

Two Factor Authentication

Dss

- **How Does It Work?**

Navigate to System > Permissions > All Users

Users

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

Add New User

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

| 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 |

- **Configuring user authentication options**

Navigate to User > TFA Settings

Admin

Enable the preferred verification method. You may also activate both methods. Please use only one of the 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 Disable

Mobile Device Verification Disable

Note: When both verification are enabled upon logging in to the system, the user will be prompted to verify their identity using both methods.

Server Time Correction +00 h (Server Time: 10:09:35)

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

Time difference between your device and the server may cause a one-time password mismatch. Leave this field unchanged in any other cases.

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.

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

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


We recommend keeping both authentication methods enabled. That way you will always have an option to choose which method to use.

The screenshot shows the 'User Two-Factor Authentication Settings' page. On the left is a sidebar with 'USER INFORMATION' and 'TFA Settings' (selected). The main content area has two sections: 'Email Verification' with a 'Disable' dropdown, and 'Mobile Device Verification' with an 'Enable' dropdown. A callout bubble points to the 'Mobile Device Verification' dropdown with the text: 'Sync the extension with the mobile authentication app before the first use of the mobile verification method.' Below these is a 'Note' about using both methods and an 'Attention' warning about time zone differences. There is a time zone selector set to '+00 h' (Server Time: 11:28:59). A 'Secret Key' field contains '624AJDQ7ZKEOKEN' and a QR code. A callout bubble points to the QR code with the text: 'To link the mobile device to your admin account, you need to either enter the Secret Key manually or scan the barcode.' Below the QR code is a 'One-Time Password Verification' section with a 'Password' input field. A callout bubble points to this field with the text: '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.'

- **Whitelisting trusted IPs**
Navigate to User > IP Restriction

The screenshot shows the 'Admin IP Restrictions' page. At the top is an 'Admin' header with a search icon, a notification bell with '2', and a user profile 'admin'. Below the header are buttons: 'Back', 'Delete User', 'Reset', 'Force Sign-In', and 'Save User'. The main content area has a sidebar with 'USER INFORMATION' and 'IP Restriction' (selected). The main content area has a 'Admin IP Restrictions' section with a text input field. A callout bubble points to this field with the text: 'Add authorized IP addresses to the whitelist to secure the Admin account. Separate IPs with a space. All IPs must be static for this option to work properly. If some of the IPs are dynamic, the respective admins will not be able to access their accounts.' Below the input field is a note: 'Use a space to separate IPs. Example: 192.168.135.65 192.168.18.230. Leave empty for access from any location.' At the bottom, there is a 'Your Current IP' field showing '192.168.90.93'.

- Admin login procedure

 **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.

 **Magento®**

✓ The email with verification code has been successfully sent to your account address.

Enter the code to complete sign in.

* Code:

Login

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