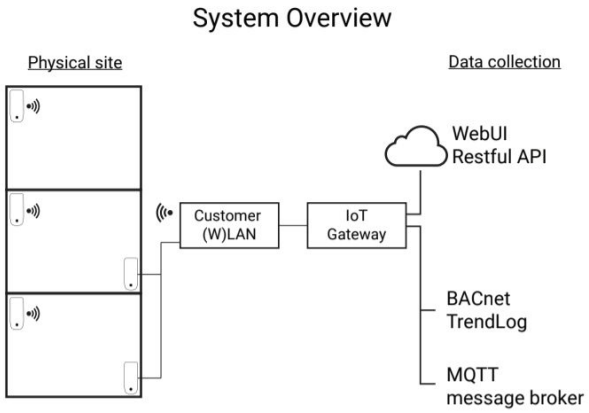
Ubiqisense

Smart Sensor Solution - 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
- 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
- SSID not hidden. Contact support if required

Note that this means that:
- Legacy modes like WEP and WPA1 are not supported
- TKIP ciphers have known vulnerabilities and are not supported
- WPA enterprise (e.g. using 802.1x authentication) is not supported (under development)

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 prefered. 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.

Ubiqisense

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 22
```

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	Dest. FQDN	Comment
Sensor	TCP 8247	ccd43efa0eeba12b.ubiqisense.com	Certificate server
Sensor	TCP 22	*.gateways.ubiqisense.com	SW management
Sensor	TCP 5555	*.gateways.ubiqisense.com	SSL web socket toward gateway
Sensor	UDP 123	*.gateways.ubiqisense.com, time.google.com	NTP
Sensor	UDP 1194	vpn.ubiqisense.com	Remote monitoring
Sensor	TCP 443	callback-apigw.ubiqisense.com	Provisioning logging
Sensor	TCP 443	s3.eu-central-1.amazonaws.com	SW management

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

Source	Dest. port	Dest. FQDN	Comment
Sensor	TCP 8247	ccd43efa0eeba12b.ubiqisense.com	Certificate server
Sensor	TCP 22	<local gateway location>	SW management
Sensor	TCP 5555	<local gateway location>	SSL web socket toward gateway
Sensor	UDP 123	<local gateway location>, time.google.com	NTP
Sensor	UDP 1194	vpn.ubiqisense.com	Remote monitoring
Sensor	TCP 443	callback-apigw.ubiqisense.com	Provisioning logging
Sensor	TCP 443	s3.eu-central-1.amazonaws.com	SW management
Gateway	TCP 1883	<local mqtt broker>	MQTT message broker (if using)
Gateway	TCP 8883	*.iot.eu-central-1.amazonaws.com	Cloud application / MQTT message broker
Gateway	TCP 47808	<local BACnet BMS>	BACnet BMS (if using)

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.