

International Cybersecurity Olympiad 2026 Rulebook

Date: 18/05/2026

Information

Release: Version 1

Revisions:

Version	Date	Description
Draft	17 February 2026	Draft Public Release
1	20 May 2026	First Public Release

Changelog	4
1. Introduction	5
1.1. Language.....	5
1.2. Official Websites.....	5
1.3. Time.....	5
2. Interpretation	6
3. Schedule	6
4. Venue	6
5. Staff and Roles	8
5.1. The International Committee.....	8
5.2. The International Scientific Committee.....	8
5.3. Teams.....	8
6. Competition format, setup and general rules	9
6.1. Contest Duration and Pre-Contest Setup.....	9
6.2. Infrastructure and Access.....	9
6.3. Tasks and subtasks.....	9
6.4. Task Resolution and Flags.....	9
6.5. Prohibition of Unauthorized Communication.....	10
6.6. Rules of Engagement and Scope of Operations.....	10
6.7. Prohibited Offensive Actions.....	10
6.8. Enforcement and Disciplinary Actions.....	11
7. Allowed software and hardware tools	12
7.1. Software equipment.....	12
7.2. Hardware equipment.....	12
8. Syllabus and task distribution	13
8.1. Competition syllabus.....	13
8.2. Task distribution.....	13
8.3. Task examples.....	14
9. Communication and support	15
9.1. Pre-Event Contact.....	15
9.2. Contact during the event.....	15
9.2.1. Official Channels.....	15
9.2.2. Communication rules.....	15
10. Use of Artificial Intelligence	16
11. Audit and Verification of Submissions	16
11.1. Organisers' Right to Audit.....	16
11.2. Mandatory Documentation of Methodology.....	17
11.3. Mandatory Screen Recording.....	17
11.3.1. Evidentiary Presumption and Failure to Comply.....	17
11.4. Penalties for Failure to Substantiate.....	17
Appendix A: Screen Recording Procedures	19
Installing OBS.....	19

Configuring OBS.....	20
Creating a Display Capture.....	20
Configure Base Resolution.....	21
Configure Recording Resolution.....	23
Configure Output.....	25
Configure Audio.....	27
Starting and Stopping Recording.....	28

Changelog

Draft - Draft Public Release

- This should be used solely only as a draft reference, rules may slightly change before the competition date.

Version 1 - First Public Release

Released the following sections:

- Section 1: Introduction
- Section 2: Interpretation
- Section 3: Schedule
- Section 4: Venue
- Section 5: Staff and Roles
- Section 6: Competition format, setup and general rules
- Section 7: Allowed software and hardware tools
- Section 8: Syllabus and task distribution
- Section 9: Communication and support
- Section 10: Use of Artificial Intelligence
- Section 11: Audit and Verification of Submissions
- Appendix A: Screen Recording Procedures

1. Introduction

This document is intended to be a comprehensive and self-contained guide for International Cybersecurity Olympiad (ICO) 2026 Contestants. This document is subject to changes depending on feedback and possible organizational updates. Any such changes will be reported in the changelog of this document. If you have any doubts, please reach out to the International Committee or the International Scientific Committee through your country representative.

1.1. Language

English shall be the official language for communication, written or otherwise. This includes all information related to the tasks contained during ICO 2026.

1.2. Official Websites

The ICO Official Website can be found at <https://ico-official.net>. It contains information related to past, present and future ICO editions.

The ICO 2026 Official Website can be found at <https://ico2026.tn>. It contains all information related to ICO 2026 held in Tunisia. The latest version of this document shall be found on this website.

1.3. Time

All times contained in this document, unless otherwise specified, are in Tunisian Local Time (UTC+1).

2. Interpretation

In this document, unless otherwise specified:

1. “Arena” means the physical location in which Contestants will take part in ICO during the competition days.
2. “AI” means Artificial Intelligence.
3. “Contest” or “Competition” or “ICO” means International Cybersecurity Olympiad 2026.
4. “Contestants” or “Competitors” means persons taking part in the competition.
5. “Example” or “e.g.” means a non-exhaustive list of scenarios or things used solely for illustration.
6. “Flag” means a unique, verifiable string associated with a specific task or challenge, which serves as proof of successful completion of a "Subtask", and which must be submitted to the Contest’s platform to receive the points associated with the “Subtask”.
7. “IC” means the ICO International Committee.
8. “ISC” means the ICO Scientific Committee.
9. “Organisers” means the IC, the ISC and the host country.
10. “Watchdog” is a person from the event staff with the role of monitoring the arena.
11. “Subtask” is a part of a task.
12. “Task” means a problem that is presented to the competitors.
13. “TBD” means “To Be Determined”
14. “TBC” means “To be Confirmed”

3. Schedule

Date	Program
Saturday, June 27th	Arrival
Sunday, June 28th	Opening Ceremony / Practice Session
Monday, June 29th	Contest Day 1 / Cultural & Recreational Programs
Tuesday, June 30th	Contest Day 2 / Cultural & Recreational Programs
Wednesday, July 1st	Excursion / Closing Ceremony
Thursday, July 2nd	Departure

4. Venue

ICO 2026 will be hosted at Hotel Diar Lemdina, located at Rue de la Medina, 8050 Hammamet South, Tunisia.

5. Staff and Roles

This section gives an overview of the roles involved in the ICO from the contestant point of view. More detailed information is available for team leaders and committee members.

5.1. The International Committee

The IC is a long-term, standing committee, which consists of voting members from different participating countries. The IC is responsible for, among the other tasks, making proposals about future hosts, selecting them, meeting and examining the host organization of the ICO. The IC has a president elected by the participating countries during the ICO from the committee members.

5.2. The International Scientific Committee

The ISC is established to work with the Host Country to ensure continuity and quality control for ICO competitions.

The ISC, a long-term standing committee, is responsible for ensuring that problem set has been created, overseeing the test data, and supervising creation and implementation of the grading system. The ISC has a chair elected from and by the committee members. The ISC reports directly to the IC.

5.3. Teams

For the ICO, a Team is a nation, state or a region that has an officially recognized relationship with the United Nations, UNESCO, or which has already taken part in one or more past ICOs.

A National Delegation of a Team is headed by a Delegation Leader.

The status of the Team Delegation can be:

- Participating, the Delegation includes in general a team of one to four Contestants, a Leader and optionally a Deputy Leader;
- Observing, the Delegation may include a Leader, optionally a Deputy Leader, but no Contestants.

A Contestant is a student who was enrolled at a school for secondary education during the period September to December in the year before the ICO, and is not older than twenty (20) years on the 1st of July of the year of ICO. No polytechnic nor university students are allowed to participate.

6. Competition format, setup and general rules

6.1. Contest Duration and Pre-Contest Setup

The Contest consists of two separate, 7-hours long, competition days. Each day features tasks that are completely independent from the other. In other words, no task is repeated between the two days and there is no dependency on tasks between the two days.

Prior to the official commencement of the Contest, Contestants will be allotted a designated period to verify their technical setups. This includes, but is not limited to, the verification of hardware functionality, internet connectivity, and proper access to all required internal competition platforms.

6.2. Infrastructure and Access

The competition network shall be hosted within a secure cloud environment. Contestants shall reach the competition platform and the tasks through a Wireguard VPN connection. Participants are required to ensure that they have the necessary equipment for network connectivity. For the avoidance of doubt, Organisers will not loan any equipment.

