

Secure your app with 2FA

Rob Allen ~ @akrabat ~ October 2015

Your users' passwords will
be leaked

(It might not even be your fault)

Passwords have leaked from

Sony

Facebook

Adobe

Evernote

Kickstarter

HP

Gmail

Ubuntu

Zappos

Twitter

Target

Yahoo!

Home Depot

AOL

last.fm

D&B

JP Morgan

eBay

Blizzard

Steam

TK Maxx

Citigroup

Apple

Formspring

Gap

AT&T

Drupal

Ubisoft

Vodafone

WorldPay

SnapChat

Betfair

It will take 14 minutes* to crack
one of your users' passwords

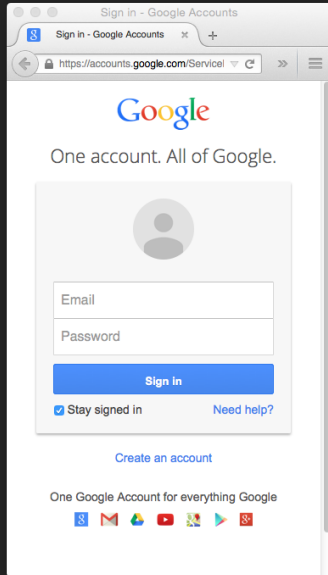
(English word, stored using bcrypt)

Two-factor authentication
protects your users

What is 2FA?



Implementation on a website



Sign in - Google Accounts

https://accounts.google.com/Service

Google

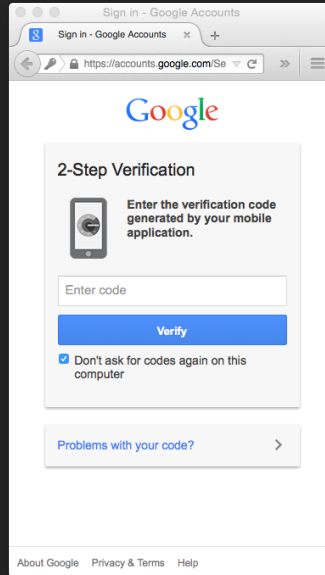
One account. All of Google.

[Sign in](#)

Stay signed in [Need help?](#)

[Create an account](#)

One Google Account for everything Google




Sign in - Google Accounts

https://accounts.google.com/Se

Google

2-Step Verification

 Enter the verification code generated by your mobile application.

[Verify](#)

Don't ask for codes again on this computer

[Problems with your code?](#) >

[About Google](#) [Privacy & Terms](#) [Help](#)

How do we send the code?

Email

- Used by Steam
- Wide adoption (everyone has an email address!)
- Likely failures: delivery problems, blocking, spam etc
- Usually slow!
- Same system as recover password...

SMS

- Used by Twitter & LinkedIn
- Wide adoption
- But, SMS can be delayed & could cost to receive



Physical device

- Used by banks, YubiKey, Blizzard, etc
- Small, long battery life
- But, expensive



App

- Easy to use
- No Internet or cellular connection required
- App is free and trusted

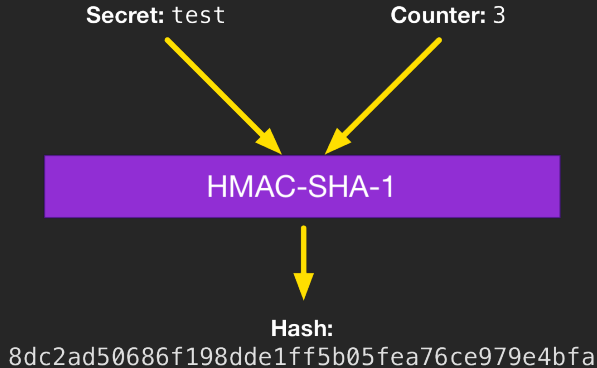


One Time Password algorithms

HOTP

- HMAC-based One-Time Password algorithm
- Computed from shared secret and counter
- New code each time you press the button
- RFC 4226

