Using Application Passwords

History

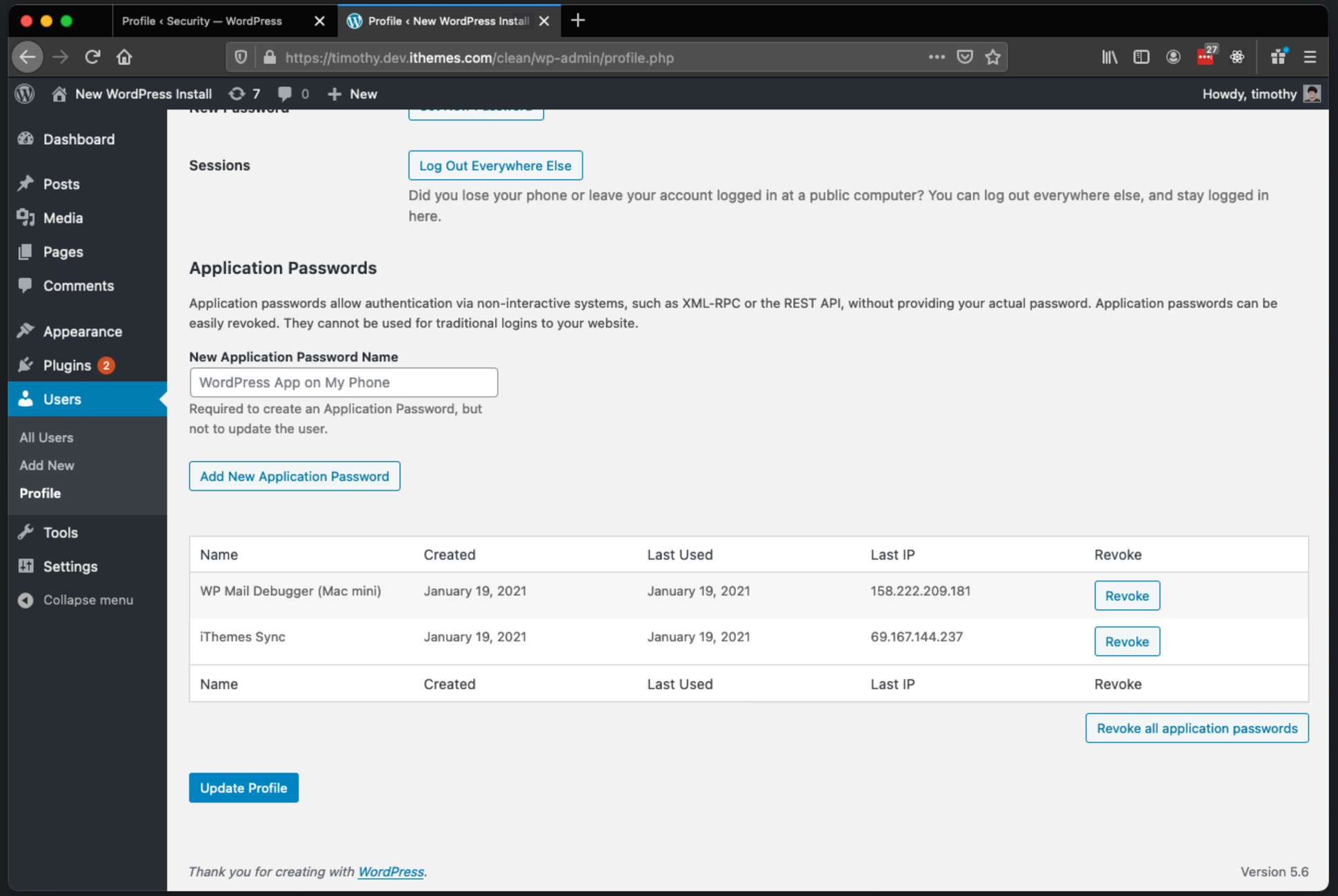
- XML/RPC always on since 3.5
  - Username & Password
- REST API content introduced in 4.7
  - Auth cookies
- Official/Unofficial REST API auth plugins
  - OAuth
  - JWT
  - App Passwords
- Plugins developed their own

