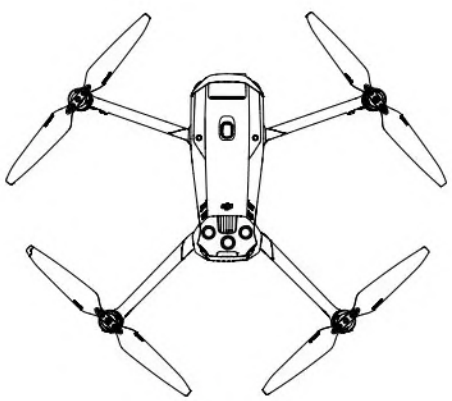
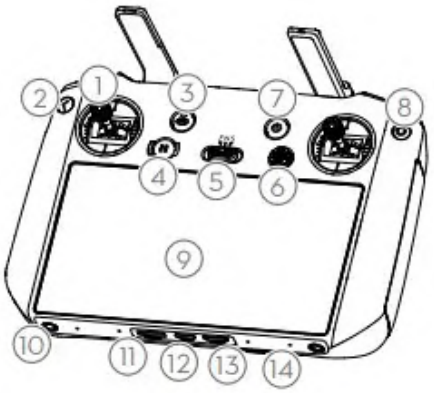
DroneControl FirstResponder

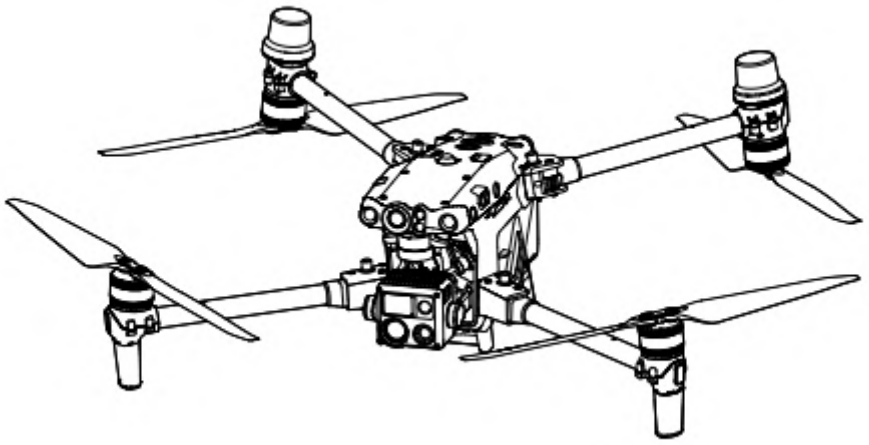
User Manual

Version 1.1

2023.08







DroneControl
Swiss Engineered, Swiss Precision

User Manuals, instructions and other material about product functions and specifics are DroneControl confidential Materials. Users are licensed to use these materials only for purposes of operating and using DroneControl Products. Unless otherwise authorized in this Terms, you are not eligible to use or allow others to use the Materials or any part of the Materials by reproducing, transferring or selling the Materials. Users should only refer to this document and the content thereof as instructions to operate DroneControl. The document should not be used for other purposes.

Contents

1.0 Introduction

2.0 Installation
- 2.1 Downloading the APK
- 2.2 Selecting the correct APK for your Drone.
- 2.3 Unpacking the APK
- 2.4 Enabling DC FirstResponder Auto start
- 2.5 Registration
- 2.6 Enabling correct region for signaling
- 2.7 Trial Period
- 2.8 License activation code
- 2.9 License terms and conditions

3.0 Drone Operation

4.0 Live Streaming

5.0 Remote Control

6.0 Viewer Controls

7.0 what3words and mapbox compatibility

8.0 AirData Compatibility

9.0 WebRTC
- 9.1 What is WebRTC?
- 9.2 Maximizing WebRTC Performance
- 9.3 IPv6

10.0 Data Security and Encryption
- 10.1 WebRTC Security Protocols
- 10.2 Detailed WebRTC Security Protocols
- 10.3 WebRTC Signaling
- 10.4 Use of TURN Servers
- 10.5 Independant API Analysis

11.0 Troubleshooting

12.0 Terms and Conditions

1.0 Introduction

Congratulations on choosing DroneControl FirstResponder as your software solution for your DJI Drone.

This software has been designed in conjunction with emergency services across Europe to meet your specific needs and help improve your incident response.

At the core of our technology is our secure peer-to-peer live streaming and remote control to improve incident responsiveness and collaboration. Our solution is designed for all DJI enterprise drones with compatibility for many consumer models.

We utilize Google's WebRTC to provide highly encrypted data channels to deliver hi res video and audio stream from the drone to the viewer and ultra-low latency remote control from the viewer to the drone.

There are also several customizations included in the application to enable you to protect lives better every day in the field. We are continuously updating the software based on user feedback so please reach out with feedback directly to us @ feedback@dronecontrol.co or through your local market Drone Solution Provider.

2.0 Installation

2.1 Downloading the APK

Using your DJI RC or Android device used to control the drone please navigate to:

https://www.dronecontrol.co/fr-apk-download-page

or use the QR code below

2.2 Selecting the correct APK for the compatible Drone.

Please download the correct APK for your Drone

DroneControl First Responder
Compatible with DJI Enterprise Drones released in 2022 onwards (SDK V5) Including: Mavic Series - 3 Enterprise, 3 Enterprise Thermal Matrice - 30, 30T Matrice 300, 350 Mini 3, Mini 3 pro (using DJI RC NR-1)

2.3 Installing the APK

Locate the APK file on your device and unpack the file. Please follow the on-screen instructions to install DroneControl FirstResponder.

