>jetrails_

Two Factor Authentication

Magento 1.9

USER GUIDE

Version 1.0.9

Table of Contents:

License

About JetRails TFA

The JetRails TFA plugin helps to ensure that all log-ins are authorized. This plugin was tested with Magento Open Source 1.6 - 1.9. Our plugin comes with the following features:

- Backup codes as an alternate authentication method
- Force TFA usage based on Magento role
- Remember authentication for 7 days
- Send email to account owner and admins on account block
- Brute force protection (10 min. block between 10 failed attempts)

Installing JetRails TFA

Download TGZ archive file that contains the JetRails TFA plugin from the Magento Marketplace

```
> pwd

  /var/www/html

> ls

  magento/
  jetrails_tfa.tgz
```

1

Place it into the desired Magento installation directory

```
> pwd

  /var/www/html

> ls

  magento/
  jetrails_tfa.tgz

> mv jetrails_tfa.tgz magento/
```

2

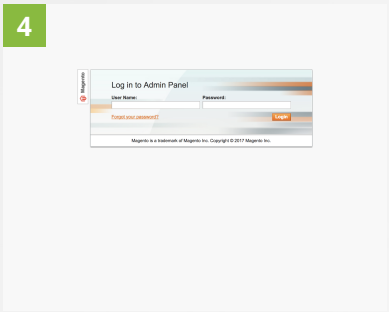
Go into the Magento installation directory and extract the archive

```
> pwd

  /var/www/html

> ls

  magento/
  jetrails_tfa.tgz

> mv jetrails_tfa.tgz magento/

> cd magento/

> tar -zxvf jetrails_tfa.tgz
```

3

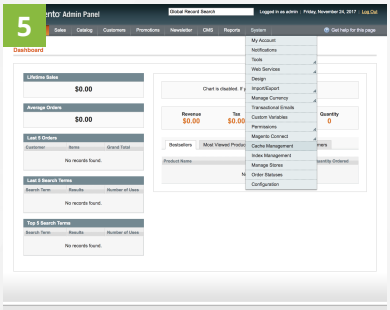
Go to your store's Magento backend and log into an Administrator account

4



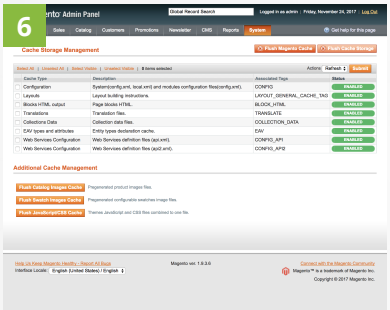
Navigate to System > Cache Management

5



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

6

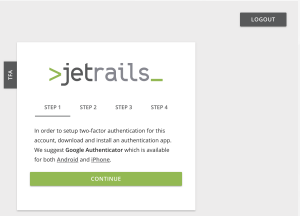


If any users were logged in during installation, then they will be logged out

7

Log back in, and you will be redirected with the TFA setup page

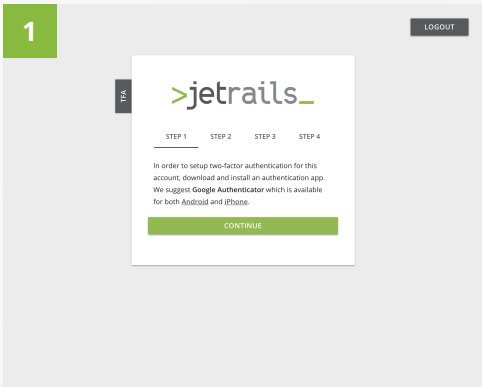
8



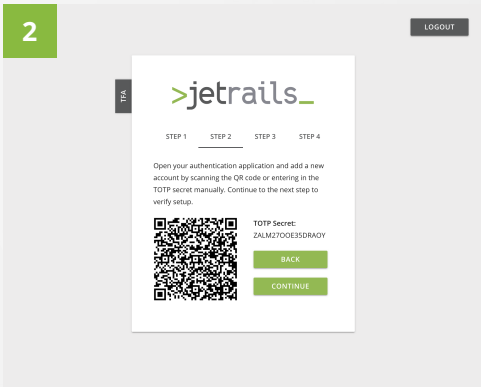
Setting Up TFA Account

If TFA is not setup for a user, then the user will be redirected to the TFA setup page on successful login. Below are all the steps that need to be taken to setup a TFA account.

