AXON

Fleet 2 Network Information and Configuration Guide

Rev: 08 Aug 2024

Axon Enterprise, Inc.
17800 N 85th St
Scottsdale AZ 85255
USA

Contents

Introduction 1

Axon Evidence configuration requirements 1

Software and firmware updates 1

Network configuration 2

Mobile Data Terminal/Computer (MDT/C) 2

Fleet cameras (front and back) 3

Wireless configuration 3

Vehicle network configuration 4

Network configuration – Wi-Fi offload using wireless offload server 5

VPN configuration 7

Method 1: Local network exemption (split tunnel) 7

Method 2: Application exemption 7

Wireless offload server with VPN 7

APN configuration 8

Wireless offload server with APN 8

Proxy considerations 9

Introduction

The Axon Fleet 3 solution is a purpose-built in-vehicle, AI-driven recording system for capturing audio and video in high-risk environments encountered by law enforcement, corrections, military, emergency medical services (EMS), and private security. The system records events for secure storage, retrieval, and analysis leveraging Axon Evidence services. Recordings transfer securely to Axon Evidence using LTE, Wi-Fi, or manual operations.

Fleet 3 typically consists of at least two cameras: one in the front of the vehicle in a windshield mount and the second pointed at the law enforcement vehicle's prisoner compartment. These cameras are connected to and controlled by the Fleet Hub, which can control additional cameras, such as for side views. Add an Axon Signal Vehicle device to automatically activate nearby Axon Body-Worn Cameras (BWC) during Fleet recording events.

This guide describes network requirements for Axon Fleet 2. It outlines the minimum required configurations and addresses common implementations such as VPN, APN, and proxy.

Axon Evidence configuration requirements

Axon Evidence offers a graphical configuration UI for fast setup of Fleet 2 vehicle information. Configure new vehicles with a few clicks and modify existing configurations as needed.

When Axon View XL is connect to Axon Evidence, it automatically downloads the correct configuration. For details, see the **Axon Evidence Fleet Setup Guide** on the Fleet 1 and 2 product page.

Software and firmware updates

Axon View XL automatically downloads the latest software version. When you sign into View XL, you can initiate the update.

Axon View XL downloads camera firmware updates automatically as needed. Install an update when you're signed into View XL.

Network configuration

This topic discusses system ports, traffic flows, configurations, and how the system deals with updates for Axon Fleet 2 software and firmware.

Mobile Data Terminal/Computer (MDT/C)

Hereafter, we'll refer to this as the MDT.

Inbound traffic ports

The Axon View XL installation program creates the following Windows Firewall rules during installation:

- Inbound Rule: "Fleet GPS"
  Program Allowed: `%installdir%\axon-agent.exe`
  Protocol and Port: UDP 10110
  Scope: Local subnet
  Currently the GPS port configuration can only be overridden using conf.toml file.
- Inbound Rule: "Fleet RTP"
  Program Allowed: `%installdir%\axon-agent.exe`
  Protocol and Port: UDP 5004-6004
  Scope: Local subnet
  Currently RTP (Live View) only uses UDP. The port range can be overridden via conf.toml

The HUD uses service port TCP 18888 bound to localhost for the login flow only. This port is used as long as the authentication flow is executing before closing the connection.

The HUD uses service ports 7777 and 7878 for communication, but these should only be bound to localhost.

Outbound traffic

All outbound traffic is from non-privileged ports above port 1024:

- To camera ports outlined in the Fleet Cameras section below.
- To Axon Evidence, port 443
  - Encryption: HTTP/TLS
- To Axon Evidence, port 80
  - For time synchronization. This is done on an hourly interval using the HTTPDate protocol. Expected volume is 2 KB per hour.
  - Encryption: none
  - Authentication: none

Fleet cameras (front and back)

Open ports

- TCP 80 (HTTP)
  - Provides a webservice API for use by the Axon View XL application.
  - The webservice does not respond to plaintext requests and does not provide index pages to reduce discoverability.
  - Encryption: Yes for command handling, using Diffie-Hellman with SHA-256 for key exchange and the cipher is AES-256. Bulk data endpoints for pulling media, logs, or pinging the camera are not encrypted.
  - Authentication: None. Assumes cameras are Axon Fleet cameras with specific serial numbers.
- TCP 554 (RTSP)
  - Provides a streaming server for preview of videos by the Axon View XL application. This endpoint can stream video but cannot issue any commands to the camera.
  - Encryption: None
  - Authentication: None

Outbound traffic

The cameras have outbound traffic for offloading video evidence and for live view over the local area network.