HOTP algorithm: step 1



HOTP algorithm: step 2

Hash:

8dc2ad50686f198dde1ff5b05fea76ce979e4bfa



Find lower 4 bits of last byte

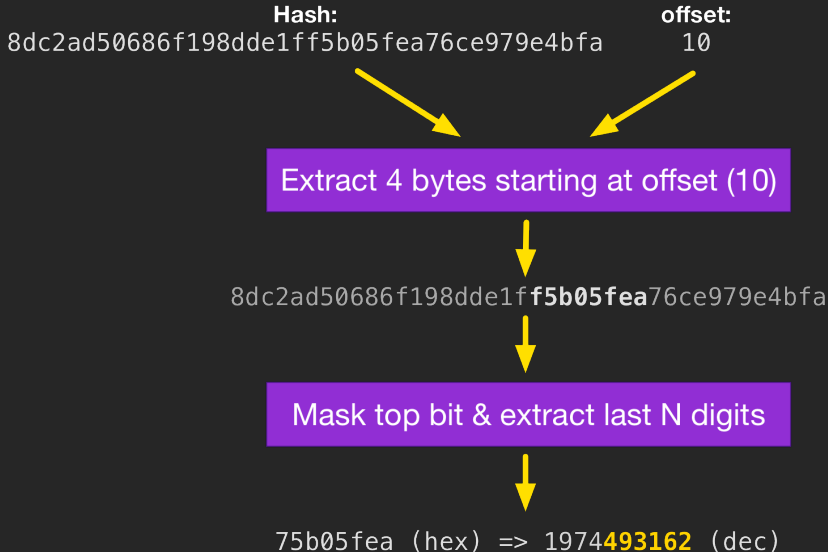


8dc2ad50686f198dde1ff5b05fea76ce979e4bfa

offset:

0x0A (hex) => 10 (decimal)

HOTP algorithm: step 3



HOTP in PHP

```
1 function hotp($secret, $counter)
2 {
3     $bin_counter = pack('J*', $counter);
4     $hash = hash_hmac('sha1', $bin_counter, $secret, true);
5
6     $offset = ord($hash[19]) & 0xf;
7
8     $bin_code =
9         ((ord($hash[$offset+0]) & 0x7f) << 24 ) |
10        ((ord($hash[$offset+1]) & 0xff) << 16 ) |
11        ((ord($hash[$offset+2]) & 0xff) << 8 ) |
12        (ord($hash[$offset+3]) & 0xff);
13
14     return $bin_code % pow(10, 6);
15 }
```

Validation process

If the user's code matches, then increment counter by 1

If the user's code does not match, then look-ahead a little

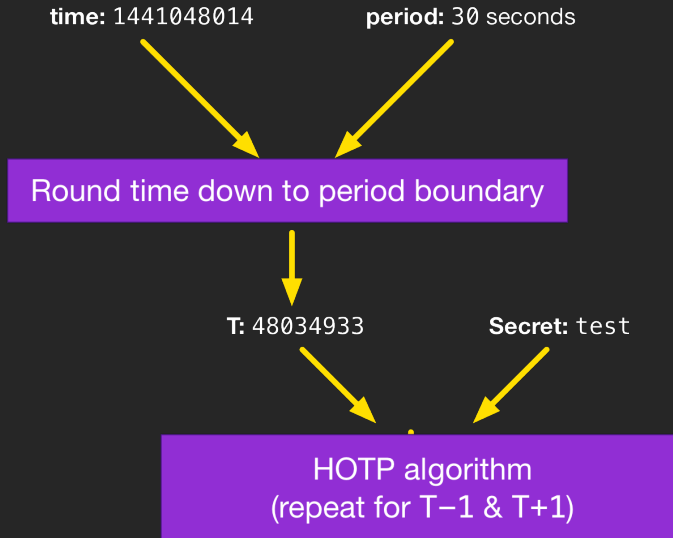
Resync if can't find in look-ahead:

1. Ask the user for two consecutive codes
2. Look ahead further from last known counter until the 2 codes are found
3. Limit look-ahead to minimise attack area. e.g. 400

TOTP

- Time-based One-Time Password algorithm
- Computed from shared secret and current time
- Increases in 30 second intervals
- RFC 6238

TOTP Algorithm



TOTP in PHP

```
1 function totp($secret)
2 {
3     $counter = floor(time() / 30);
4
5     return hotp($secret, $counter);
6 }
```

Implementing 2FA in your application

Things to do

1. Registration of Authenticator
2. Check 2FA TOTP code during login

Registration

User enables 2FA on their account

Registration

User enables 2FA on their account



Site generates secret key and then displays QR code & confirmation field

Registration

User enables 2FA on their account



Site generates secret key and then displays QR code & confirmation field



User adds to Authenticator

Registration

User enables 2FA on their account



Site generates secret key and then displays QR code & confirmation field



User adds to Authenticator



User enters Authenticator 2FA code into site to complete registration

Registration

User enables 2FA on their account



Site generates secret key and then displays QR code & confirmation field



User adds to Authenticator



User enters Authenticator 2FA code into site to complete registration



Site confirms code & stores secret to database

Logging in

After login form, prompt for 2FA code

Logging in

After login form, prompt for 2FA code



User enters 2FA code

Logging in

After login form, prompt for 2FA code



User enters 2FA code



Site generates own 2FA code based on user's secret and current time

Logging in

After login form, prompt for 2FA code



User enters 2FA code



Site generates own 2FA code based on user's secret and current time



Site compares own 2FA code with user's supplied one

Logging in

After login form, prompt for 2FA code



User enters 2FA code



Site generates own 2FA code based on user's secret and current time



Site compares own 2FA code with user's supplied one



User allowed into website

Coding it

```
$composer require sonata-project/google-authenticator
```

Usage:

```
$g = new \Google\Authenticator\GoogleAuthenticator();
```

```
// create new secret and QR code
```

```
$secret = $g->generateSecret();
```

```
$qrCode = $g->getURL('rob', 'akrabat.com', $secret);
```

```
// validation of code
```

```
$g->checkCode($secret, $_POST['code']);
```

Example project: <https://github.com/akrabat/slim-2fa>

Registration


2FA example application

2FA example application Log out rob

Set up 2FA

It's a good idea to set up 2FA!

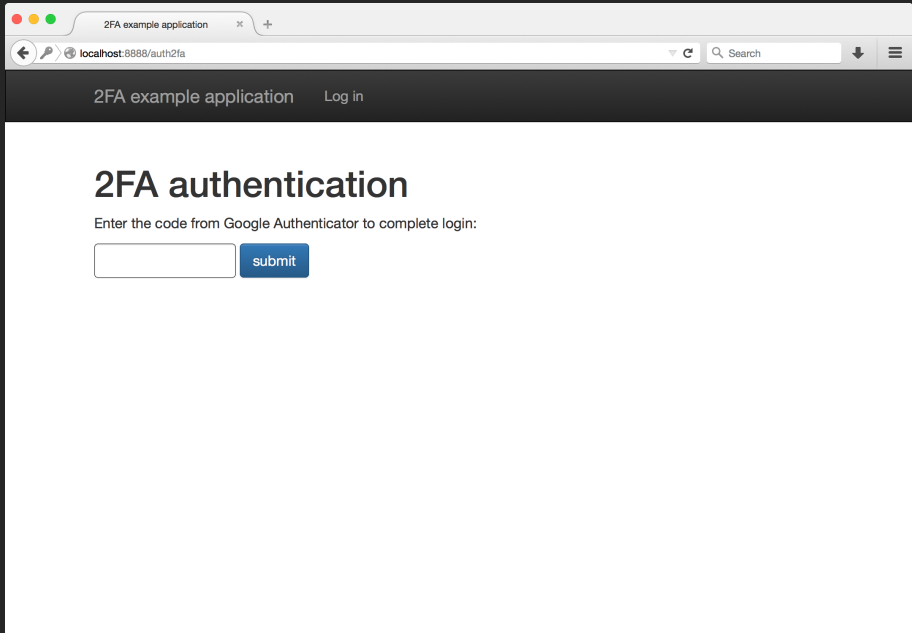
Scan this code into Google Authenticator



or enter this code: OCEFCIAGRGETOH

Enter code from Google Authenticator to confirm:

Login



A screenshot of a web browser window. The browser's address bar shows the URL `localhost:8888/auth2fa`. The page title is "2FA example application" and there is a "Log in" link in the top right corner. The main content area features a heading "2FA authentication" followed by the instruction "Enter the code from Google Authenticator to complete login:". Below this is a text input field and a blue "submit" button.

2FA example application Log in

2FA authentication

Enter the code from Google Authenticator to complete login:

Round out solution

- Prevent brute force attacks
- Consider adding a “remember this browser” feature
- Need a solution for a lost/new phone

Hardware OTP: YubiKey



Operation

1. Insert YubiKey into USB slot
2. Select input field on form
3. Press button to fill in OTP field
4. Server validates OTP with YubiCloud service

Yubikey's OTP

cdccccetfjnfjgkkgudlkcbjnfnfrkhkbelbhfvnhcj
cdccccetfjnfuhtrebhjekcciljdbifgfrlccbnjhkf
cdccccetfjnljrhetskvi~~jc~~gddkenbtuiknktejgnv**gb**



Public id



Yubico OTP

6 byte private identity field
Counter
Timer field
Random number
CRC16 checksum

Coding it

```
$composer require enygma/yubikey
```

Usage:

```
$v = new \Yubikey\Validate($apiKey, $clientId);  
$response = $v->check($_POST['yubikey_code']);
```

```
if ($response->success() === true) {  
    // allow into website  
}
```

Pre-built plugins

Pre-built plugins

Drupal:

- Two-factor Authentication
- Yubikey

WordPress:

- Google Authenticator
- yubikey-plugin

Joomla:

- Built-in!

Drupal

The screenshot shows a web browser window with the URL <https://www.drupal.org/project/tfa>. The page features a blue header with the Drupal logo and navigation links: Get Started, Community, Documentation, Support, Download & Extend, Jobs, Marketplace, and About. A search bar is located in the top right of the header. Below the header, there are buttons for "Drupal Homepage" and "Log In / Register". The main content area is titled "Download & Extend" and includes sub-navigation for "Download & Extend Home", "Drupal Core", "Distributions", "Modules", and "Themes". The primary heading is "Two-factor Authentication (TFA)". Below this heading, there are buttons for "View", "Version control", and "Automated Testing". The text indicates the page was posted by [coltrane](#) on March 21, 2011, at 3:19am. The main body text describes TFA as a base module for providing two-factor authentication for Drupal sites, mentioning various solutions like Time-based One Time Passwords (TOTP), SMS-delivered codes, and integrations with services like Authy and Duo. A sidebar on the right contains sections for "Maintainers for Two-factor Authentication (TFA)" listing [coltrane](#) (70 commits) and [greggles](#) (2 commits), and "Issues for Two-factor Authentication (TFA)" with a note to avoid duplicates and a link to "Advanced search".

Two-factor Authentication (TFA)

[View](#) [Version control](#) [Automated Testing](#)

Posted by [coltrane](#) on March 21, 2011 at 3:19am

Second-factor authentication for Drupal sites. Drupal provides authentication via something you *know* -- a username and password while TFA module adds a second step of authentication with a check for something you *have* -- such as a code sent to (or generated by) your mobile phone.

TFA is a base module for providing two-factor authentication for your Drupal site. As a base module, TFA handles the work of integrating with Drupal, providing flexible and well tested interfaces to enable your choice of various two-factor authentication solutions like Time-based One Time Passwords (TOTP), SMS-delivered codes, pre-generated codes, or integrations with third-party services like Authy, Duo and others.

