

Aitoc



Two-Factor Authentication

User Manual for Magento 2

Table of Contents

1. Installing Two-Factor Authentication in Magento 2.
2. User-specific configuration.
3. Setting up user authentication options.
4. Whitelisting trusted IPs.
5. Admin login procedure.

1. Unzip and paste the extension file into your root Magento folder.

2. Connect to your server by SSH.

3. Go to your Magento root folder.

4. To install the extension, perform this command:

```
php bin/magento setup:upgrade
```

5. Reset JavaScript cache by removing all folders in pub/static:

```
_requirejs; adminhtml; frontend.
```

6. To switch the extension on/off, perform these commands:

```
php bin/magento module:enable Aitoc_TwoFactorAuthentication
```

```
php bin/magento module:disable Aitoc_TwoFactorAuthentication
```

You can activate/deactivate several Aitoc extensions at once by specifying their names separated by space in the command.

Users

Navigate to System > Permissions > All Users and click the specific user to start configuring authentication settings.

Add New User

Search [Reset Filter](#) 6 records found 20 per page 1 of 1

ID	User Name	First Name	Last Name	Email	Status
1	admin	Dave	Berger	main_admin@example.com	Active
2	Brand_Manager	Kevin	Smiths	brand_manager@example.com	Active
7	ger_admin	Dan	Simmons	de_admin@example.com	Active
6	fradmin	Pitt	Smiths	fr_admin@example.com	Active
4	content_manager	Jesse	Lee	jesse@example.com	Active
5	sales_manager	Mario	Avanti	mario@example.com	Active



Enable the preferred verification method. You can also activate both methods. Please use only one of them when you log in.

← Back

Delete User

Reset

Force Sign-In

Save User

USER INFORMATION

TFA Settings

IP Restriction

User Info

User Role

User Two-Factor Authentication Settings

Email Verification

Mobile Device Verification

Note: When both verification are enabled upon logging in to the

Change the default field value if custom time (not the time zone!) is manually set on your mobile device.

Time difference between your device and the server may cause a one-time password mismatch. Otherwise leave this field unchanged.

Server Time Correction (Server Time: 10:09:35)

Attention: You can use this option only in case if you manually changed time (not time zone!) on your mobile device. Please note that time differences between the server and your device can cause a one-time password mismatch.

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

Select the Email Verification method to receive email messages with authentication codes. One-time passwords will be sent to the email address specified in user account settings.

USER INFORMATION Authentication Settings

TFA Settings 

IP Restriction

User Info

User Role

Email Verification

Mobile Device Verification


Server Time Correction (Server Time: 10:09:35)

Note: When both **mobile device verification** and **email verification** are enabled, you can use any of the verification options upon logging in to the Admin panel.

Attention: You can use this option only in case if you manually changed time (not time zone!) on your mobile device. Please note that time differences between the server and your device can cause a one-time password mismatch.

Enable Mobile Device Verification to generate one-time passwords in the mobile authentication app. We recommend using Google Authenticator for mobile verification.

USER INFORMATION

- TFA Settings 
- IP Restriction
- User Info
- User Role

User Two-Factor Authentication Settings

Email Verification

Mobile Device Verification

Sync the extension with the mobile authentication app before the first use of the mobile verification method.


Note: When both **mobile device verification** and **email verification** are enabled, you can use any of the verification options upon logging in to the Admin panel.

Server Time Correction (Server Time: 11:28:59)

Attention: You can use this option only in case if you manually changed time (not time zone!) on your mobile device. Please note that time differences between the server and your device can cause a one-time password mismatch.

To link the mobile device to your admin account, you need to either enter the Secret Key manually or scan the barcode.

Secret Key



To test the app, enter the generated verification code in the "Password" field. Then click the "Save User" button at the top of the page to finish the synchronization process.

One-Time Password Verification

Password *

Add the secret key to your mobile app and enter a one-time password to verify the settings.



Add authorized IP addresses to the whitelist to secure the Admin account. Separate IPs with a space.

← Back

Delete User

Reset

Force Sign-In

Save User

USER INFORMATION

TFA Settings

IP Restriction

User Info

User Role


Admin IP Restrictions

Whitelisted IPs

Use a **space** to separate IPs. Example: 192.168.135.65 192.168.18.230
Leave empty for access from any location.