2.4 IMPORTANT – You must force stop Pilot 2 and enable DC FirstResponder to auto start otherwise the app will not correctly work

2.4.1 Force Stop Pilot/Pilot 2

Please Complete the following steps:

- Enter "Settings menu" on RC or Android device
- Enter "Apps and notifications" menu
- Select "Pilot2" app under "recently opened apps"
- Click "FORCE STOP" and then "OK"

Or follow the below link to see how:

https://youtu.be/pTXZXpdQkbg

or follow the QR below:

2.4.2 Enable DroneControl FirstResponder to Auto Start

Please Complete the following steps:

- Enter “Settings menu” on RC or Android device
- Enter “Apps and notifications” menu
- Scroll down and select “Auto start application selection”
- Select “DroneControl FirstResponder”

Or follow the below link to see how:

https://youtu.be/o-T14bJM6rY

or follow the QR below:

Your device should now Auto Start DC FirstResponder

2.5 Registration

Please use your email to create an account for your free two-week trial account.

2.6 Enabling correct region for signaling.

To enable best performance, within the account settings menu please select your specific region for initial signaling. For more information on the signaling server process see section 4.1

2.7 Trial period

Your initial account registration activates a free two-week trial.

The app will automatically stop connecting to your drone after the two weeks have ended. In order to obtain the full license activation code please contact DroneControl directly or speak to your local drone solution provider

2.8 License activation code

Once you have received your license activation code, please enter the “account information” section of the app and when prompted enter your license activation code.. You may now use DC FirstResponder uninterrupted for the license duration.

2.9 License terms and conditions

For full terms and conditions please see market specific documentation

3.0 Drone Operational Instructions

Your DC FirstResponder app is designed to mimic your native drone software with the same features, so no retraining is needed.

Please refer to the user manual provided with your drone for more information.

4.0 Live Streaming

Enabling Live Stream Feed

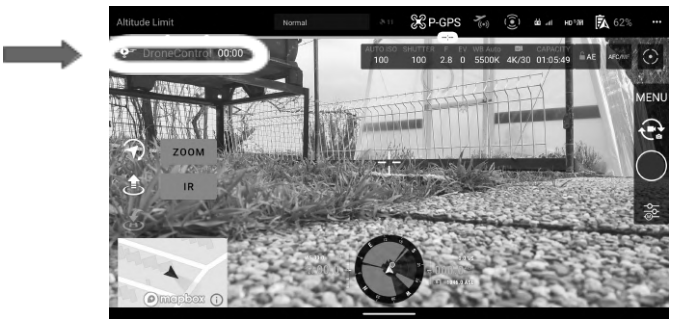
This will instruct you on how to start live streaming using DroneControl First Responder.

DroneControl FirstResponder provides users with a constant master streaming link to share with regular remote viewers or command centre for immediate connection.

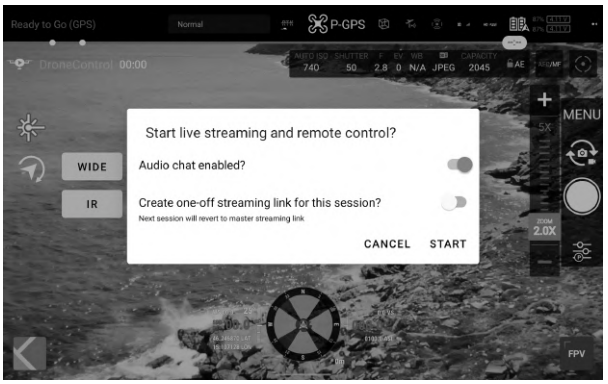
The user also has the option to create a one-off stream if they do not wish to grant access to the master stream to the viewers.

If the user creates a one-off stream for a session, for the next streaming session the link will revert to the master session.

- Enter the flight mode of DC FirstResponder
- Click the top left DroneControl logo

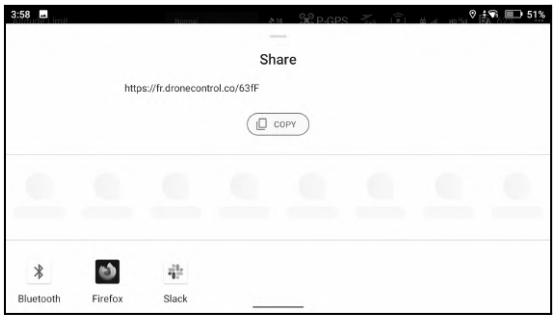


- On the white pop up select whether you wish to share audio chat and if you wish to generate a new streaming link and click START
- If you do not select “create one-off streaming link” you will maintain your master streaming link

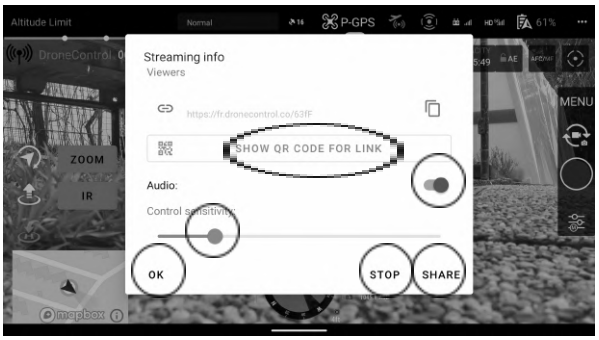


- You will have a notification message on the bottom of the screen confirming live streaming has started
- Network bandwidth speed test upon starting streaming session - you will see a traffic light symbol next to the streaming timer to indicator quality of the data connection-. Red - Poor, Orange - Moderate, Blue - Good, Green - Excellent.

- A white pop up with all methods for sharing the URL will appear. Select your chosen method (email, Bluetooth, message etc..) and the URL will appear to send to your chosen viewer



- After you share a red instruction pop will appear – click through and the streaming configuration pop up will appear. You can use this to 1) Reshare link 2) Toggle audio on/off 3) Stop streaming 4) Control Viewer control sensitivity (see remote control section) 5) Return to flight view 6) Use QR code to share link



- You may share the stream with as many viewers as you like but the quality of the stream to multiple viewers will depend on the available network bandwidth.
- The stream remains active until the pilot stops sharing, disconnects the drone or shuts down the app. The stream remains active even if the viewer closes the web browser.

