TeleConsult Video Conference Trouble Shooting Guide

1.1 Google Chrome Setup

To allow Google Chrome (Both Mac and PS) to access your camera and microphone please follow each step listed below.

1. When entering a TeleConsult conference, if you are prompted to allow camera and microphone though, click 'Yes'

If the prompt does not show up, please go through the next steps.

1. Open Chrome.
2. At the top right, click More ⋮ › Settings.
3. At the bottom, click Advanced.
4. Under "Privacy and Security" click site settings.
5. Click Camera and Microphone.
6. Turn Ask Before Accessing ON.

If neither of these solutions do not work please try;

1. Shut down any programs or extensions that use, or have used the camera and microphone in the past as some programs can lock access to the camera and microphone from the browser. And example would be Skype or FaceTime.
2. Restart your computer. This may reset any permission settings that blocks access to the camera and microphone.

1.2   Mozilla Firefox Setup

To allow Mozilla Firefox (Both Mac and PC) to access your camera and microphone please follow each step listed below.

1. When entering a TeleConsult conference, if you are prompted to allow camera and microphone though, click 'Yes'

If the prompt does not show up, please go through the next steps.

Changing camera permissions

1. Click the menu button ☰ and select **Options** .
2. Click Privacy & Security from the left menu.
3. Scroll down to the Permissions section.
4. Click the **Settings...** button for the Camera option.
5. Enter the website URL in the Search field for the site that you want to access your camera.
6. Press the Enter key.
   The website displays in the list below. You can remove it at any time by selecting it from the list and clicking the **Remove Website** .
7. Select the **Block new requests asking to access your camera** checkbox if you do not want to give any other sites access to your camera.
8. Click the **Save Changes** button.

Changing microphone permissions

1. Click the menu button ☰ and select **Options** .
2. Click Privacy & Security from the left menu.
3. Scroll down to the Permissions section.
4. Click the **Settings...** button for the Microphone option.
5. Enter the website URL in the Search field for the site that you want to access your microphone.
6. Press the Enter key.
   The website displays in the list below. You can remove it at any time by selecting it from the list and clicking the **Remove Website** .
7. Select the **Block new requests asking to access your microphone** checkbox if you do not want to give any other sites access to your microphone.
8. Click the **Save Changes** button.

1.3 Safari Setup

To allow Safari to access your camera and microphone please follow each step listed below.

1. When entering a TeleConsult conference, if you are prompted to allow camera and microphone though, click 'Yes'.

If the prompt does not show up, please go through the next steps.

1. On your Mac, choose Apple menu > System Preferences, click Security & Privacy, then click Privacy.

2. Select Camera.

3. Select the tick box next to an app to allow it to access your camera.

   Unselect the tick box to turn off access for that app.

   If you turn off access for an app, you're asked to turn it on again the next time that app tries to use your camera.

1.4 Microsoft Edge Setup

To allow Microsoft Edge to access your camera and microphone please follow each step listed below.

1. When entering a TeleConsult conference, if you are prompted to allow camera and microphone though, click 'Yes'.

If the prompt does not show up, please go through the next steps.

1. Open **Microsoft Edge**.
2. Navigate to the website you want to manage.
3. Click the **Lock** icon ⌒ next the website link in the address bar.
4. Click **Site Permissions** Options.
5. Use the drop-down menus to allow camera and microphones through for this website.

If neither of these solutions do not work please try;

1. Shut down any programs or extensions that use, or have used the camera and microphone in the past as some programs can lock access to the camera and microphone from the browser. And example would be Skype or FaceTime.
2. Restart your computer. This may reset any permission settings that blocks access to the camera and microphone.

