

Prerequisites

The series of steps below describes how to restore FaceTime service for unsupported macOS systems, targeting the incompatibility with the official general and minimum iCloud system requirements as of July 2025, the date this tutorial was compiled. Therefore, your setup must satisfy the following requirements:

✓ **Legacy Mac Proxy** or **Aqua Proxy** by **Jonathan Alland** (u/wowfunhappy: MacRumors, GitHub, Apple StackExchange)

✓ **Charles Proxy** by **xk72 Limited**

⚠ **Charles Proxy must be routed to listen on the default port used by either Mac Legacy Proxy or Aqua Proxy. Charles Proxy will monitor and intercept all the TLS connections that are passing through the former or the latter. The default port is localhost:3128 for Mac Legacy and localhost:6531 for Aqua.**

⚠ **For optimal performance, Aqua Proxy is recommended.**


🔧 **The valid Charles configuration:**

✓ Proxy (menu bar) ► MacProxy checked

✓ Charles is a startup item. Proxy (menu bar) ► Proxy Settings ► MacOS. Check everything except SOCKS, then “OK”.

✓ Proxy (menu bar) ► External Proxy settings. Enable Web Proxy and Secure Web Proxy, and set both to either localhost:3128 (Mac Legacy Proxy) or localhost:6531 (Aqua Proxy), then “OK”.

Step 1: Compose a new request

In the menu bar, choose Edit ► Compose (or press ⌘M); alternatively, click on  in the tool bar of the main Charles window.

Step 2: Assemble the new request to send the following headers

✓ **URL:** `https://setup.icloud.com/setup/iosbuddy/loginDelegates`

✓ **Method:** `POST`

✓ **Content type:** `text/plist`

After filling in the headers, select the tab “**Raw**” at the bottom of the window (underneath the large text box “**Query Parameters**”)

Step 3: “Query Parameters”

Paste the text below to this box.

```
POST /setup/iosbuddy/loginDelegates HTTP/1.1
Host: setup.icloud.com
Proxy-Connection: keep-alive
Accept: */*
Accept-Encoding: gzip, deflate
Content-Type: text/plist
Accept-Language: en-us
X-MMe-Country: US
X-MMe-Client-Info: <iPod4,1> <iPhone OS;6.1.6;10B500> <com.apple.AppleAccount/
1.0 (com.apple.Accounts/113)>
Connection: keep-alive
User-Agent: Accounts/113 CFNetwork/609.1.4 Darwin/13.0.0
Content-Length: 546
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>apple-id</key>
<string>YOUR ID HERE</string>
<key>client-id</key>
<string></string>
<key>delegates</key>
<dict>
<key>com.apple.facetime</key>
<dict/>
<key>com.apple.gamecenter</key>
<dict/>
<key>com.apple.madrid</key>
<dict/>
<key>com.apple.mobileme</key>
<dict/>
</dict>
<key>password</key>
<string>YOUR PASSWORD HERE</string>
</dict>
</plist>
```

Step 4. Providing the required values to the XML payload of the request

- In the text you've just pasted, find the text block enclosed in the tags `<plist>...</plist>`.
- Identify the key ***apple-id*** and replace the placeholder YOUR ID HERE with your **actual AppleID**.
- Do the same with the key ***password***, only replace "YOUR PASSWORD HERE" with your **actual AppleID account password**.

Step 5: Adding a verification code

You have two options:

Option #1:

Click **Execute** button. A 6-digit verification code will be sent to your trusted devices.


Append the code to your password you entered in the previous step (that is, to your **AppleID** password you entered in place of the “YOUR PASSWORD HERE” dummy text).

Option #2 (easier):

On your trusted Apple devices (iOS or iPadOS):

Navigate **Settings** ► **AppleID** (or **iCloud**, depending on the system) ► **Password & Security**. Tap **Get Verification Code**.

Append the on-the-fly generated verification code to your **AppleID** password from **Step 4**.

 Keep monitoring all the activity in the **Sequence View** of the main Charles window.

Step 6: Extracting the Apple Authorization Token

Click **Execute**

You will receive a response from Apple, containing another XML-formatted payload, which stores the required authorization token.

Pause the session recording temporarily. Switch to the **Response** tab of the current connection inspection view.

Following which Do this:

Response: look for the label **com.apple.facetime** inside the XML payload and the sublabel **auth-token** inside **com.apple.facetime**.

Copy the entire value (the garbled text) of the auth-token key. You may save it to the “Notes” notepad of the requests inspection window. You’ll need it later.

Step 7: Activate the Rewrite tool.

Tools ► Rewrite... (or press   E)

Add a new set: Add ► Locations. Paste ***.ess.apple.com**, then **“OK”**.

Make a new rule (Rule #1) by clicking on **“Add”** underneath the **Body** listbox.


Choose **“Body”** from the **“Type”** dropdown menu and set the target by selecting the checkbox **“Response”**.

Paste `<key>retry-interval</key><integer>3600</integer>` into the **“Match Value”** box, then **“OK”**

Make **Rule #2** with the identical parameters except for **“Match Value”**.

Paste `<key>message</key>` into the **“Match Value”** box, then **“OK”**.


Make **Rule #3** with the identical parameters except for **“Match Value”**.

 **Critical:** the box **“Regex”** must be checked for this rule!

Paste `<string>SED:3:VEN-PROD:+:EM</string>` into the **“Match Value”** box, then **“OK”**.

Make **Rule #4** with the identical parameters except for **“Match Value”**.

Paste `<key>status</key><integer>5068</integer>` into the **“Match Value”** box, then **“OK”**.

 **Resume the session recording and keep the Rules pane open for setting the replace value later!**

Step 8: Getting Verification Code Again.

Follow the procedure from **Step 5** to generate the 6-digit verification code on your iOS or iPadOS device.

Use the most recent verification code to log into **FaceTime** by appending it to your password (no spaces between the password and the code!), then **“Sign in”**.

Back to the **Sequence View**: track changes for a sender with the URL **https://profile.ess.apple.com/WebObjects/VCPProfileService.woa/wa/authenticateUser** and highlight it when it turns up. `·HYrk] `l`] `k] kkaḡf `j] [gj\af _l] e hgjYjatt` and switch to the **Response** tab of the current inspection view.

Response: in the XML-formatted payload, locate the key **“profile id”** pointing to your account login name.


✓ Copy **everything from** `<key>profile-id</key>` **all the way up to** `</string>` **inclusive** .

✓ Back to the rewrite **Rules** pane you opened previously (**Step 7**): **paste this text into the “Replace Value” box**.


 **The last step:** plugging in the *Apple Authorisation Token* saved in **Step 6**.

✓ Replace the token under the label *"auth-token"* inside the text you've just pasted with the **saved Apple Authorisation Token**.

✓ Save the changes: **OK** the rewrite **Rules** pane and **OK** the rewrite tool window.

 Resume the session recording.

✓ Sign out of your **FaceTime** account and sign back in with your password (no verification code!).

 **Security Notice!** *Since sensitive login information (the auth token sent by Apple and added to the new response structure) was essentially hardcoded as the result of this approach, and a potential security breach can allow third parties to log into your account with any credentials, **disabling this rewrite set is highly recommended!***