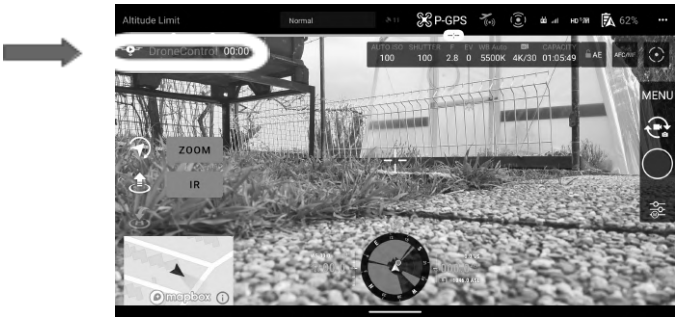
DroneControl
Swiss Engineered, Swiss Precision

5.0 Remote Control

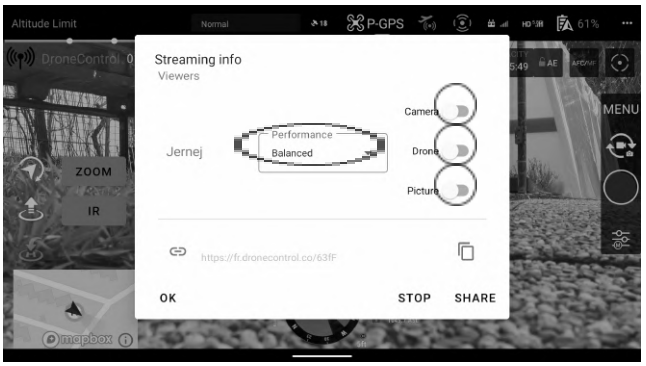
Enabling Remote Control

This will instruct you on how to share the remote control function of DroneControl First Responder.

- Once you have enabled live streaming above, click on the DroneControl icon on top left



- The streaming configuration pop up will appear but this time with the current viewers listed. For each viewer the pilot can give control for 1) Camera Gimbal 2) Drone 3) Take pictures/video. It is possible to give control to any configuration of the three. Select which controls you want the viewer to have and click "OK"



- There is also the option on the "Performance" drop down box to select which streaming attribute you wish the app to prioritize.

Setting	Priority	Example use case
Balanced	The app balances' framerate and resolution to maximize both	General flight
Framerate	Prioritizes Framerate so user may experience drop in resolution	When drone is moving quickly over a large distance
Resolution	Prioritizes Resolution so user may experience drop in Framerate	When drone is stationary overlooking an incident scene

- You can adapt the sensitivity of the viewer's controls to ensure safety of the drone and the surrounding area. Please toggle the sidebar left and right to adapt this setting.

- To change the control configuration please click back into the streaming configuration pop up box via the DroneControl logo at any time.

- As a safety protocol if the pilot touches any of the controls on the RC that have been shared to the viewer, the remote-control function cuts out and control returns to the pilot. The pilot will need to reshare the remote control as above.

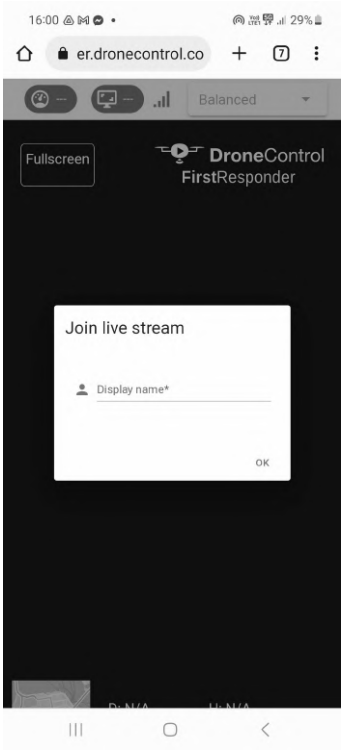
6.0 Viewer Control

This will instruct you on how to control from the viewer side of DroneControl First Responder.

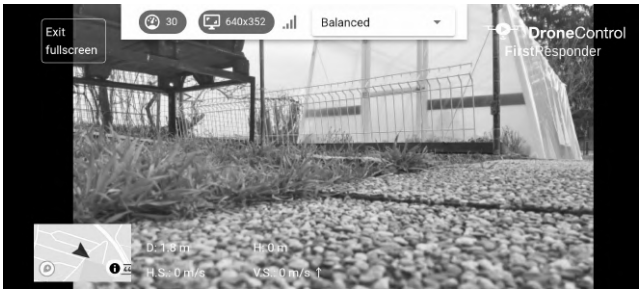
- Click on the link provided by the drone pilot (email, Bluetooth, message, QR code etc..)

- The link will open full screen using your default web browser – please refer to 7.1 for list of best performing browsers. DroneControl FirstResponder viewer is also optimized to work on mobile devices.

- Enter your names as defined by your organization – this allows the pilot to identify you and ensures no unauthorized viewers to the stream.



- After a brief moment the feed will connect,and you will see the live stream from the Drone with key information displayed 1) Map overview 2) Height 3) Distance from pilot 4) Speed 5) Vertical speed 6) Streaming performance (frames per second, resolution) 7) Exit full screen



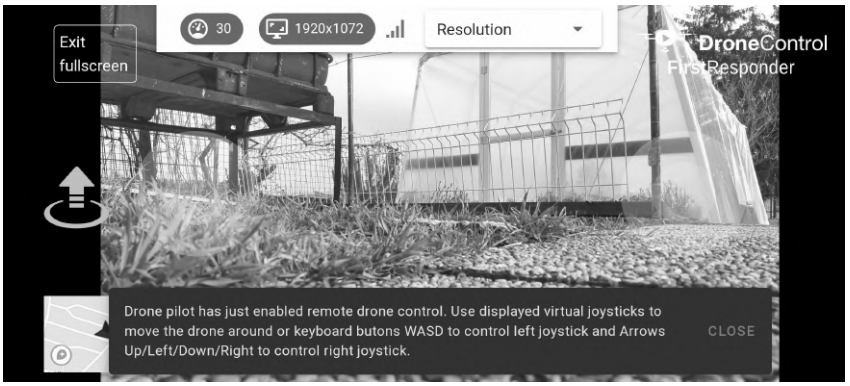
- The viewer can also adapt the stream using the “optimization” drop down box select which streaming attribute you wish the app to prioritize.

