



## TWO-FACTOR AUTHENTICATION

Version 1.1.1



User Guide for Magento 1.9



## Table of Contents

1	.....	The MIT License
2	.....	About JetRails 2FA
4	.....	Installing JetRails 2FA
5	.....	Setting Up 2FA Account
6	.....	Authenticating After Login
7	.....	Configuring 2FA Settings
8	.....	Managing 2FA Accounts
9	.....	Account Blocking
10	.....	Account Recovery Using Database (Advanced)
11	.....	Feature Request / Bug Submission
12	.....	JetRails Security Assessment



## The MIT License

Copyright 2017 JetRails®

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.



## About JetRails 2FA

Your Magento storefront is vulnerable. Eliminate your security risk by downloading the JetRails Two-factor authentication module. Two-factor authentication, also known as 2FA, is a critical component for Magento security and is used widely by Magento backend admin users. Authentication is a security process to verify a user's identity. Authentication consists of three factors; something they know (ie. password), something they have (ie. phone), or something they are (ie. fingerprint).

With a stock Magento installation a user is only given one method of authentication -- something they know. This usually consists of their administrative username and password. While having one method of authentication is typically secure, it has its limitations. By adding one additional layer of authentication, security is significantly strengthened. Having multiple methods of authentication is known as multi-factor authentication. It is often recommended that you choose at least two out of the three methods of authentication to ensure strong security.

This plugin works with "something they know" and "something they have". A Magento admin user that has the JetRails 2FA plugin enabled will not only be authenticated with "something they know", which would be their admin username and password, but they will also authenticate with "something they have", such as their phone or tablet.

Once the JetRails 2FA plugin is installed for your Magento store and an admin successfully logs into their account, the JetRails 2FA plugin will prompt the user to set up their 2FA account. The typical user enrollment process takes up to five minutes including installation of the Google Authenticator application on their device.

2FA has become an industry standard and is implemented using the Time-Based One-Time Password (TOTP) algorithm. In developing this plugin, RFC-6238 was used for reference. Since 2FA gives an extra layer of protection to Magento's authentication process, it is vital to every Magento installation.



## About JetRails 2FA (continued)

**This plugin comes with the following features and benefits:**

- A Master Administrator can require 2FA to be utilized by specific users.
- Usage of 2FA can be enforced and required for log in.
- Once you use the 2FA to log in, there is an option to bypass authentication for a pre-configured number of days.
- A Master Administrator can oversee every user's authentication process.
- In the event of lost or misplaced 2FA account, backup codes are available as an alternate method for authentication.
- In the event of an attempted account breach, prevention protocols are in place via brute-force protection, which will temporarily block the account.
- The threshold for the number of failed authentication attempts before a temporary ban is imposed is configurable.
- The duration of a user's temporary ban is configurable.
- An automatic instantaneous alert will be sent to the account owner and store admins informing them of an attempted breach. Any security warning will be logged with any relevant data such as the offender's IP address.
- The 2FA account can be setup for devices (something they have) using the Google Authenticator app, which is available for every platform including iPhone and Android.



## Installing JetRails 2FA

### STEP #1

Download TGZ archive file that contains the JetRails Two-Factor Authentication module from the Magento Marketplace.

### STEP #2

Place it into the desired Magento installation directory. This should be at the same level as the app and skin folders.

### STEP #3

While in the Magento installation directory, extract the archive containing the module. This will extract the module's contents into the Magento installation.

### STEP #4

Go to the Magento store's backend and login using an admin account that has permission to clear the cache.

