FREQUENTLY ASKED QUESTIONS
FOR WIRELESS SOLUTIONS

Use these links to view FAQs by topic:

Wireless Sensors

Wireless Sensor Batteries

Wireless Gateways

Wireless Sensor + Wireless Gateway Functionality

ACCESS360 Network Requirements

ACCESS2000 Network Requirements

Wireless Sensor FAQs

Q **What happens if I accidentally delete a ConnectSens™ Wireless Sensor from the ConnectView™ Web App?**

A If you delete a sensor from the web app, it will reappear automatically as long as the sensor is discovered by a nearby gateway.

Q **How many times can I reprogram a ConnectSens™ Wireless Sensor?**

A **WS200 and WS300 Sensors:** Unlimited reprogramming is allowed through the ConnectView™ Web App.

WS100 Sensors: Factory-configurable only (not re-programmable by user). All factory configurations are final and WS100 sensors are unable to be returned to CTC for reprogramming.

Q **Will a ConnectSens™ Wireless Sensor lose its settings if power is cycled or the battery is replaced?**

A No, the sensor will retain all of its settings, even after a power cycle or battery replacement.

Q **If I take a reading on demand, will it change the preset reading interval?**

A An on-demand reading does not change the programmed automatic reading period, but it will reset the interval timer.
E.g. 1 hour reading interval:
- » First automatic reading occurs at 1:00 (next reading due at 2:00)
- » On demand reading taken at 1:30
- » Next automatic reading due 1 hour later at 2:30 (no automatic reading at 2:00 anymore)

Q **Can I directly integrate ConnectSens™ Wireless Sensors with Bluetooth devices such as phones, tablets, or third-party hardware?**

A No, CTC does not support direct Bluetooth communication between CTC ConnectSens™ Wireless Sensors and Bluetooth devices such as phones, tablets, or third-party hardware without a CTC Gateway. CTC will not provide documentation, support materials, or remote technical support for direct Bluetooth integrations.

Q **Can I configure temperature and vibration readings independently?**

A **WS100 Series**: Temperature and vibration readings are concurrent

WS200 and WS300 Series: Temperature readings occur every time a vibration reading occurs. At the sensor level, temperature readings cannot be automatically triggered on a set timer independent from the vibration reading timer.

Q **Are there any areas or environments where I should NOT install ConnectSens™ Wireless Sensors?**

A DO NOT install CTC wireless sensors under metal guards, behind machine safety cages, or in locations shielded by metal structures.

Metal obstructions can significantly attenuate RF signals, leading to reduced range, intermittent communication, or data loss. Wireless sensors should be installed with a clear RF path to the gateway or access point.

Q **When does the ConnectSens™ Wireless Sensor's time interval start?**

A The time interval begins as soon as a sensor is plugged in. If you take a manual reading, the next automatic reading will be rescheduled based on when that manual reading was taken.

Q **Why is the frequency response of the Z-axis different from the X and Y axes on triaxial ConnectSens™ Wireless Sensor models?**

A The difference in frequency response is inherent to the MEMS device used in the sensor.

Wireless Sensor - Battery FAQs

Q **What should I do if I replace a sensor battery, but the battery level doesn't show as full?**

A If the battery level indicator doesn't show a full charge after replacing the battery, follow the instructions in the user manual to reset the battery level. This process ensures the sensor accurately reflects the new battery's status.

Q **What type of battery does a ConnectSens™ Wireless Sensor use and how does it function?**

A CTC ConnectSens™ Wireless Sensors use lithium *primary* (non-rechargeable) batteries, which behave differently from lithium ion batteries. These cells maintain a very stable voltage throughout most of their life, followed by a rapid drop-off near end-of-life. Because of this flat discharge curve, voltage is not a reliable indicator of remaining battery life, especially since voltage also varies with temperature.

Q **How is the battery life of a ConnectSens™ Wireless Sensor calculated?**

A Battery life is tracked in firmware using a conservative coulomb counting model. The sensor:

- Accounts for energy consumed during all operating events (idle time, advertising, connections, transmissions, measurements, etc.)
- Maintains a running total of charge used vs. nominal battery capacity.
- Uses conservative assumptions to avoid overestimating remaining life.

This approach provides more reliable battery life estimation than voltage-based methods for this battery chemistry.

Q **What are key considerations and limitations of the battery used in a ConnectSens™ Wireless Sensor?**

A There are several factors that can affect real-world battery performance:

- **Temperature:** Extreme temperatures can reduce usable battery capacity and increase current consumption. For this reason, we recommend earlier battery replacement when operating in harsh environments.
- **Battery Age:** Cells degrade over time regardless of use. We recommend replacing batteries based on age as ell as reported remaining life, particularly older inventory.
- **Wireless Conditions:** In poor signal environments, additional BLE transmissions (which occur below the application layer) can increase power consumption.
- **Outdated Firmware:** Please ensure your wireless sensors are updated to optimize power draw.