Setting	Priority	Example use case
Balanced	The app balances' framerate and resolution to maximize both	General flight
Framerate	Prioritizes Framerate so user may experience drop in resolution	When drone is moving quickly over a large distance
Resolution	Prioritizes Resolution so user may experience drop in Framerate	When drone is stationary overlooking an incident scene

Taking Control

Once the pilot has activated the remote control features you can take control of the Drone. You will see a notification at the bottom of the screen once the remote control is activated.

Drone Control – Two translucent white circles will appear on the screen.

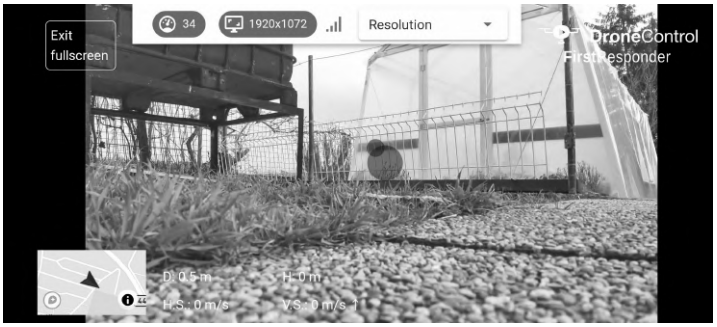


1. Take off / Landing icon
2. Left Control Stick (forward, back, turn left, turn right)
3. Right Control Stick (up, down, move left, move right)

Drone Control can be operated by:

1. Mouse – using the mouse point click and hold dragging the circles in the direction you wish to control the drone.
2. Keyboard – left control stick – WASD, Right control stick – keyboard arrows.
3. Please note with keyboard control the direction is either full on or full off. Please adjust the sensitivity accordingly.
4. Third party gaming controller – please connect to the device to use the controller.
5. Touch screen devices - using your fingers use the circles to control the drone

Camera Gimbal Control – Translucent blue circle will appear anywhere on the screen when clicked with the mouse.



1. Gimbal control
2. Zoom Control
3. Camera Lens Mode

Gimbal Control can be operated by:

1. Mouse – using the mouse point click and hold anywhere on the screen dragging the circle in the direction you wish to control the gimbal.
2. Touch screen devices - using your finger touch anywhere on the screen and drag the circle in the direction you wish to control the gimbal.

Zoom Control can be operated by:

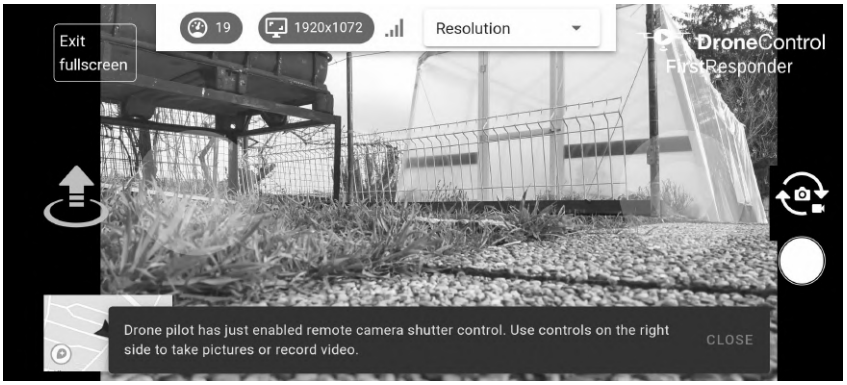
1. Mouse - using the mouse scroll wheel to zoom in and out
2. Keyboard touch pad - using two fingers move up and down to zoom in and out

Camera Lens Control can be operated by:

1. Mouse - using the mouse click on the buttons on the left to toggle between Zoom/Wide/IR
2. Touch screen - click on the buttons on the left to toggle between Zoom/Wide/IR

When the gimbal remote control is activated the drone automatically switches to Gimbal Free mode. If gimbal control is taken away, Gimbal mode switches back to Follow mode - this gives the viewer full range of motion of the camera gimbal without limitation.

Camera Control – Camera functional control will appear on the right of the screen.



1. Switch between photo / video
2. Start / stop recording / Take photo

Camera control can be operated by:

1. Mouse – using the mouse point click on icons to select mode / take video/photo
2. Touch Screen - click on icons to select mode and take photo/video

7.0 what3words and mapbox compatibility.

what3words

What3words is a proprietary geocode system designed to identify any location on the surface of Earth with a resolution of about 3 metres. The system encodes geographic coordinates into three permanently fixed dictionary words.

mapbox

Mapbox is a location data platform that provides customizable maps, search, and navigation experiences for developers to embed into their applications and websites.

