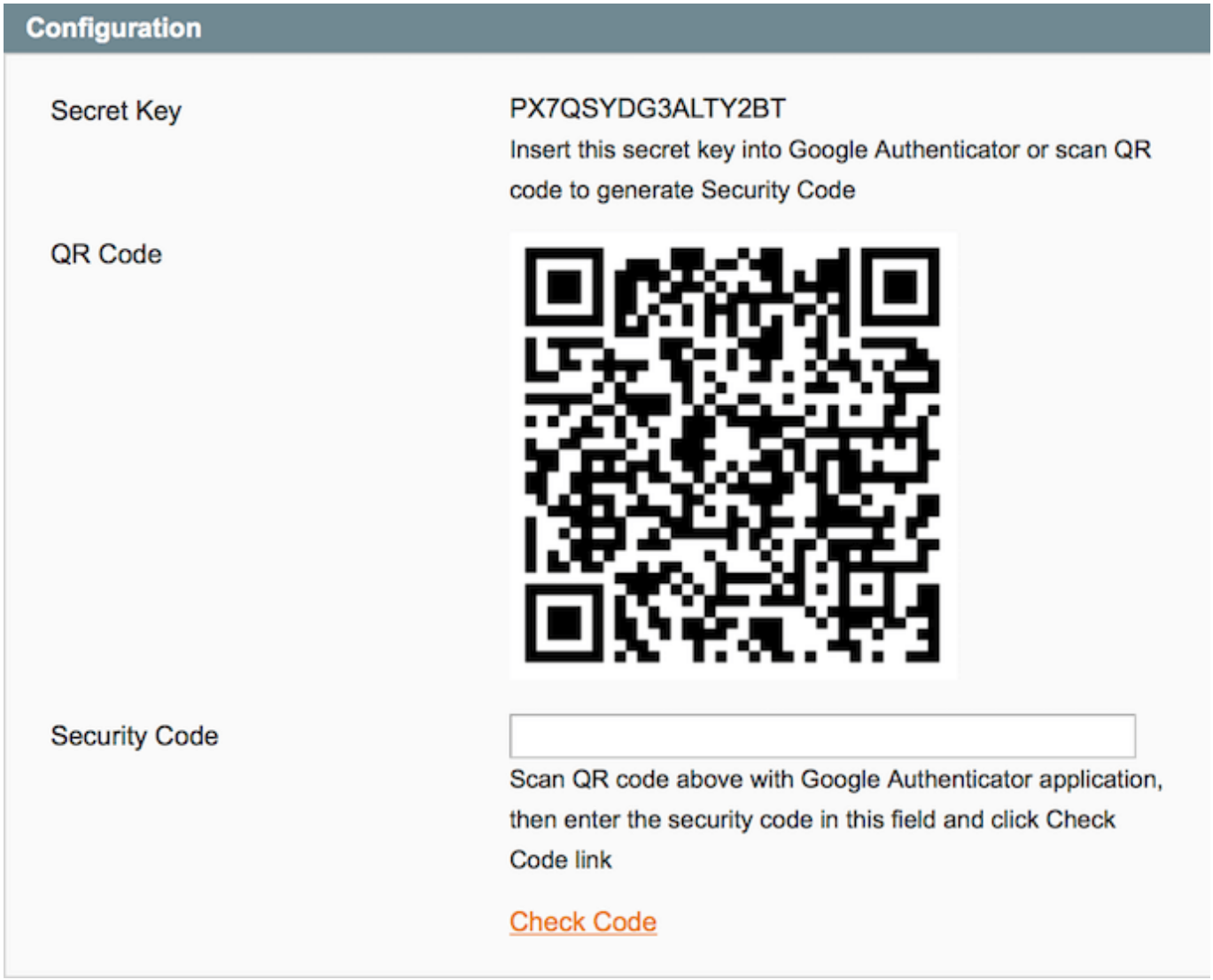


Switch to the **Two-Factor Settings** tab. Then, tick the Two-Factor Authentication checkbox.