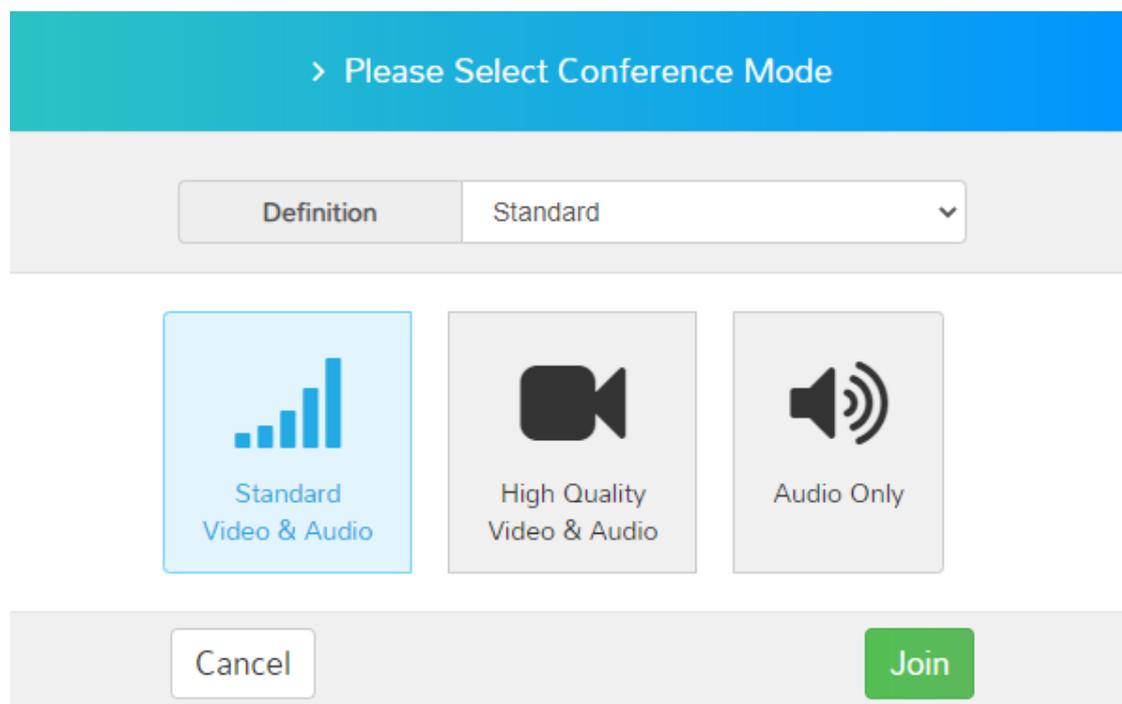## 1.5 Video Conference Quality and Screen Sharing

1.5.1 Video Conference Quality

There are multiple factors which should determine which type of conference you should be on.

Currently TeleConsult supports three types of conferences;

1. High Quality
2. Standard Quality
3. Audio Only
4. Dial-In

The image shown below is what you will see when you enter the conference.

When to Select High Quality

High Quality Video and Audio is always the best option to join on as it will give you the best quality internet. High Quality requires a fast-stable internet connection. Some devices and internet connections may start to see streaming issues if more than 4 people are joined on the conference. If you experience this, please press the **Leave** button at the bottom of the conference and then press **Enter** again. This time, you can lower the definition of the conference in the dropdown to reduce the bandwidth usage or select **Standard Mode** or **Audio Only** (discussed below).

When to Select Standard Quality

Standard Video and Audio using MCU algorithms to produce a single image with all of the conference attendees. Selecting this mode will result in reduced quality but performs much better on bad internet connections. We only recommend using this after trying **High Quality Video and Audio**.

When to Select Audio Only

Audio only is available only for Google Chrome. This option should be used for conferences that do not require video to preserve resources as well as for devices that have poor internet connection or are low powered devices.

When to Select Dial-In

Dial In is available for users who have either no internet or poor internet connection. To dial in, call (03) 8330 9205 and follow the prompts.