7.1 Drone Position

- Click on Longitude/Latitude data on the bottom dial
- what3words location will appear underneath
- Click on what3words location to toggle to postal address

7.2 Laser Range Finder

- Activate Laser Range Finder
- Click on Longitude/Latitude data above the mapbox
- what3words location will appear
- Click on what3words location to toggle to postal address

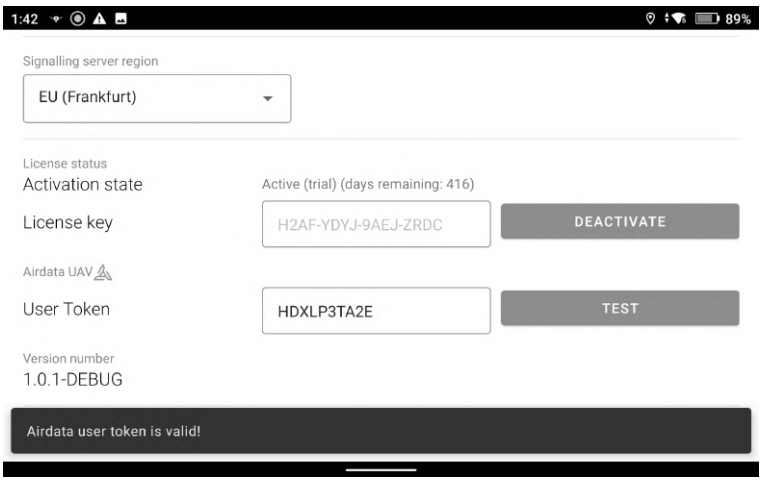
8.0 Airdata Compatibility

AirData is the largest online drone fleet data management and real-time flight streaming platform, serving over 250,000 users with 26 million flights uploaded to date, processing an average of 25,000 flights a day, with high-resolution data stored per each flight. It is used by large fleet operators around the world as a comprehensive flight safety data analysis and crash prevention platform, with advanced maintenance, mission planning, pilot tracking, and easy-to-use live streaming.

8.1 Instructions to connect DroneControl FirstResponder with AirData account.

All flight logs from DroneControl FirstResponder can be automatically uploaded to the AirData system.

- In account settings enter the auto upload token from AirData and click test to validate the connection



- If configured, Litchi will automatically upload flight records to Airdata.com when:
  - The motors are turned off at the end of the flight
  - Immediately after App starts and internet connection is detected
  - The upload is deferred until internet connection becomes available

9.0 WebRTC

9.1 What is WebRTC?

WebRTC stands for Web Real-Time Communication. It is an open-source technology that enables real-time communication between web browsers and mobile applications using simple APIs (Application Programming Interfaces). WebRTC is based on peer-to-peer communication and allows users to share data such as voice, video, and files, in real-time without the need for plug-ins or external software. It was developed by Google in 2011 and is now supported by all major browsers such as Chrome, Firefox, Safari, and Opera.

WebRTC works by establishing a direct connection between two users, bypassing the need for a server. This means that data is transferred directly between the two parties, making communication faster, more efficient, and more secure.

WebRTC is commonly used for video conferencing, live streaming, screen sharing, and file sharing. It has become an important technology for many industries including healthcare, education, and business, as it enables remote collaboration and real-time communication without the need for expensive and complicated software.

9.2 Maximizing WebRTC Performance

WebRTC is a powerful tool that enables real-time communication via browsers. However, it can be a bit tricky to use and may not perform optimally in certain situations. Here are some tips to help you improve your WebRTC performance:

1. **Use a good internet connection:**
   WebRTC requires a stable and fast internet connection. The higher the bandwidth, the better the quality of the video and audio. Make sure you have a reliable and fast internet connection to avoid latency issues.

2. **Optimize your browser settings:**
   Ensure that your browser settings are optimized for WebRTC. Check the browser's WebRTC settings and enable hardware acceleration to improve performance.

3. **Use a wired connection:**
   For better performance, connect your computer to the internet via a wired connection instead of using Wi-Fi. Wired connections provide better and more stable connectivity.

4. **Reduce the number of open tabs:**
   WebRTC is a resource-intensive tool. If you have multiple tabs open, the performance of WebRTC will be affected. Close any unnecessary tabs to improve performance.

5. **Use the latest browser version:**
   The latest versions of browsers are designed to work better with WebRTC. Ensure that your browser is updated to the latest version to take advantage of the latest improvements.

6. **Use a high-performance computer**:
   WebRTC requires a high-performance computer to function optimally. Upgrade your computer's hardware if necessary, to ensure it can handle the demands of WebRTC.

   By implementing these tips, you can improve the performance of WebRTC and enjoy high-quality, real-time communication.

9.3 IPv6

IPv6 is the latest version of the Internet Protocol, which is designed to replace IPv4.

9.3.1 IPv6 and WebRTC

IPv6 affects WebRTC in several ways:

1. Addressing: IPv6 provides a much larger address space than IPv4, allowing for more efficient addressing and routing of WebRTC traffic.
2. NAT traversal: WebRTC relies on NAT traversal techniques to allow communication between devices on different networks. IPv6 can simplify this process, as it eliminates the need for NAT in many cases.
3. Security: IPv6 includes improved security features such as IPsec, which can be used to secure WebRTC traffic.
4. Performance: IPv6 can potentially offer better performance for WebRTC, as it provides faster routing and lower latency.

Overall, the adoption of IPv6 is expected to improve the performance, security, and scalability of WebRTC, making it more efficient and reliable for real-time communication over the Internet.

9.3.2 Implementing IPv6

Implementing IPv6 involves several steps. Here is a high-level overview of the process:

1. Determine if your network infrastructure is ready for IPv6. This includes checking that your routers, switches, and other networking equipment support IPv6 and that your Internet Service Provider (ISP) can provide IPv6 connectivity.
2. Assign IPv6 addresses to your network devices. You can do this manually or by using a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server to automatically assign addresses.
3. Configure your network devices to support IPv6. This involves enabling IPv6 on your routers, switches, firewalls, and other network devices.
4. Update your DNS server to support IPv6. This ensures that your IPv6 addresses can be resolved to domain names.
5. Test your IPv6 connectivity. Use an IPv6 testing tool to verify that your network devices can communicate using IPv6.
6. Deploy security measures for IPv6. This includes setting up firewalls and ensuring that your IPv6 traffic is encrypted using protocols such as IPsec.
7. Monitor and manage your IPv6 network. Use network management tools to monitor your network traffic and performance, and to troubleshoot any issues that arise.

