Forest Studio

SKYSHARE
SHARE THE SKIES

SKYSHARE
SHARED COCKPIT CONTROLS

General Operations Manual

Please read the following document thoroughly, as it ensures the proper steps are followed for your SkyShare experience to be enjoyable.
Thank you for using SkyShare!

TABLE OF CONTENTS

SECTION 1: OVERALL OPERATION

- ## SECTION 1.1: WELCOME

  - Thank for your purchase of SkyShare: Shared Cockpit Controls for MSFS. To get started, please make sure you go through this manual, as it contains important information on how to use our product.

- ## SECTION 1.2: INTRO TO THE CONCEPT

  - SkyShare uses a TCP server and client to communicate with each other. The client is built with the MSFS SDK, while the Server sends joystick data through the internet directly to the client. To ensure you are getting maximum speeds for data transfer, we have decided not to use a centralized "hub" server to process all of the server-client interactions; instead, we opted to have you port-forward.
  - The correct steps to getting everything setup is:
    1) Port forward
    2) Disable antivirus if you have any 3rd party antivirus
    3) Start the server (for the person connecting to the simulator)
    4) Allow the server connection in the client (for the person already flying)
    5) Enjoy your shared cockpit controls experience

- ## SECTION 1.3: SPECIAL THANK-YOU LIST

Forest Studio Team:

CEO & Code Team Lead: **Henry Chen**

Marketing Team Lead: **Ioan Constantin**

Graphics: **Daryl**

Company Infrastructure: **V1_Rotate**

Manual & Quality Assurance: **Drew Flomen**

Legal Team: **(wishes anonymous), LL.M., JD Candidate**

Hardware Test Team:

Brian Robinson

Ian (Captaincat)

SECTION 2: PORT FORWARD INSTRUCTIONS

- SECTION 2.1: WHAT IS PORT FORWARDING?

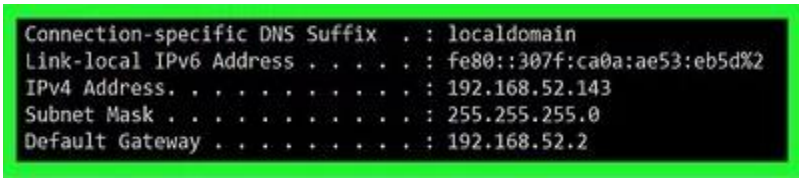
- If you have a home or office router, in order for the SkyShare server to be able to pick up your external connection, you will need to forward ports so that the outside traffic can get into your network. Your router comes preconfigured with a few of those ports open to let you access the internet, but the others are closed. To run the SkyShare server you will need to open an extra port in your router for the outside traffic to get inside. This is called Port Forwarding.

- SECTION 2.2: HOW DO I PORT FORWARD?

- **Step 1:** Login to your router via the **default gateway address**.

1. For Windows, you simply need to access a Command Prompt to find out what the IPv4 Address is. To access a Command Prompt, click on the "**Start**" menu button and search for "**CMD**".

2. In the Command Prompt window, type "**ipconfig**" and press "**Enter**" on your keyboard. You will see a lot of information generated in this window and if you scroll up you should see "**IPv4 Address**" with the device's IP address listed.



3. Once you have located the **IPv4 Address**, open any web browser, and input the IP address into the search bar located at the top.
   A box should appear prompting you to enter the **router's username and password**. This information can sometimes be found on your router, or in the router information guide.

Device	Username	Password
D-Link	admin	(leave blank)
Netgear	admin	password
Linksys	admin	admin
ASUS	admin	admin
DrayTek	admin	admin
ZyXel	admin	1234
TP-Link	admin	admin
TRENDnet	admin	admin
Belkin	admin	(leave blank)

- **Step 2:** Enter your router credentials into the login page.
  Please Note: Your router credentials should be on a sticker on the bottom of your router. *Some examples of router login details are:*

- **Step 3:** For proper connection, locate the port forwarding settings in your router settings portal. Typically, this will be under **Advanced** and then **Port Forwarding** or **Virtual Server** settings in your router settings portal depending on the device type and brand.

- **Step 4:** On the **Port Forwarding** page enter in a name for the connection, such as "SkyShare" and then enter the port you are forwarding in the port field (for SkyShare you must forward to **Port 32000** and select "TCP" under **protocol**). Next, enter the internal IP address of the device you are port forwarding to and click "**Apply**" or "**Save**" to store the changes so next time it will be a breeze to share the skies.

- **Step 5:** Finally, check to see if the port is working by verifying in your router settings portal and attempting a connection to the **SkyShare Server**.

- To make it more accessible and provide visual help, below you will see interfaces from the 4 most popular manufacturers. Be aware that your router may display a different interface. If you have any questions or are unsure what to do, we recommend finding a guide that provides more information about your router and internet provider. You can also contact Forest Studio Support through our forum at https://foreststudio.ca/forum/ or submit a support ticket at https://foreststudio.freshdesk.com/support/home

- **We would like to note that Australian ISP Telstra's newer router models may not support port forwarding. Please check with your ISP for router port forwarding support. Another solution is to purchase a router from big name brands such as DLink and connect it to the existing router. Please contact our Support Team for any further questions about this.**

SECTION 3: ANTI-VIRUS INSTRUCTIONS

- SECTION 3.1: WHAT IS AN ANTI-VIRUS?

- Antivirus software, or anti-malware, is a computer program used to prevent, detect, and remove malware. Antivirus software was originally developed to detect and remove computer viruses, hence the name.

