Xovis Technical Documentation

PC-Series

Data Privacy and Security

Document History

Version	Date	Author	Comment
1.0	07.11.2017	T.Luethi	First version
1.1	26.02.2018	T.Luethi	Added stereovision
1.2	20.07.2018	D.Jokic	Updated for FW3.7

Copyright reminder

While Xovis AG believes the information included in this publication is correct as of the date of publication, it is subject to change without notice.

Non-disclosure reminder

All information in this document is strictly confidential and may only be published by Xovis AG, Switzerland.

Table of Contents

1 Xovis sensors and data protection

Data privacy and data security are global concerns. Most countries have laws in place to protect personal data from misuse and destruction. The details and impact are country-specific, vary greatly and must be assessed by each company individually.

The aim of regulations such as the General Data Protection Regulation in Europe is to reinforce data protection rights of individuals, facilitate the free flow of personal data in the digital single market and reduce the administrative burden of managing personal data.

Anything that can personally identify someone, be it their name, address, financial details, or posts across social media, is covered by the regulation. As a result, more data than ever before will fall under protection legislation.

While Xovis sensors provide data for person counting and tracking, specific technical functions are offered to provide data securely and in a de-personalized manner. It is the sole responsibility of the data processor using Xovis systems, to guarantee compliance with local regulation. The data processor needs to apply suitable technical and formal processes to data recording and treatment.

2 Providing Security/Privacy

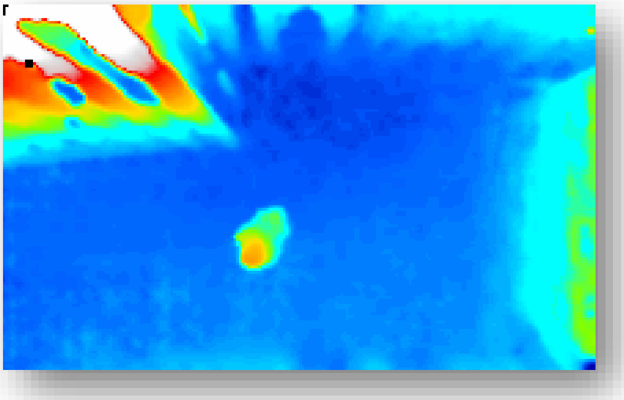
2.1 General settings

Xovis sensors are network-based devices. Many security features are provided to set up a sensor correctly for data privacy laws compliance and IT security. The person in charge of installation is obligated to follow all state-of-the-art cyber security implementations to place Xovis sensors in a protected and trusted network environment.

2.2 Image processing

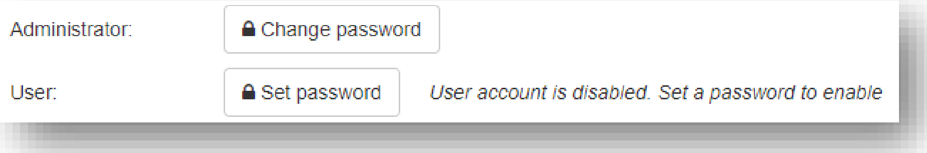
The functionality of Xovis 3D stereo vision sensors is based on two optical CMOS image sensors arranged at a small distance. A powerful, specialized processing engine makes full-image individual people tracking on the sensor possible.

The processed images to track individual people are not stored. Neither will these images leave the sensor at any time. The only data leaving the sensor is a fully anonymized object stream (constant stream of the coordinates of moving dots).



2.3 Password protection

Access to the sensor is password protected. Setting a strong individual password is the basic security measure for all sensors.