### STEP #5

Using the navigation menu go to System > Cache Management

### STEP #6

Click on the Flush Cache Storage button, on confirmation click Ok

### STEP #7

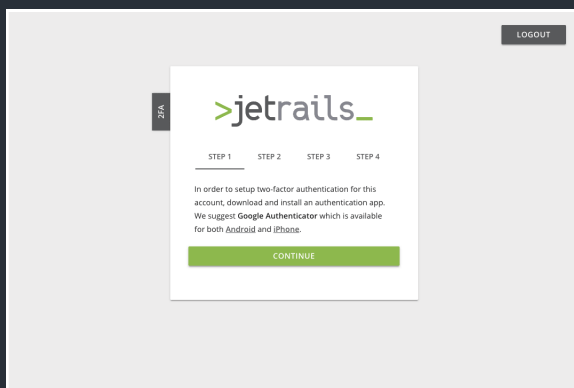
The module is now installed. By default, all users are required to setup 2FA. Everyone who is logged in or will login will be redirected to the 2FA setup page.

## Setting Up 2FA Account

If 2FA is not setup for a user, then the user will be redirected to the 2FA setup page upon successful login. Below are all the steps that need to be taken to setup a 2FA account. Each stage in the 2FA setup process should provide detailed information on how to proceed with the setup.

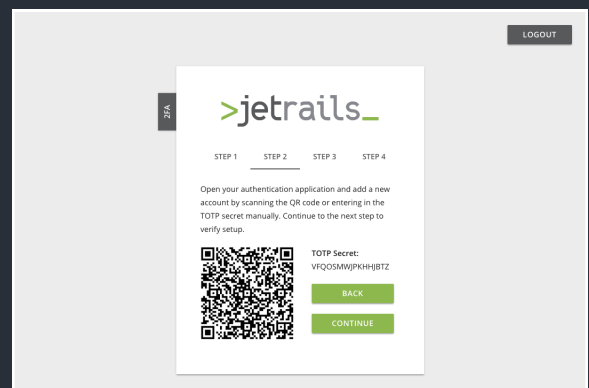
### STEP #1

Follow instructions to install an authentication application, then click CONTINUE.



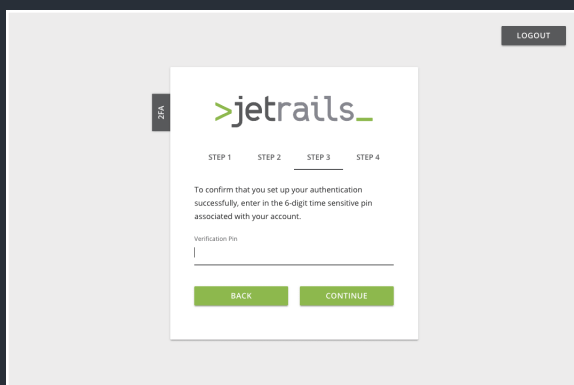
### STEP #2

Follow instructions to setup authentication account, then click CONTINUE.



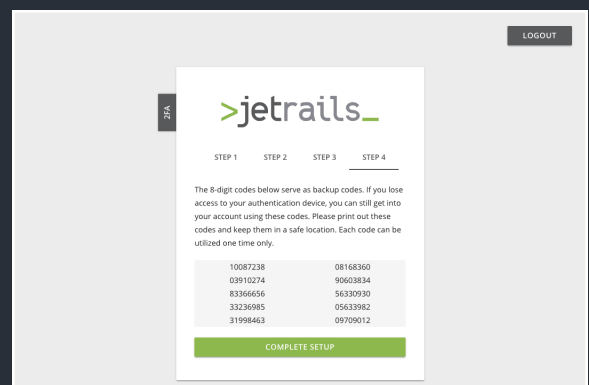
### STEP #3

Enter verification pin to ensure that TFA account is set up correctly, then click CONTINUE.



### STEP #4

Save backup codes in case you lose access to authentication app, then click COMPLETE SETUP.



## Authenticating After Admin Login

Once an admin user sets up their authentication account and logs in successfully, they will be greeted with a verification page. The user can choose to authenticate using a 6 Digit Pin or a Backup Code.

