https://www.utest.com/articles/an-introduction-to-charles-web-proxy-for-desktops-and-smartphones

Daniel D.
3 years ago

An introduction to Charles Web Proxy for Desktops and Smartphones

Tools Learning

favorite_border 262 Likes

flag notifications

Some test cycles require extended logging of the internet traffic from and to your device or a connection routed through a proxy server. For that purpose, you will probably have to deal with the **Charles Web Proxy** software. This article shall guide you through your first steps and the overall configuration. The procedure may seem to be a little complicated at the beginning, but bear with me: once you have finished the initial setup, its future use just requires about 30 seconds to get everything ready. *So let's get started!*

We want to...

1. ... download and install *Charles*
2. ... connect a Smartphone or Tablet to *Charles*
3. ... capture SSL traffic using *Charles*
4. ... export device logs for attaching them to bug reports

1. Download and installation

Although *Charles* is not an open source software or a free tool, a demo version is available. It can be downloaded and used for free, but limits each session to **30 minutes**. Consequently, you have to restart the software now and then, if you want to use it for a more extended period. But now head to the link below and download the appropriate version for your operating system.

Download Charles Web Proxy

As I am using Windows, I am going to download the *Windows 64bit* edition, and I will stick to this version within the next steps. Once you have finished the installation, start the software via the start menu. You will have to wait 10 seconds at every start. It should look something like below.

---

2. Connecting your devices

As *Charles* is running now, we want to route all the network traffic from and to our devices through it. Depending on the device you plan to use, please perform the following steps matching your device(s).

Desktops

You are already done! As soon as *Charles* is running, it will automatically capture and record all browser traffic. This procedure typically covers the most common browsers like Chrome, Firefox, Safari, Edge and the Internet Explorer. You can quickly check the proxy connection though:

1. Be sure, that **Windows Proxy** is enabled in the **Proxy** menu.
2. May click the broom button (leftmost) in the *Charles* toolbar to clean the logs.
3. Open your browser and navigate to a random site.
4. You shall see new log entries popping up in the *Charles* log now.
5. You can also pause and resume the logging at any time using the second red/ grey button in the toolbar.

/api/v1/uploads/36793/2017-10-26_20h21_22_3.gif

If you can see your log filling up, you are good to go!

Mobile devices

Gathering two crucial information first

Before we can configure your mobile device to use *Charles*, we need to know the IP address of your computer (running *Charles*) and the port. This can quickly be done:

1. Click **Help** > **Local IP Address** to locate your IP. The address consists of four blocks of one to three digits each. It most certainly starts with `192` and must not end with `1`. It is `192.168.178.100` in my case.

2. We will also need to know the port, that *Charles* is using. It is `8888` by default, but you may check via **Proxy** > **Proxy Settings...**. It is the *HTTP Proxy Port*. You can also click the gear icon in the toolbar and select **Proxy Settings...** there.

/api/v1/uploads/36794/2017-10-26_20h39_33.gif

You are going to need both numbers in the next step.

Important note when connecting new mobile devices

Once a new device tries to connect to your *Charles* session, *Charles* will ask you to **grant the permission** to do so. Be sure to allow your connection. Please also **disable or appropriately configure any firewall or internet security** and be sure to permit incoming traffic to *Charles* respectively to port *8888* or the port, you determined for *Charles* before.

Connect your Android smartphone

To connect your Android smartphone, just head to the WiFi settings and proceed:

1. Go to **Settings** > **Network & Internet** > **Wi-Fi**
2. Locate your active connection, long-tap it and select **Modify network**
3. Expand the *Advanced options*, tap at **None** below *Proxy* and select **Manual**
4. Enter your IP address from the previous step in the *Proxy hostname* field and the port into the *Proxy port* field
5. Tap **Save**. Done!

/api/v1/uploads/36816/2017 10 27 02 58 17-1_1.gif

The settings on your device may look slightly different, but you should find the right area to modify the WiFi network. It will be located around the WiFi network, to which you are currently connected.

Connect your iOS device

To connect your iOS device, please follow these steps:

1. Tap **Settings**
2. Tap **WiFi**
3. Tap **(i)** right to your selected WiFi network
4. Scroll to the bottom to the **HTTP PROXY** section
5. Tap **Manual**
6. Enter the IP address from above in *Server*
7. Enter the port from above in *Port*

Connect your Windows Phone

To connect your Windows Phone device, please do the following:

1. Tap **Settings**
2. Tap **Network & Wireless ***
3. Tap **WiFi**
4. Long tap your connected network
5. Tap **Edit**
6. Tap **Proxy** > **Manual Setup**
7. Enter the IP address from above in *Address*
8. Enter the port from above in *Port*

---

3. Capturing and decrypting SSL traffic

As soon as customers require you to use *Charles*, they want to know what your mobile device is doing during its communication with their services. If this communication is encrypted, which is great for our day to day security, this traffic needs to be decrypted using a certificate. We are now going to install this certificate to allow *Charles* to listen to that communication. Let's start with the desktops again.