Read the [TFA module documentation](#) or read more about the [theory of two-factor authentication](#) in my [Drupal Watchdog](#) article.

Features

- Pluggable – Supports multiple methods of 2nd factor verification and can work with any number of 3rd party systems

Maintainers for Two-factor Authentication (TFA)

[coltrane](#) – 70 commits
last: 1 month ago, first: 4 years ago

[greggles](#) – 2 commits
last: 1 year ago, first: 1 year ago

[View all committers](#)
[View commits](#)

Issues for Two-factor Authentication (TFA)

To avoid duplicates, please search before submitting a new issue.
[Advanced search](#)

Set up

The screenshot shows a web browser window displaying the configuration page for Two-factor Authentication in Drupal. The browser's address bar shows the URL `drupal.akrobat.com/overlay=admin/config/people/tfa`. The navigation menu includes Dashboard, Content, Structure, Appearance, People, Modules, Configuration (selected), Reports, and Help. The user is logged in as 'Hello roballen' and can click 'Log out'. Below the navigation is a search bar and a 'Search' button. The main content area is titled 'Two-factor Authentication' and includes a breadcrumb trail: 'Home » Administration » Configuration » People'. A white modal window is open, displaying the configuration options for TFA. It lists 'AVAILABLE PLUGINS' with four items: 'TOTP (validation) - active validator', 'Trusted Browsers (login) - active login', 'Recovery Codes (validation) - unused', and 'Twilio SMS (validation, send) - unused'. Below this, there is a checked checkbox for 'Enable TFA' with the text 'Enable TFA for account authentication.'. Under 'Default validation plugin', a dropdown menu is set to 'TOTP' with the text 'Plugin that will be used as the default TFA process.'. At the bottom, there is a section for 'VALIDATION FALLBACK PLUGINS' with the text 'Fallback plugins and order. Note, if a fallback plugin is not setup for an account it will not be active in the TFA form.' and a single unchecked checkbox for 'Recovery Codes'.

Two-factor Authentication

Home » Administration » Configuration » People

AVAILABLE PLUGINS

- **TOTP** (*validation*) - active validator
- **Trusted Browsers** (*login*) - active login
- **Recovery Codes** (*validation*) - unused
- **Twilio SMS** (*validation, send*) - unused
- **Help page** (*validation*) - unused

Enable TFA
Enable TFA for account authentication.

Default validation plugin

TOTP

Plugin that will be used as the default TFA process.

VALIDATION FALLBACK PLUGINS

Fallback plugins and order. Note, if a fallback plugin is not setup for an account it will not be active in the TFA form.

Recovery Codes

Set up

TFA setup - Application | Ro... x +

drupal.akrabat.com/user/1/security/tfa/app-setup

Search

Dashboard Content Structure Appearance People Modules Configuration Reports Help Hello roballen Log out

Add content Find content Edit shortcuts


TFA setup - Application

Install authentication code application on your mobile or desktop device:

- [Google Authenticator \(Android/iPhone/BlackBerry\)](#)
- [Authy \(Android/iPhone\)](#)
- [Authenticator \(Windows Phone\)](#)
- [FreeOTP \(Android\)](#)
- [GAuth Authenticator \(desktop\)](#)

The two-factor authentication application will be used during this setup and for generating codes during regular authentication. If the application supports it, scan the QR code below to get the setup code otherwise you can manually enter the text code.