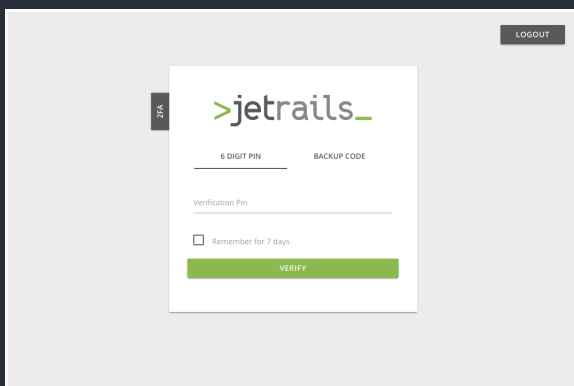
It is important to note that the admin user will have a total of 10 authentication attempts, independent from method used, until they are blocked. An authentication block lasts 10 minutes; after the block expires, the user can attempt to authenticate their login again.

The user also has an option to remember the authentication for 7 days. This will create a cookie and so long as the user is logged in on the same device with the same IP address, they will be authenticated automatically without the need to enter a verification pin or backup code.

Backup codes are used when your authentication device is unavailable. It is recommended that a user resets their account if they lose their authentication device. Please remember that once all the backup codes are used up, you will have no other option than to use the verification pin.

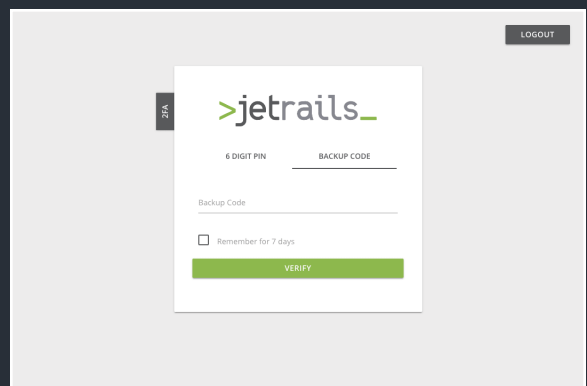
### Verification Pin

Authenticate normally using your accounts 6 Digit Pin.

A screenshot of the authentication interface for the '>jetrails\_' application. The page has a light gray background with a 'LOGOUT' button in the top right corner. A central white card contains the application logo, two tabs labeled '6 DIGIT PIN' and 'BACKUP CODE', and a 'Verification Pin' input field. Below the input field is a checkbox labeled 'Remember for 7 days' and a green 'VERIFY' button.

### Backup Code

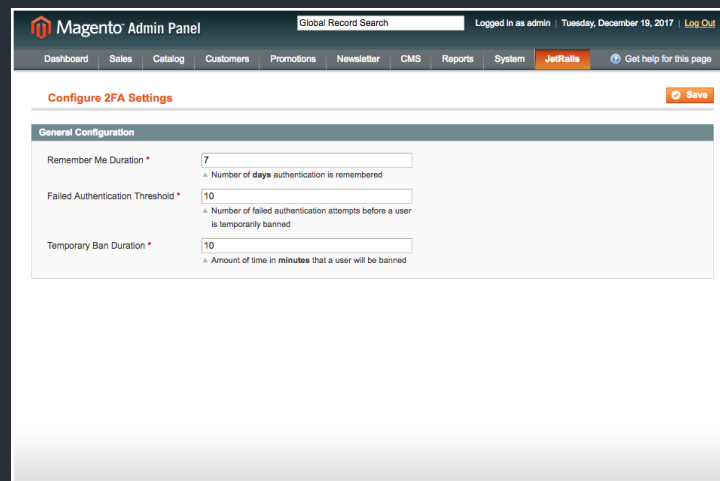
Recover account by authenticating with one of your Backup Codes.

A screenshot of the authentication interface for the '>jetrails\_' application, showing the 'Backup Code' tab selected. The layout is identical to the verification pin page, with a 'Backup Code' input field instead of a pin field, and a green 'VERIFY' button at the bottom.



