≡ **Tealium** **Learning Center**

Sign In   Help

Tealium for Android

| Search the Tealium Learning Center | This Board | 🔍 |

⚙

≡

Setting up Charles to Proxy your Android Device

This article describes the steps required to set up your Android device to proxy network requests through Charles, which is helpful for troubleshooting or debugging your implementation of Tealium for Android.

In this article:

- Configuring Charles Proxy
  - Identifying Your IP Address
  - Configuring Your Android Device to use the Charles Proxy
  - Additional Configuration Steps for Android N and Above
- Tips to Filter Your View of Network Traffic
- Clearing Certificates and Removing the PIN from a Device
- Additional Resources

Configuring Charles Proxy

Use the following steps to configure Charles Proxy:

1. Go to **Proxy > Proxy Settings**.
2. In the **Proxies** tab enter 8888 in the **HTTP Proxy Port** field.
3. Go to **Proxy > SSL Proxying Settings**.
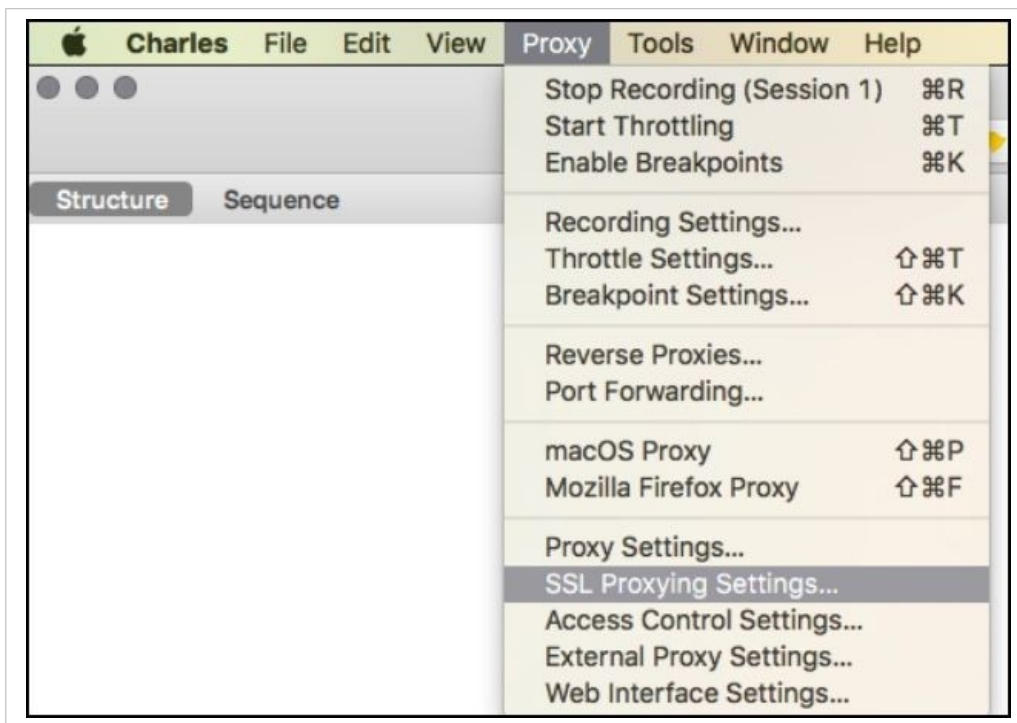
4. Click the **SSL Proxying** tab and check the **Enable SSL Proxying** checkbox
   to configure a location.
   By default, Charles will only perform SSL proxying for specific domains you include in
   the list.
   To save listing all URLs you wish to inspect, you can use a location of `*.*` as a
   wildcard, and SSL proxying will be enabled for all domains:

> ℹ **Note**
>
> If your app ceases to function correctly, it is possible that the app is rejecting the

self-signed certificate from Charles Proxy. If this happens, disable the wildcard match, and list only the Tealium domains. Recommended domains are: `*.tealiumiq.com` `*.tiqcdn.com` .
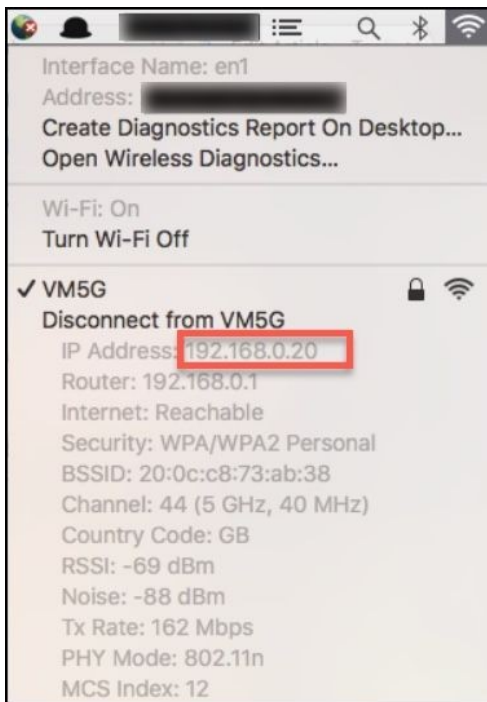
5. The port default value is `443` .

You can leave this field blank, as Charles will set it automatically.

Identifying Your IP Address

1. Go to **System Preferences** > **Network** > **Wifi** > **Advanced** > **TCP/IP**.

⭐**Tip**

On a Mac, you can hold down the Option key while clicking on the network icon in the system tray.

2. Make note of the **IPV4 Address**, as it will be needed in later steps.

Configuring Your Android Device to use the Charles Proxy

Use the following steps to configure your Android device to use Charles proxy:

1. Go to **Settings > Wifi**.

2. Press and hold down the power key on the Wifi Network device you are currently

connected to.

3. When the modal displays, select **Modify Network**.

4. Select **Show Advanced Options** to display proxying options.

5. Under *Proxy*, select **Manual**.

6. In the *Proxy Host Name* box, enter the IPV4 Address you previously saved from your development machine.

7. In the *Proxy Port* field, enter 8888 , as when configuring Charles.

8. Click **Save** to save the settings and exit.

9. Open a browser on your device to test.

   Charles displays a dialog prompting you to allow or deny SSL proxying.

10. Click **Allow**.

    If you are not prompted to allow SSL proxying, restart Charles and try again.

11. Go to http://charlesproxy.com/getssl from your device and download the Charles SSL certificate.

    On newer versions of Android, you may get an error on downloading, such as "download unsuccessful".

    If this happens, use the following instructions:

    - Go to **Help** > **SSL Proxying** > **Save Charles Root Certificate**.
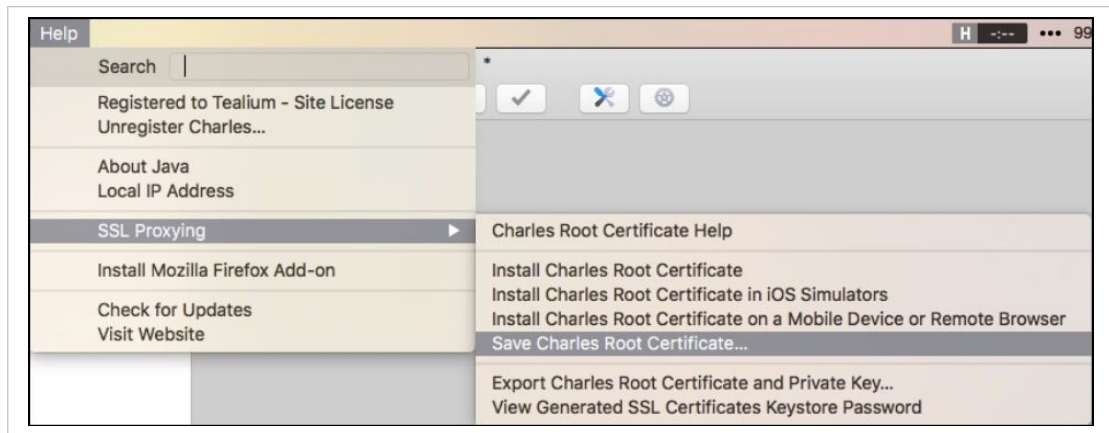
- Change the file type from the default `.pem` to `.cer` and save in a location that you will remember for later.
- Transfer the `.cer` file to your device using an SD Card, USB Cable, or remote transfer such as Google Drive.
- Open the file from a file manager such as the Android File Manager, or a third party file manager such as File Commander.
  You will be prompted to save the certificate.
- Continue with the remaining steps.