Requirements

— Secure
— Interactive Auth
— Revokable
— Decentralized

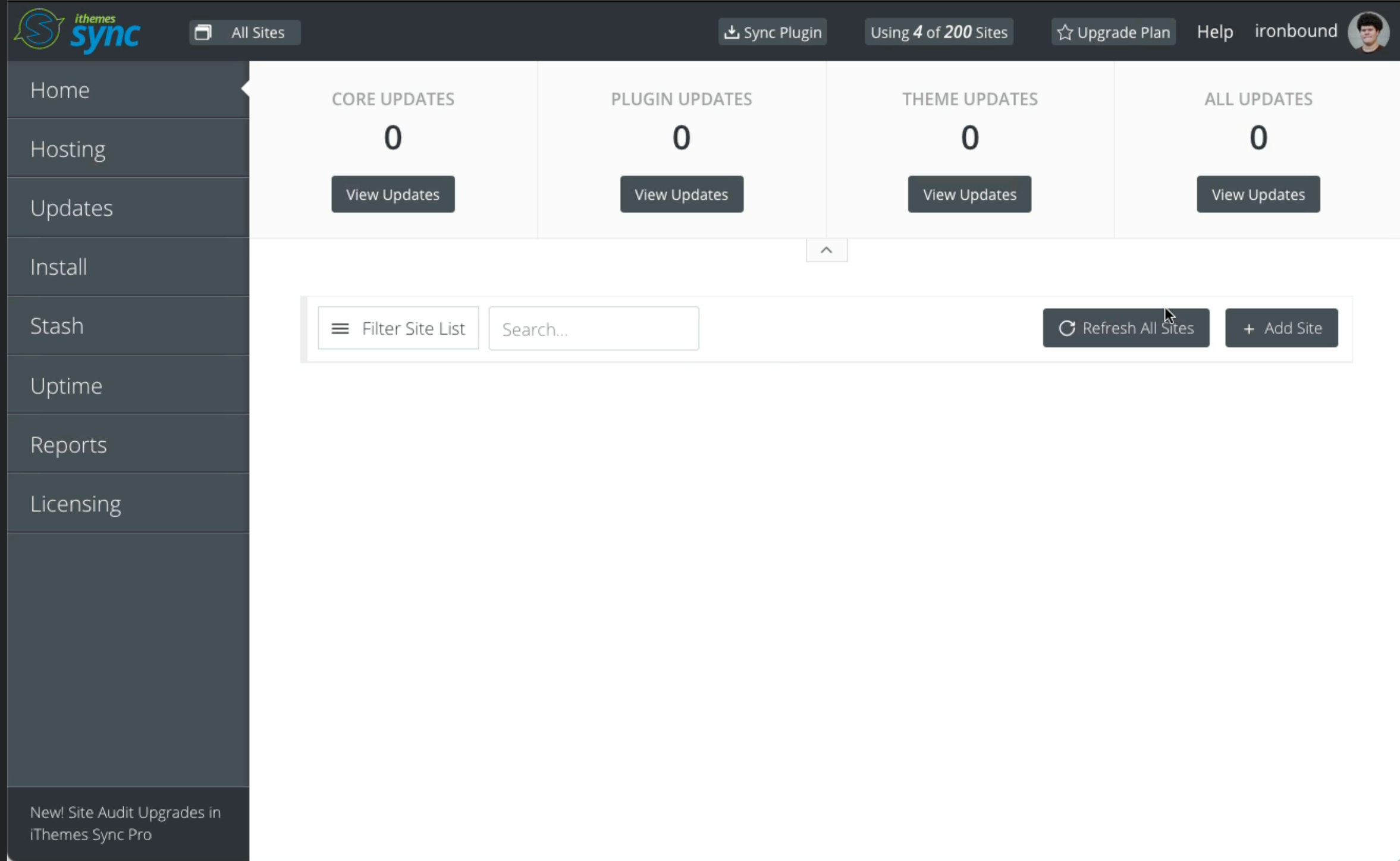
App Passwords

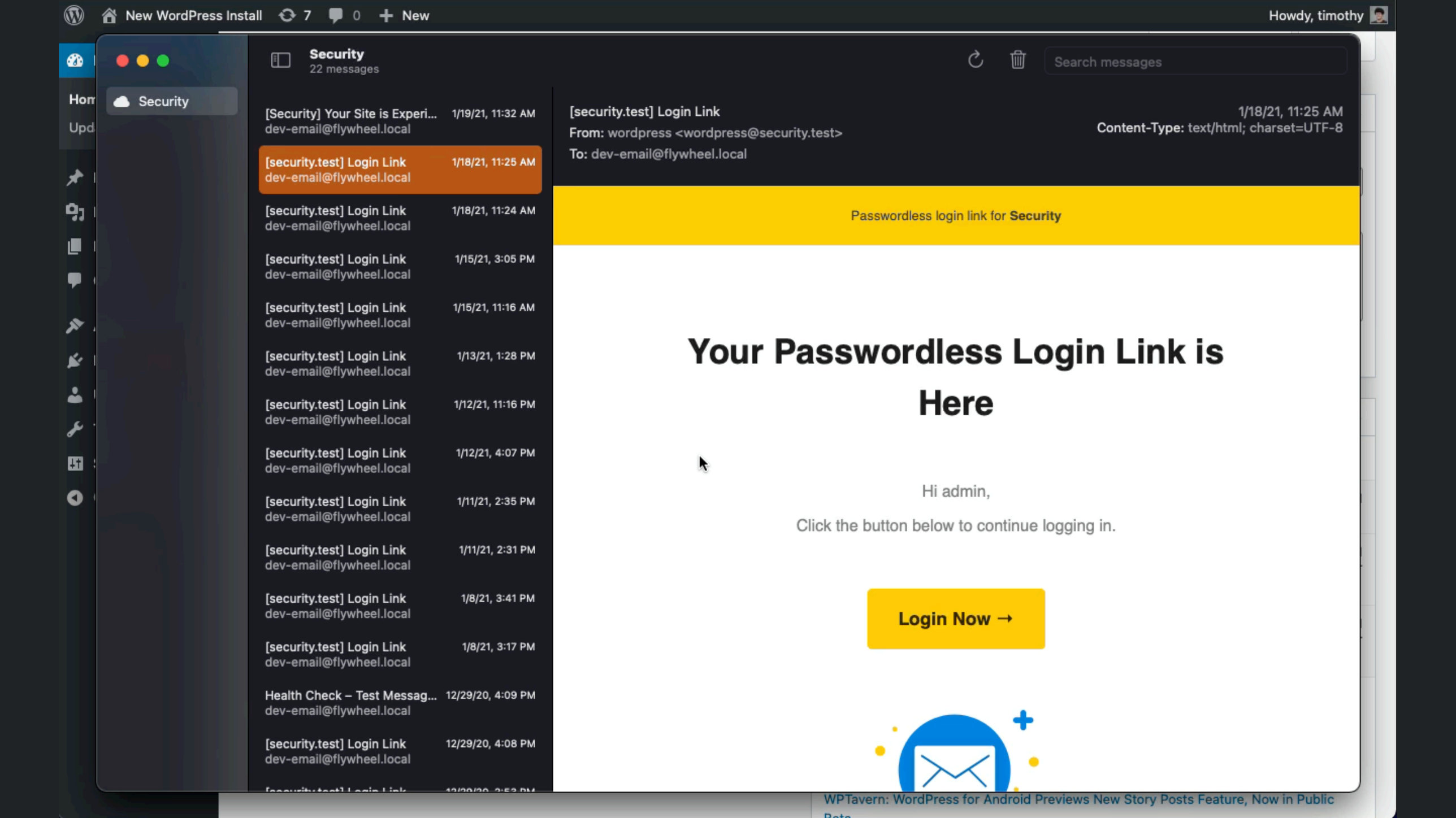
— Per-app passwords
— Can’t be used to login
— Not brute forceable
— Basic Auth
— Profile UI
— Authorize Application UI


Profile ‹ Security — WordPress
Profile ‹ New WordPress Install
https://timothy.dev.ithemes.com/clean/wp-admin/profile.php
New WordPress Install
7
0
New
Howdy, timothy
Dashboard
Posts
Media
Pages
Comments
Appearance
Plugins
2
Users
All Users
Add New
Profile
Tools
Settings
Collapse menu
Sessions
Log Out Everywhere Else
Did you lose your phone or leave your account logged in at a public computer? You can log out everywhere else, and stay logged in here.
Application Passwords
Application passwords allow authentication via non-interactive systems, such as XML-RPC or the REST API, without providing your actual password. Application passwords can be easily revoked. They cannot be used for traditional logins to your website.
New Application Password Name
WordPress App on My Phone
Required to create an Application Password, but not to update the user.
Add New Application Password
Name
Created
Last Used
Last IP
Revoke
WP Mail Debugger (Mac mini)
January 19, 2021
January 19, 2021
158.222.209.181
Revoke
iThemes Sync
January 19, 2021
January 19, 2021
69.167.144.237
Revoke
Name
Created
Last Used
Last IP
Revoke
Revoke all application passwords
Update Profile
Thank you for creating with WordPress.
Version 5.6

Use Cases

- Import/Export
- Desktop publishing
  - Mars Edit
- WordPress Mobile App
- 3rd party services
  - Zapier/IFTTT
- Plugin setup


ithemes sync
All Sites
Sync Plugin
Using 4 of 200 Sites
Upgrade Plan
Help
ironbound
Home
Hosting
Updates
Install
Stash
Uptime
Reports
Licensing
New! Site Audit Upgrades in iThemes Sync Pro
CORE UPDATES
0
View Updates
PLUGIN UPDATES
0
View Updates
THEME UPDATES
0
View Updates
ALL UPDATES
0
View Updates
Filter Site List
Search...
Refresh All Sites
Add Site