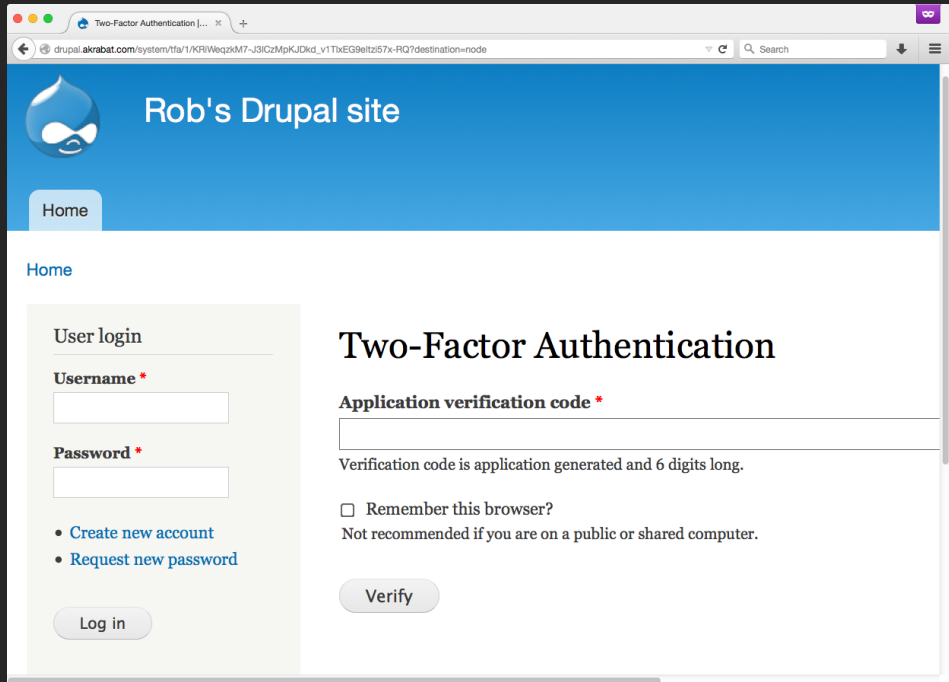
Enter this code into your two-factor authentication app or scan the QR code below.



Application verification code *

A verification code will be generated after you scan the above QR code or manually enter the setup code. The verification code is six digits long.

Log in



The screenshot shows a web browser window with the following elements:

- Browser Address Bar:** Shows the URL `drupal.akrabat.com/system/tfa/1/KRiWeqzKM7-J3iCzMpKJdKd_v1TxEG9eltz57x-RQ?destination=node`.
- Page Header:** A blue banner with the Drupal logo on the left and the text "Rob's Drupal site" on the right.
- Navigation:** A "Home" button is located below the header.
- Left Column (User Login):**
 - Section title: "User login"
 - Form field: "Username *" with an asterisk indicating it is required.
 - Form field: "Password *" with an asterisk indicating it is required.
 - Links: "Create new account" and "Request new password".
 - Button: "Log in".
- Right Column (Two-Factor Authentication):**
 - Section title: "Two-Factor Authentication"
 - Form field: "Application verification code *" with an asterisk indicating it is required.
 - Text: "Verification code is application generated and 6 digits long."
 - Form element: A checkbox labeled "Remember this browser?".
 - Text: "Not recommended if you are on a public or shared computer."
 - Button: "Verify".

WordPress

WordPress • Search for 'Go... x +

https://wordpress.org/plugins/search.php?type-term&q="Google+Authenticator"

Have you taken the WordPress 2015 Survey yet?

WORDPRESS.ORG

Showcase Themes **Plugins** Mobile Support Get Involved About Blog Hosting

Search WordPress.org

Download WordPress


Plugin Directory

Username Password Log in (forgot?) or Register

Search Results Featured Popular Favorites Beta Testing

Developers Keyword "Google Authenticator"

Showing 1-30 of 37 plugins 1 2 Next >



Google Authenticator

Google Authenticator for your WordPress blog.


By: *Henrik Schack*

★★★★★ (67)

10,000+ active installs

Last Updated: 2 years ago

Compatible up to: 3.8.10



Two-Factor Authentication (Google Authenticator)

Easily add Two Factor Authentication(2FA) to protect sites from unauthorized login attempts.Support Phone Call,SMS,QR Code,Push,Google Authenticator.


By: *miniOrange*

★★★★★ (8)

100+ active installs


Last Updated: 1 day ago

Compatible up to: 4.3



Google Authenticator for WordPress

Adds 2-factor authentication to your site.