12. Name the certificate and okay it as a trusted certificate.
    Ensure that you disable or remove it when complete.
13. Once the certificate is installed, you are prompted to set up a PIN.
14. When prompted, add the new PIN.

Additional Configuration Steps for Android N and Above

As of Android N, additional steps area required to to add configuration to your application so that it trusts the SSL certificates generated by Charles SSL proxying. This means that you can only use SSL proxying with applications that you control.

In order to configure your app to trust Charles, you must first add a Network Security Configuration File to your app. This file can override the system default, enabling your app to trust user-installed CA certificates, such as the Charles Root Certificate.

> ☆Tip
>
> In your configuration file, you can optionally specify that this only applies in debug builds of your application, so that production builds use the default trust profile.

Use the following steps to add the Network Security Configuration File and reference the

file in the manifest for your app:

1. Use the following example to create a Security Network Configuration file.

```
<network-security-config>
    <debug-overrides>
      <trust-anchors>
        <!-- Trust user added CAs while debuggable only -->
        <certificates src="user" />
      </trust-anchors>
    </debug-overrides>
</network-security-config>
```

2. Name the file `network_security_config.xml`.

3. Copy the file to `res/xml/network_security_config.xml`.

4. Next, use the following example to add a reference to the `network_security_config.xml` file to the manifest for your app.

```
<?xml version="1.0" encoding="utf-8"?>
<manifest ... >
    <application android:networkSecurityConfig="@xml/network_security_confi
        ...
    </application>
</manifest>
```

For additional information, go to the Charles Proxy SSL Certificates and scroll down to the **Android** section.

Tips to Filter Your View of Network Traffic

The following table provides tips used to filter your view of network traffic:

FILTER	ACTION
Filter by device	- To ensure that you only view traffic from your Android device and not the local machine, go to the Proxy menu and uncheck **macOS/Windows** proxy. - This step will disable Charles proxy for local traffic from your machine and Charles will only display traffic from remotely-connected devices

Filter by domain	• Filter your traffic to view only what you are interested in by clicking the **Sequence** tab in Charles and use the filter field to filter by domain, such as `collect.tealiumiq.com`. • Regex is also an option if you enable it in the search settings. • Enabling Regex allows you to use `*.tealiumiq.com` to view all hits going to the Tealium servers.

Clearing Certificates and Removing the PIN from a Device

Clearing the certificate and removing the PIN from an Android device is optional.

Use the following steps to clear the certificate, remove the PIN, or both:

1. Open the Settings application on your Android device.
2. Navigate to **Security > Clear Credentials** at the bottom of the list of options.
3. Click **Clear Credentials**.
4. Confirm that you want to clear the credentials.
5. To remove the PIN, navigate to **Settings > Lock Screen > Screen Lock** and remove the PIN.

Additional Resources

- Charles: SSL Proxying
- Tealium: Setting up Charles to Proxy your iOS Device

Tags: Charles Proxy   proxy app

Products

Tealium iQ Tag Management

Tealium EventStream

Tealium AudienceStream

Tealium DataAccess

Tealium for Mobile

Company

Tealium.com

Blog

Careers

Contact Us

Events

Copyright All Rights Reserved © 2008-2020