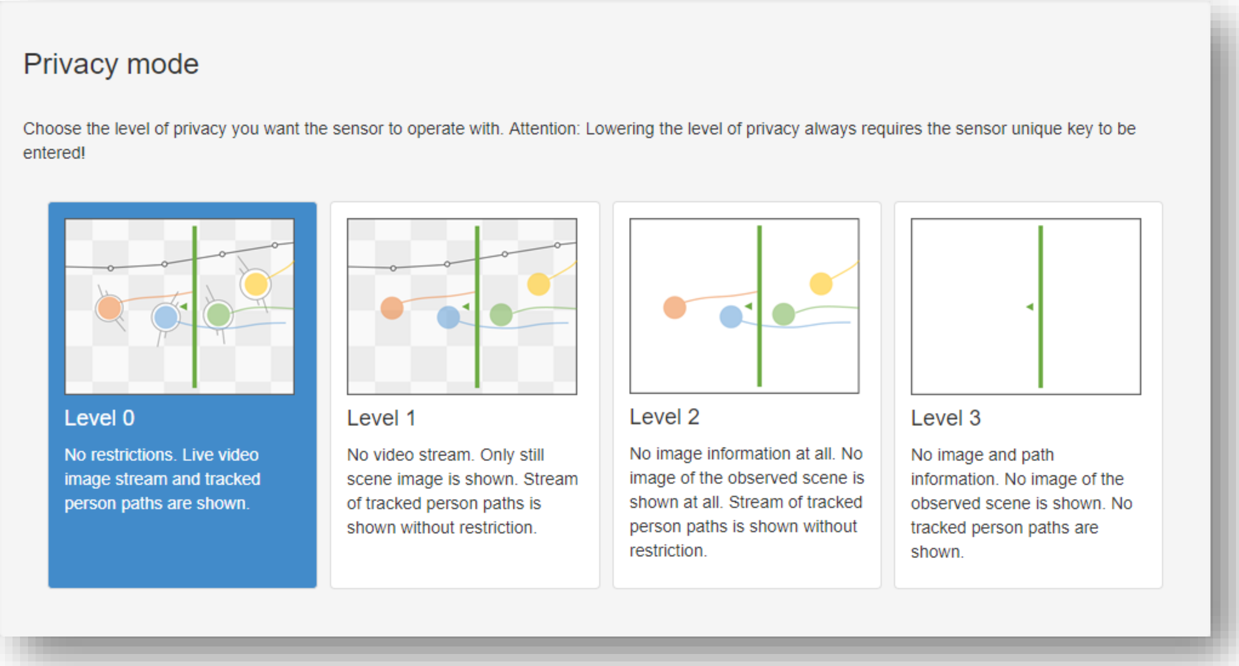


User account is disabled. Set a password to enable

2.4 Privacy level settings

Xovis sensors are optical person counting and tracking devices. Powerful data processing happens in the device itself. As it provides several types of data output streams, it is in the responsibility of the installer to select the appropriate privacy level when setting up a device. By raising the sensors privacy level setting the access to the image data can be switched off. Visual identification of humans by the user is no longer possible. Only anonymized data output can be processed after this change. The privacy mode level can be increased at any time.

Attention: The Sensor Master Key (SMK) is needed to lower the privacy level. The SMK is a unique key created for each sensor. It is only available from Xovis upon request.



Privacy mode

Choose the level of privacy you want the sensor to operate with. Attention: Lowering the level of privacy always requires the sensor unique key to be entered!

Level 0

No restrictions. Live video image stream and tracked person paths are shown.

Level 1

No video stream. Only still scene image is shown. Stream of tracked person paths is shown without restriction.

Level 2

No image information at all. No image of the observed scene is shown at all. Stream of tracked person paths is shown without restriction.

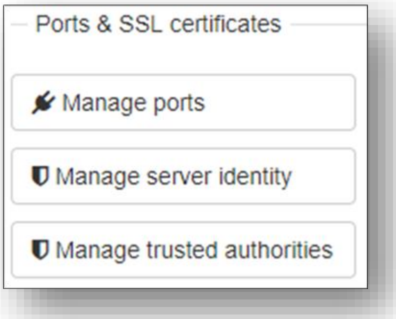
Level 3

No image and path information. No image of the observed scene is shown. No tracked person paths are shown.

Level	Description
0	- No restrictions - Live video image stream and tracked person paths are shown
1	- No video stream - Only still scene image is shown - Stream of tracked person paths is shown without restrictions
2	- No image at all - Stream of tracked person paths is shown without restrictions
3	- No image of the observed scene is shown - No tracked person paths are shown

2.5 Ports & SSL certificates

Xovis sensors provide the functionality to control all network ports such as HTTP(s) and streaming ports. The administrator can manage server identities (SSL key and certificate) and trusted authorities. It is in the responsibility of the installer to establish secure connections for data transfer. The "Ports and SSL certificates" settings provide useful tools for that matter.



Manage ports

Every port the sensor uses can be changed and most of the services can be disabled.

HTTP can be disabled permanently here. Any non-encrypted access to the sensor API and WebUI is prevented.

Manage server identity

Custom SSL keys and certificates can be uploaded and applied to the sensor. This overwrites the Xovis default key/certificate or any previous server identity.

Manage trusted authorities

Users can manage their own trusted authorities. Certificates can simply be uploaded and will automatically be applied. Any uploaded certificate can be removed at any time. The Xovis default certificate authority (CA) can be enabled and disabled.

2.6 WiFi/BLE monitoring

Dedicated Xovis sensors can monitor WiFi and Bluetooth signals from devices in the vicinity. An URL can be specified to identify a server which gathers the IDs of all detected wireless devices in a defined time interval. Each item contains the device ID (MAC), the signal strength in dB, and the corresponding device type (Bluetooth, Bluetooth low energy, or WiFi). In case of the detection of a Bluetooth device, its UUID is transmitted additionally.

The sensor settings provide the possibility to

- turn the monitoring feature on and off
- set up a whitelist
- set up a blacklist

With a whitelist in use, only listed devices get monitored by the sensor. Devices listed in a blacklist are not being monitored by the sensor.

The legal operation of such a device depends on specific country regulations.

Example: In Germany it is not allowed to place WiFi/Bluetooth monitoring systems in public areas. It is the user’s responsibility to assure legal compliance of all Xovis devices.