

WiFi Sensors

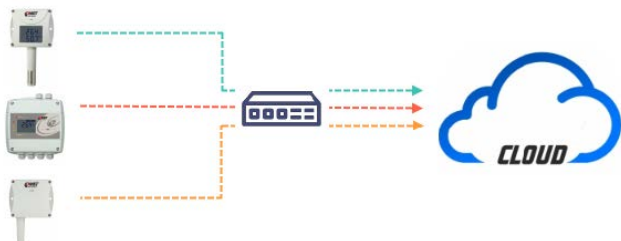


WiFi sensors send data into Cloud at selected interval via common 2.4 GHz WiFi infrastructure. WiFi sensors are equipped by own non-volatile memory for samples which cannot be sent in case of WiFi or ISP connectivity outage.

WiFi sensors supports state of the art WLAN security standards for WiFi connectivity. In addition to the usual standards like a WEP and WPA/WPA2 WiFi sensors supports latest standards WPA3 and WPA2 PMF (protected management frames). All data communication between WiFi sensors and Cloud is encrypted and transferred via HTTPS protocol. Each communication between WiFi sensor and Cloud is verified by mutual authentication.

Due to using well proven security standards, WiFi sensors provides high level of protection against potential attacker. Regardless protection of data content or protection against sending malicious data into Cloud.

Web Sensors (t-line, p-line, h-line)

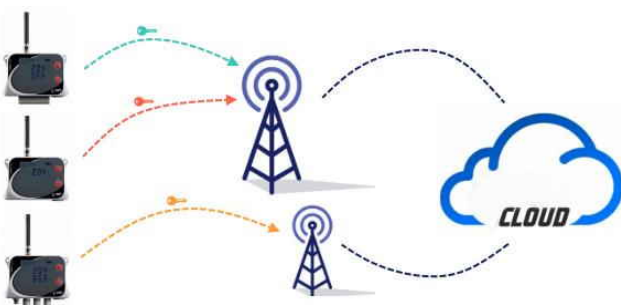


Web sensors send data into Cloud via Ethernet infrastructure. Measured values are sent via SOAP protocol transported by HTTP transfers.

Authenticity of data transmission is done via unique entry point for each Web Sensor. This entry point is generated at Cloud web interface and needs to be inserted to each Web Sensor separately. Authenticity of messages from Web sensors is secured when unique entry point is kept at secret.

Cloud is equipped by automatic incoming data integrity protection system. Data flow from device is suspended in case of unusual activity is detected like a shorter sending interval than is allowed.

IoT Wireless data loggers with built-in GSM modem



IoT Wireless data loggers with built-in GSM modem uses for data transfers HTTP

communication via GSM connection. IoT wireless data loggers are equipped by the own non-volatile memory where samples are stored in case of the GSM network outage. This memory can be used for optimising data transfers in conjunction with saving energy from internal battery.

Protection of data content is provided by GSM network. Incoming messages into Cloud are before processing check for their integrity.

Which data are stored in Cloud?

Apart measured values from devices are e-mail addresses stored at the Cloud. These addresses are used for purposes of sending alarms warnings from devices or service information. These emails are not used for marketing purpose by any kind. No other personal data are stored. Stored data differs according to device model:

IoT Sensors powered by Sigfox

- Measured values
- Device state and alarm states
- Device configuration
- Localisation data

Localisation of Sigfox devices is based on triangulation from BTS. Accuracy of localisation depends on counts of BTS in range and accuracy is not better than street or town district range. Purpose of localisation data is showing device positions at map. Position at map may to be rewritten by end-user if needed.

WiFi Sensors

- Measured values
- Device state and alarm states
- Local IP address

Local IP address of device is transferred from device. Purpose of this IP address is allowing to open device webpage from Cloud. No

other network infrastructure related information is transferred into Cloud from WiFi sensors. External IP addresses of data connections from successfully authenticated WiFi sensors are not logged.

Web Sensors (t-line, p-line, h-line)

- Measured values
- Device state and alarm states

No other data than stated above are provided by Web Sensors. External IP addresses of data connections from successfully authenticated messages are not logged.