Wireless configuration

Each Fleet vehicle must host an 802.11 wireless network using 5 GHz band because Fleet cameras are not wired to an ethernet network.

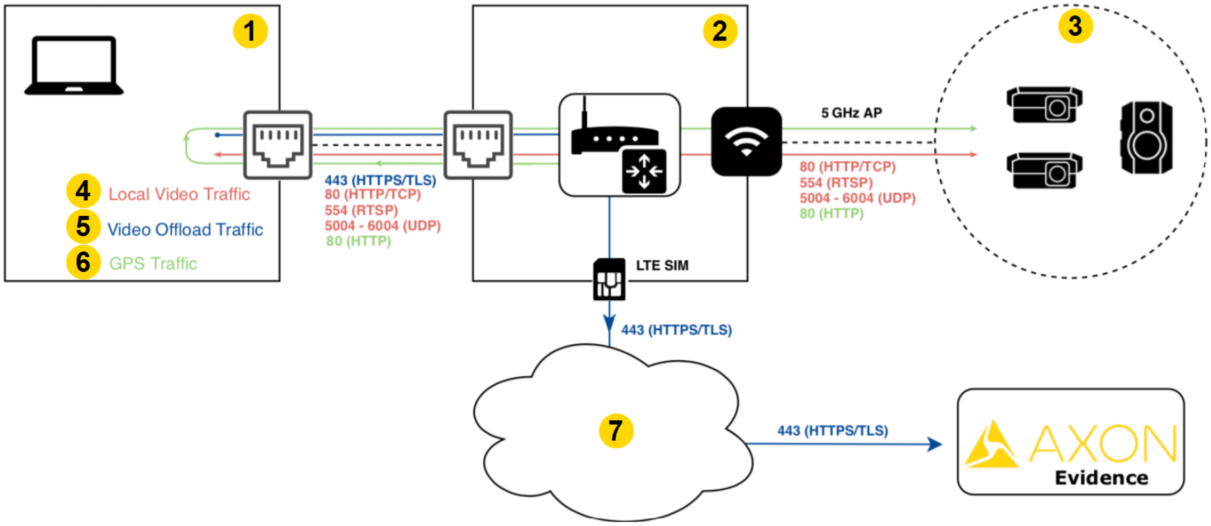
Requirements

- 802.11n @ 5 GHz with a 20 MHz channel width
- Non-DFS channels required
- WPA2-PSK security required
- Unique SSID per vehicle, using only 5 GHz; SSID may be hidden
- DHCP service on the wireless network

Vehicle network configuration

Within the vehicle, the MDT needs connectivity to the cameras on the local network and Axon Evidence.

Axon Fleet 2 Network Architecture – LTE Offload



Port	Protocol	Description	Callouts
80	TCP	Webservice API	1. Agency MDT 2. In-car router 3. 5 GHz AP 4. Local video traffic 5. Video offload traffic 6. GPS traffic 7. WAN
554	RTSP	Local live view/video preview server	
5004–6004	UDP	Local live view for axon-agent.exe	
443	HTTPS/TLS	Outbound to Axon Evidence for authentication	
10110	UDP	GPS	

Requirements

- DHCP service for the cameras. The cameras query for an IP address at startup. The MDT/MDC running Axon View XL can hold a static IP.
  - Axon Fleet 2 integrates with Axon body cameras, so the DHCP pool should contain a minimum of three camera IP addresses (two Fleet and one body camera).
- Layer 3 reachability between the Axon View XL app and the cameras. The devices don't rely on broadcasts in layer 2, so they can be placed in different VLANs, provided the subnets can route between each other.