- SECTION 3.2: FALSE POSITIVES

(SEE NEXT PAGE)

- SkyShare has been tested through various Anti-Virus software and have found that there have been no false positives or threats present at this stage in its current state. For confirmation here is the results from our testing:
- Since the Forest Studio team is making updates regularly it does not guarantee that some Anti-Viruses will detect SkyShare as a virus at some point in its lifetime. If you do happen to get a positive result we encourage you to disable your Anti-Virus, which you can find out how to do it in the following sections, and we ask that you open a support ticket through our website where our team can then look into this issue further and ensure that it is fixed in a reasonable amount of time.

Acronis	Undetected	Ad-Aware	Undetected
AegisLab	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	SecureAge APEX	Undetected
Arcabit	Undetected	Avast	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
BitDefenderTheta	Undetected	Bkav	Undetected
CAT-QuickHeal	Undetected	ClamAV	Undetected
CMC	Undetected	Comodo	Undetected
CrowdStrike Falcon	Undetected	Cybereason	Undetected
Cylance	Undetected	Cynet	Undetected
Cyren	Undetected	DrWeb	Undetected
eGambit	Undetected	Elastic	Undetected
eScan	Undetected	ESET-NOD32	Undetected
F-Prot	Undetected	F-Secure	Undetected
FireEye	Undetected	Fortinet	Undetected
GData	Undetected	Ikarus	Undetected
Jiangmin	Undetected	K7AntiVirus	Undetected
K7GW	Undetected	Kaspersky	Undetected
Kingsoft	Undetected	Malwarebytes	Undetected
MAX	Undetected	McAfee	Undetected
Microsoft	Undetected	NANO-Antivirus	Undetected
Palo Alto Networks	Undetected	Panda	Undetected
Qihoo-360	Undetected	Rising	Undetected
Sangfor Engine Zero	Undetected	SentinelOne (Static ML)	Undetected
Sophos AV	Undetected	Sophos ML	Undetected
SUPERAntiSpyware	Undetected	Symantec	Undetected
TACHYON	Undetected	Tencent	Undetected
TrendMicro	Undetected	TrendMicro-HouseCall	Undetected
VBA32	Undetected	VIPRE	Undetected
ViRobot	Undetected	Webroot	Undetected
Yandex	Undetected	Zillya	Undetected
ZoneAlarm by Check Point	Undetected	Zoner	Undetected

- ## Section 3.3: How can I prevent my anti-virus from interfering?

  - We have created the following guides for some of the most popular Anti-Virus Software. If you do not find the software that you use in this Manual we ask that you create a support ticket through our website so we can help you sort this issue out and potentially update our guides to include it.

1. Kaspersky:

- Step 1. Launch the Kaspersky total security application.

- Step 2. Click on the option more tools near the bottom. This button will be centered on the screen.

- Step 3. On the side menu, click on manage applications, then navigate to application control.

- Step 4. Near the top under the "**applications**" area, click on manage applications once again.

- Step 5. Upon scrolling to the bottom under "**low restricted**," you will see 3 items labeled "**SkyShare Server**", go ahead and right-click each, click on the restrictions pop-out, and set them to trusted.

***Please Note**:* the first time you set an application to trusted, it will create a pop-up that will ask you if you want to save your choice for the next selection for 30 minutes. Hit yes, this will prevent the pop-up from coming back each time you set an application to trusted within the next 30 minutes.

2. Norton:

- Step 1. Right-click the Norton Security icon located in the notification section of your Windows taskbar.

- Step 2. When the pop-up menu appears, select **Disable Auto-Protect**.

- Step 3. A **Security Request** dialog should now appear, overlaying your desktop and other active applications. Select the drop-down menu labeled **Select the duration**.

- Step 4. Choose the amount of time that you'd like Norton's Auto-Protect functionality to remain off by selecting one of the following options: **15 minutes**, **1 hour**, **5 hours**, **Until system restart** or **Permanently**.

- Step 5. Select **OK** to turn off Norton protection for the specified duration.

- Step 6. If you would like to re-enable Norton protection at any point prior to the time specified, repeat steps 1 and 2 above and select **Enable Auto-Protect**.

3. McAfee:

- Step 1. Right-click the **McAfee** icon at the bottom-right corner of your Windows Desktop.

- Step 2. Select **Change settings > Real-time Scanning** from the menu.

- Step 3. In the **Real-Time Scanning** status window, click the **Turn off** button.

- Step 4. You can now specify when you want Real-Time Scanning to resume. It is recommended to select **When I restart my PC** from the drop-down menu. Click on the **Turn off** button to confirm your selection.

- Step 5. McAfee AntiVirus has now been successfully disabled until the next computer restart.

4. Malwarebytes:

- Step 1. Open Malwarebytes Application

- Step 2. Click on Settings from the side menu on the left

- Step 3. Click on the Protection tab that is along the top.

- Step 4. Under Real-Time Protection you will find 4 toggle switches.

- Step 5. Switch them to the off position

- Step 6. There may be a User Account Control menu appear, click Yes to confirm your changes

5. Bitdefender:

- Step 1. Launch the Bitdefender Security Center.
- Step 2. Click on Protection from the side menu on the left.
- Step 3. Find the Antivirus section and click on Settings.
- Step 4. Toggle the Bitdefender Shield to off.
- Step 5. A User Account Control menu may appear, click Yes to confirm your changes.

6. Avast:

- Step 1. Go to the windows taskbar and right click on the Avast Icon.
- Step 2. Hover over the Avast shield control selection.
- Step 3. Select Disable for however long you wish.

7. Windows Defender:

- Step 1. Open start menu and type "Windows Defender".
- Step 2. Click on Virus & Threat Protection.
- Step 3. Select Manage Settings, Exclusions, Add or remove Exclusions.
- Step 4. Select Add an Exclusion, then navigate to and select the file SkyShare_Server.exe downloaded file.