New WordPress Install
7
0
New
Howdy, timothy
Security
22 messages
Search messages
Security
[Security] Your Site is Experi... 1/19/21, 11:32 AM
dev-email@flywheel.local
[security.test] Login Link 1/18/21, 11:25 AM
dev-email@flywheel.local
[security.test] Login Link 1/18/21, 11:24 AM
dev-email@flywheel.local
[security.test] Login Link 1/15/21, 3:05 PM
dev-email@flywheel.local
[security.test] Login Link 1/15/21, 11:16 AM
dev-email@flywheel.local
[security.test] Login Link 1/13/21, 1:28 PM
dev-email@flywheel.local
[security.test] Login Link 1/12/21, 11:16 PM
dev-email@flywheel.local
[security.test] Login Link 1/12/21, 4:07 PM
dev-email@flywheel.local
[security.test] Login Link 1/11/21, 2:35 PM
dev-email@flywheel.local
[security.test] Login Link 1/11/21, 2:31 PM
dev-email@flywheel.local
[security.test] Login Link 1/8/21, 3:41 PM
dev-email@flywheel.local
[security.test] Login Link 1/8/21, 3:17 PM
dev-email@flywheel.local
Health Check – Test Messag... 12/29/20, 4:09 PM
dev-email@flywheel.local
[security.test] Login Link 12/29/20, 4:08 PM
dev-email@flywheel.local
[security.test] Login Link
From: wordpress <wordpress@security.test>
To: dev-email@flywheel.local
1/18/21, 11:25 AM
Content-Type: text/html; charset=UTF-8
Passwordless login link for Security
Your Passwordless Login Link is Here
Hi admin,
Click the button below to continue logging in.
Login Now →
WPTavern: WordPress for Android Previews New Story Posts Feature, Now in Public

Dashboard
Posts
Media
Pages
Comments
Appearance
Plugins 1
Users
Tools
Available Tools
Import
Export
Site Health
Export Personal Data
Erase Personal Data
App Passwords Demo
WP Mail Debugger
Settings
Security
Collapse menu

App Passwords Demo

Website

https://timothy.dev.ithemes.com

Connect

Availability

— WordPress 5.6+
— SSL required

Authorization Flow

1. Collect Site URL
2. Discover REST API
3. Lookup index
4. Redirect to `authentication.application-passwords.endpoints.authorization`
5. Receive redirected user
6. Store credentials
7. Make authenticated requests

REST API Discovery

developer.wordpress.org/rest-api/using-the-rest-api/discovery/

`wp-api/discovery`

REST API Discovery

`Link` header with `https://api.w.org` relation.

```
Link: <http://trunk.test/wp-json/>; rel="https://
api.w.org/"
```

REST API Discovery

`<link>` element in the head.

```
<link rel="https://api.w.org/" href="http://trunk.test/wp-json/" />
```

REST API Discovery

CORS will block reading the response.

`http://trunk.test/index.php?rest_route=/`

Lookup Index

— Request the REST API root
— Grab site name or other details
— Lookup `authentication.application-passwords`

Lookup Index


```
{
  "name": "My Site",
  "timezone_string": "America/New_York",
  "namespaces": [ "wp/v2" ],
  "authentication": {
    "application-passwords": {
      "endpoints": {
        "authorization": "http://trunk.test/wp-admin/authorize-application.php"
      }
    }
  }
}
```

App ID

— uuidtools.com/v5

— `ns:DNS` + domain name for your app

— `ns:URL` + URL for your app

UUID Version-5 Generator

Enter identifier for pre-defined UUIDs

ns:DNS - for domain names

Select pre-defined UUID identifier. We translate the selected identifier to the corresponding well-known UUID internally. Toggle the switch above to enter your own namespace UUID.

wpmaildebugger.com

Required. Name can be anything. The same namespace with the same name will always produce the same UUID.

Generate UUID

Results:

Copy UUID | Copy API Call

35b7de34-b0e0-53be-9f75-1404a667b41b

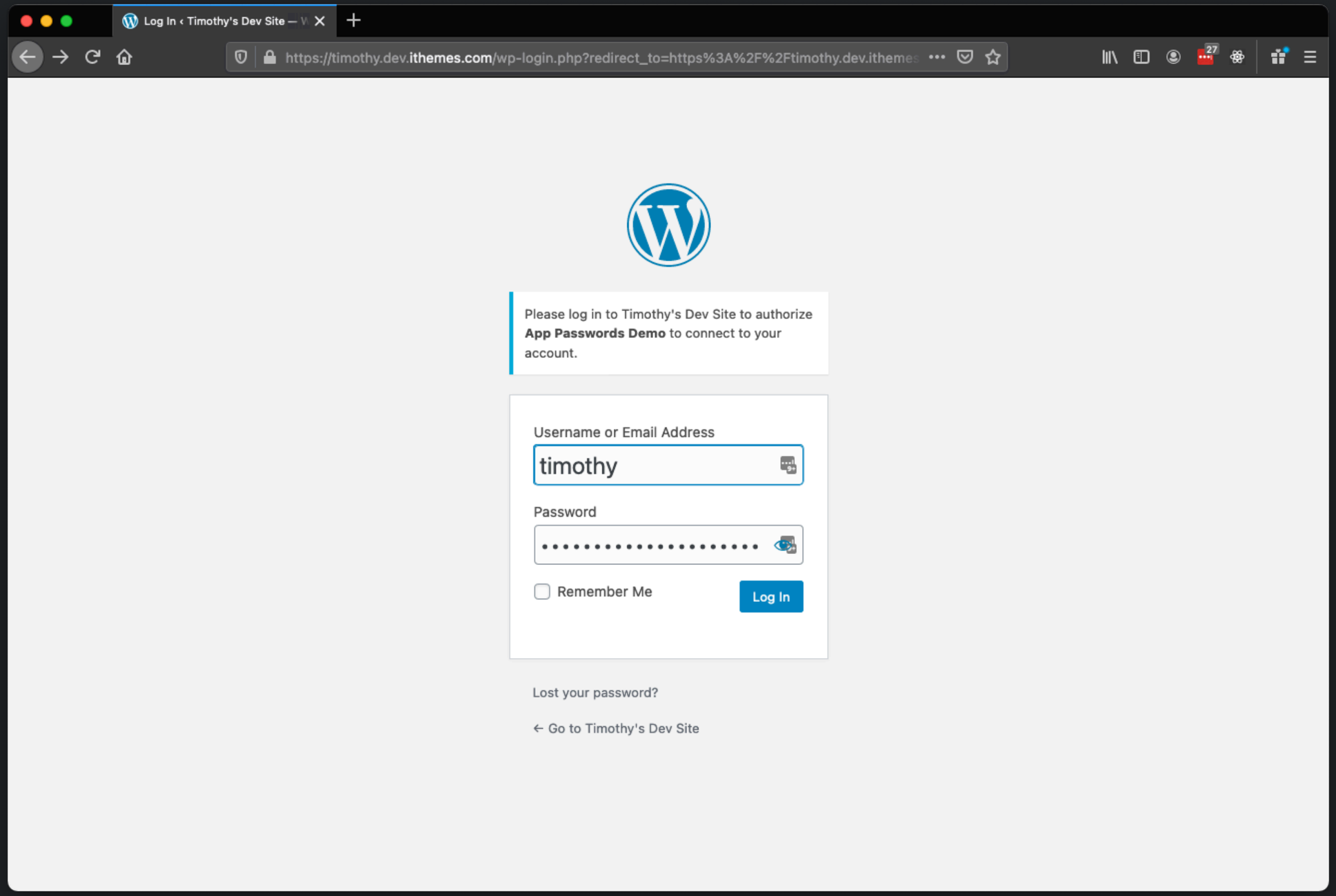
Redirect

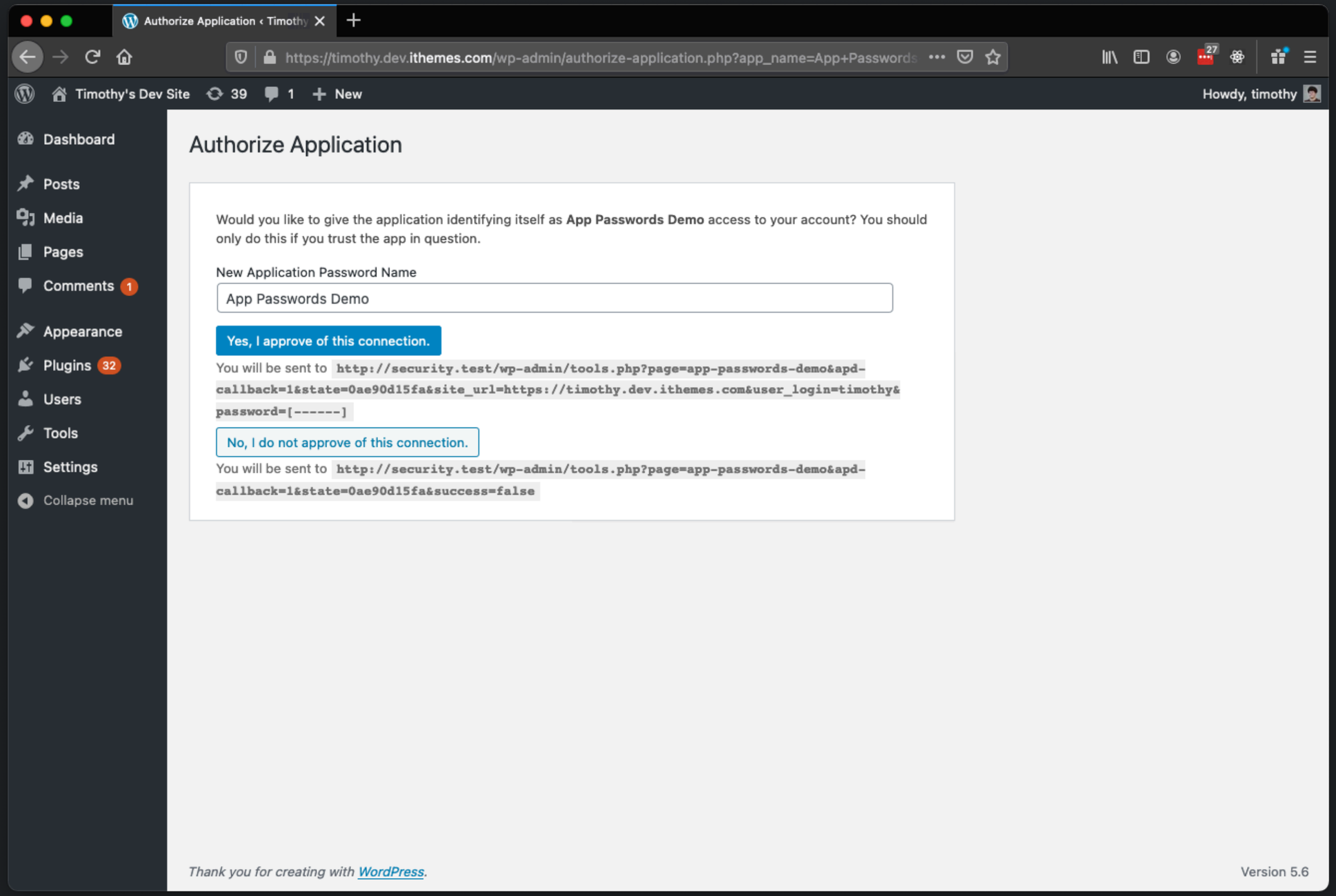
— `app_name` The name of your application. Shown to your users when they are authorizing your app. Can be changed.