6.3. Tasks and subtasks

Each Contest day will feature three (3) tasks. Each task is split into subtasks, and it is worth the same fixed amount of points (100). The point value for each subtask is revealed at the beginning of the competition day.

At the end of each day a scoreboard is created, where Contestants are ranked based on their total number of points. The final scoreboard is based on the sum of the points gathered by a contestant in the two competition days, in descending order. If more than one Contestants end up with the same number of points, the tie is broken using the sum of the times of their last point increase during each day, in ascending order.

Each task can be seen as a set of jeopardy-style CTF challenges with multiple flags but a common codebase. Each task contains a set of subtasks, granting each a certain amount of points when solved. There is no strict rule about the number of subtasks for each task, expect roughly 4-6 of them. When the correct flag is submitted for a subtask, the corresponding points are awarded. There are no bonus points for being the first one solving a task or subtask, or for particularly clever solutions.

Tasks and subtasks can have different categories in it. Further information is available in the Syllabus section.

6.4. Task Resolution and Flags

A task shall be deemed “solved” when a Contestant successfully extracts and submits the correct Flag corresponding to that task via the official competition platform. Flags may be acquired through various methodologies, including but not limited to active interaction with

remote services, analysis of distributed files, or any other methods deemed reasonable by the Organisers.

6.5. Prohibition of Unauthorized Communication

Contestants are strictly prohibited from communicating, discussing, sharing or transmitting any information pertaining to the Contest tasks with other Contestants, Team Leaders or any third party during the Contest, unless explicit written permission is sought from the Organisers. The sole exception to this prohibition is official communication directed to the Organisers via explicitly designated channels. This restriction encompasses all external communication mediums, including, but is not limited to, the use of social media platforms, posting on forums (e.g. Stack Overflow, Reddit), and the use of public or private messaging services (e.g. Discord, Whatsapp). Any suspected breach of these regulations will be investigated and may result in disqualification. For the avoidance of doubt, passive activities such as searching for or reading content on forums are permitted, provided no interaction or disclosure of Contest-related information occurs.

6.6. Rules of Engagement and Scope of Operations

Contestants are expressly forbidden from attempting to attack, probe, scan, enumerate, exploit, or otherwise interfere with the competition infrastructure. This prohibition extends to all systems the Contestant does not own, including but not limited to, the systems, networks, or software utilised by the ICO Organisers for the administration and hosting of the Contest, as well as the devices, systems, networks, or accounts belonging to other Contestants.

Contestants are authorized to interact solely with the specific systems, services, and resources explicitly designated by the Organisers for the purposes of the competition. Any attempt to access, engage or interfere with systems outside this defined scope is strictly prohibited.

In the event of any ambiguity or uncertainty regarding the permitted scope of interaction, Contestants bear the absolute responsibility to seek direct and prior clarification via Discord from the Organisers. Under no circumstances shall the benefit of the doubt be afforded to any Contestant found to have breached these rules.

6.7. Prohibited Offensive Actions

Any unauthorised attempt to access, disrupt, degrade, or otherwise interfere with any systems the Contestant does not own, including but not limited to, the systems, competition network, the competition platform, devices and systems of other Contestants, or any out-of-scope systems is strictly forbidden. Prohibited activities include, but not limited to, port scanning, vulnerability scanning, denial-of-service attacks, traffic interception, or unauthorised enumeration of services.

6.8. Enforcement and Disciplinary Actions

Any activity deemed by the Organisers to constitute a violation of these rules, to disrupt the operations of the Contest, harmful to other Contestants, or to compromise the fairness or integrity of the Contest shall result in immediate disqualification and any further sanctions deemed appropriate by the Organisers. Furthermore, the Organisers expressly reserve the right to pursue civil litigation or refer the matter for criminal prosecution under Tunisian law.

Additionally, Contestants bear sole and absolute responsibility for all network traffic originating from their systems. Any offensive operations, probing, or unauthorized interactions directed at infrastructure outside the explicitly defined Contest network are strictly prohibited. In the event a Contestant violates these boundaries, the Organizers will fully cooperate with local, national, and international law enforcement agencies to the extent required by law.

7. Allowed software and hardware tools

7.1. Software equipment

Every task proposed during both competition days is guaranteed to be solvable by using just open source or freely available software.

7.2. Hardware equipment

Players are allowed to bring basic hardware equipment setup: **one** laptop each, mouses, keyboards, power, adapters, and external drives. No external monitors or desktop computers are allowed. If something is not mentioned in the list above, it is not allowed, and explicit approval must be sought. This applies to electronics such as bulky objects, which may annoy other teams in the arena. If Contestants are unsure about something, then it is recommended that Contestants request it through their country representatives.

- All Contestants are required to bring all the power adapters they need. Each table will have at least one Type C or E socket available.
- No additional devices are allowed in the competition arena, including mobile phones. Any such devices found with Contestants will constitute cheating and may result in disqualification.
- Any approved devices brought in should not cause disturbances to other Contestants. In the event of any complaints, watchdogs will decide the merit of the complaint. If the complaint is valid, watchdogs will decide on the appropriate remedy, which may include removal of the device from the Arena. Any decisions made are final and not subject to appeal.

Contestants are required to ensure that the devices they bring are sufficient to solve all tasks in the categories listed in this document. The utilization of remote servers, cloud computing instances, or any external infrastructure to augment local computational resources is strictly forbidden. **With specific regard to Binary Exploitation tasks, which shall consist exclusively of x86_64 binaries, Contestants must ensure that they have access to the appropriate tooling on their devices to execute, analyse or otherwise work with x86_64 binaries.**

Additional equipment must be requested in advance for approval by the organisers. The request must be received via email before 21st June 2026, and its approval/rejection will be communicated to Contestants before 24th June 2026 2359Hrs AoE. Contestants must submit all requests via their respective country representatives, unless otherwise specified. All other requests will be ignored. If a request is allowed for a contestant, then it is allowed for all Contestants, unless otherwise specified.

In case of a contestant's hardware failure, Contestants can request a device replacement. The request must be made through the watchdogs in the room, which can either accept it or raise it to the organisers. If the request is accepted, team leaders may deliver a replacement device to the contestant. The malfunctioning device will be kept with the organisers and may not be removed from the arena.

8. Syllabus and task distribution

8.1. Competition syllabus

Contestants will compete in binary exploitation, cryptography, digital forensics, reverse engineering, web security and miscellaneous tasks. In this section, we provide a brief description of these categories.

- **Binary exploitation.** This category of tasks involves the exploitation of a binary on a remote machine by memory corruption. For the purpose of the competition, binaries will be available only in the x86_64 architecture. Tasks in this category may also include shellcoding and/or escaping constrained environments.
- **Cryptography.** This category of tasks involves understanding and exploitation of modern cryptographic protocols. Vulnerabilities range from heavy mathematical ones to algorithmic/implementation-oriented ones.
- **Digital Forensics.** This category of tasks involves analyzing files with the objective of extracting hidden data from them. Tasks can range from post-exploitation analysis to finding hidden information in images or audio files (steganography).
- **Reverse engineering.** This category requires Contestants to analyze and understand software in the form of compiled binaries, bytecode, obfuscated source code, etc, to extract flags from them.
- **Web security.** This category requires Contestants to analyze custom web applications, possibly exploiting both server and client side vulnerabilities.
- **Miscellaneous.** This category includes tasks that do not strictly fit in the previous ones. Tasks may require skills of mobile security, network security, algorithmic/programming, AI, cloud, radio, etc.