## Configure 2FA Settings

Please note that this page is only accessible for super admin users. Adjusting its accessibility with different roles can be controlled through the Magento ACL system by giving the role permission to use the **JetRails > Two-Factor Authentication > Manage 2FA Accounts** resource. To get to the configuration page for this module, go to the **Configure 2FA Settings** page. It can be found by looking under in the navigation menu under **JetRails > Two-Factor Authentication**. Only positive integer values are accepted as values for all the fields found on this page. For more information about what each of the fields pertains to, read the descriptions below:



The screenshot shows the 'Configure 2FA Settings' page in the Magento Admin Panel. The page has a top navigation bar with links like Dashboard, Sales, Catalog, Customers, Promotions, Newsletter, CMS, Reports, System, and JetRails. Below the navigation bar, there's a 'Configure 2FA Settings' section with a 'Save' button. The 'General Configuration' section contains three fields: 'Remember Me Duration' (7), 'Failed Authentication Threshold' (10), and 'Temporary Ban Duration' (10). Each field has a description below it.

Field	Value	Description
Remember Me Duration *	7	Number of days authentication is remembered
Failed Authentication Threshold *	10	Number of failed authentication attempts before a user is temporarily banned
Temporary Ban Duration *	10	Amount of time in minutes that a user will be banned

### Remember Me Duration

Number of days authentication is remembered. When authenticating, a user has an option to remember authentication so they don't need to authenticate again.

### Failed Authentication Threshold

Number of failed two-factor authentication attempts that need to occur before an account gets temporarily banned.

### Temporary Ban Duration

Number of time in minutes that a banned user has to wait until they can attempt to authenticate again.

## Manage 2FA Accounts

Please note that this page is only accessible for super admin users. Adjusting its accessibility with different roles can be controlled through the Magento ACL system by giving the role permission to use the **JetRails > Two-Factor Authentication > Manage 2FA Accounts** resource. To get to the configuration page for this module, go to the **Manage 2FA Accounts** page. It can be found by looking under the navigation menu under **JetRails > Two-Factor Authentication**. To use this interface, select the rows to manipulate, select desired action from the top right select menu, then click submit. Descriptions of each action can be found below.

Username	Firstname	Lastname	Email Address	Last Authenticated On	Last Authenticated From	2FA Enabled	2FA State
admin	Admin	User	admin@localhost.com	12/19/2017 02:32:15 PM	172.18.0.1	ENABLED	COMPLETED
baz	Baz	Qux	baz.qux@localhost.com	12/19/2017 01:52:00 PM	172.18.0.1	ENABLED	REQUIRES SETUP
corge	Corge	Grault	corge.grault@localhost.com	12/19/2017 03:08:36 PM	172.18.0.1	ENABLED	TEMP BAN
foo	Foo	Bar	foo.bar@localhost.com	12/19/2017 01:52:00 PM	172.18.0.1	ENABLED	COMPLETED
quux	Quux	Quuz	quux.quuz@localhost.com	12/19/2017 01:52:00 PM	172.18.0.1	DISABLED	

### Enable

This will enable and enforce two-factor authentication on selected users.

### Disable

This will disable two-factor authentication on selected users. When 2FA is not enabled, users cannot choose to use 2FA.

### Remove Temp Ban

If a user gets banned because of too many failed authentication attempts, then you as a super admin can remove the ban instead of making them wait for the temporary ban to expire.

### Re-Enroll User

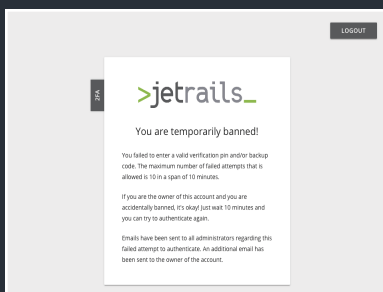
This action will reset the user's 2FA secret and generate a new one. The user will have to re-setup their account after this action is executed.