1.5.2 Screen Sharing

Screen sharing is only available on google chrome. To share your screen click on the screen share button at the bottom of your conference screen (See below).
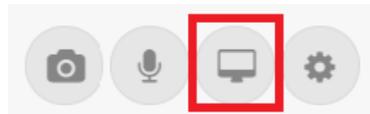
You will then be asked to select which screen you want to share. Once you are sharing your screen a banner will appear to indicate that this process has started.
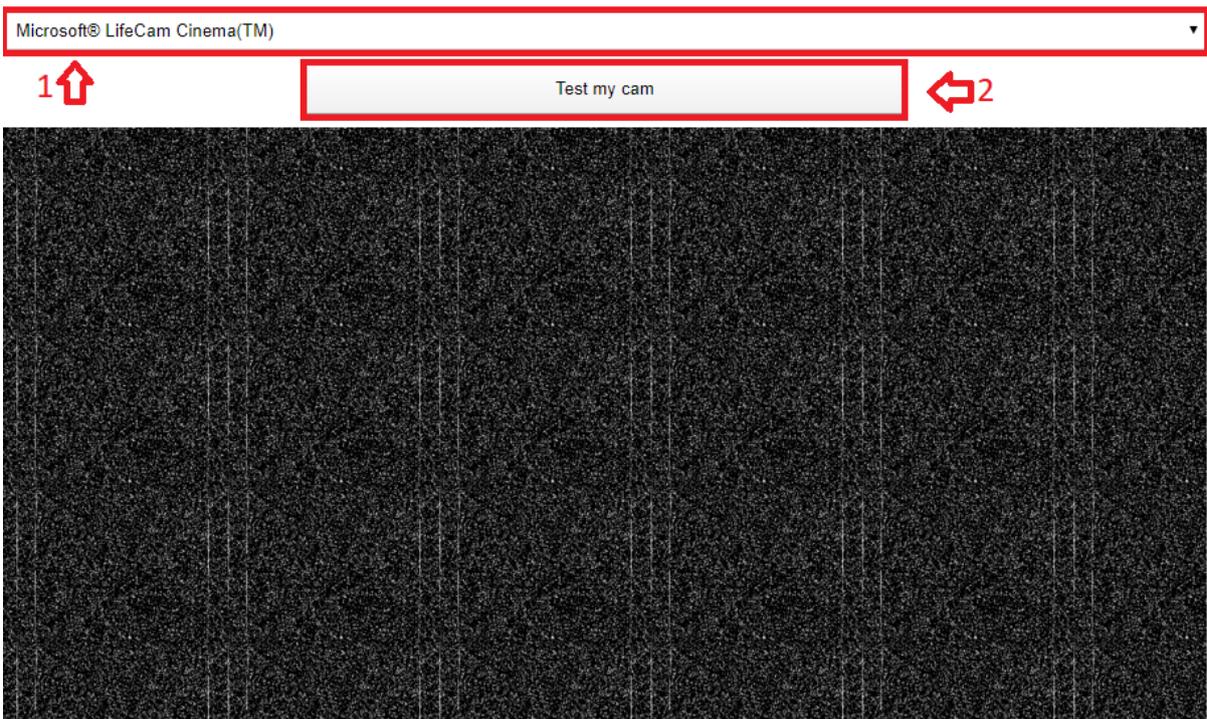
Phase 2 Check For Blocking of Video

2.0 Webcam Test

If you have completed phase 1 of troubleshooting and are unable to get access to the camera please go through the following steps.

1. Ask the user on the browser they are trying to troubleshoot to go to www.webcamtests.com
2. Ask the user to select the camera they wish to test (1) and then 'Test my Webcam' (2)