8.2. Task distribution

The rationale behind task distribution is that getting a medal should require skills in a large subset of topics, and being proficient in just one of them is not enough. In general tasks may require skills from different categories and subtasks will involve only a specific one.

The number of points corresponding to each category are similar, as well as the difficulty levels, but **it is not guaranteed** that every category is worth the exact same amount of points. Moreover, it is not guaranteed that the point distribution among categories in the two days of competition remains the same, nor the number of subtasks is (both between problems and between competition days).

Example of a competition day:

Task 1 - 100 points

- Subtask 1 - Cryptography (20 points)
- Subtask 2 - Reverse engineering (15 points)
- Subtask 3 - Binary exploitation (30 points)
- Subtask 4 - Binary exploitation (10 points)

- Subtask 5 - Miscellaneous (25 points)

Task 2 - 100 points

- Subtask 1 - Web security (35 points)
- Subtask 2 - Digital forensics (20 points)
- Subtask 3 - Reverse engineering (20 points)
- Subtask 4 - Cryptography (25 points)

Task 3 - 100 points

- Subtask 1 - Reverse engineering (25 points)
- Subtask 2 - Binary exploitation (10 points)
- Subtask 3 - Miscellaneous (20 points)
- Subtask 4 - Digital forensics (30 points)
- Subtask 5 - Web security (10 points)
- Subtask 6 - Web security (5 points)

8.3. Task examples

An example of the task structure is available at demo.ico-official.net. Please note that this task is not intended to reflect the actual difficulty level of the competition tasks; it is provided solely as an example of the expected structure. Registration to the platform will open by the end of May 2026.

9. Communication and support

9.1. Pre-Event Contact

All Contestants should contact the organisers through their country representatives. Country representatives will be provided with the official point of contact. Email shall be the only medium of contact with the organisers prior to ICO 2026. The organisers will aim to reply to all emails within seven (7) calendar days.

Country representatives and Contestants should ensure that all official communication and information published on the website have been read and any queries have not been addressed prior to contacting organisers.

9.2. Contact during the event

9.2.1. Official Channels

All announcements, clarifications, and updates will be shared exclusively through the official platform and designated channels.

The primary official communication channel is the Discord Server, which Contestants can join via the link provided by the organizers via <https://discord.com/invite/KzPNk9wW2E>.

Once a contestant is confirmed by their country representative, they will receive a token to authenticate in the Discord server and receive access to the competition-specific channels.

9.2.2. Communication rules

Effective communication between Contestants, team leaders and the ICO representatives is essential for the smooth operation of the International Cybersecurity Olympiad. To ensure clarity and efficiency, communication is divided into three categories:

- **Emergencies:** This category includes, but is not limited to, cover health and safety issues, but also inappropriate behavior, bullying, discrimination, illegal activities, or any situations that may result in, or has resulted in, harm or injury. In such situations, Contestants are permitted to use any method of communication that is most immediate and effective. Examples include:
 - Direct communication with volunteers present in the Arena or submission of an emergency ticket on the Discord server; OR
 - Opening an emergency ticket on the Discord server; OR
 - Posting in the dedicated emergency channel on Discord
- **Competition-related communication:** This category covers issues related to the technical aspects of the competition (e.g. rules, format, technical issues affecting the competition, formal complaints or disputes regarding scoring and rankings, reporting possible disruptive behavior from other Contestants). Contestants shall raise any complaints related to disruptive behaviours by raising a ticket in the Discord server.
- **Event-related communication:** This category includes logistical matters, and any other non-competition matters, such as meal schedules, dietary requirements, health

and safety concerns, general inquiries about event arrangements. Contestants or their Team Leaders may raise these matters either by submitting a ticket in the Discord server or by raising their concerns directly to the volunteers in the Arena. If an issue is raised to the volunteers, it is the volunteer's job to decide whether the issue should be raised via Discord, escalated or requires immediate attention.

10. Use of Artificial Intelligence

The unrestricted use of Artificial Intelligence (AI) systems, models, or tools by Contestants during the Contest is strictly prohibited. This restriction applies to, but not limited to, all third-party, cloud-based AI services, as well as any locally hosted, offline Large Language Models, generative AI applications deployed on the Contestant's hardware. All AI usage shall be monitored through a designated AI chat platform provided by the Organisers. All interactions and data transmissions conducted upon this platform shall be subject to continuous monitoring and auditing to ensure strict compliance with Contest regulations. Any unauthorized access, deployment, or utilization of non-sanctioned AI tools shall constitute a material breach of these rules, prompting an immediate formal investigation and rendering the offending Contestant liable to summary disqualification.

For the avoidance of doubt, all restrictions and prohibitions codified within Section 10 pertain exclusively to AI use during the Contest. The Organisers explicitly impose no restrictions on AI use during the preparation phase leading up to ICO 2026.

An in-house AI chat interface which will allow participants to access the model **gpt-5-mini-2025-08-07** with configurable reasoning effort (low, medium, high). It has the following restrictions:

- Chat only. In other words, file uploads and MCP are not allowed
- Each Contestant will be provided a fixed amount of tokens for use during each Contest day. Exact amount TBC
- Input, output and reasoning tokens will be taken into account in the limit: higher is the reasoning level, higher is the number of tokens spent
- Token usage is directly monitored through the OpenAI API

A demo of the platform and the exact number of provided tokens will be made available before the competition for the Contestants to familiarize with it.

11. Audit and Verification of Submissions

11.1. Organisers' Right to Audit

The Organisers reserve the unilateral right to audit the validity of any submitted Flag to ensure the integrity of the competition. Should the Organisers, at their sole discretion, deem it necessary, a Contestant may be formally required to articulate, demonstrate, or otherwise substantiate the precise technical methodology (the "solve path") employed to successfully complete a task.

Additionally, all network traffic during ICO through the competition network, including outgoing internet traffic, are logged and stored for analysis, investigation or any other purposes deemed necessary by the Organisers to ensure the conduct of ICO 2026 and uphold the competition integrity.

11.2. Mandatory Documentation of Methodology

Contestants shall bear the sole responsibility to document and maintain a comprehensive record of all actions, commands, scripts, and analytical steps executed in the course of solving any tasks.

11.3. Mandatory Screen Recording

All Contestants participating are subject to a strict, mandatory recording requirement. These Contestants must ensure a continuous, uninterrupted screen recording of their hardware for the entire, seven-hour duration of each day of the Contest. This recording must be facilitated exclusively via Open Broadcaster Software (OBS) and must be explicitly configured to capture the entirety of the Contestant's visual workspace (i.e., the full, uncropped laptop screen on the host) without occlusion, filtering, or obfuscation. In the event that the recording fails or stops during the competition, Contestants are to inform the volunteers immediately and resume the recording at the earliest possible time.