— `app_id` A UUID identifying your application.

— `success_url` Where the user is redirected after approving the connection

— `reject_url` Optional. Where the user is redirected after rejecting the connection.


Log In ‹ Timothy's Dev Site —
https://timothy.dev.ithemes.com/wp-login.php?redirect_to=https%3A%2F%2Ftimothy.dev.itheme
Please log in to Timothy's Dev Site to authorize **App Passwords Demo** to connect to your account.
Username or Email Address
timothy
Password
Remember Me
Log In
Lost your password?
← Go to Timothy's Dev Site


Authorize Application ‹ Timothy
https://timothy.dev.ithemes.com/wp-admin/authorize-application.php?app_name=App+Passwords
Timothy's Dev Site
39
1
New
Howdy, timothy
Dashboard
Posts
Media
Pages
Comments 1
Appearance
Plugins 32
Users
Tools
Settings
Collapse menu
Authorize Application
Would you like to give the application identifying itself as App Passwords Demo access to your account? You should only do this if you trust the app in question.
New Application Password Name
App Passwords Demo
Yes, I approve of this connection.
You will be sent to http://security.test/wp-admin/tools.php?page=app-passwords-demo&apd-callback=1&state=0ae90d15fa&site_url=https://timothy.dev.ithemes.com&user_login=timothy&password=[------]
No, I do not approve of this connection.
You will be sent to http://security.test/wp-admin/tools.php?page=app-passwords-demo&apd-callback=1&state=0ae90d15fa&success=false
Thank you for creating with WordPress.
Version 5.6

Handling the Redirect

— CSRF. Use a nonce.
— `site_url` The connected website's `site_url()`
— `user_login` The username of the user
— `password` The app password

Handling the Redirect

```
http://security.test/wp-admin/tools.php?
page=app-passwords-demo&
apd-callback=1&
state=0ae90d15fa&
site_url=https://timothy.dev.ithemes.com&
user_login=timothy&
password=[------]
```

Handling the Redirect

abcd EFGH 1234 ijkl MNOP 6789

Credentials Storage

— App Passwords have the same permissions as the user.
— Must be stored securely.
— PHP `defuse/php-encryption`
— WordPress sodium-compat

Credentials Storage

```php
function store_credentials( $user_id, $api_root, $username, $password ) {
    $key        = get_secret_key();
    $nonce      = \Sodium\randombytes_buf( \Sodium\CRYPTO_SECRETBOX_NONCEBYTES );
    $ciphertext = \Sodium\crypto_secretbox( $password, $nonce, $key );

    update_user_meta( $user_id, META_KEY, [
        'ciphertext' => bin2hex( $ciphertext ),
        'nonce'      => bin2hex( $nonce ),
        'username'   => $username,
        'api_root'   => $api_root,
    ] );
}
```

Credentials Storage

```php
function get_credentials( $user_id ) {
    $meta = get_user_meta( $user_id, META_KEY, true );

    $key        = get_secret_key();
    $nonce      = hex2bin( $meta['nonce'] );
    $ciphertext = hex2bin( $meta['ciphertext'] );
    $plaintext  = \Sodium\crypto_secretbox_open( $ciphertext, $nonce, $key );

    return [ $meta['api_root'], $meta['username'], $plaintext ];
}
```

