XY SENSE

Sensor Network Profile

Version 3.4

Table of Contents

Table of Contents **1**
Version History **2**
XY Sense Device Network Profile **4**
Protocols, Ports and Endpoints 4
Area Sensor 5
Entry Sensor 6
Air Quality Sensors 6
Presence Sensors 7
Primary Hub (with Internal Router; Layer 3 Device) 8
Estimated Data Usage 9
Area Sensor 9
Entry Sensor 9
Network Topology Options **10**
Option 1 10
Option 2 11
Option 3 12
Option 4 13

Version History

v3.0 / November 2024 / S.Doolan, K.Chang

- Add Presence Sensor Network Requirements

v3.1 / May 2025 / B.Woods

- Add Milesight UG-56 Presence Gateway requirements
- Add Presence Gateway CUPS endpoint

v3.2 / Sep 2025 / B.Woods

- Add further Memfault endpoints (key additions device.memfault.com and memfault-tmp-production--use1-az4--x-s3.s3express-use1-az4.us-east-1.amazonaws.com)
- Documented port 443 as alternative for area sensor MQTT

v3.3 / Nov 2025 / B.Woods

- Add Memfault endpoints for the Milesight LoRaWAN gateway
- Separate endpoints for the MultiTech gateway vs. the Milesight gateway

v3.4 / Jan 2026 / B.Woods

- Add secondary Entry Sensor timeserver and note that DHCP Option 42 for specifying an NTP server is not supported by the Entry Sensor

XY Sense Device Network Profile

This section aims to provide a profile of the networking protocols, endpoints and bandwidth used by the XY Sense sensors and hubs.

Protocols, Ports and Endpoints

We highly recommend making internet access to our hardware as open as possible for convenience, as requirements will change in future. We endeavour to keep these changes to a minimum, but we rely on third-party vendors so some changes are beyond our control.

Below are detailed minimum requirements for each Layer 3 device in an XY Sense installation.

Area Sensor

Required in all scenarios where area sensors are installed, except Option 1 in the "Network Connectivity Options" of this document.

All connections are initiated by the sensor outbound to the XY Sense platform.

Application	Transport	Port	Endpoint	Purpose
MQTT	TCP	8883	a3iun0ocnfkxx9-ats.iot.ap-southeast-2.amazonaws.com	AWS IoT Endpoint for sensor connectivity
		443		Alternative to 8883
NTP	UDP	123	time1.google.com time2.google.com time3.google.com time4.google.com	Time server *Note: these default servers can be overridden by the customer via DHCP in topology Option 2 and Option 3*
HTTPS	TCP	443	core-api.app.xysense.io	Configuration
HTTPS	TCP	443	hosted.mender.io s3.amazonaws.com c271964d41749feb10da762816c952ee.r2.cloudflarestorage.com api.memfault.com ota-cdn.memfault.com device.memfault.com memfault-tmp-production--use1-az4--x-s3.s3express-use1-az4.us-east-1.amazonaws.com files.memfault.com ingress.memfault.com memfault-prod-east1.s3.amazonaws.com memfault-tmp-production-us-east-1.s3.amazonaws.com memfault-expires-never-production-us-east-1.s3.amazonaws.com	OTA update

DNS	UDP and TCP	53	Default DNS server provided by your network to DHCP clients.	

Entry Sensor

*Required in all scenarios where entry sensors are installed, except Option 1 in the "*Network Connectivity Options" of this document.

All connections are initiated by the sensor outbound to the XY Sense platform.

Application	Transport	Port	Endpoint	Purpose
NTP	UDP	123	time1.google.com pool.ntp.org	Time server *Note: as of FW 5.6.4 these default servers **cannot** be overridden via DHCP*
HTTPS	TCP	443	in.app.xysense.io	HTTPS data push to XY Sense Server
HTTPS	TCP	443	*.xovis.cloud *.xovis.com	Remote Management and OTA update services for Entry Sensors

Air Quality Sensor (Airthings)

*Required in all scenarios where air quality hubs are installed, except Option 1 in the "*Network Connectivity Options" of this document.

All connections are initiated by the sensor outbound to the Airthings platform.

Application	Transport	Port	Endpoint	Purpose
HTTPS	TCP	443	hub-api.airthin.gs	Remote Management Server
HTTP	TCP	443	hub-api.dev.airthin.gs	Development Remote Management Server
HTTPS	TCP	443	global-api.airthin.gs	HTTPS API access for the sensors

Presence Sensor

Required in all scenarios where Presence sensors hubs are installed, except Option 1 in the "Network Connectivity Options" of this document.

