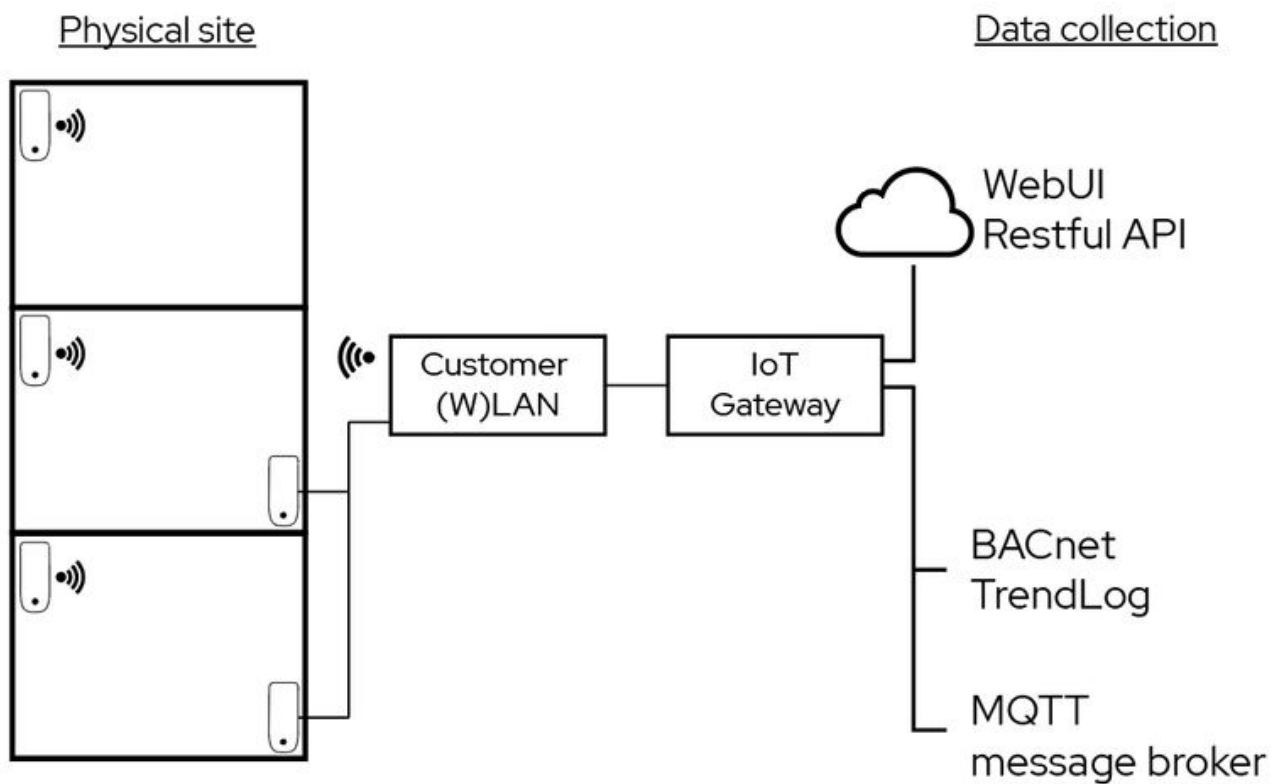


Ubiquisense

System Overview



Network Guide

Network Guide

Network requirements, WiFi and Ethernet

The smart sensors connect to the local network using Wi-Fi or Ethernet (Ethernet only supported by UC2).

This is shown as Customer (W)LAN above.

If using Wi-Fi the network must comply to the following requirements:

- Security: WPA2-Personal or WPA2-Enterprise (using 802.1x authentication)
- Modes (UC1): 802.11b/g, (only 2.4GHz)
- Modes (UC2): 802.11ac/a/b/g/n (2.4 and 5GHz)
- Group cipher: CCMP
- Pairwise ciphers: CCMP
- Supported 2.4GHz channels: 1-11
- Supported 5GHz channels: 36, 40, 44, 48 (UNII-1 band) 52, 56, 60, 64 (UNII-2 band) 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144 (UNII-2 extended)

Note that this means that:

- Legacy modes like WEP and WPA1 are not supported
- TKIP ciphers have known vulnerabilities and are not supported

It is recommended to use a dedicated device Wi-Fi network or device SSID.