Make Authenticated Requests

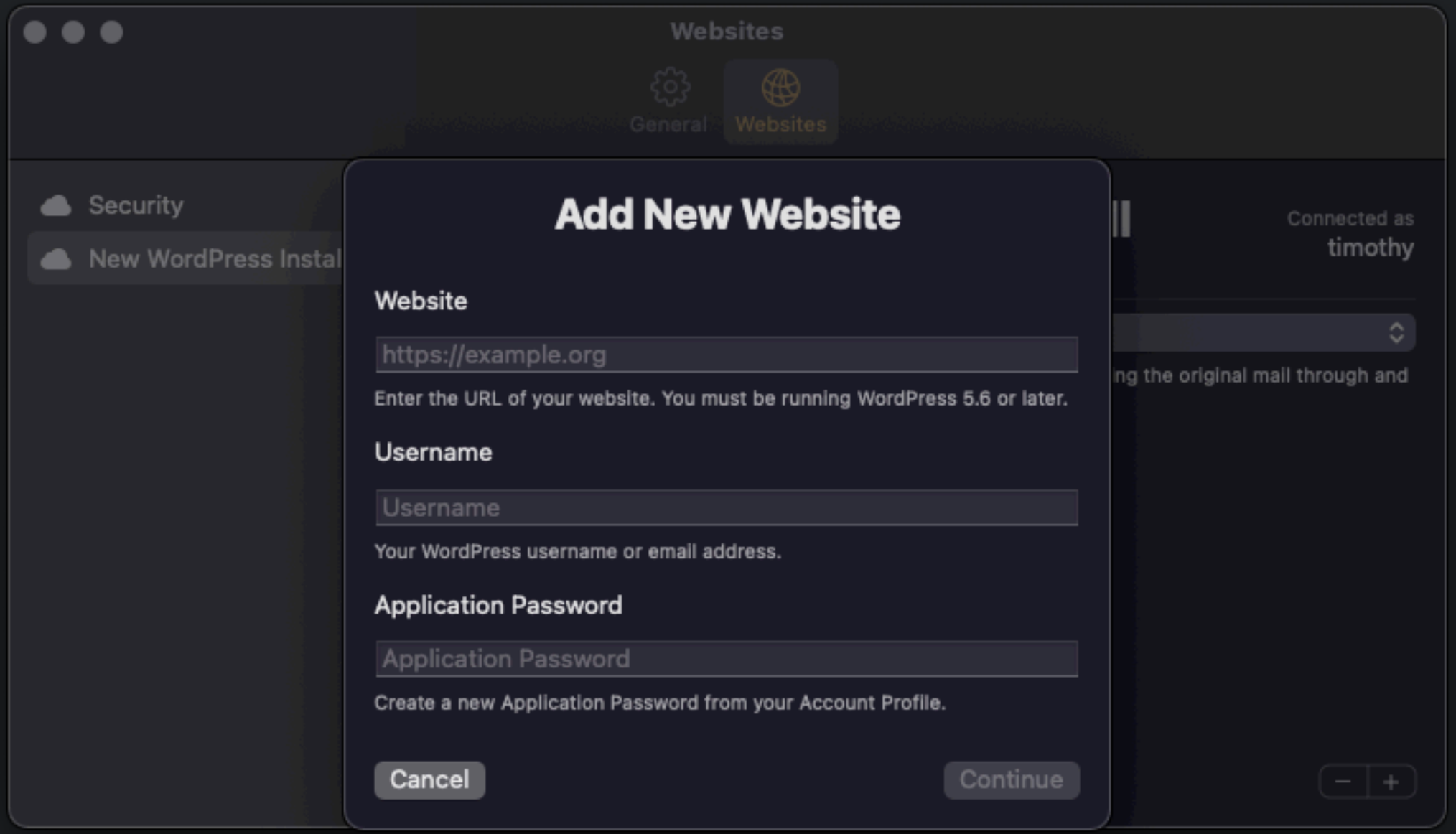
Basic Authentication

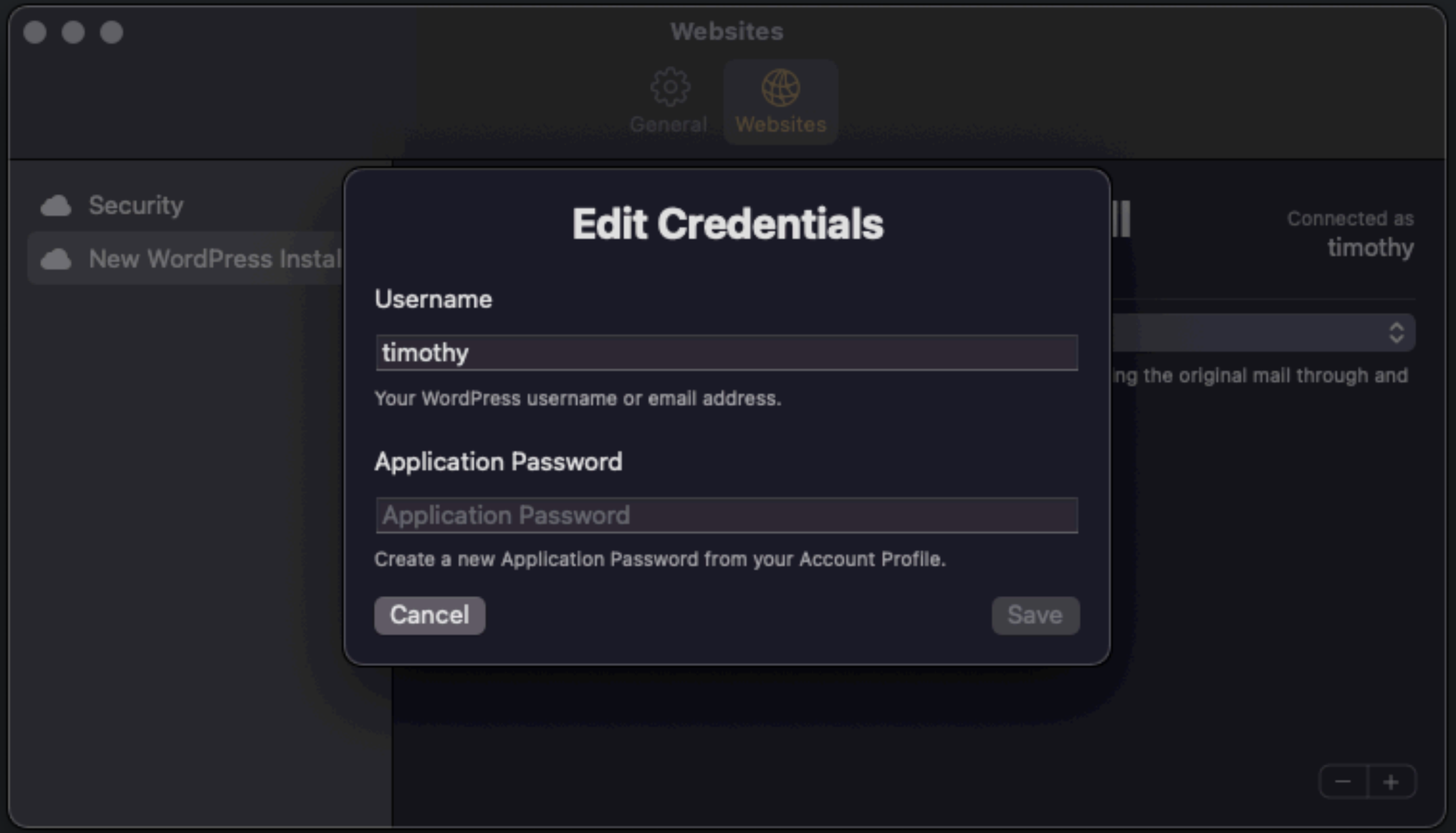
```php
$auth = 'Basic ' . base64_encode( "{$username}:{$password}" );
$headers['Authorization'] = $auth;
```

```js
const auth = 'Basic ' + btoa( username + ':' + password );
headers.Authorization = auth;
```

Keep in Mind

— Allow non-interactive authentication
— Editing credentials
— May be disabled for users
— Handle revocation (`incorrect_password`)
— Uninstall


Websites
General
Websites
Security
New WordPress Instal
Connected as
timothy
ng the original mail through and
Add New Website
Website
https://example.org
Enter the URL of your website. You must be running WordPress 5.6 or later.
Username
Username
Your WordPress username or email address.
Application Password
Application Password
Create a new Application Password from your Account Profile.
Cancel
Continue


Websites
General
Websites
Security
New WordPress Instal
Connected as
timothy
ng the original mail through and
Edit Credentials
Username
timothy
Your WordPress username or email address.
Application Password
Application Password
Create a new Application Password from your Account Profile.
Cancel
Save

Gotchas

The Authorize Application request is not allowed. The success url must be served over a secure connection. The rejection url must be served over a secure connection.

```
add_action( 'wp_authorize_application_password_request_errors', function ( $error ) {
    $error->remove( 'invalid_redirect_scheme' );
} );
```

Gotchas

Application passwords are not available.

```
define( 'WP_ENVIRONMENT_TYPE', 'local' );
```

Gotchas

```
401 Unauthorized

fetch( url, {
    // ...
    credentials: 'omit'
} );
```

Gotchas

Your website appears to use Basic Authentication, which is not currently compatible with Application Passwords.

#52066

Roadmap

- 5.7
  - Introspection
  - Fine Grained Capabilities
- 5.8
  - Capability Scoping

Resources

make.wordpress.org/core/2020/11/05/application-passwords-integration-guide/
gist.github.com/TimothyBJacobs/94de611c0d36cec70249feac7cf3eda9