3. If the user is unable to connect their camera through this website then it is likely that their network does not allow video to be sent or their camera is being blocked up by another program. If this problem exists please close ALL programs that have access to the camera and microphone.
   - Simply closing a program may not be sufficient. You must make sure that the program is not open in any sense but exiting from the windows quick launch menu.
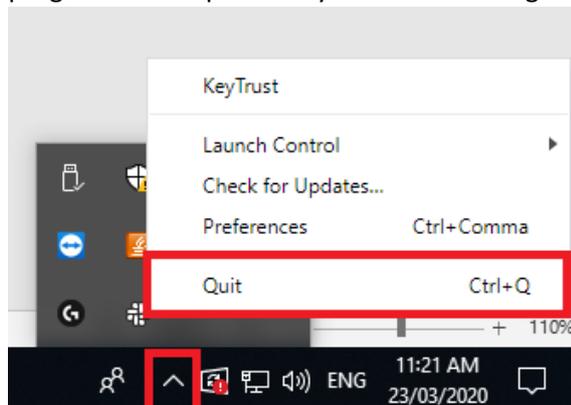
- Remove any extensions from the browser that may need access to the camera and microphone.
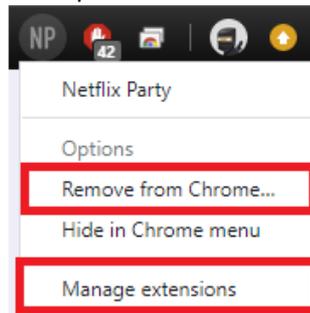
- If none of these issues solve the problem, please restart your computer and remove any programs from starting up automatically on login. Please follow these steps:
    1. Right-click on an empty area on the Taskbar and select Task Manager. Image (1)