All connections are initiated by the sensor/gateways outbound to the XY Sense platform. There are two different LoRaWAN gateway options available which require different services.

Application	Transport	Port	Endpoint	Purpose
WWS	TCP	443	A3IUN0OCNFKXX9.lns.lorawan.ap-southeast-2.amazonaws.com	AWS IoT Core for LoRaWAN endpoint for sensor connectivity
TLS	TCP	443	A3IUN0OCNFKXX9.cups.lorawan.ap-southeast-2.amazonaws.com	AWS IoT Core for LoRaWAN endpoint for configuration and updates of LoRaWAN gateway
NTP	UDP	123	time1.google.com time2.google.com	Time server.
Milesight gateway option				
HTTPS	TCP	443	ec2-54-206-255-171.ap-southeast-2.compute.amazonaws.com	OTA updates and remote management service for Milesight Presence Sensor gateways.
HTTPS	TCP	443	api.memfault.com ota-cdn.memfault.com	OTA updates and remote management service for Milesight Presence Sensor gateways.
MultiTech gateway option				
HTTPS	TCP	5798	ds.devicehq.com	OTA updates and remote management service for MultiTech Presence Sensor gateways.
HTTPS	TCP	443	www.devicehq.com	OTA updates and remote management service for MultiTech Presence Sensor gateways.

Primary Hub (with Internal Router; Layer 3 Device)

Required only when using the Primary Hub (with Internal Router) on a corporate network - Option 4 in the "Network Connectivity Options" of this document.

In this situation, we highly recommend opening all ports and protocols on the specified endpoints, particularly for rms.teltonika.lt and 3.69.106.81

Application	**Transport**	**Port**	**Endpoint**	**Purpose**
DNS	UDP and TCP	53	Default DNS server provided by your network to DHCP clients.	The hub will use this for its own DNS resolution, and that of the sensors connected to it.
Ping	ICMP	N/A	1.1.1.1	Used for checking the health of the internet connection.
NTP	UDP	123	0.pool.ntp.org 0.openwrt.pool.ntp.org 1.pool.ntp.org 1.openwrt.pool.ntp.org	Time server
HTTP (over SSH)	TCP	20080	18.192.27.240	WebUI remote configuration access.
SSH	TCP	20022	18.192.27.240	Remote reverse SSH tunnel. Remote management.
	TCP	15010, 15011, 15009, 15039, 15040, 15041-15100	rms.teltonika.lt	Health analytics and remote management
OPENVPN	UDP	30000-39999	3.69.106.81 3.65.167.143	Remote management of the hub and install

Estimated Data Usage

Area Sensor

Purpose	Application	Frequency	Estimate Data Usage
XY Coordinate Messages	MQTT	Every 2 seconds	500KB to 1000KB **per hour** Depending on amount of sightings
XY Diagnostic Messages	MQTT	Every 30 minutes	1KB - 2KB **per hour**
XY Configuration Messages	MQTT	Every hour	1KB - 2KB **per hour**
Connectivity check	ICMP	Every 5 minutes	2KB **per hour**
Time server sync	NTP	Every minute	10KB **per hour**
Sensor configuration download	HTTPS	Once per day	10KB **per day**
OTA Update Poll	HTTPS	Every 30 minutes	20KB **per hour**
OTA Update Download	HTTPS	Once a month	30MB **per month**
Estimated Monthly Total			405MB to 760MB **per month**

Entry Sensor

Purpose	Application	Frequency	Estimate Data Usage
Connection to WebUI over remote connection	HTTPS	Adhoc / every login	1mb **per connection**
Line count event	HTTPS	Every event	~2kB **per event** ~400KB per 200 people
Remote connection heartbeat		Every hour	2KB **per hour**
Time server sync	NTP	Once every 5-10 min	10KB **per hour**
OTA Update Download	HTTPS	Once a month	30MB **per month**
Estimated Monthly Total[1] [1] Based on 200 people per day			250MB to 300MB **per month**

