

**A**masty

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**.

### Two-Factor Authentication

The screenshot shows the configuration interface for the Two-Factor Authentication extension. It features a 'General' tab. Under this tab, there are two main settings: 'Enable Two-Factor Authentication', which is currently set to 'Yes' via a dropdown menu, and 'Ip White List', which is a text input field containing '10.12.10.1'. Below the input field, there is a tooltip with an upward-pointing triangle and the text 'Specify IP addresses separated by comma'.

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

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

## Configuring Two-Factor Authentication per User

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

**Users** Add New User

Page 1 of 1 pages | View 20 per page | Total 3 records found Reset Filter Search

ID	User Name	First Name	Last Name	Email	Status
1	admin	admin	admin	admin@example.com	Active
3	demouser	demouser	demouser	demouser@test.com	Active
2	user	user	user	user@example.com	Active

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

### User Information

- User Info
- User Role
- REST Role
- Two-Factor Settings**

### Edit User 'user'

**General**

Enable Two-Factor Authentication

Status Configured


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**.

### Configuration

**Secret Key** PX7QSYDG3ALTY2BT  
Insert this secret key into Google Authenticator or scan QR code to generate Security Code

**QR Code**



**Security Code**

Scan QR code above with Google Authenticator application, then enter the security code in this field and click [Check Code link](#)

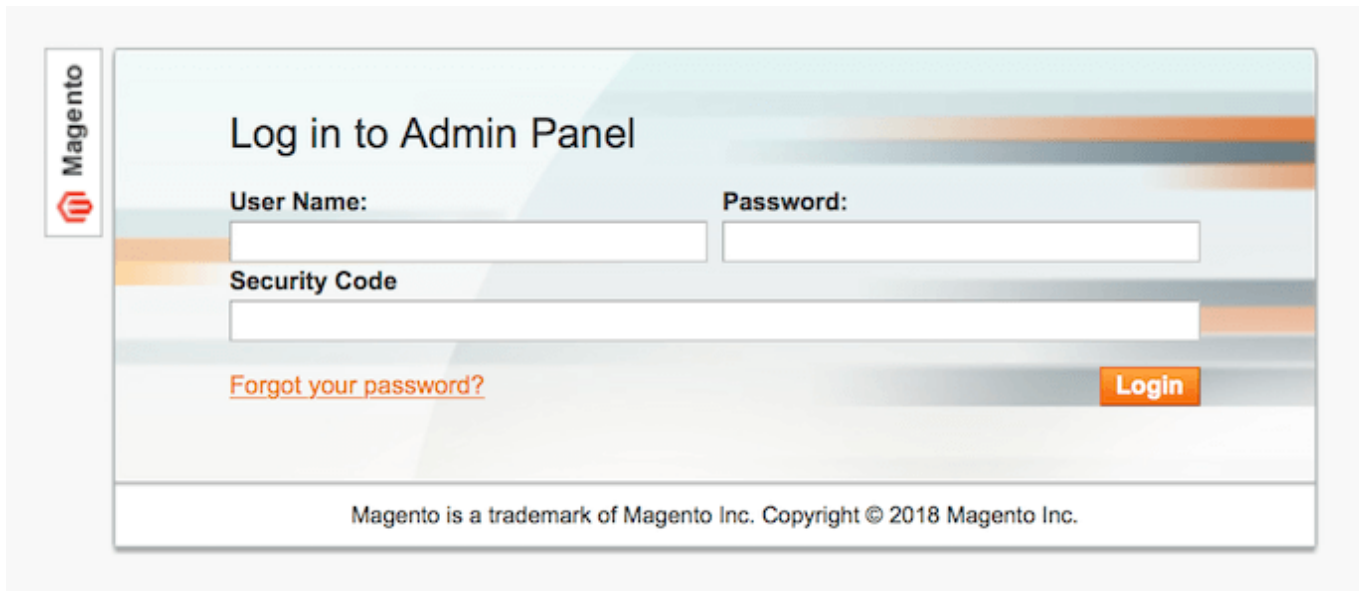
[Check Code](#)

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.

## 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.



Rate the user guide

☆☆☆☆☆ from 0 votes ([Details](#))

○ ○ ○ ○ ○

★☆☆☆☆ 0 visitor votes

★★☆☆☆ 0 visitor votes

★★★☆☆ 0 visitor votes

★★★★☆ 0 visitor votes

★★★★★ 0 visitor votes

From:

<https://amasty.com/docs/> - **Amasty Extensions FAQ**

Permanent link:

[https://amasty.com/docs/doku.php?id=magento\\_1:two-step\\_authentication](https://amasty.com/docs/doku.php?id=magento_1:two-step_authentication)

Last update: **2018/01/16 12:35**