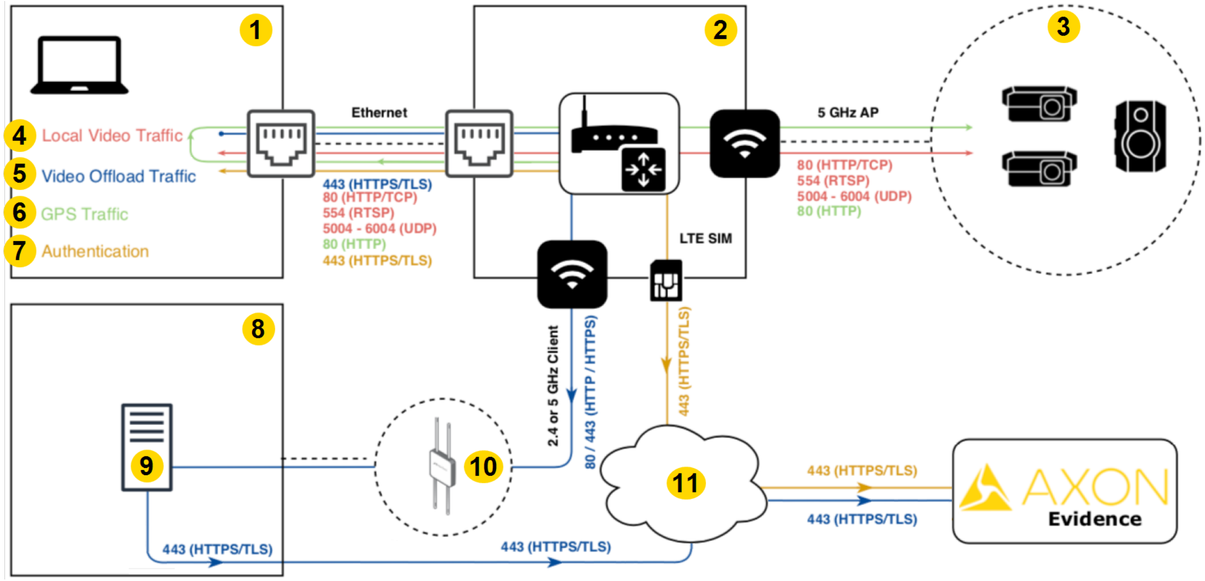
- GPS Setup: Axon View XL listens for GPS on port 10110 UDP (NMEA or TAIP). Recommended GPS reporting interval is one second.
- For full tunnel VPNs, make exceptions for local traffic to the cameras.

Network configuration – Wi-Fi offload using wireless offload server

For qualified customers, Axon offers an optional offload method with an on-premises server. When a vehicle's router connects to a pre-configured wireless offload infrastructure, Axon View XL establishes a connection to the offload server. Video is copied to the offload server from the in-car environment. Videos on the offload server are then uploaded to Axon Evidence.

Before starting this section, complete Vehicle Network Configuration on page 4.

Axon Fleet 2 Network Architecture – Wi-Fi Offload



Port	Protocol	Description	Callouts
80	TCP	Webservice API	1. Agency MDT 2. In-car router
554	RTSP	Local live view/video preview server	3. 5 GHz AP 4. Local video traffic 5. Video offload traffic
5004–6004	UDP	Local live view for axon-agent.exe	6. GPS traffic 7. Authentication
443	HTTPS/TLS	Outbound to Axon Evidence for authentication	8. Agency network 9. Wireless offload server
10110	UDP	GPS	10. Agency AP 11. WAN

Requirements

In addition to the network requirements outlined in Network configuration on page 2, using a wireless offload server requires additional changes.

- An active Wireless Offload Server and qualified wireless infrastructure are required – please contact your Axon Sales Engineer for more information.
- Wi-Fi as WAN connection from the in-car router to wireless offload infrastructure. Axon recommends a dedicated radio for video offload.
- Complete network path from View XL to the wireless offload server.
- Avoid network IP conflicts between the onsite wireless infrastructure and the in-car network.
- If using VPN or APN, traffic bound for the wireless offload server must be exempt from the tunnel.

> **Warning** Failure to exempt this traffic from the tunnel may result in offload to the wireless offload server over the LTE connection.

VPN configuration

Depending on agency configurations, a VPN may force all IP-based traffic to travel through its tunnel to a remote network. To let software on the MDC communicate locally to the cameras installed in the car, the traffic must be exempt from the tunnel.

A VPN administrator be available during the Axon Fleet 2 installation.

Method 1: Local network exemption (split tunnel)

Refer to your VPN provider documentation for instructions on configuring this exemption.

Example – If the local in-car network is 192.168.0.0/24, implement a rule to exempt traffic bound for this network; this View XL communicate with the cameras.