Following the official conclusion of the Contest, all Contestants are obligated to submit their complete screen recordings to the Organisers. These recordings shall be subject to review and analysis to ascertain the Contestant's strict compliance with all rules, regulations, and directives codified within this document, as well as any instructions communicated during the Contest.

Refer to Appendix A for more instructions

11.3.1. Evidentiary Presumption and Failure to Comply

The submission of a complete, valid, and continuous screen recording is a material condition for participation. In the event that a Contestant fails to submit this recording, or if the submitted video file is corrupted, paused, incomplete, or does not show the entire laptop screen, the Contestant are to inform the volunteers on site as soon as possible. Failure to do so will expressly forfeit the "benefit of the doubt."

In practical terms, this means that if the Organisers investigate a Contestant for a potential rule violation, suspicious activity, or an unexplained solve path, the Organisers shall not rely on the Contestant's word alone. Without the required video evidence to prove compliance with the rules, the Organisers will assume non-compliance. Any uncertainties in such disputes shall be judged strictly against the Contestant, which may result in disqualification.

11.4. Penalties for Failure to Substantiate

The failure, inability, or refusal of a Contestant to provide a satisfactory, coherent, and technically sound explanation of their solve path upon formal request shall be construed as a

International Cybersecurity Olympiad 2026

Document title: ICO 2026 Rulebook

Document Classification: Official (Open)

breach of competition integrity, rendering the Contestant liable to disqualification from ICO 2026.

Appendix A: Screen Recording Procedures

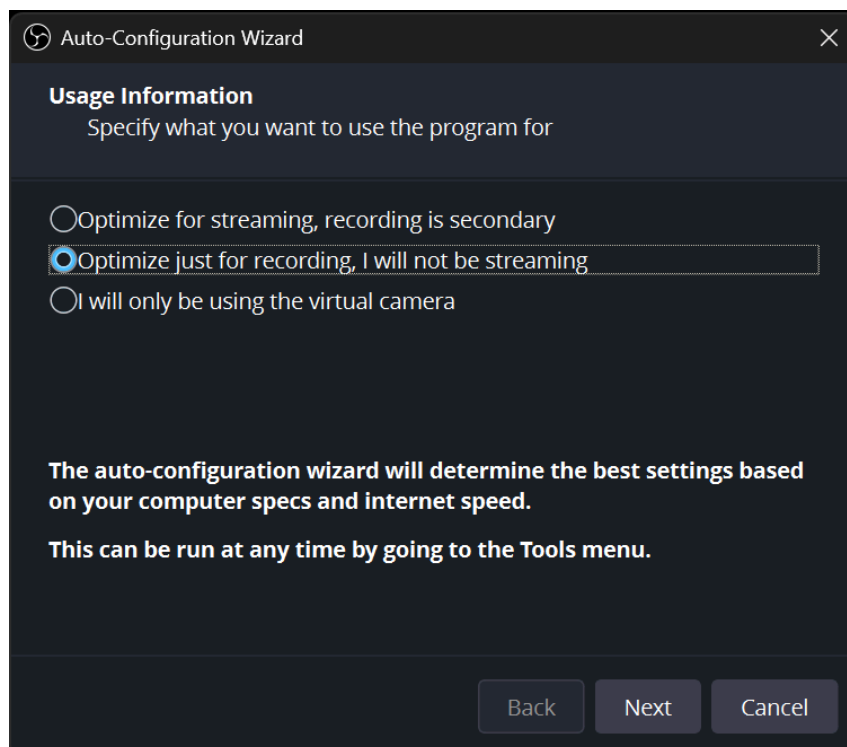
This section is prepared on OBS version 32.1.2. Updates to this section will be done on a best effort basis.

Installing OBS

*For Contestants using a Virtual Machine (VM), OBS should be installed on the **Host Machine** not the VM.*

Download and install the latest version of OBS from this link for your respective Operating System: <https://obsproject.com/download>.

It is highly recommended to select “Optimize just for recording, I will not be streaming” when prompted on the first launch. A screenshot of the prompt is shown below.



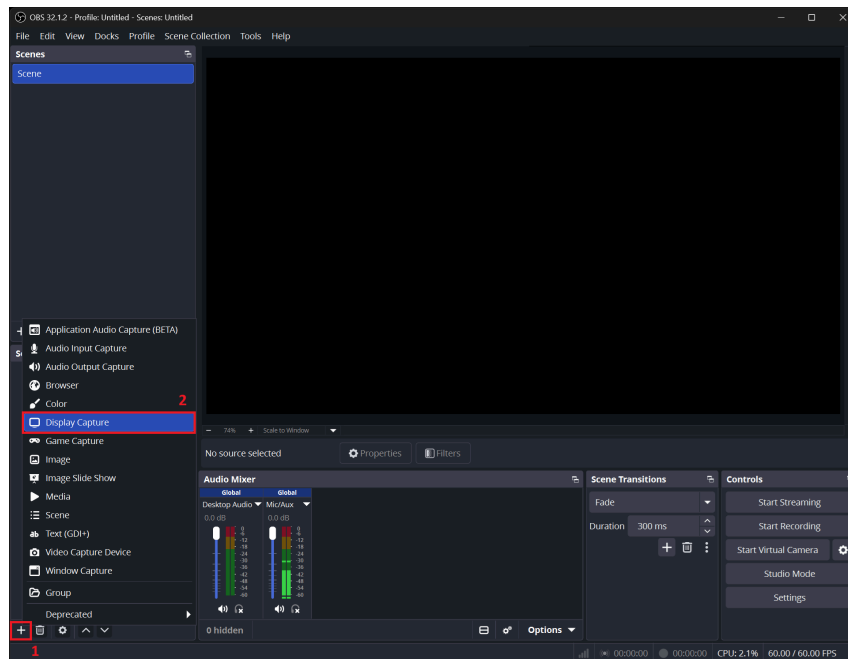
Accept default values for all other configurations.

Configuring OBS

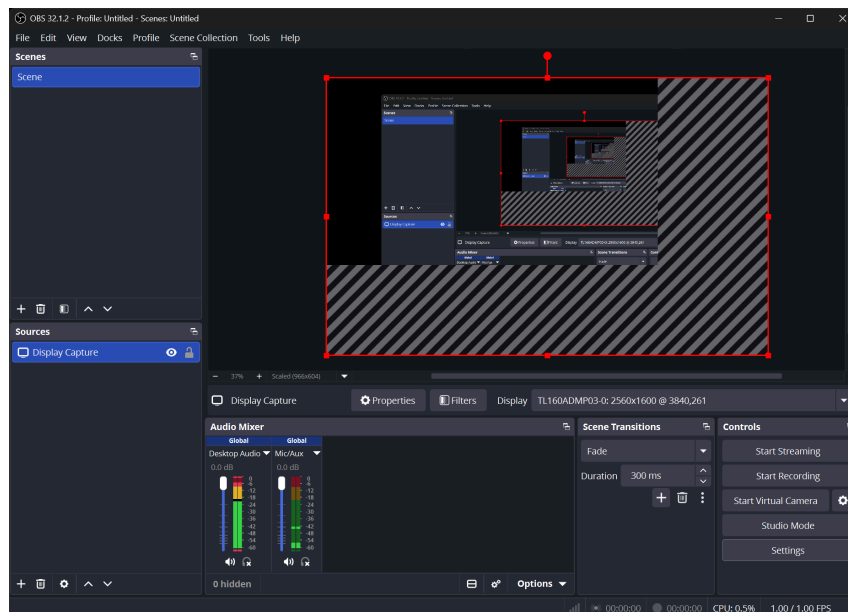
To facilitate screen recording, all Contestants are required to configure OBS with a singular Display Capture as the source as shown below.