IoT Wireless data loggers with built-in GSM modem

- Measured values
- Device state and alarm states

All collected data from IoT Wireless data loggers are stated above. External IP addresses of data connections from successfully authenticated messages are not logged. Localization data from GSM network are not collected.

Data communication between Cloud and web browser may to be logged from servicing purpose order to ensure the operation of the system. This communication is not used to monitoring behaviours of end-users.

Where are my data stored?

Cloud uses for data storage and processing infrastructure of Microsoft Azure Cloud services. Data centres located at EU countries are used for Cloud. Used data centres are certified according to ISO/IEC 27001:2013 standard.

Are my data safe?

Cloud is designed as high availability service. For operation of Cloud is used multiple server clusters including offsite back-up. Status of Cloud services is continually monitored by automated system and authorized employees of System s.r.o. Any deviation of the services availability is addressed immediately.

When newly arrived measured values are saved, older measured values are not overwritten. Measured values are stored together with timestamps and alarm states. This allows to show all values as time progression.

Cloud is provided as service paid by annual subscription. Newly purchased IoT Sensors powered by Sigfox are shipped with one year subscription. Other models are shipped with three months free subscription. Subscription for each device can be prolonged by purchasing credits. When subscription of device expire, incoming data from device are suspended. Data which are already stored are not deleted and access for data for end-user is preserved.

Privacy protection of data transfers between Cloud and internet browser is secured the HTTPs connection. Cloud uses trusted certificate issued by DigiCert Inc.

Who has access to my stored data?

Access to data have person which were approved by owner of device. Access to data have stuff which provides technical support for proper function of Cloud. System s.r.o. does not provide access to end-user's data to 3rd party.

Cloud devices and user accounts are sorted by tree structure. User can view devices at same and lower branches of organisation structure. Number of user accounts for each organisation is not limited.

Cloud have integrated extensive system of access rules. This allows to limit actions possible by each user. Levels of user rights:

- Administrator
- Device administrator
- Alarm administrator
- User
- Guest administrator (for demo purpose)
- Guest
- View by measured places

ORGANIZATION SELECT [X]

Search

- [-] Demo data
 - [] Company Building
 - [] Outdoor environment
 - [] Warehouse

Include Sub-Organizations

Select highest organization

What is a related data protection legislation?

End-user data are protected by the data protection law of Czech Republic. This data protection law is harmonised with EU law.

Which certificates are there?

Data centres are certified according to ISO/IEC 27001:2013 standard.

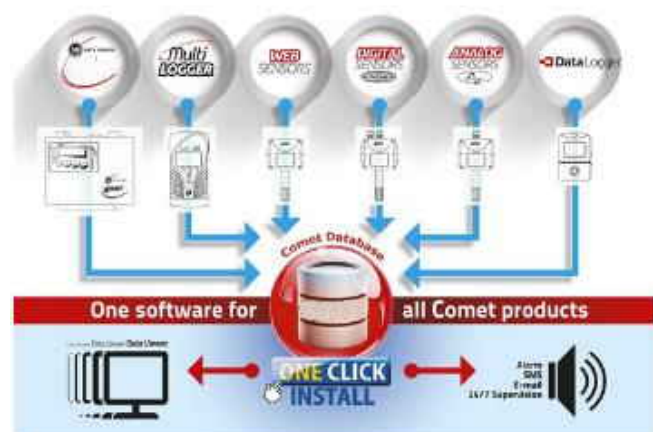
Internal processes are certified according to quality management system ISO 9001:2015.

How safely use devices at own network infrastructure?

WiFi sensors and Web Sensors uses end-users network infrastructure for data transfers into Cloud. For securing data transfers from devices into are following measures recommended.

It is recommended to enable device security at final deployment to protect devices from unauthorised access. Please follow IT security advices from instruction manual for WiFi sensors.

I cannot use 3rd party Cloud services. What option I have?



For customers which cannot use 3rd party Cloud service from the security reasons or users which want to execute data acquisition system at own server infrastructure is here Database solution. Database is a solution using Microsoft SQL database server as data storage and Viewer software installed at client stations.

Database solution allow to capture data from multiple types of devices, including Web Sensors, WiFi sensors and IoT Wireless data loggers.