Please note, the factors listed above are not possible to account for in battery life calculations, thus can lead to a battery dying earlier than reported by the estimated percentage left.

Wireless Gateways - General FAQs

Q **What happens if my Connect Wireless Gateway gets damaged?**

A If your gateway gets damaged, it may stop receiving sensor data. However, all sensors will retain their configurations, including settings, serial numbers, and reading intervals.

Q **How many readings can a Connect Wireless Gateway store if it is not connected to a network?**

A ConnectBridge™ ACCESS360 Gateways come preinstalled with a 32 GB SD card (removable and expandable) which can store thousands of readings when not connected to a network.

ACCESS2000 Long-Range Wireless Gateways come with 64 GB of preinstalled storage which can store thousands of readings when not connected to a network.

Please note, you cannot interact with the gateway while it is not on a network.

Q **Are there any areas or environments where I should NOT mount Connect Wireless Gateways?**

A DO NOT mount gateways inside of a metal enclosure.

Metal enclosures will significantly attenuate RF signals and can severely degrade wireless performance, range, and reliability.

Mounting gateways inside a *non-metallic* enclosure is also not recommended.

The impact on signal strength and overall system performance is unknown and may vary based on enclosure material, thickness, size, and internal layout. Performance degradation is especially likely if additional electronics or hardware are installed inside the enclosure alongside the gateway.

For optimal performance, the gateway should be mounted in an open environment with a clear RF path to the sensors.

Q **Is there a limit to the number of secondary Connect Wireless Gateways that can communicate with the primary gateway?**

A No, there is no limit.

Wireless Sensor + Wireless Gateway Functionality FAQs

Q **How easy is it to replace ConnectSens™ Wireless Sensors and Connect Wireless Gateways in the system?**

A

Replacing a sensor:
Once a new sensor is powered on and within range of an existing gateway, it will automatically establish a connection. Using the ConnectView™ Web App, you can easily locate the new sensor, assign it to the appropriate group or system, and configure its settings (such as reading intervals or thresholds).

Replacing a gateway:
For gateways, once the new unit is physically connected to your network, follow the step-by-step instructions in the manual to configure it. Once added, the gateway will automatically begin communicating with any discoverable sensors in its range, ensuring seamless integration into your existing setup.

For ACCESS360 - If you still have your previous gateway, you can swap the SD cards to transfer the readings and sensor data to the new gateway.

For ACCESS2000 - If you still have your previous gateway, you can swap the USB isolator and USB drive to transfer the readings and sensor data to the new gateway.

Q **How many ConnectSens™ Wireless Sensors can be connected to a Connect Wireless Gateway?**

A

ACCESS360: 10 sensor inputs* - mix and match WS100, WS200, and WS300 wireless sensors.

*Each ACCESS360 is capable of discovering more than 10 dynamic sensors; however, each gateway is only capable of maintaining 10 active BLE connections at one time. Sensors beyond this will be in advertising mode until there is time to service them. CTC recommends 1 gateway per 10 dynamic sensors for maximum validated and supported system performance.

ACCESS2000: 30 sensor inputs* - mix and match WS100, WS200, and WS300 wireless sensors.

*Each ACCESS2000 is capable of discovering more than 30 dynamic sensors; however, each gateway is only capable of maintaining 30 active BLE connections at one time. Sensors beyond this will be in advertising mode until there is time to service them. CTC recommends 1 gateway per 30 dynamic sensors for maximum validated and supported system performance.

What happens if I connect more than 10 ConnectSens™ Wireless Sensors to a single ACCESS360 ConnectBridge™ Wireless Gateway?

The ACCESS360 is only capable of maintaining 10 active BLE connections at one time. Sensors beyond this will be in advertising mode until there is time to service them. We recommend 1 gateway per 10 dynamic sensors for maximum validated and supported system performance.

What happens if I connect more than 30 ConnectSens™ Wireless Sensors to a single ACCESS2000 Wireless Gateway?

The ACCESS2000 is only capable of maintaining 30 active BLE connections at one time. Sensors beyond this will be in advertising mode until there is time to service them. We recommend 1 gateway per 30 dynamic sensors for maximum validated and supported system performance.

How do multiple Connect Wireless Gateways handle ConnectSens™ Wireless Sensor connections in the same area?