Creating a Display Capture

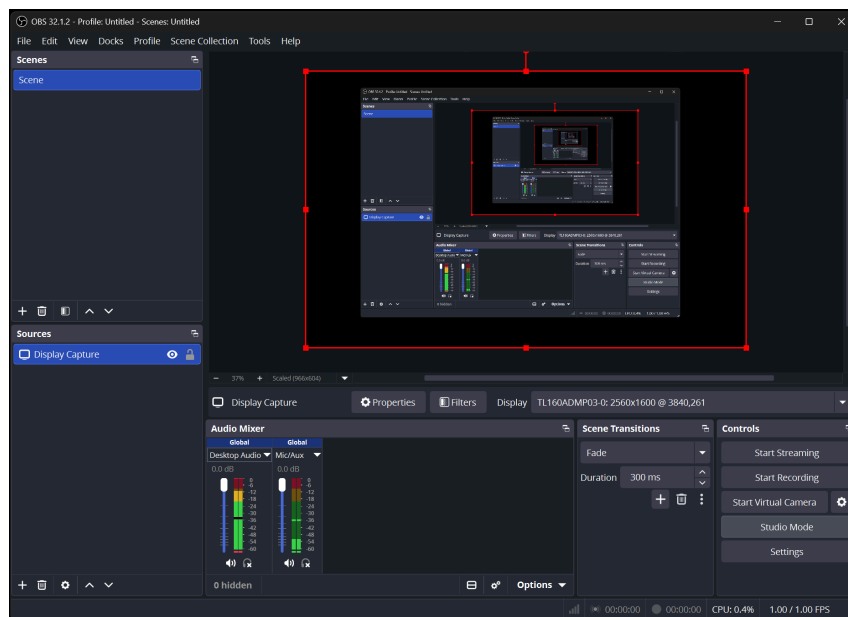
To create a new Display Capture by clicking on + > **Display Capture** as shown in the screenshot below.



The Display Capture must fit completely within the recording frame. Refer to the following:



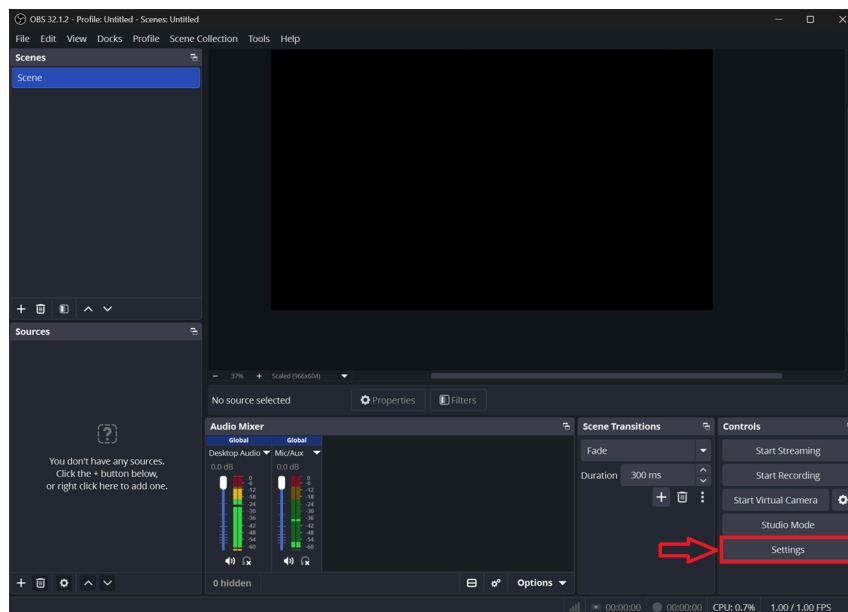
The above shows that the aspect ratio is misconfigured. Refer to “Configuring Base Resolution” for instructions on rectifying this.



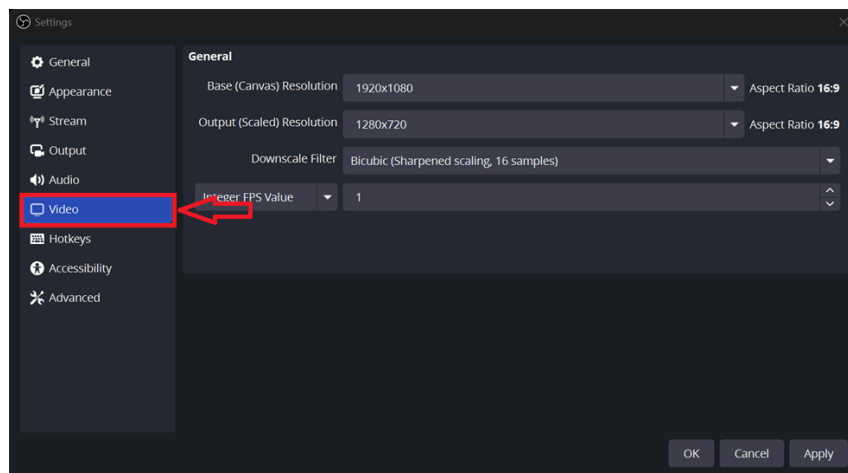
The above shows correct configuration.

Configure Base Resolution

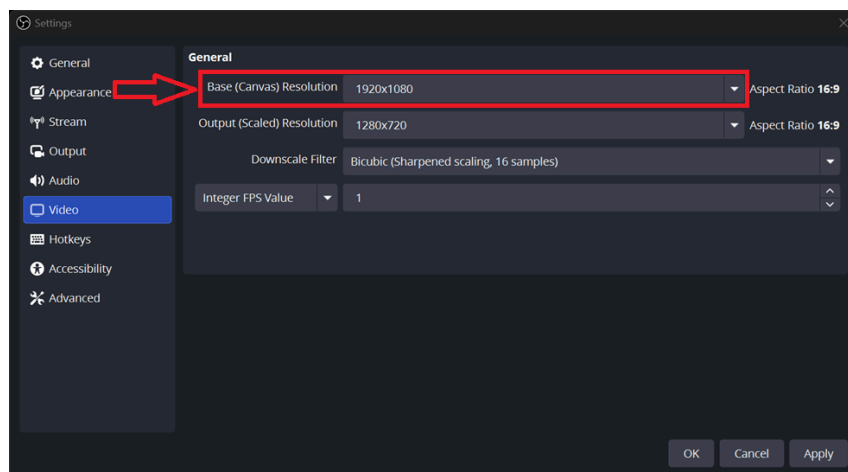
Ensure that the **“Base (Canvas) Resolution”** matches your device’s configured resolution. To configure this, click on **“Settings”** as shown below



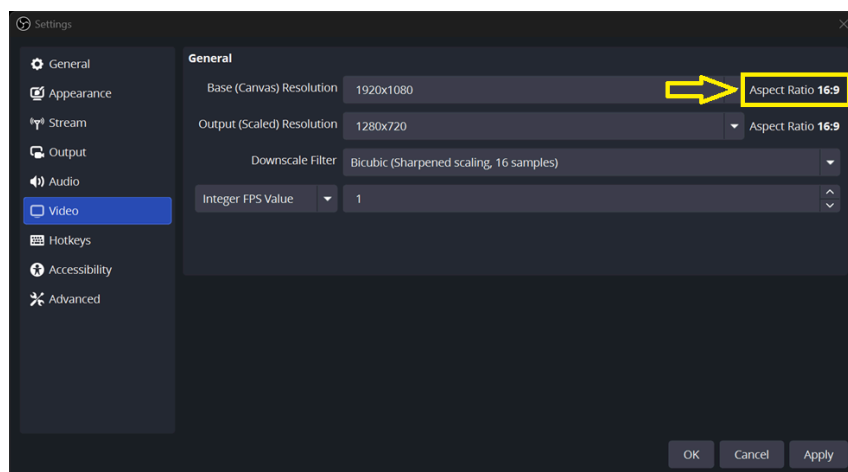
In the popup window, click on **“Video”**.