OTP and Passwords for Google Authenticator, McAfee, DS3 ...

Easy secure login, use password or OTP as

Set up

Profile · Rob Allen's DevNotes ... x +

dev.akrabat.com/wp-admin/profile.php

Rob Allen's DevNotes 0 + New Delete Cache Howdy, Rob

- Dashboard
- Posts
- Media
- Pages
- Comments
- Appearance
- Plugins
- Users**
- All Users
- Add New
- Your Profile
- Tools
- Settings
- Collapse menu


Google Authenticator Settings

Active

Relaxed mode *Relaxed mode allows for more time drifting on your phone clock (±4 min).*

Description *Description that you'll see in the Google Authenticator app on your phone.*

Secret




Scan this with the Google Authenticator app.

Log in

Rob Allen's DevNotes - Log In

dev.akrabat.com/wp-login.php?redirect_to=http%3A%2F%2Fdev.akrabat.com%2Fwp-admin%2F&reauth=1

Search



Username

roballen

Password

.....

Google Authenticator code

123456

Remember Me

Log In

[Lost your password?](#)

[← Back to Rob Allen's DevNotes](#)

Joomla

The screenshot shows the Joomla! administrator interface for editing the profile of the Super User. The browser address bar shows the URL: `localhost/joomla/administrator/index.php?option=com_users&view=user&layout=edit&id=567`. The navigation menu includes System, Users, Menus, Content, Components, Extensions, and Help. The current page is titled "User Manager: Edit Profile".

At the top of the profile edit area, there are buttons for "Save", "Save & Close", "Save & New", "Close", and "Help".

The "Super User" section has four tabs: "Account Details", "Assigned User Groups", "Basic Settings", and "Two Factor Authentication". The "Two Factor Authentication" tab is active.

Under "Two Factor Authentication", the "Authentication Method" is set to "YubiKey".

A text box explains the feature: "This feature allows you to use a YubiKey secure hardware token for two factor authentication. In addition to your username and password you will also need to insert your YubiKey into your computer's USB port, click inside the Secret Key area of the site's login area and touch YubiKey's gold disk. The secret code generated by your YubiKey is unique to your device and changes constantly. This provides extra protection against hackers logging in to your account even if they were able to get hold of your password."

The "Set up" section provides instructions: "Please insert your YubiKey device into your computer's USB port. Click on the Security Code field below. Then touch the gold disk on your YubiKey device for one second. Afterwards, please save your user profile. If the code generated by your YubiKey is validated by YubiCloud the Two Factor Authentication feature will be enabled and this YubiKey will be linked with your user account." Below the text is a "Security Code" input field.

The "One time emergency passwords" section has a light blue background with the text: "If you do not have access to your two factor authentication device you can use any of the following passwords instead of a regular security code. Each one of".

The footer shows the Joomla! logo, navigation icons, and the text: "View Site 1 Visitor 1 Admin 0 Log out". On the right side, it says "Joomla! 3.4.3 — © 2015 Rob's Joomla".

Log in



The image shows a web browser window with the Joomla! administrator login page. The browser's address bar shows the URL `localhost/joomla/administrator/`. The page features the Joomla! logo at the top, followed by three input fields for 'Username', 'Password', and 'Secret Key', each with a help icon. A blue 'Log in' button is positioned below the fields. At the bottom of the page, there is a link to the site home page, a Joomla! logo, and a copyright notice for 2015 Rob's Joomla!

Rob's Joomla! - Administration

localhost/joomla/administrator/

Search

 Joomla!®

 Username 

 Password 

 Secret Key 

 Log in

[Go to site home page.](#)



© 2015 Rob's Joomla!

To sum up

To sum up

Two-factor authentication isn't hard!

Questions?

<https://joind.in/15444>

Rob Allen - <http://akrabat.com> - @akrabat

Thank you!

<https://joind.in/15444>

Rob Allen - <http://akrabat.com> - @akrabat