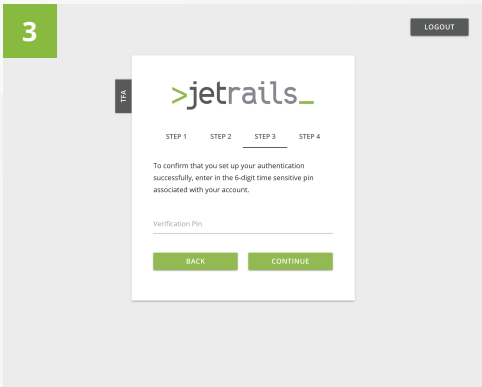
Follow instructions to install an Authentication application, then click CONTINUE.



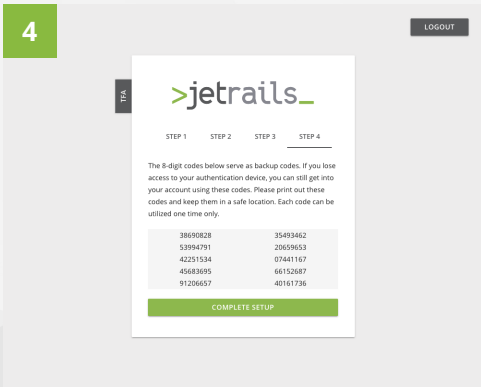
Follow instructions to setup authentication account, then click CONTINUE.



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



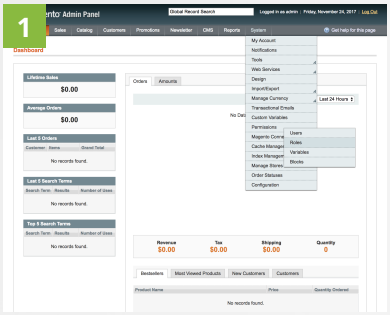
Save backup codes in case you lose access to authentication app, then click COMPLETE SETUP.



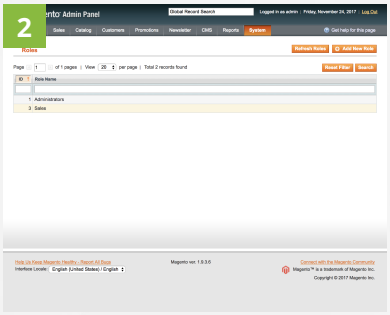
Enforcing TFA with Magento Roles

TFA is forced on Magento admin accounts using the ACL Roles that are built into Magento. Once a resource is applied to the role, all users in the role are required to setup a TFA account. Since users in the Administrators role have access to all resources, they are forced to use TFA, which is a good thing.

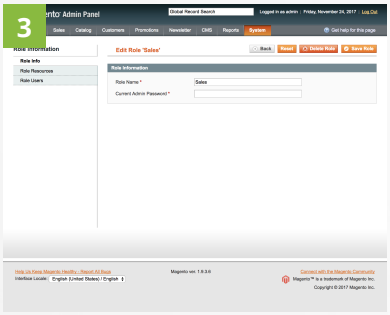
In Magento admin backend, go to System > Permissions > Roles



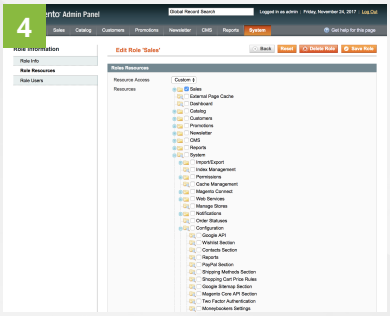
Edit desired role where TFA should be enforced.