When done, open your **Google Authenticator** application and register the login by scanning the QR Code or entering the Secret Key. Once your Google Authenticator application is properly configured it will show a one- time passcode that changes every 30 seconds. Fill it in the **Security Code** field, and click the **Check Code** link.

The status should change to **Verified**.



Now, press the **Save User** button. If the entered verification code is correct the form will be saved. The user will now be required to enter one-time security code when logging in to admin panel.

Troubleshooting

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

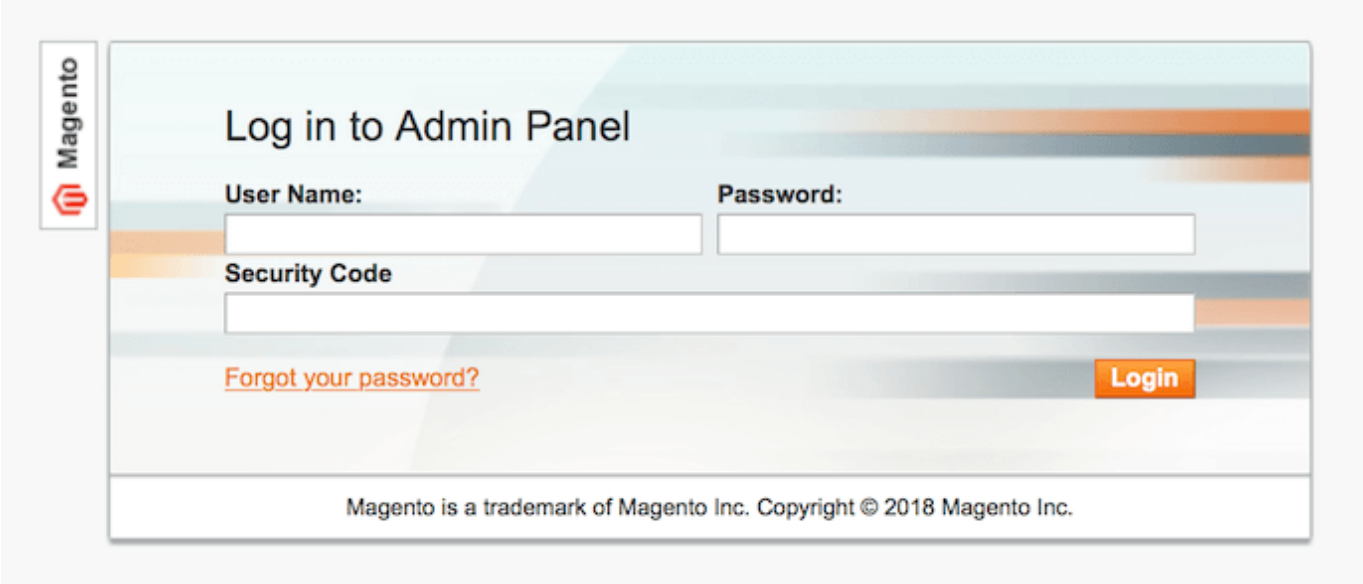
Try increasing the value by 1, save changes, and try the verification procedure once again. If you'll face the Invalid value again, please, try to increase a discrepancy one more time.

Testing Two-Factor Authentication

To test two-factor authentication you will need to login.

1. Log out of the admin area;

2. Go to the administrative login screen;
3. Login with the account you have configured to use two-factor authentication.



Troubleshooting

In case you have lost the authenticated device and can't login to the admin panel, there is a solution:

1. Open the *admin_user* database table and find your account using the username or email. You can use one of the following SQL requests to find the required information:

```
SELECT `user_id` FROM `admin_user` WHERE `email` = 'your_email_address'
```

or

```
SELECT `user_id` FROM `admin_user` WHERE `username` = 'your_username';
```

2. Copy your user_id.

3. Execute the following request to the database:

```
UPDATE `amasty_securityauth_admin_user` SET `enable` = 0 WHERE `user_id` =
specify_your_user_id_here;
```

4. Next, clear the cache: var/cache/* or execute this command if you are using redis: redis-cli flushall

5. Now, you can login to the admin panel of your store and get access to your admin account. Here, you can enable the two-factor authentication for a new device.