Method 2: Application exemption

Video files may be quite large. To prevent offload traffic from being steered through a remote network, add an exemption for the Fleet 2 application, Axon View XL. This will prevent View XL traffic from traversing the tunnel, mitigating potential bandwidth congestion.

Add the following exemptions:

- `%installdir%\axon-agent.exe` – Responsible for communication with cameras, Axon Evidence, and evidence offload.
- `%installdir%\Axon Fleet.exe` – Handles user authentication against Axon Evidence, including optional single sign on (SSO). The space in “Axon Fleet” is intentional.

Wireless offload server with VPN

When implementing a wireless offload server, design a network architecture to prevent access from outside the local network. Traffic destined for the wireless offload server should not traverse a VPN tunnel. Add a rule to exempt traffic to the wireless offload server. Failure exempt traffic from the tunnel may result in upload to the wireless offload server over the LTE connection.

APN configuration

Some agencies may use a private network through their cellular carrier. Similar to a VPN, some traffic may need to be exempt or split from the APN traffic rules.

If traversing an APN, Axon Evidence must be accessible from the MDT. Contact Axon support for a list of Axon Evidence IP addresses in your area.

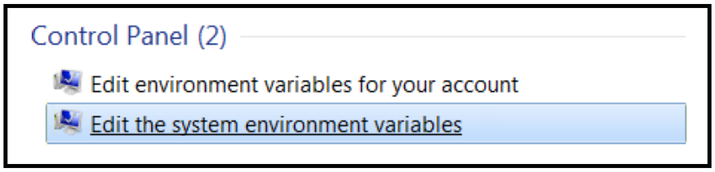
Wireless offload server with APN

When implementing a wireless offload server, design the network architecture to prevent access from outside the local network. Traffic destined for the wireless offload server should not traverse an APN. Add a rule to prevent traffic to the wireless offload server through the APN. Failure to exempt this traffic may result in upload to the wireless offload server over the LTE connection.

Proxy considerations

Agencies that require an internet proxy must implement configurations in Windows environment variables to facilitate Axon View XL’s communication with Axon Evidence.

1. Select **Start** and search for and select **Edit the system environment variables**.

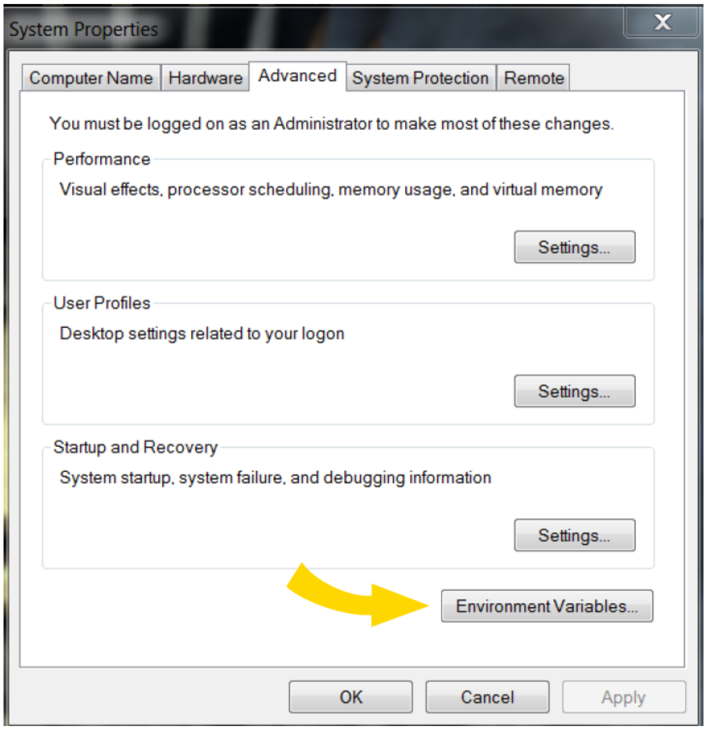


Control Panel (2)

Edit environment variables for your account

Edit the system environment variables

2. Select **Environment Variables**.



System Properties

You must be logged on as an Administrator to make most of these changes.