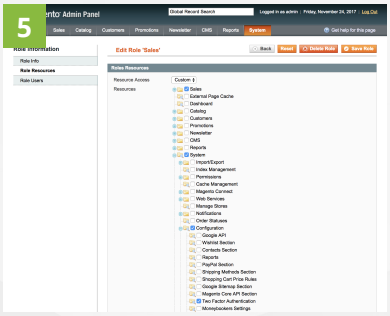
On the menu on the left, click on the Role Resources tab



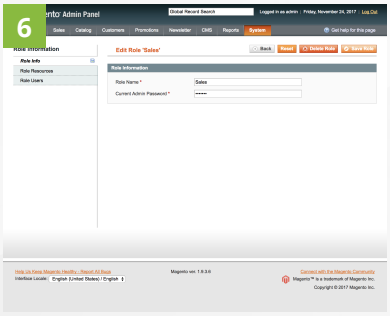
You should see all the allowed resources for the role



Add System > Configuration > Two Factor Authentication resource to role



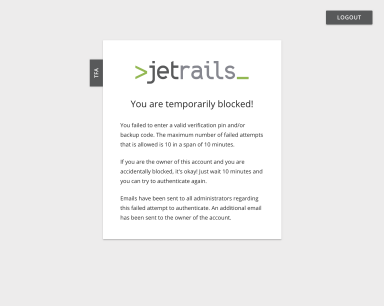
Go back to Role Info tab , enter admin password and click Save Role button.



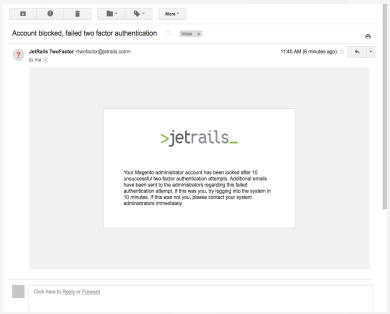
Account Blocking:

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 temporarly blocked for 10 minutes. The backend will be unaccessible 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 emails will be sent out to warn 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.

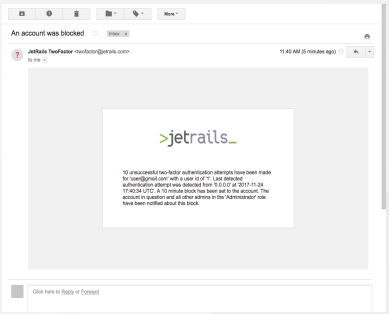
Once the admin user is blocked, they will see this page.



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



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



Authenticating After Admin Login:

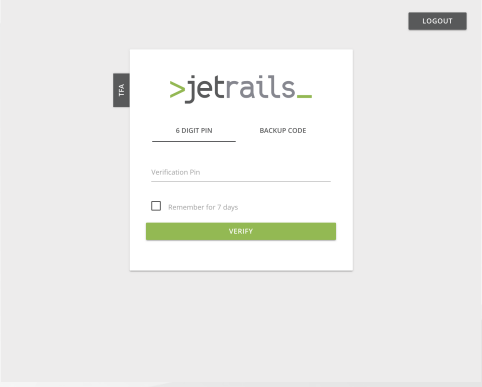
Once an admin user sets up their authentication account and logs in successfully, they will be greeted with a verification page. The user can choose to authenticate using a 6 Digit Pin or a Backup Code.

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.

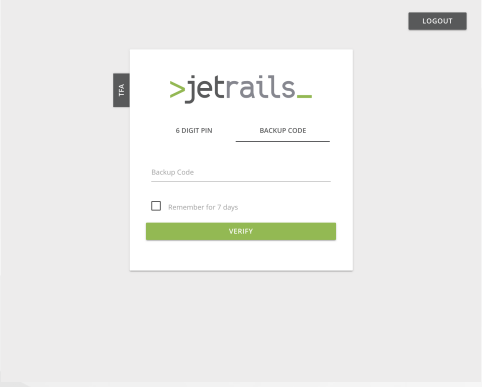
The user also has an option to remember the authentication for 7 days. This will create a cookie and so long as the user is logged in on the same device with the same IP address, they will be authenticated automatically without the need to enter a verification pin or backup code.

