



Casia Ground

Networking Requirements

Contents

Contents	Error! Bookmark not defined.
Revision History	3
Description	3
Basic Networking	3
Local IP Address Assignment.....	3
Device Hostname	3
Remote Device Management.....	3
Real Time Airspace Surveillance	4
Remote Support.....	5
Network Time Protocol.....	5

Revision History

Rev	Date	Description	Author
1.0	2024-10-31	Initial Release.	James H
1.1	2025-05-15	Add ubuntu package repository requirements.	James H

Description

This document details the networking requirements for the Casia G device to function correctly on a tightly controlled or firewalled network.

The Casia G device functionally requires network access for four distinct purposes, remote device management, realtime airspace surveillance, remote support, and timekeeping. Each functional area is detailed in the following sections, along with other basic networking information.

Basic Networking

Local IP Address Assignment

Casia G devices are configured by default to receive a local IP address from a DHCP server.

If a static IP address is required for a specific deployment, we recommend the IP address be reserved on the DHCP server for the device's specific MAC address.

Device Hostname

All Casia G devices broadcast a hostname that matches their device serial number. This can be useful for tracking down the device on a busy network with lots of clients.

For example the hostname would look similar to "GACM-0100-000123".

Remote Device Management

Remote device management enables the operator or the Casia G to alter the configuration of the device remotely including deploying software updates and security fixes, altering the software configuration, viewing the status of the device, and configuring the device cameras.

To enable remote management infrastructure we utilize Amazon Web Services (AWS) and the following associated network services and connections should be allowed.

Note: AWS services are hosted on load balanced and ephemeral servers, therefore the IP address of each service can (and will) change without notice, usually within minutes, therefore they are not included in the following list.

Description	URL	IP	Port	Tx	Protocol
AWS IoT (device management)	flightdeck.irisonboard.com Aliases: dms-production-load-balance-1993248188.us-west-2.elb.amazonaws.com	54.188.15.131 44.232.12.82 52.88.153.53 52.25.38.204	443, 8883	TCP	
Amazon ECR (software updates)	064815029719.dkr.ecr.us-west-2.amazonaws.com	-	443	TCP	
Amazon ECR (software updates)	161b231b478fe029.elb.us-west-2.amazonaws.com	-	443	TCP	
Amazon S3 Storage (misc. functionality)	s3-us-west-2-w.amazonaws.com	-	443	TCP	
Ubuntu Package Repository	ports.ubuntu.com	-	80	TCP	

Updates

When Casia G updates to the latest version of our software it may also need to update dependent software packages hosted on the Ubuntu package repository. These updates can include security fixes and other changes.

Without access to this repository, software updates will fail.

Note: Ubuntu services are hosted on load balanced and ephemeral servers, therefore the IP address of each service can (and will) change without notice, usually within minutes, therefore they are not included in the following list.

Description	URL	IP	Port	Tx	Protocol
Ubuntu Package Repository	ports.ubuntu.com	-	80	TCP	

Real Time Airspace Surveillance

To communicate aircraft detections in real time Casia G sends data to a centrally managed MQTT Broker provided by uAvionix. From here the Broker disseminates data to the correct clients for each device. This data can then be viewed using applications such as the Casia Groundstation.

To enable real time airspace surveillance data to be transmitted, the following network services and connections should be allowed.

Description	URL	IP	Port	Tx	Protocol
MQTT Broker	mqtt.irisonboard.com	35.232.246.231	8883	TCP	MQTTS

Remote Support

Occasionally an error may occur that requires uAvionix support, or a customized configuration change is needed for a specific deployment. In order to support our customers and make these changes without charging on-site support fees we utilize a remote support tool called Teleport.

Teleport allows us to securely reverse SSH into the devices. To enable Teleport to function correctly the following network services and connections should be allowed.

Description	URL	IP	Port	Tx	Protocol
Teleport Secure Reverse SSH	tele.irisonboard.com	35.86.132.118	443	TCP	TLS

Network Time Protocol

To keep the clock of the Casia G synchronized the device uses the Network Time Protocol (NTP) to determine accurate time from trusted servers. Keeping accurate time is crucial as all communications from the Casia G are encrypted and encryption signatures are highly sensitive to incorrect timing. A desynchronized clock can prevent Casia G from functioning altogether.

To enable NTP for the device, the following network services and connections should be allowed.

Description	URL	IP	Port	Tx	Protocol
NTP Server	ntp.ubuntu.com	185.125.190.57 185.125.190.56 91.189.91.157 185.125.190	123	TCP	NTP
NTP Server	0.arch.pool.ntp.org	45.61.187.39 51.81.226.229 212.227.240.160 104.167.215.195	123	TCP	NTP
NTP Server	1.arch.pool.ntp.org	135.134.111.122	123	TCP	NTP
NTP Server	2.arch.pool.ntp.org	5.78.62.36	123	TCP	NTP