It is recommended to consult with an experienced network administrator or consultant to ensure a successful IPv6 implementation.

10.0 Data Security and Encryption

10.1 WebRTC Security Protocols

WebRTC was designed with security in mind and has several built-in security features that make it a secure protocol for real-time communication.

Here are some of the security features of WebRTC:

1. Encryption: WebRTC uses Secure Real-time Transport Protocol (SRTP) to encrypt data, which provides end-to-end encryption for voice and video communication. This means that the communication is encrypted from the sender's browser to the recipient's browser, making it difficult for an attacker to intercept and read the communication.

2. Peer-to-peer communication: WebRTC uses peer-to-peer communication, which means that the data is transmitted directly between the browsers of the participants without going through a central server. This reduces the attack surface and makes it more difficult for an attacker to intercept or manipulate the communication.

3. Permission-based access: WebRTC requires user permission to access the camera and microphone, which means that users have control over the use of their devices and data.

4. Network address translation (NAT) traversal: WebRTC has built-in support for NAT traversal, which allows communication between devices that are behind different NATs or firewalls. This helps to ensure that communication is secure and not compromised by network vulnerabilities.

10.2 Detailed WebRTC Security Protocols

Raw data download of DroneControl WebRTC security protocols

```
transport (iceState=connected, dtlsState=connected, id=T01)
Statistics T01
timestamp 8/23/2023, 3:18:21 PM
bytesSent 3456618
[bytesSent_in_bits/s] 54688.50271581135
packetsSent 31578
[packetsSent/s] 61.991501542714346
bytesReceived 166832972
[bytesReceived_in_bits/s] 2813414.3071111226
packetsReceived 182303
[packetsReceived/s] 377.9481868249358
dtlsState connected
selectedCandidatePairId CPBfwV6UI7_qz8ArKFo
localCertificateId CF54:C1:EC:BB:B6:E2:2B:AD:94:B6:13:9E:3B:86:8F:FA:56:5E:D9:41:24:2D:A4:57:85:38:2C:00:98:A9:10:C8
remoteCertificateId CF29:C3:10:22:F4:71:5B:FD:44:4F:5E:AE:B6:CE:29:00:FE:D8:FA:51:E8:37:F4:A2:25:FB:3B:97:08:AC:07:F6
tlsVersion FEFD
dtlsCipher TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
dtlsRole server
srtpCipher AES_CM_128_HMAC_SHA1_80
selectedCandidatePairChanges 1
iceRole controlling
iceLocalUsernameFragment bEEg
iceState connected
```

Cipher key break down

AES_CM_128_HMAC_SHA1_80 refers to a specific cryptographic profile used to secure media in real-time communication protocols, such as in SRTP (Secure Real-Time Transport Protocol). Here's a breakdown of what this cipher suite means:

AES_CM_128: AES (Advanced Encryption Standard) is the encryption algorithm used. "CM" stands for Counter Mode, which is a way that AES can be used to encrypt data in a streaming fashion. The "128" refers to the key length in bits, so this part tells us that 128-bit keys are used for AES encryption.

HMAC_SHA1_80: HMAC (Hash-Based Message Authentication Code) with SHA-1 (Secure Hash Algorithm 1) is used for integrity protection and authentication. The "80" refers to the length of the authentication tag in bits. This means that a truncated 80-bit MAC (Message Authentication Code) is used, which helps verify that the data has not been tampered with.

So, in summary, AES_CM_128_HMAC_SHA1_80 means that AES in counter mode with 128-bit keys is used for encryption, and HMAC with SHA-1 and an 80-bit tag is used for authentication. This combination provides both confidentiality and integrity for the protected media streams.

10.3 WebRTC Signaling

WebRTC (Web Real-Time Communication) is a peer-to-peer communication technology that allows browsers or devices to communicate directly with each other without going through a central server. However, for WebRTC to establish a connection between two devices, it requires a signaling mechanism to exchange information such as network addresses and media capabilities.

Signaling is the process of exchanging information between two devices to establish a communication session. In the case of WebRTC, signaling is responsible for exchanging the following information:

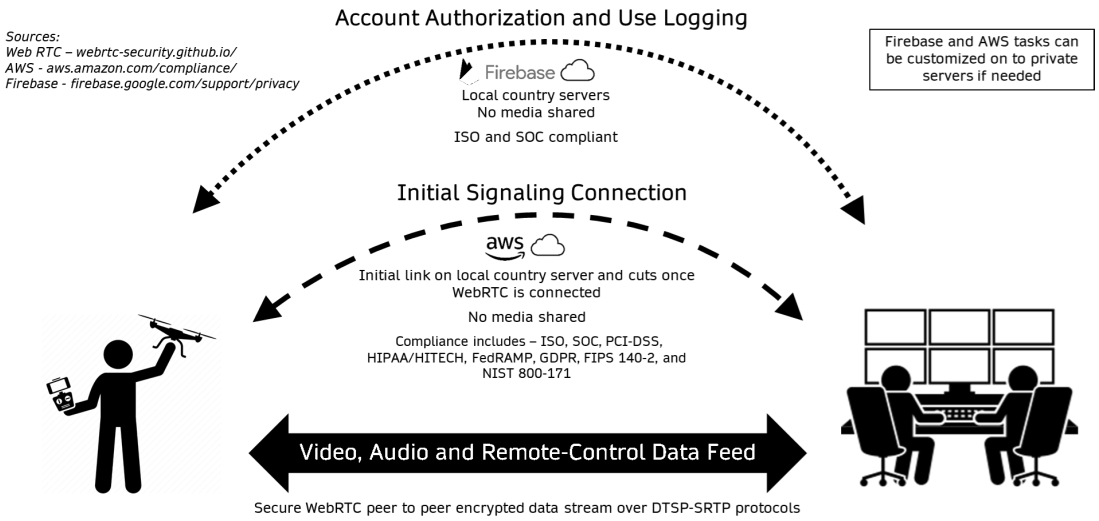
1. Session Description Protocol (SDP): SDP is a text-based protocol that describes the media capabilities of the devices. The SDP contains information such as the codecs supported by the device, network addresses, and session duration.
2. ICE candidates: ICE (Interactive Connectivity Establishment) is a technique used to establish a connection between devices that are behind different NATs (Network Address Translators) or firewalls. ICE candidates are network addresses used to establish a connection between devices.
3. Signaling protocol: WebRTC uses a signaling protocol such as WebSocket, HTTP, or SIP to exchange signaling messages between devices.