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.

Authenticate normally using your accounts 6 Digit Pin.



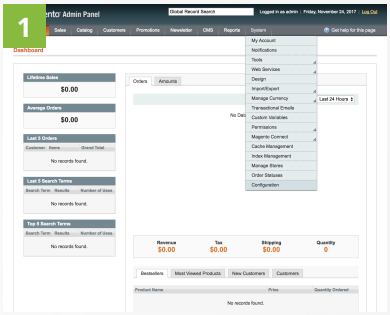
Recover account by authenticating with Backup Code.



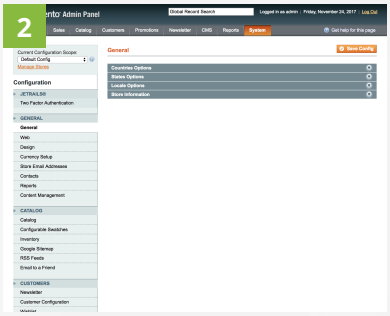
Account Recovery using TFA Plugin

If you lose access to your TFA account and authenticate using a backup code, you can always reset you TFA account. Follow the instructions below and your TFA account will be reset. You will be logged out and the next time you log in, you will be prompted to setup your TFA account.

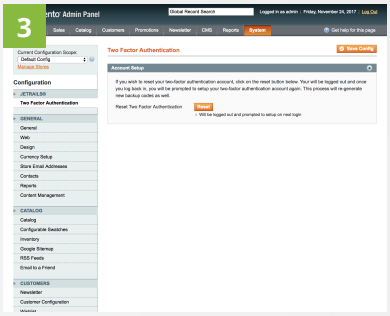
In Magento admin backend, go to System > Configuration



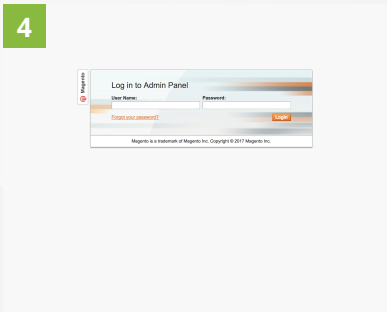
Click on Two Factor Authentication tab under the JETRAILS category



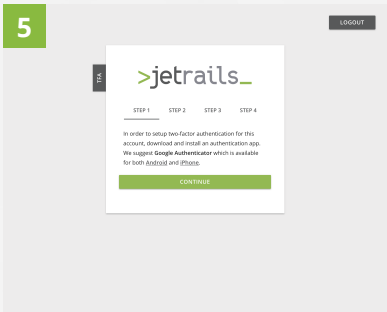
Click on the Reset button under the Account Setup panel



To protect your account, you will be logged out, log back in to continue



On successful login, you will be redirected to the TFA setup page



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.

1. Connect to database backend
2. Find target admin user's id from the admin_user table.
3. See contents of jetrails_twofactor_auth table.
4. Update entry to reset account authentication state to setup (replace {USER_ID} with the admin user id that was found in step 2):

   UPDATE jetrails_twofactor_auth SET state = 0, attempts = 0
   where id = {USER_ID} LIMIT 1

5. Once this is complete, then user can login to their account and they will redirected to the TFA setup page.

Feature Requests / 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
- Magento Version
- Description of bug
- Steps to recreate bug
- Expected behavior
- Resulting behavior

JetRails Security Assessment

See other great Magento plugins from JetRails:

Two Factor Authentication: Additional security for your Magento backend.
Security Suite: Essential security tools missing from regular Magento.
Black Box: 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 flexable 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