Verify that “**Base (Canvas) Resolution**” matches your device’s configured resolution.



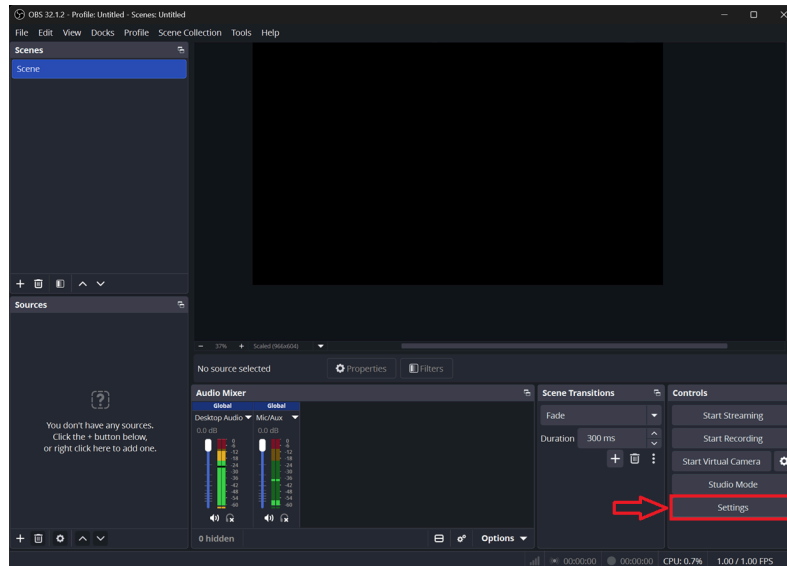
At this point, take note of the “**Aspect Ratio**” of the Base Resolution.



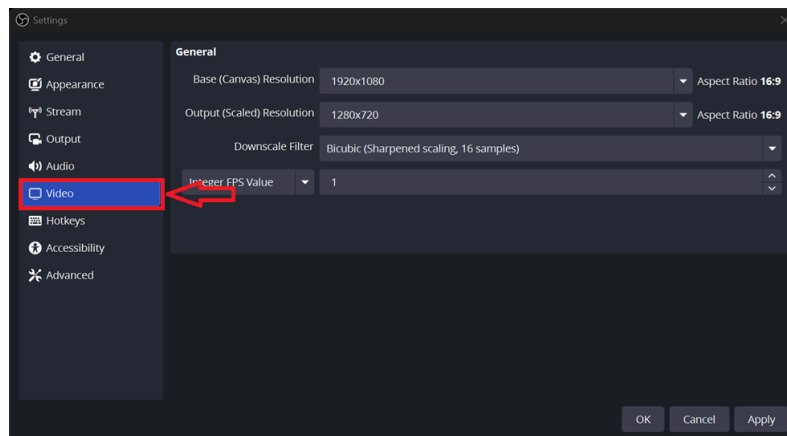
Click “**Apply**” before moving on.

Configure Recording Resolution

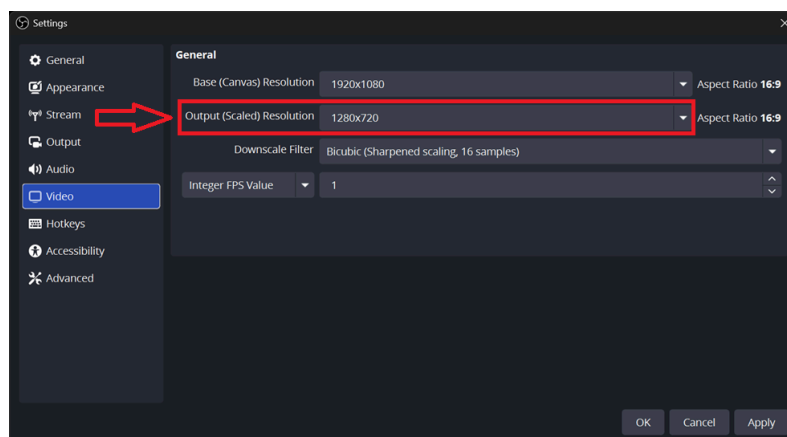
Click on “**Settings**” as shown below



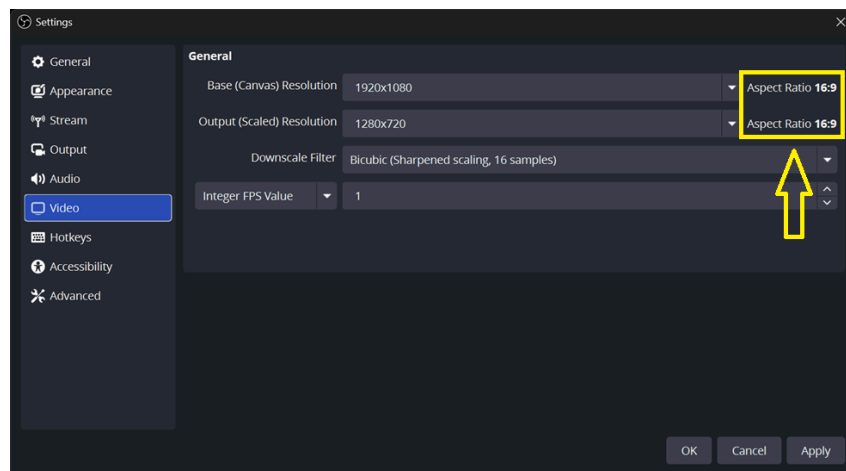
In the popup window, click on “**Video**”.



For the field of “**Output (Scaled) Resolution**”, set to an appropriate resolution of at least “**1280x720**”.