Installing the desktop certificate

Fortunately *Charles* already includes this certificate and allows us to install it using the menu easily. We have to circumvent a possible pitfall though. Just follow me through the process:

1. Within *Charles* click **Help** > **SSL Proxying** > **Install Charles Root Certificate**
2. In the new window click **Install certificate** and confirm the first screen unchanged
3. Now select the second option **Place all certificates in the following store**
4. Choose **Trusted Root Certification Authorities** as the store and finish the certificate installation wizard

/api/v1/uploads/36799/2017-10-26_22h09_25.gif

Please don't mind my German certificate wizard, but I you should be able to follow the general procedure nonetheless. After finishing the wizard, you can close the certificate window.

Installing the certificate on your mobile device

To install the certificate on your mobile device, just do the following:

1. Be sure, that your device is successfully connected to your *Charles* session:
   a. Proxy is set to *Manual* and configured in your WiFi settings
   b. Please disconnect any active **VPNs** to avoid issues during the *Charles* session
   c. Charles is running and the permission for your device has been granted
   d. You can browse on your phone and new logging entries appear within *Charles*
2. Head to the address chls.pro/ssl (which leads to charlesproxy.com/getssl/) on your mobile device
3. This downloads the certificate and should automatically open an installation prompt
4. May insert a name for the certificate like *Charles Proxy*, if you have to, and confirm the installation
5. Please use Google and try searching for *iOS install certificate* for instance, if the installation process is unclear

If you are using iOS 10.3 or higher
Please additionally follow these steps to trust the certificate:

1. Navigate to **Settings**
2. Tap **About**
3. Tap **Certificate Trust Settings** (bottom of the list)
4. Trust the *Charles Root Certificate*

Enabling HTTPS proxying

As our devices are set up for SSL logging now, we just have to enable SSL proxying within *Charles*. Don't mind; this is quickly done:

1. Within *Charles* click **Proxy** > **SSL Proxying Settings...**
2. In the *SSL Proxying* tab tick **Enable SSL Proxying** and click the **Add** button below
3. Enter an asterisk `*` as *Host* and `443` as *Port*
4. Now click **OK** and **OK** again

/api/v1/uploads/36800/2017-10-26_22h24_02.gif

Please restart *Charles* afterwards.

Tailoring the coverage to your needs

In step 3. you were asked to enter `*` as the *Host*. This *wildcard* character enables the SSL proxying for every possible web address or service, you may visit. Though you might want to tailor the

proxying and therefore logging to your needs via specifically including certain addresses or parts of addresses. Using wildcards provides a very versatile way of *filtering* specific URLs, which you want to cover.

This can become very handy, if you want to limit the coverage to an app or page under test. Let me provide some examples:

1. `*utest*` would cover every traffic from and to *utest*, which includes *platform.utest.com*, *utest.com/articles* and so on
2. `*platform.utest*` would include everything from and to *platform.utest.com*, but not *utest.com/articles* for instance
3. `*utest.com/articles*` would cover the entire *articles* section, but no other section or *platform.utest.com*. Though it *would* cover *platform.utest.com/articles/...* if such websites would exist.

So just take the relevant part of the address, may include, exclude or limit to sub domains like *platform* in `platform.utest.com` and replace the rest of the address with a `*` to allow every string or even no string (zero or more characters) at its place. You can also use the wildcard `?`, which exactly replaces one single character. So `ut?st` would match *utest* or *utast*, but not *utst* or *uteast*.

Nearly done! Just one step.

---

4. Capture SSL logs

Now as *Charles* is running with the right settings, as the certificates have been installed, as your devices are configured to use *Charles* on your computer and as SSL proxying is enabled, **we are good to go**!

Let us conclude the steps to collect logging information and to export them for to the benefit of a bug report:

1. Clear the *Charles* log using the broom button
2. Be sure, that logging is active (red button in the toolbar)
3. Perform your actions or steps to reproduce an issue
4. Stop the logging by clicking the red button

5. Head to **File** > **Save Session as...**
6. Choose a folder and pick a file name (please do not use periods in the name)
7. Upload the log ending with `.chls` to your bug report
8. **Done!**

More Charles resources

This article shall cover the basic usage of Charles with your devices. However, may also have a look at this uTest article by @wk Wei Kee Teoh which provides some more details and useful info. You can also find many more Charles articles with tips and tricks on the platform.

Tidying up

After you have finished your *Charles* session be sure to close the software and to revert your WiFi settings on your mobile devices to their prior state. Therefore set the *Proxy* to **None** again in the WiFi settings. You also want to remove the certificate from your devices if they are your privately used desktops, smartphones and tablets and not only meant for testing. Please just use Google to receive instructions on how to remove a certificate. It mostly required a few steps only. And now:

Congratulations to your first *Charles* log!

/api/v1/uploads/36810/badge@2x.png

Thank you for not giving up. Let me grant you the (yet unofficial) **Logging Badge Of Endurance**

If you ever want to start logging in the future, just start *Charles* and add the IP address and port to your WiFi settings again. If you should have removed the certificate, remember to add it back, too. *I hope, everything was working out in your environment. Please let me know in the comments, if steps remain unclear or if other issues arise.* ***Good logging!***