CrossBrowserTesting
A SMARTBEAR COMPANY

# CrossBrowserTesting's Platform Security

## Introduction

CrossBrowserTesting in the all-in-one web testing platform that allows users to run parallel automated tests, compare screenshots, and remotely debug on 1500+ real desktop and mobile browsers. With one of the largest Selenium grids in the cloud, users trust CrossBrowserTesting for testing responsiveness, functionality, and debugging in order to derive top quality from their web applications. Whether manual testing or through automation, users can confidently know they have access to the very configurations their users are on.

## Summary

At CrossBrowserTesting we hope to enable you to test faster, broader, and with more accuracy. We also recognize that entrusting your applications with us requires a certain degree of trust, which is why we have worked hard to create a platform that allows customers of all sizes from individual designers to large enterprises to test their web based applications without having to worry or think about security.

The privacy of our customers' testing and data is paramount and the entire service has been built around ensuring we protect both. The following includes details outlining how we continually prioritize security at CrossBrowserTesting to ensure uncompromised trust from our users.

## Application Level Security

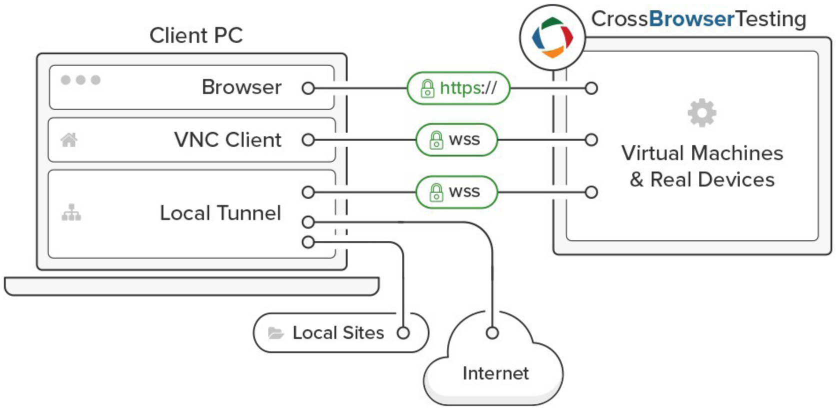
CrossBrowserTesting stores customer passwords in an encrypted format, and all login and payment information is passed over secure HTTPS connections. We utilize Authorize.net for maintaining credit card account information and do not store any credit card information at CrossBrowserTesting. This means we can not access this information during or after testing, so you won't be surprised to see hundreds of dollars of online shopping charges from someone at the Memphis HQ, or anyone else for that matter.

## Network Access

HTTPS is used throughout the entire platform, providing a secure, encrypted connection that ensures safety of any data passing through the application. In addition, the HTML5 based VNC viewer utilizes secure websockets (WSS) as the transport protocol between the CrossBrowserTesting servers and the end user's client, adding an additional layer of security.

## Local Tunnels

CrossBrowserTesting allows you to test not only public sites, but also develop and test sites behind firewalls and within your network. We create a secure shell (SSH) tunnel from your machine to our server. When you launch a test in our system while you have a local tunnel connected, that browser sends all traffic via this secure tunnel to your machine, where the request is handled and sent back to the remote browser to be rendered. This allows you to test your website on full-scale browsers before going live, allowing you to keep information private from the access of the rest of the internet you don't want seeing your content and data. With our SSH technology, you cane easily test behind your firewall, across a proxy, or on local files.



### We have two methods for creating the local connection:

- Chrome extension
- Node.js module

Both the Node.js module command line tool and the Chrome browser extension create a secure connection between CrossBrowserTesting servers and the client PC using secure websockets (WSS). The tunnel is strictly limited to the user account that created the tunnel. All tunnels must be explicitly be initiated by the end user, CrossBrowserTesting has no ability to initiate connections into the user's environment.

### To disconnect the tunnel, you can:

- **Chrome Extension:**
  - Click the Disable Tunnel button in the browser.
  - Close the browser window it was launched from.
- **Node.js module**
  - Stop the command line execution.

Should a user forget to stop the local Tunnel connection, the system will automatically disconnect the tunnel after one hour of inactivity.

### Test Across a Proxy

Test websites that need to be access via a proxy server by supplying the IP and Port, allowing for GeoLocation testing.

## Privacy

All data from a testing session including cookies, browser history, cached data, and saved browser passwords are cleansed after each use to ensure the next customer to request a configuration receives a pristine environment, and none of your testing or web application data can be obtained or viewed by us or other users.

This is done in different ways depending on the environment:

### Virtual machines

The Windows, Linux, Windows Phone emulator, Android emulators, iPhone & iPad simulators and Mac OSX configurations are spun up from frozen disk images on virtual machines. These snapshotted images are reverted after each use to their original, frozen state and are images are never re-used for multiple tests. This process ensures the security and privacy of our customers' data.

### Physical Mobile Devices

Physical devices are locked down so only the browsers can be run. After each use, our unique cleaning process removes all traces of use including the browser history, cache, cookies, and any other saved data on the device. This ensures each test begins at a consistent starting point and doesn't have to worry about data getting into the wrong hands or being sold to unauthorized sources

## Test Results

CrossBrowserTesting allows users to take snapshots and videos of live tests. These recordings are critical to the QA process, allowing users to document issues and securely communicate them to others without requiring the recipient to have a license to CrossBrowserTesting. In addition, users can capture network packet recordings of any tests, allowing them to see the HTTP request stream from a page request. Similarly, the Screenshot system also captures and saves screenshots of the URLs tested. All of these resources are transported over HTTPS and stored securely on Amazon S3.

## Environment

CrossBrowserTesting uses a private hosting facility to ensure the security of the testing infrastructure. All systems, virtual machines, physical Mac minis, iPhones, iPads, and physical Android devices are located in this secured facility. This facility is located at our headquarters in Memphis, Tennessee, with restricted access where only our small team has access to these devices and has gone through extensive background check.

### Data Center Details

- Internet connectivity through multiple gigabit network connections utilizing Cisco high bandwidth routers.
- High reliability (99.9%+).
- Secure, temperature-controlled premises.
- Secured rack space for email and/or other web server(s).
- Network monitoring 24 hours a day, 7 days a week.
- Security camera surveillance 24/7.
- Controlled office alarm system.
- Security guard protection services.

## Privacy Policy

1. Before or at the time of collecting personal information, we will identify the purposes for which information is being collected.
2. We will collect and use of personal information solely with the objective of fulfilling those purposes specified by us and for other compatible purposes, unless we obtain the consent of the individual concerned or as required by law.
3. We will collect personal information by lawful and fair means and, where appropriate, with the knowledge or consent of the individual concerned.
4. Personal data should be relevant to the purposes for which it is to be used, and, to the extent necessary for those purposes, should be accurate, complete, and up-to-date.
5. We will protect personal information by reasonable security safeguards against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.
6. We will make readily available to customers information about our policies and practices relating to the management of personal information.

We're always looking for customer feedback. For additional information on security or suggestions on how we can further guarantee user privacy, reach out to us at info@crossbrowsertesting.com