## Account Blocking

If a user fails to authenticate their login with a verification code or backup code a total of 10 times in a row, then their account will be temporarily blocked for 10 minutes. The backend will be inaccessible to them until their block has expired. This is done in order to prevent any brute force attacks on your two step authentication. Once an account is blocked, multiple warning emails will be sent out to inform people about the failed authentication attempt. An email will be sent to the account owner that tried to authenticate. Additional emails will be sent to all users in the **Administrator** role. The administrators will also receive information about what IP address the last failed authentication attempt was made on. Because this module sends out emails using Magento's built in email interface, it is important to configure Magento to send emails properly so they don't end up in a user's spam folder.

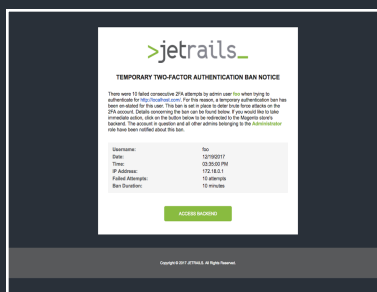
### 2FA Banned Page

Once the admin user is blocked, they will see this page.



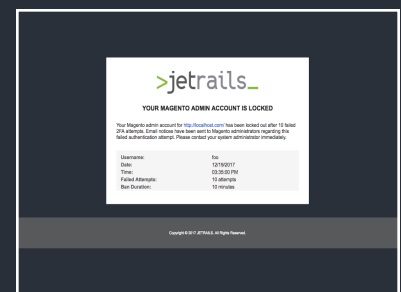
### Administrator Email Exam

An email will be sent to the owner of the account that is blocked



### User Email Example

An email will be sent to all users in the Administrators role





## Account Recovery Using Database (Advanced)

Use the following steps to place an account back into setup mode. Unfortunately one of your admin user might use up all the backup codes associated with their account and not think about resetting their account to get new backup codes. If this happens, then there is no other way for them to reset their account. The only option would be to reset their account manually. Anyone with access to the database can reset an account back into setup mode. Do this at your own risk, the following should be done only if you know how to use the database. Please note that table names are referenced without any prefix, your Magento store might have a prefix attached to them, adjust accordingly.

### STEP #1

Connect to MySQL backend

### STEP #2

Find target user's id from the admin\_user table and make a note of it.

### STEP #3

Update entry in jetrails\_twofactor\_auth based on the user id that was noted in the previous step. Then set the state and attempts to zero. Modify the SQL query below:

```
UPDATE jetrails_twofactor_auth SET state = 0, attempts = 0 WHERE id = USER_ID LIMIT 1
```

### STEP #4

Once user logs into their account, they will be redirected to the TFA setup page.



## Feature Request / Bug Submission

Please address any feature requests or found bugs to the following email address:

**development@jetrails.com**

**In subject header, please specify one of the following:**

- JetRails Two-Factor Authentication - Bug Submission
- JetRails Two-Factor Authentication - Feature Request

**If you are sending a found bug please include the following information:**

- Magento Edition (CE or EE)
- Magento Version
- Description of bug
- Steps to recreate bug
- Expected behavior
- Resulting behavior



## JetRails Security Assessment

See other great Magento plugins from JetRails:

<b>Two Factor Authentication:</b>	Additional security for your Magento backend.
<b>Security Suite:</b>	Essential security tools missing from regular Magento.
<b>Black Box:</b>	Find out what happened after the crash.

Other services from the JetRails 24/7 managed services team:

- Performance, uptime & security monitoring
- Zero downtime migration & performance enhancement
- Managed onsite/offsite Incremental backups
- Performance & security optimisation
- Technical, forensic & security support
- Booster management and flexible scalability
- DDoS preparation & security breach mitigation with code reviews
- Full hosting platform tuning and management
- Magento front end acceleration and caching

**Call us at 1-888-554-9990**