The signaling process in WebRTC usually involves the following steps:

1. User A's browser sends an SDP offer to a signaling server.
2. The signaling server forwards the SDP offer to user B's browser.
3. User B's browser receives the SDP offer and sends back an SDP answer to the signaling server.
4. The signaling server forwards the SDP answer to user A's browser.
5. User A's browser receives the SDP answer and establishes a connection with user B's browser using the ICE candidates exchanged in the SDP messages.

Once the signaling process is complete, the browsers can exchange media streams directly without going through a central server. This allows for low latency and high-quality communication between devices.

DroneControl FirstResponder uses signaling servers provided by AWS based in the local market you are in to increase the level of security.



10.4 Use of TURN Servers

A TURN (Traversal Using Relay NAT) server is a network server used in WebRTC to relay media traffic between two devices in the unlikely event when a direct peer-to-peer connection cannot be established (under 5% of streams). In WebRTC, a TURN server is used as a fallback mechanism when a direct connection between two devices cannot be established due to network constraints such as NAT (Network Address Translation) or firewall restrictions.

When two devices try to establish a WebRTC connection, they exchange ICE (Interactive Connectivity Establishment) candidates, which are network addresses used to establish a direct connection between the devices. If a direct connection cannot be established using the ICE candidates, the devices will use a TURN server as a relay to send and receive media traffic.

The media stream remains encrypted as the TURN server does not contain the encryption keys needed to read the media stream and acts purely as a relay point until peer to peer can be established. DroneControl FirstResponder uses TURN servers provided by AWS based in the local market you are in to increase the level of security.

Here's how WebRTC uses a TURN server:

1. During the signaling process, both devices exchange ICE candidates that include both public and private IP addresses.
2. The devices will attempt to establish a direct peer-to-peer connection using the ICE candidates. If a direct connection cannot be established, they will use a STUN (Session Traversal Utilities for NAT) server to identify their public IP address and NAT type.
3. If the STUN server is unable to determine the public IP address and NAT type, the devices will use a TURN server to relay media traffic.
4. One of the devices sends media traffic to the TURN server, which relays the media traffic to the other device.
5. The other device sends media traffic to the TURN server, which relays the media traffic back to the first device.
6. The TURN server acts as a relay for the media traffic until a direct connection can be established between the devices.

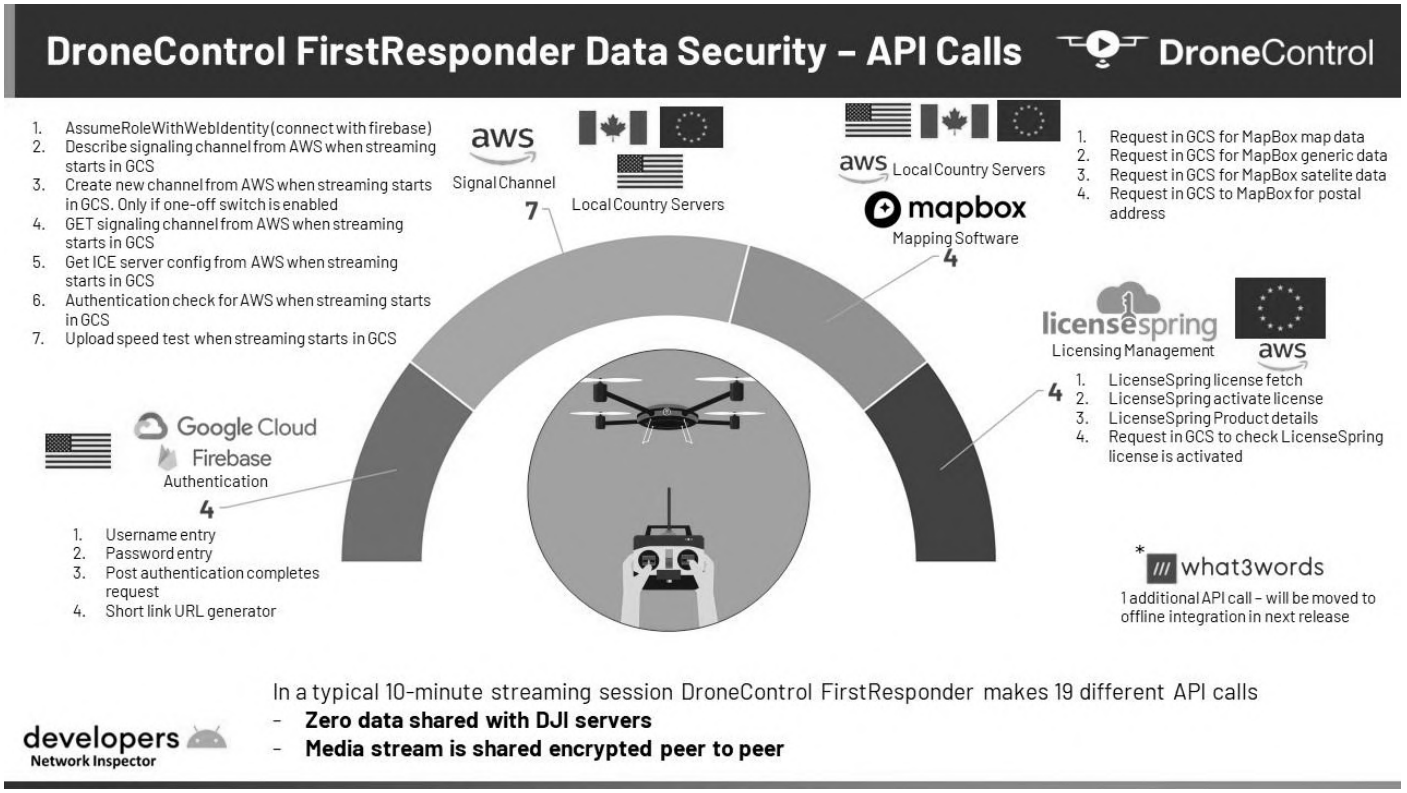
In summary, a TURN server is used as a fallback mechanism in WebRTC when a direct peer-to-peer connection cannot be established due to network constraints. The TURN server acts as a relay for media traffic until a direct connection can be established between the devices, improving the reliability of WebRTC communication.