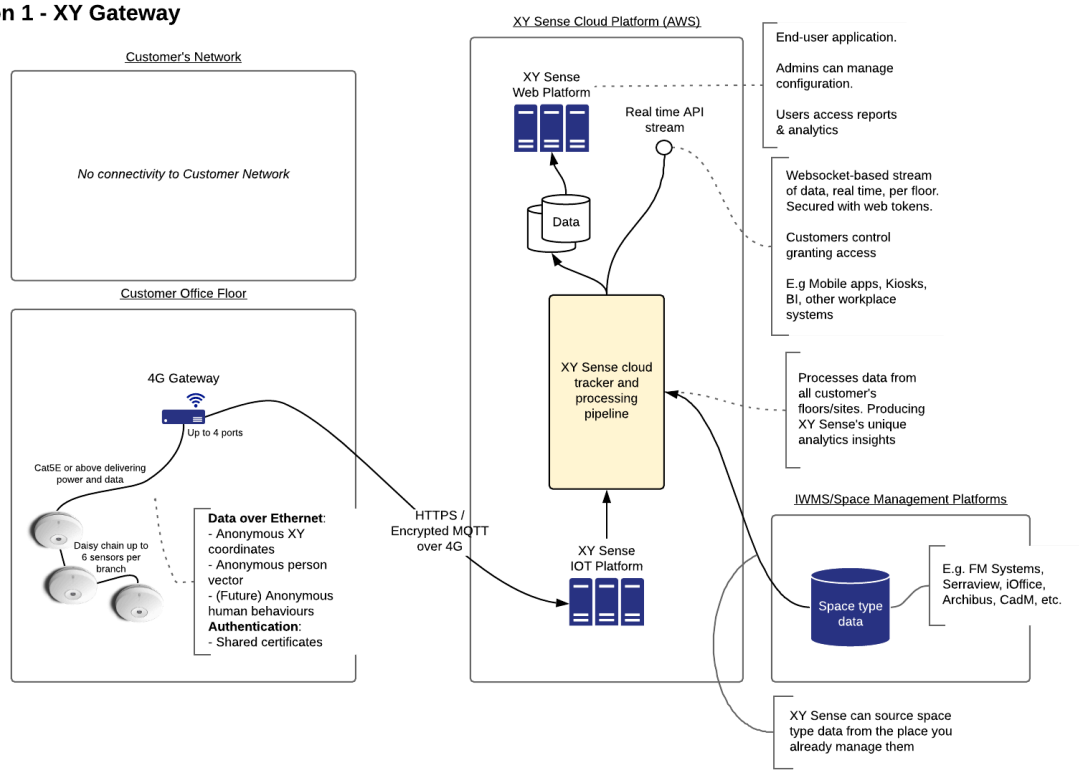
Network Topology Options

There are multiple supported ways to connect our sensors. The supported topologies are detailed in this section.

Option 1

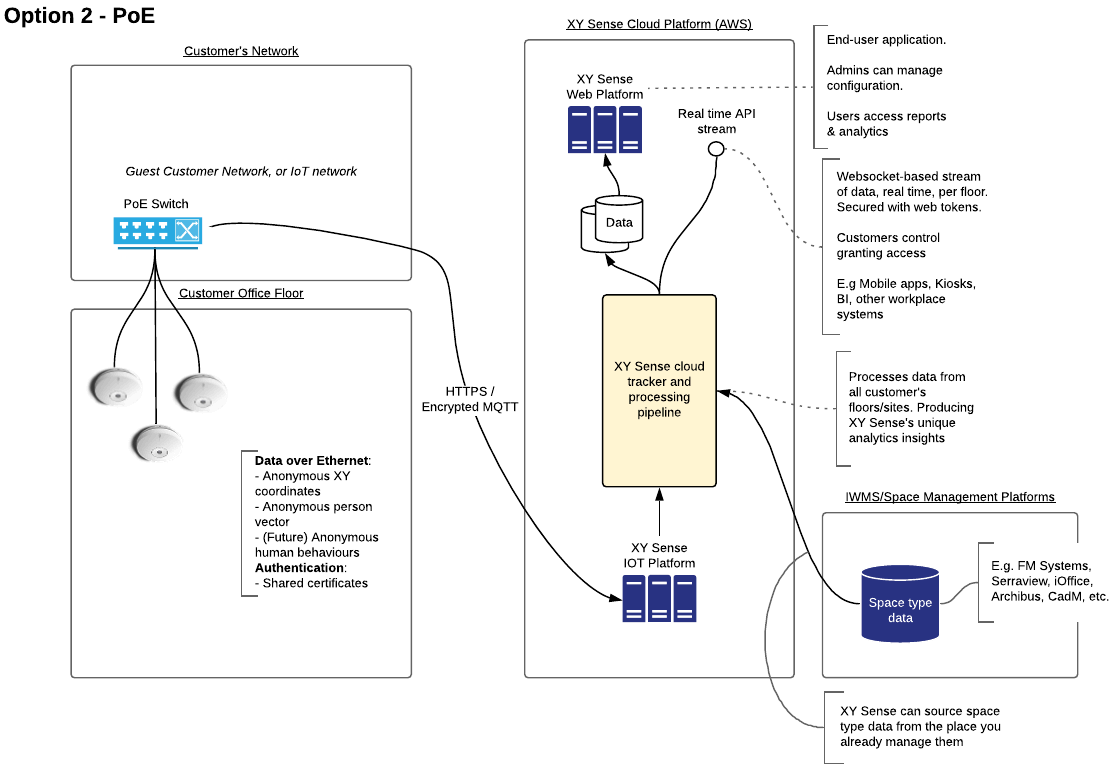
- Cellular provided by the XY Sense Hub
- Not part of the customer's network
- Fully managed by XY Sense