Performance

Visual effects, processor scheduling, memory usage, and virtual memory

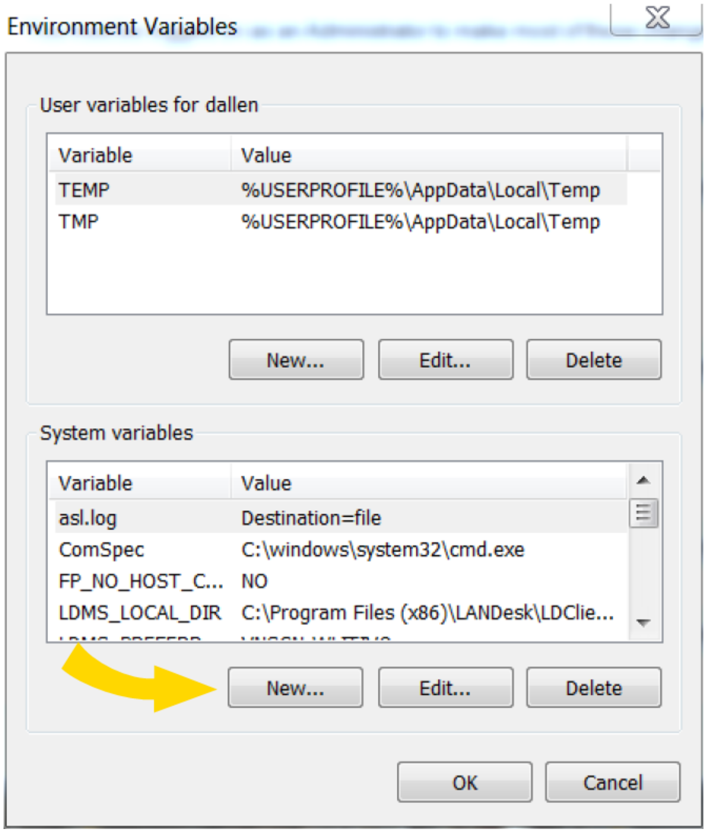
User Profiles

Desktop settings related to your logon

Startup and Recovery

System startup, system failure, and debugging information

3. Under **System variables**, select **New**.



Environment Variables

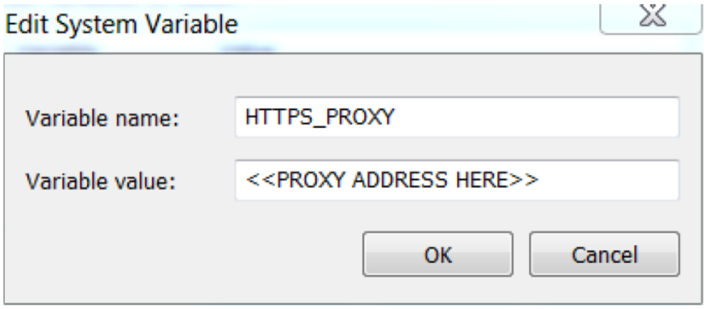
User variables for dallen

Variable	Value
TEMP	%USERPROFILE%\AppData\Local\Temp
TMP	%USERPROFILE%\AppData\Local\Temp

System variables

Variable	Value
asl.log	Destination=file
ComSpec	C:\windows\system32\cmd.exe
FP_NO_HOST_C...	NO
LDMS_LOCAL_DIR	C:\Program Files (x86)\LANDesk\LDClie...

4. Add the **Variable name** `HTTPS_PROXY` and **Variable value** (proxy address) to let Axon View XL use proxy, then select **OK**.

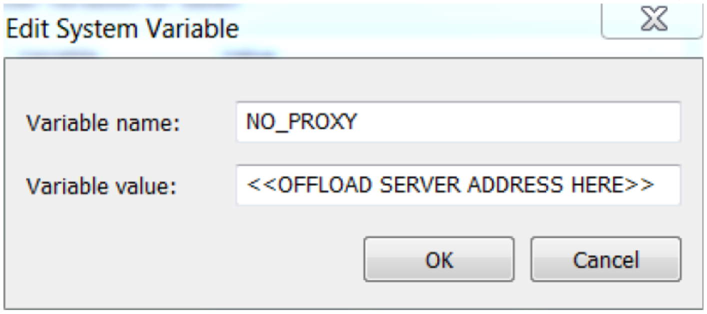


Edit System Variable

Variable name: HTTPS_PROXY

Variable value: <<PROXY ADDRESS HERE>>

5. If using a wireless offload server, add another new system variable for the server.



Edit System Variable

Variable name: NO_PROXY

Variable value: <<OFFLOAD SERVER ADDRESS HERE>>