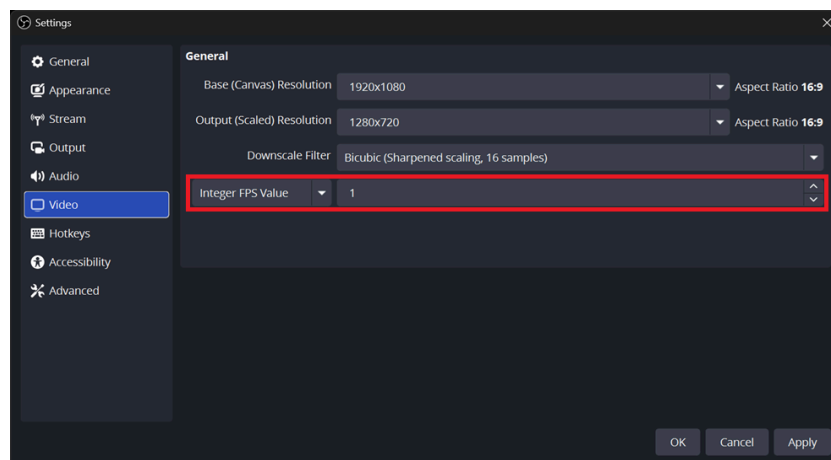
Ensure that the “**Aspect Ratio**” of the output resolution matches that of the Base Resolution.



The following are recommended Output Resolution for common laptop Aspect Ratios.

Aspect Ratio	Recommended Resolution
16:9	1280x720
16:10	1270x800

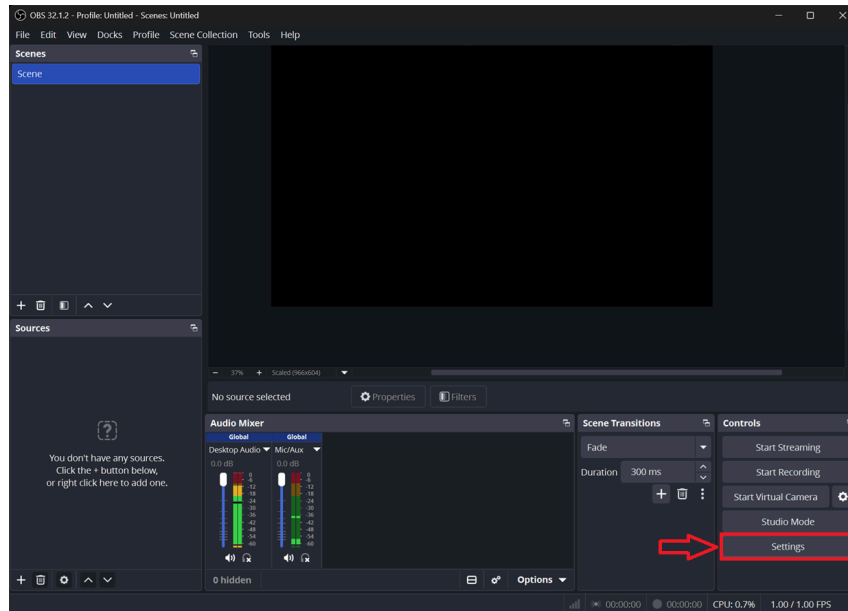
Configure the FPS to be “**Integer FPS Value**” and set it to “**1**”.



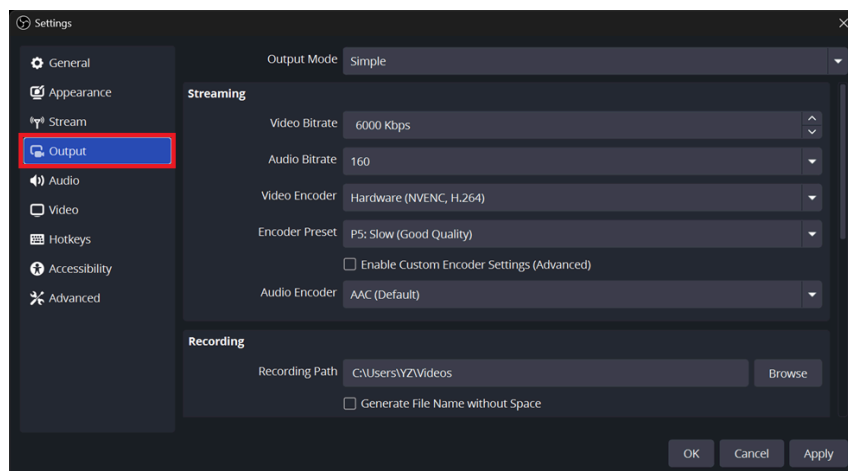
Click “**Apply**” before moving on.

Configure Output

Click on “**Settings**” as shown below

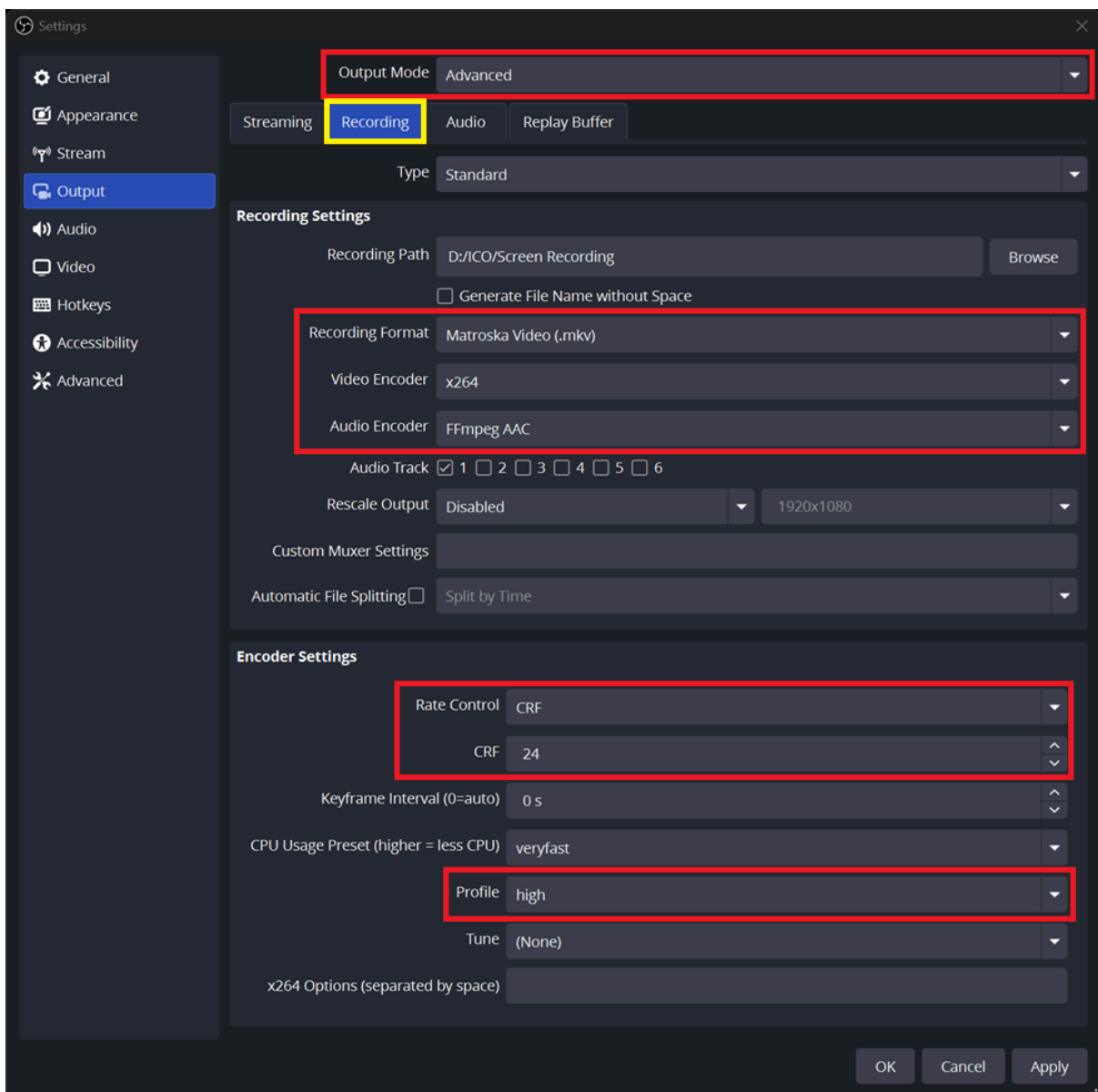


In the popup window, click on “**Output**”.