Option 1 - XY Gateway



Option 2

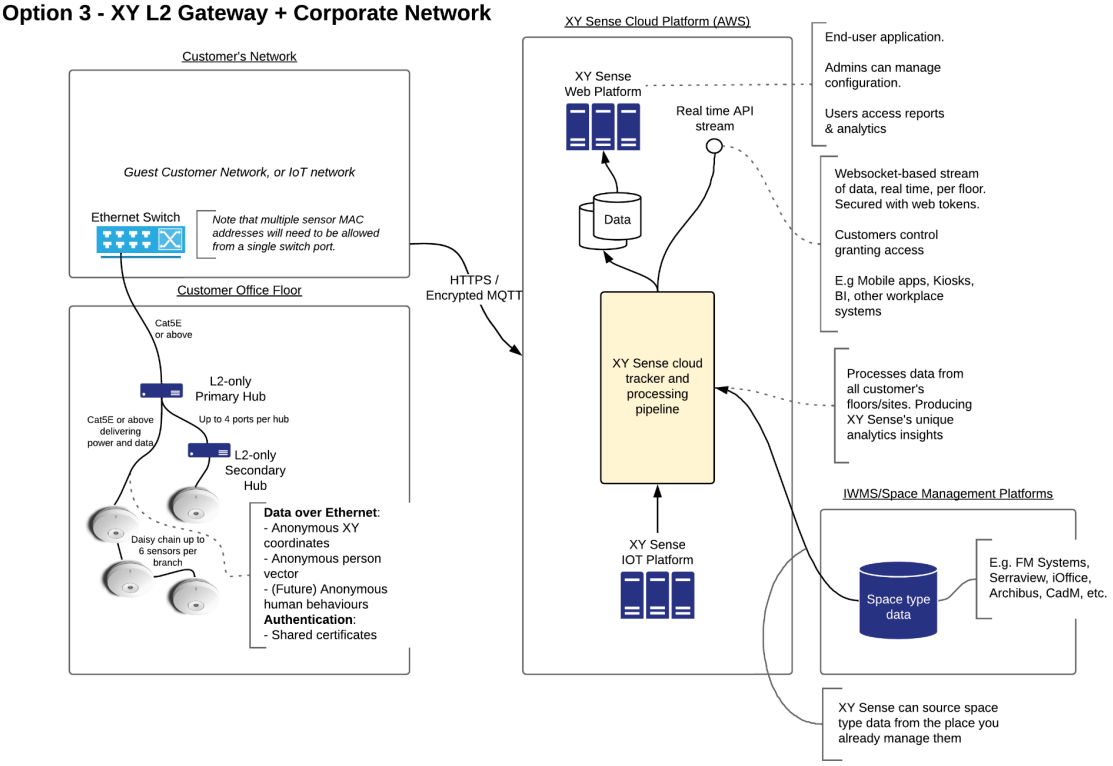
- PoE supplied by the customer's switch
- For area sensors, our PoE adapter (at additional cost) allows you to have a single sensor per PoE port.
- The customer's network will provide sensors with an IP (via DHCP) and provide the required connectivity
- MAC addresses for each sensor can be provided



Option 3

- Each XY Sense primary hub is plugged into a switch port on the customer's network.
- The primary hub does not contain an internal router so it is a Layer 2 device only
- The customer's network will provide sensors with an IP (via DHCP) and provide the required connectivity
- Each sensor will be visible on the customer's switch port
- MAC addresses for each sensor can be provided

Option 3 - XY L2 Gateway + Corporate Network



Option 4

- Each XY Sense gateway/primary hub (with an internal router) is plugged into a switch port on the customer's network.
- The primary hub is a Layer 3 device in this option.
- Only the primary hub's MAC will be visible to the customer's network and it will receive an IP via DHCP
- The hub needs to be allowed access to all its services and also access to the services required by the sensors connected to it

Option 4 - XY L3 Gateway + Corporate Network