IoT gateway variants and network topology

The IoT gateway can be installed in 3 different variants.

- Cloud gateway (recommended): runs on public cloud provider infrastructure, managed by Ubiqisense

In special cases an on premise gateway may be preferred. Two types are supported:

- Gateway HW appliance: on premises mini PC
- Virtual gateway: virtual machine running on customer virtual infrastructure

Contact Ubiqisense for further information.

If gateway is on-premise it is recommended to host the sensors and the gateway on the same network.

In case there is a firewall or NAT device between sensors and the gateway, forwarding rules need to be configured on the firewall or NAT device corresponding to the network requirements listed below.

Firewall port test

In order for the system to work it is required to have connectivity between

- Sensors and IoT gateway
- IoT gateway and data collector. Data collector can be cloud application, BACnet BMS or MQTT message broker
- Sensors / Gateway and remote monitoring / SW download

This can be tested using a Windows client connected to the network used for the sensors.

Run the following from PowerShell and take note of the output:

Test-NetConnection -ComputerName portcheck.ubiqisense.com -Port 8883

Test-NetConnection -ComputerName portcheck.ubiqisense.com -Port 8247

Test-NetConnection -ComputerName portcheck.ubiqisense.com -Port 5555

Test-NetConnection -ComputerName portcheck.ubiqisense.com -Port 35443

Specific network requirements and firewall settings

The following network configuration must be implemented prior to provisioning the first sensor

Network requirements - Using Cloud Gateway (standard option)

If the cloud gateway is used the requirements can be simplified as follows. In other cases refer to the table beneath.

Source	Dest. port
Sensor	TCP 8247
Sensor	TCP 35443
Sensor	TCP 5555
Sensor	UDP 123
Sensor	UDP 1194
Sensor	TCP 443
Sensor	TCP 8883

For specific information regarding FQDN addresses and the type of traffic over each port contact Ubiqisense at support@ubiqisense.com

*Sensor TCP 8883: iot.eu-central-1.amazonaws.com Cloud application / MQTT message broker.

Network requirements - Not using Cloud Gateway (VM or Physical Gateway)

Source	Dest. port
Sensor	TCP 8247
Sensor	TCP 35443
Sensor	TCP 5555
Sensor	UDP 123
Sensor	UDP 1194
Sensor	TCP 443
Gateway	TCP 1883
Gateway	TCP 8883
Gateway	TCP 47808

For specific information regarding FQDN addresses and the type of traffic over each port contact Ubiqisense at support@ubiqisense.com

BACnet requirements

If BACnet is used as data collector the IoT gateway will act as a BACnet device providing a BACnet/IP interface.

The following information is required in order to configure the IoT gateway:

- Gateway device id
- Gateway IP address for the BACnet/IP interface

If a BBMD is used in the BACnet/IP network the following information is required

- BBMD IP address and port

Note that the IoT gateway HW appliance is responsible for sending data to the data collector and is shipped with a single power supply. In case the data protection plan does not allow data loss during a single power source failure it is recommended to use an external UPS.

Time Synchronization (NTP):

To ensure sensors and on-premise gateways maintain accurate date and time, synchronization is performed using the following NTP servers:

- time.google.com
- time.cloudflare.com
- nts.netnod.se
- ptbtime1.ptb.de
- ptbtime2.ptb.de
- ntp.pool1.time.nl
- time.txryan.com

Please adjust firewall rules to permit traffic to these endpoints.

Network activity from sensor:

The sensor monitors the network state by doing a simple ping check to the following endpoint:

- 8.8.8.8 (IP of the public dns.google.com)
- 10.25.0.1 (VPN tunnel)

The sensor also tries to resolve the following dns:

- usgXXX.gateways.ubiquisense.com (DNS of gateway)