Ensure that “**Output Mode**” is “**Advanced**” with the “**Recording**” tab selected. Ensure that the following fields are configured as seen in the screenshot below.

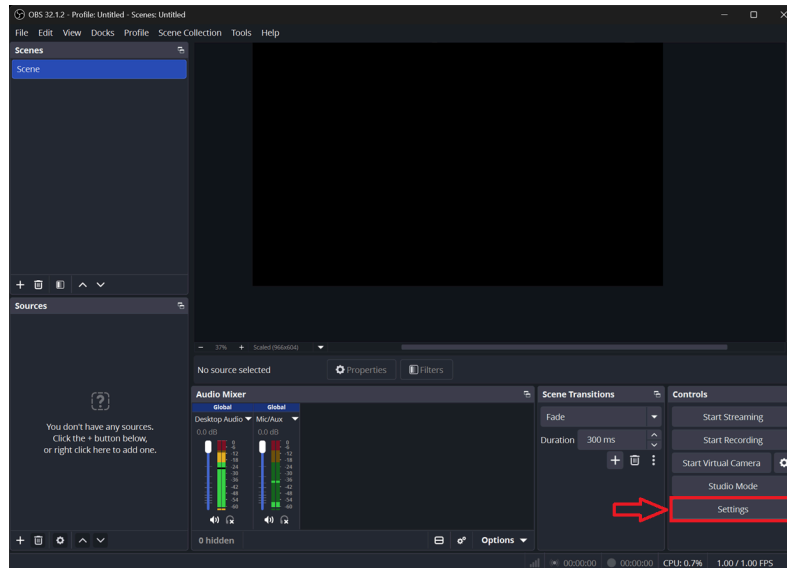
- “**Recording Format**” is “**Matroska Video (.mkv)**”
- “**Video Encoder**” is “**x264**”
- “**Audio Encoder**” is “**FFmpeg AAC**”
- “**Rate Control**” is “**CRF**”
- “**CRF**” is “**24**”
- “**Profile**” is “**high**”



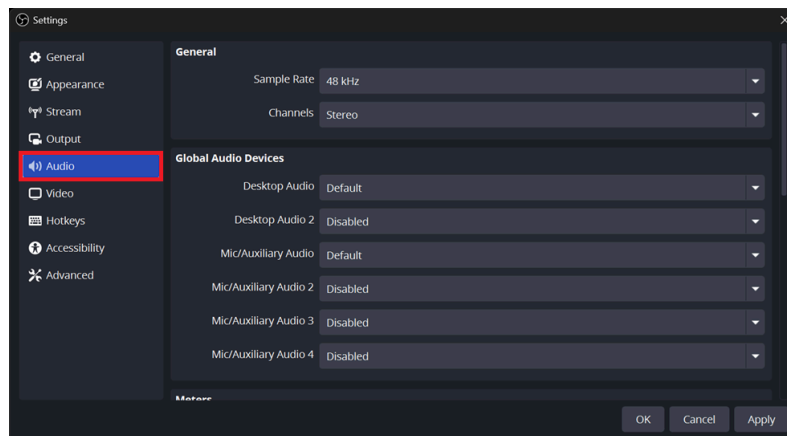
Click “**Apply**” before moving on.

Configure Audio

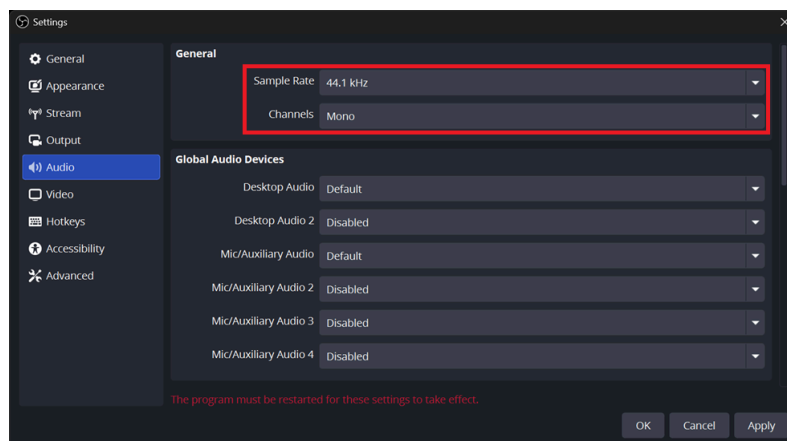
Click on **“Settings”** as shown below



In the popup window, click on **“Audio”**.



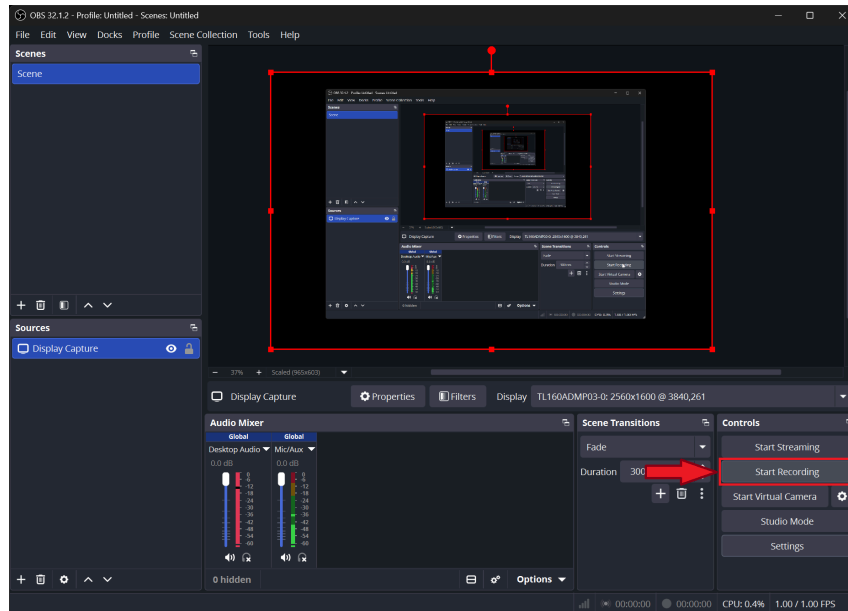
Set **“Sample Rate”** to **“44.1 kHz”** and **“Channels”** to **“Mono”**.



Click **“Apply”** and restart OBS before moving on.

Starting and Stopping Recording

Click **“Start Recording”** to start the recording



Click **“Stop Recording”** to stop the recording

