

- [Home](#)

-- Main Menu --

Jan
14

By [chovy](#)

0

Tweet

0

Like

Self-signed certs with secure WebSockets in Node.js

Category: [Development](#), [JavaScript](#), [Node.js](#) | Tags: [JavaScript](#), [ssl](#), [websockets](#) [2 Comments](#)

First generate your self-signed certs:

```
openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 100 -nodes
```

Then create your httpsServer from an express app using node's built-in https server:

```
1  var privateKey = fs.readFileSync('sslcert/key.pem', 'utf8');
2  var certificate = fs.readFileSync('sslcert/cert.pem', 'utf8');
3
4  var credentials = {key: privateKey, cert: certificate};
5  var express = require('express');
6  var app = express();
7
8  //... bunch of other express stuff here ...
9
10 //pass in your express app and credentials to create an https server
11 var httpsServer = https.createServer(credentials, app);
12 httpsServer.listen(8443);
```

Then setup your websocket server (ironically this will use the same port as the http server, I didn't know this but I guess protocols can share ports? — this had me going for awhile).

```
1  var WebSocketServer = require('ws').Server;
```

```

2   var wss = new WebSocketServer({
3       server: httpsServer
4   });
5
6   wss.on('connection', function connection(ws) {
7       ws.on('message', function incoming(message) {
8           console.log('received: %s', message);
9       });
10
11      ws.send('something');
12  });

```

Now browse to `https://0.0.0.0:8443` server and accept the self-signed cert in Chrome. Then websockets should now work inside the browser.

Open a chrome devtools console and type:

```

1   var ws = new WebSocket('wss://0.0.0.0:8443');
2   ws.send('foo');

```

...or whatever host:port you used for `httpsServer`, the key here is you're using `wss://` protocol

In your node express web server you should see a message logged to the console. Start the server with `node ./server.js`

Related Posts:

- [Restart a Node.js app when the server reboots](#) I had some issues when I first setup my Debian VPS for my node.js app over at Wishd.me when the ISP rebooted my server a couple of times unexpectedly and my node app didn't come back online. I didn't find many options out there, so I wrote a node-startup script...
- [Setup email forwarding with Postfix on Debian](#) As you are probably aware, setting up a fully functional email server is a daunting task to say the least. On my dedicated server I wanted to have simple email forwarding for email aliases on my domain. For example `help@example.com` would forward to my Gmail account. I didn't want to...
- [Testing a node.js express app with Mocha and Should.js](#) I've been doing more Test Driven Development the past few months with my node.js application code base. With my latest project Wishd.me, I decided to get started early with writing tests. While skeptical at first, I have to admit it does save quite a bit of effort in debugging and...

2 Comments

Chovy's Blog

 Login ▾

 Recommend

 Share

Sort by Best ▾



Join the discussion...



Henry Umbo CV · 3 months ago

Hi Chovy,

thanks for this wss: tutorial, but I'm struggling to get it to work as

while running that node.js server,

I get this error from the Chrome browser debug console:

```
> var ws = new WebSocket('wss://0.0.0.0:8443');
```

```
< undefined
```

x WebSocket connection to 'wss://0.0.0.0:8443/' failed: WebSocket opening handshake was canceled

The Chrome version I'm using is 42.0.2311.135.

The firefox (version 37.0.2) returns undefined as well.

TsongHong

1 ^ | v • Reply • Share ›



Ahmed Sabry → Henry Umbo CV • 2 months ago

you can fix this problem via:

From you browser (eg. chrome) go to https://0.0.0.0:8443 you will get an warning "Your connection isn't private" -> click "Advanced" button Proceed to 0.0.0.0 (unsafe) and now you can try wss without problems.

^ | v • Reply • Share ›

ALSO ON CHOVY'S BLOG

WHAT'S THIS?

Cool AJAX Sites

5 comments • 5 years ago



Greg — Pikipimp One of the most fun website out there. Upload a photo and add objects. An ajax style interface ...

Make samba create files with usable group permissions

3 comments • 3 years ago



pkelly — I'm about to pull my hair out over this stuff...it would be great if you could help me. I want to accomplish ...

Javascript Loop: Multidimensional Associative Arrays

1 comment • 3 years ago



DarrenPRILEREURSERT — The best forum so far

Gimp: Rounded Corners Radius

1 comment • 3 years ago



chovy — i will probably update this soon enough, as i've been playing with gimp alot lately.



Subscribe



Add Disqus to your site



Privacy



-
- [chovy](#)
- UI Engineer



Tip me in Bitcoin

1HE1pmb27RMc298gkerJX333oshNtL6NQ2



Recent Posts

- [Self-signed certs with secure WebSockets in Node.js](#)
- [Fibonacci generator using EcmaScript 6 \(es6\)](#)
- [A gentle introduction to bitcoin](#)
- [Example of \\$resource in Angular.js with update and save using a resolver.](#)
- [Setup email forwarding with Postfix on Debian](#)

Categories

- [Bitcoin](#) (1)
- [Development](#) (25)
- [JavaScript](#) (7)
- [Linux](#) (12)
- [Node.js](#) (5)
- [NoSQL](#) (1)
- [Perl](#) (3)
- [PHP](#) (2)
- [Ruby on Rails](#) (4)
- [UI Design](#) (61)

Projects

- [Github Projects](#)
 - [Wishd.me social wishlist](#)
-

© 2015 [Chovy's Blog](#)

Powered by [WordPress](#) and the [Designfolio Theme](#).