When multiple gateways are deployed in the same area, they automatically distribute the sensor connections to optimize performance and minimize latency.

Example:
if you have ***40 sensors*** and ***2 gateways***, the systems will balance the load between them. Instead of one gateway attempting to manage all 40 sensors - leading to increased latency - ***Gateway 1 may connect to 20 sensors***, while ***Gateway 2 connects to the remaining 20 sensors***. This ensures efficient data collection and prevents communication delays. For larger deployments, adding more gateways helps maintain optimal performance.

Why am I only seeing temperature data and limited sensor data when using an MQTT server?

If you are seeing temperature data, but only seeing limited sensor data when publishing to an MQTT server, it is likely t hat your MQTT broker is not configured to accept a sufficiently large packet or payload size.

CTC devices publish sensor data in message packets that may be larger than the broker's default maximum size. When this limit is too low, smaller messages (such as temperature data) may be received successfully, while larger sensor data packets are rejected.

This configuration setting is on the customer's MQTT broker, not on the CTC device. To resolve the issue, increase the broker's maximum packet or message size to allow full sensor data transmission.

I got the error message "Reading Failed - Reading decoding failed" - what does that mean?

That means the ConnectBridge™ Gateway is unable to process the data being sent by the sensor. It is recommended to reconfigure the sensor and try again.

What happens if two Connect Wireless Gateways are within range of one ConnectSens™ Wireless Sensor?

The sensor will connect to the gateway with the stronger connection. If the connection is lost for any reason, the sensor will start advertising again and connect another gateway if one is within range.

ACCESS360 Wireless Gateway - Network Requirements FAQs

PLEASE NOTE:
When installing CTC Connect Systems in an industrial network,
it is important to have the plant network administrative team involved.

Q **What types of deployment does the ACCESS360 ConnectBridge™ Wireless Gateway support, and what are their requirements?**

A ACCESS360 wireless gateway supports deployment using **either a wired PoE Ethernet connection or Wi-Fi**, depending on the installation environment.

CTC recommends a hardwired Ethernet connection to the gateway whenever possible. A wired connection offers the greatest stability and the lowest risk of RF interference. In some facilities, however, network restrictions may prevent a wired connection.

Wi-Fi connectivity to the gateway is best utilized in places where the network has security policies in place that will impact the functionality of the gateway, such as VPN, NTP, or other network protocols required to connect to or manage the gateway.

Ethernet (PoE) Requirements:
- **Power**: IEEE 802.3af or 8.2.3at PoE
- **Network Interface**: 10/100/1000 Mbps Ethernet
- **Backhaul**: Wired Ethernet connection to the customer's LAN

General Requirements:
- **IP Addressing**: DHCP or static IP (costumer-managed)
- **Internet Access**: Required for CTC Connect communication, data upload, and firmware updates

ACCESS360 should be installed on a **stable**, **business-class network** with sufficient uptime, bandwidth, and administrative controls.

Q **Are there specific firewall and security requirements for the ACCESS360 ConnectBridge™ Wireless Gateway?**

A Yes, there are specific firewall and security requirements for allowing required outbound traffic. The customer is responsible for allowing:

Ethernet (PoE) Requirements:
- **Outbound HTTPS (TCP 443)** to CTC Connect services
- **Outbound NTP (UDP 123)** to connect to Global NTP servers
- **DNS resolution enabled**

Q **Are there unsupported or customer-managed configurations for the ACCESS360 ConnectBridge™ Wireless Gateway?**

A Yes, there unsupported or customer-managed configurations for the ACCESS360 wireless gateway.

The following configurations **may be technically possible**, **but are not supported under CTC Connect support**. CTC does NOT provide configuration guidance, documentation, or troubleshooting for these scenarios:

- Cellular routers, cellular modems, LTE/5 gateways, or hotspots used as network backhaul
- Wi-Fi networks with captive portals, user-based authentication, splash pages, or rotating credentials
- VPN tunnels, private APNs, or secure overlay networks
- Customer-managed firewall rules, deep packet inspection, proxying, or traffic shaping
- MQTT broker hosting, configuration, or message routing infrastructure
- Network policies that block, throttle, proxy, or intermittently disrupt required outbound traffic

Any connectivity, latency, reliability, or data loss issues caused by these configurations are outside the scope of CTC Connect support.

Q **Are there requirements for the remote management of ACCESS360 ConnectBridge™ Wireless Gateways?**

A Yes, there requirements for the remote management of ACCESS360 wireless gateways.

- Internet connection to include the industrial network of the facility where the equipment is installed or cellular (such as Teltonika RUTM20) or satellite (such as Starlink).