10.5 Independant API Analysis

To understand the underpinning of this cutting-edge software, a detailed examination of the data connections utilized by the solution was conducted using Andriod's Developers Network Inspector.

19 Different API Calls in a 10-Minute Streaming Session.

- Google Firebase: Utilizes US servers for authentication.
- AWS: Leverages local market servers for signaling services to connect the peer-to-peer media streams.
- Mapbox: Employs local market servers for map features and postal addresses.
- Licensespring: Uses European servers for DroneControl License management.



11.0 Trouble Shooting

1. Ensure Auto start is enabled on DroneControl FirstResponder (see instructions 2.4)
2. If stream is not visible, please stop and restart stream
3. Check browser compatibility: Ensure that the browser being used is compatible with WebRTC technology. Supported browsers include Chrome, Firefox, Edge, and Safari.
4. Check network connectivity: WebRTC requires a stable and reliable internet connection. Verify that the network connection is strong and stable. If the network is weak or congested, it can cause issues with WebRTC.
5. Check firewall settings: Firewalls can interfere with WebRTC traffic. Ensure that the firewall is not blocking any ports that WebRTC uses, such as ports 3478-3481 and 443.
6. Check camera and microphone permissions: WebRTC requires access to the user's camera and microphone. Verify that the browser has permission to use these devices.
7. Check media constraints: WebRTC uses media constraints to control the quality of the media streams. Ensure that the constraints are properly set and not too restrictive.
8. Check the signaling server: The signaling server is responsible for negotiating the connection between peers. Verify that the signaling server is functioning correctly and that there are no issues with connectivity.
9. Check NAT traversal: WebRTC uses NAT traversal to establish connections between peers behind NAT. Verify that the NAT traversal is working correctly and that there are no issues with connectivity.
10. For any further issues please contact support@dronecontrol.co or your local market reseller.

12.0 Terms and Conditions for DroneControl FirstResponder

12.1 Introduction

12.1.1 These terms and conditions govern the use of the DroneControl FirstResponder (the "Program") provided by DroneControl (the "Provider") for use with DJI drones.

12.1.2 By using the Program, you agree to be bound by these terms and conditions. If you do not agree to these terms and conditions, you must not use the Program.

12.2 License

12.2.1 The Provider grants you a limited, non-exclusive, non-transferable license to use the Program solely for the purpose of controlling DJI drones.

12.2.2 You may not copy, modify, distribute, sell, or sublicense the Program, except as expressly permitted by these terms and conditions.

12.2.3 You acknowledge that the Program is protected by copyright and other intellectual property laws, and that you have no ownership rights in the Program.

12.2.4 The Program is provided "as is" without warranty of any kind.

12.3 Use of the Program

12.3.1 You must use the Program in accordance with all applicable laws and regulations, including the Civil Aviation Authority's rules for the operation of drones in your geographical area.

12.3.2 You are solely responsible for ensuring that you have the necessary permissions and licenses to operate the drones and use the Program.

12.3.3 You must not use the Program for any illegal or unauthorized purpose, including but not limited to spying, trespassing, or harassing individuals.

12.3.4 You must not use the Program to interfere with other drones or aviation systems, or to violate the privacy or safety of others.

12.3.5 You are solely responsible for ensuring that your DJI drone is in compliance with all applicable laws and regulations, including the Civil Aviation Authority (CAA) regulations for drone operation in your geographic area.

12.3.6 You are also solely responsible for ensuring that your DJI drone is in good working condition and is suitable for the intended use of the software.

12.4 Liability

12.4.1 The Provider is not responsible for any damages or losses resulting from the use of the Program or from the operation of your DJI drone, including but not limited to personal injury, property damage, or economic loss.

12.4.2 You agree to indemnify, defend, and hold harmless us and our affiliates, officers, directors, employees, agents, and contractors from any and all claims, damages, expenses, and liabilities (including reasonable attorney fees) arising from your use of the program or from the operation of your DJI drone.

12.5 Data Privacy

12.5.1 Our drone flight software program collects and stores certain data about your drone, including its location, flight path and stream quality (but never the media data stream)

12.5.2 We will use this data to improve the functionality of our software and to provide you with better service. We will not share your data with third parties except as required by law or as necessary to provide you with the software.

12.6 Termination

12.6.1 We may terminate your license to use our drone flight software program at any time if you breach these terms and conditions.

12.6.2 Upon termination, you must immediately stop using the software and delete all copies of the software from your computer or device.

12.7 Governing Law

12.7.1 These terms and conditions shall be governed by and construed in accordance with the laws of Switzerland. Any dispute arising out of or in connection with these terms and conditions shall be subject to the exclusive jurisdiction of the courts of Switzerland.

12.8 Changes to Terms and Conditions

12.8.1 We may change these terms and conditions at any time by posting the revised terms and conditions on our website.

12.8.2 Your continued use of our drone flight software program after the revised terms and conditions have been posted constitutes your acceptance of the revised terms and conditions.