    2. When Task Manager comes up, click the Startup tab and look through the list of programs that are enabled to run during startup. Then to stop them from running, right-click the program and select Disable. Image (2)
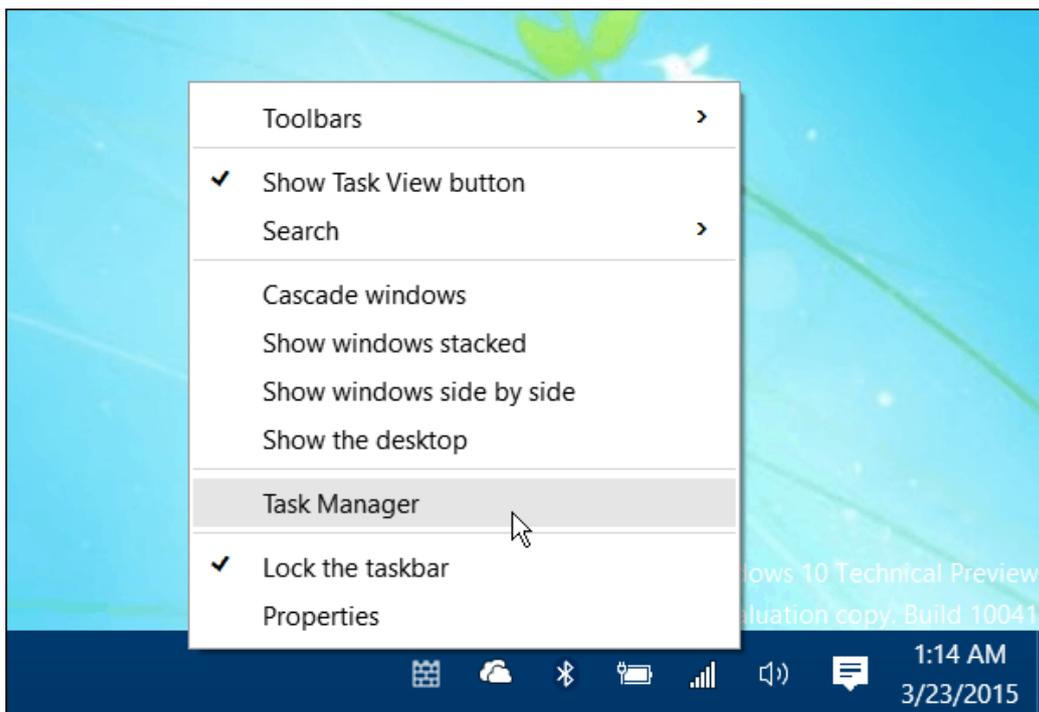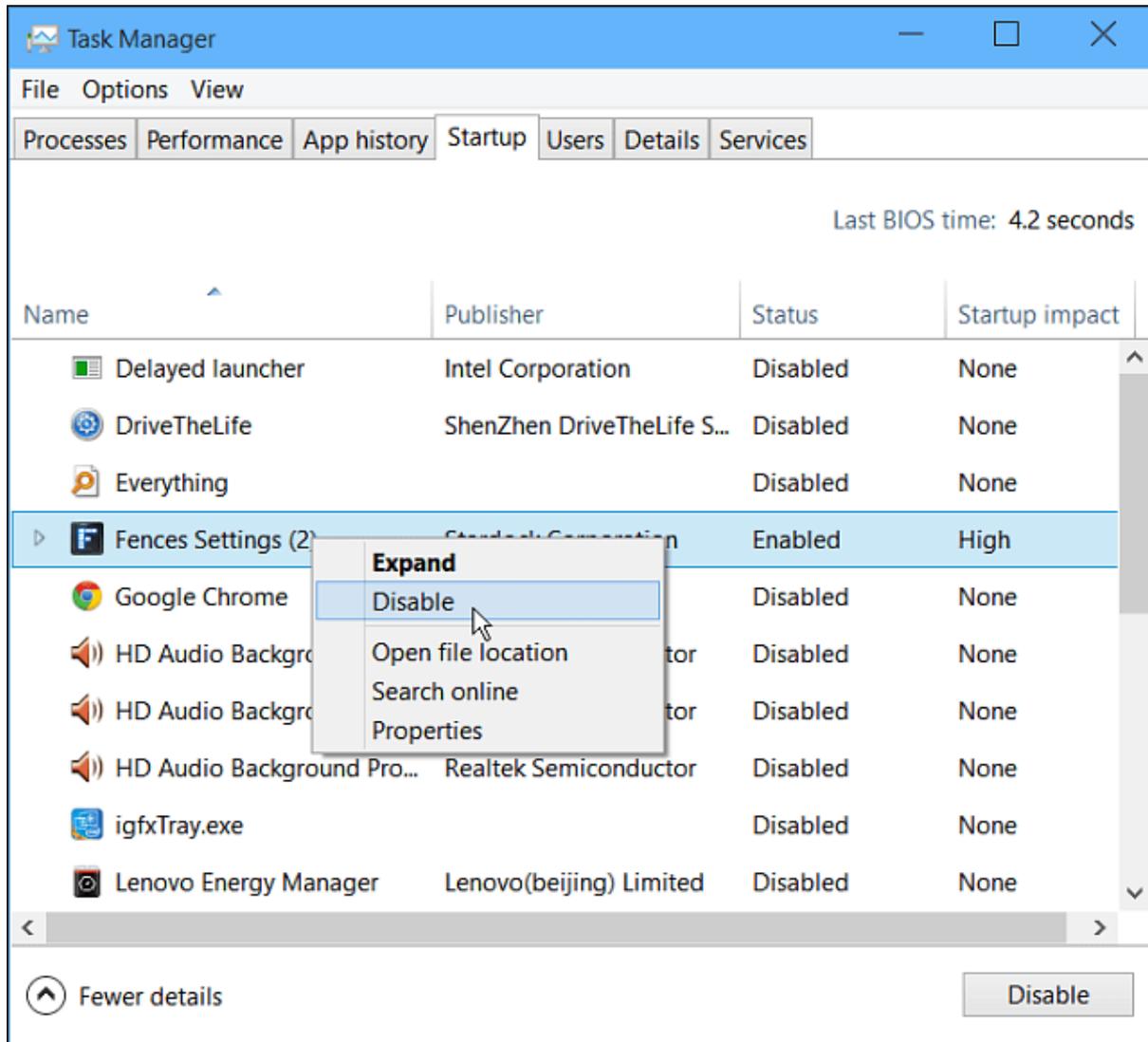
Image 1

IMAGE 2

3.0 Firewall and Outbound Ports

If none of the above steps above work you may need to speak to your IT department to allow inbound and outbound video to be allowed through the network and firewall.

TeleConsult require firewalls to have open, for outbound connections from internal clients to our servers:

TCP ports 80,443
UDP ports 49152-65535
TCP and UDP port 5060

Our public range is 203.12.31.0/24

Please make sure with the IT departments that these ports are allowing through the firewall.