Your Current IP

192.168.90.93

 **Magento**

Welcome, please sign in

* Username

* Password

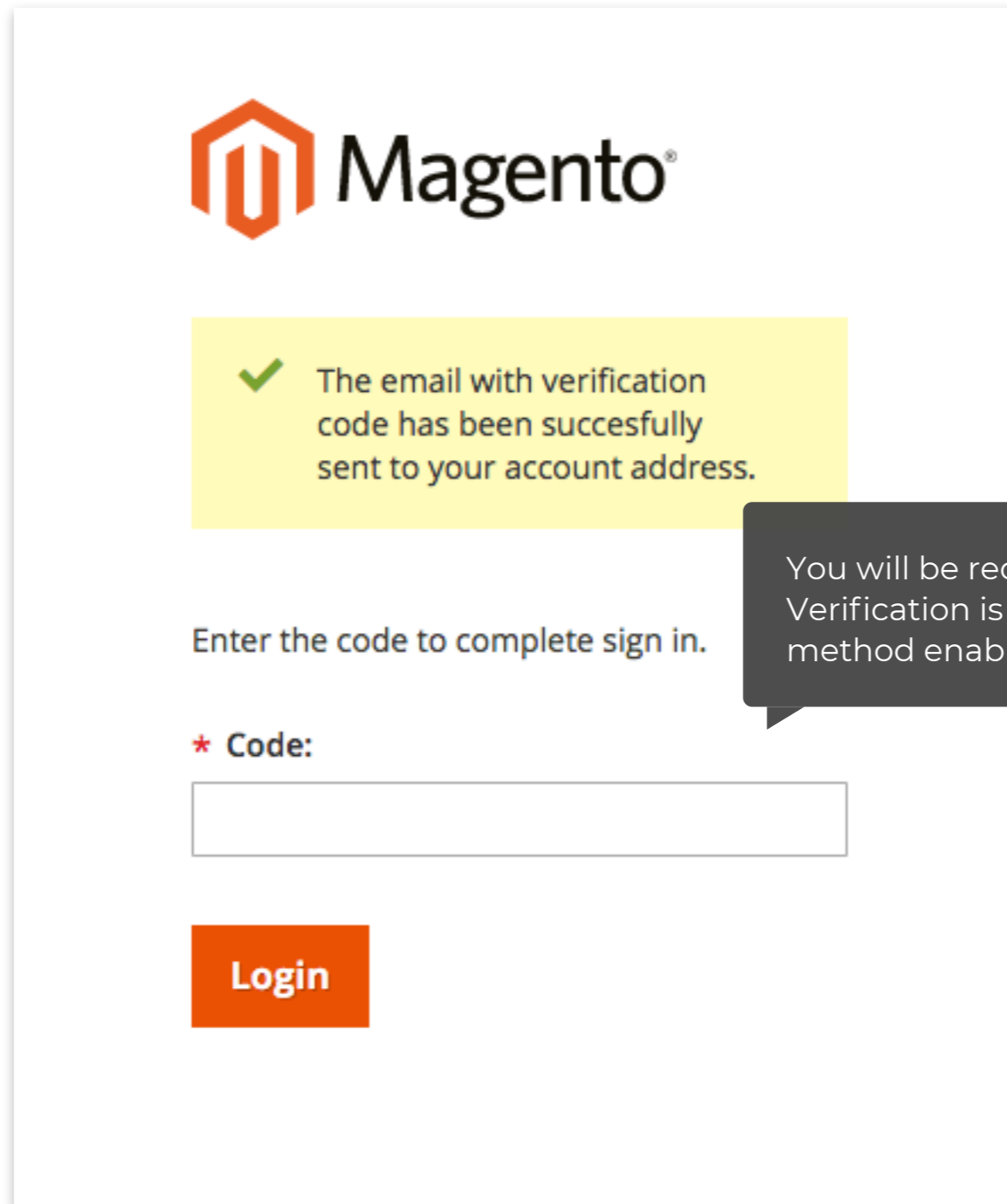
One-Time Password

Enter a code from your device or leave the field blank if not configured.

[Forgot your password?](#)

Sign in

To log in to your admin account, enter the one-time password generated by the mobile device or the one sent to your email address. Leave the field blank if both user verification options are disabled in the Admin panel.



The screenshot shows the Magento admin login interface. At the top left is the Magento logo. Below it is a yellow notification box with a green checkmark and the text: "The email with verification code has been successfully sent to your account address." Below the notification is the instruction "Enter the code to complete sign in." followed by a red asterisk and the label "Code:". Underneath is an empty text input field. At the bottom is an orange "Login" button.

You will be redirected to this page if Email Verification is the only user authentication method enabled.

Brought to you by

Aitoc

You can purchase **Two-Factor Authentication** at
www.aitoc.com

For questions please email us at sales@aitoc.com