- Software VPN connection to securely connect to the local network where the gateway is installed. VPN connection will require the use of a static IP address for the cellular connection to the gateway or use of DYNDNS (Dynamic DNS). Please note, the use of a static IP address is preferred for stability.

PLEASE NOTE: Industrial networks are often secured by a corporate firewall which will cause challenges in being able to VPN to the gateway and/or there may be port blocking rules put in place which will limit TCP/UDP connections to the gateway or internet.

ACCESS2000 Wireless Gateway - Network Requirements FAQs

PLEASE NOTE:
When installing CTC Connect Systems in an industrial network,
it is important to have the plant network administrative team involved.

Q **What types of deployment does the ACCESS2000 ConnectBridge™ Wireless Gateway support, and what are their requirements?**

A ACCESS2000 wireless gateway supports deployment using **either a wired PoE Ethernet connection or Wi-Fi**, depending on the installation environment.

CTC recommends a hardwired Ethernet connection to the gateway whenever possible. A wired connection offers the greatest stability and the lowest risk of RF interference. In some facilities, however, network restrictions may prevent a wired connection.

Wi-Fi connectivity to the gateway is best utilized in places where the network has security policies in place that will impact the functionality of the gateway, such as VPN, NTP, or other network protocols required to connect to or manage the gateway.

Ethernet (PoE) Requirements:
- **Power**: IEEE 802.3af or 802.3at PoE
- **Network Interface**: 10/100/1000 Mbps Ethernet
- **Backhaul**: Wired Ethernet connection to the customer's LAN

Wi-Fi Requirements:
- **Wi-Fi**: Customer-provided wireless network (2.4 GHz / 5 GHz, as supported by device firmware)
- **Security**: WPA2/WPA3 (per device configuration options)Required for CTC Connect communication, data upload, and firmware updates
- **Signal Quality**: Installation location must ensure stable signal strength and low interference

General Requirements:
- **IP Addressing**: DHCP or static IP (costumer-managed)
- **Internet Access**: Required for CTC Connect communication, data upload, and firmware updates

ACCESS2000 should be installed on a **stable**, **business-class network** with sufficient uptime, bandwidth, and administrative controls.

Q **Are there specific firewall and security requirements for the ACCESS2000 ConnectBridge™ Wireless Gateway?**

A Yes, there are specific firewall and security requirements for allowing required outbound traffic. The customer is responsible for allowing:

- **Outbound HTTPS (TCP 443)** to CTC Connect services
- **Outbound NTP (UDP 123)** to connect to Global NTP servers
- **DNS resolution enabled**

Q **Are there unsupported or customer-managed configurations for the ACCESS2000 ConnectBridge™ Wireless Gateway?**

A Yes, there unsupported or customer-managed configurations for the ACCESS2000 wireless gateway.

The following configurations **may be technically possible**, **but are not supported under CTC Connect support**. CTC does NOT provide configuration guidance, documentation, or troubleshooting for these scenarios:

- Cellular routers, cellular modems, LTE/5 gateways, or hotspots used as network backhaul
- Wi-Fi networks with captive portals, user-based authentication, splash pages, or rotating credentials
- VPN tunnels, private APNs, or secure overlay networks
- Customer-managed firewall rules, deep packet inspection, proxying, or traffic shaping
- MQTT broker hosting, configuration, or message routing infrastructure
- Network policies that block, throttle, proxy, or intermittently disrupt required outbound traffic

Any connectivity, latency, reliability, or data loss issues caused by these configurations are outside the scope of CTC Connect support.

Q **Are there requirements for the remote management of ACCESS2000 ConnectBridge™ Wireless Gateways?**

A Yes, there requirements for the remote management of ACCESS2000wireless gateways.

- Internet connection to include the industrial network of the facility where the equipment is installed or cellular (such as Teltonika RUTM20) or satellite (such as Starlink).

- Software VPN connection to securely connect to the local network where the gateway is installed. VPN connection will require the use of a static IP address for the cellular connection to the gateway or use of DYNDNS (Dynamic DNS). Please note, the use of a static IP address is preferred for stability.

PLEASE NOTE: Industrial networks are often secured by a corporate firewall which will cause challenges in being able to VPN to the gateway and/or there may be port blocking rules put in place which will limit TCP/UDP connections to the gateway or internet.

Need Additional Technical Support?

Need additional technical support for issues or questions about the Connect Wireless ecosystem?

Scan the QR code or use the hyperlink to access our convenient web form to submit your request online at any time.

CTC's experienced support team will review your inquiry and work quickly to resolve your issues.

scan QR code or

CLICK HERE FOR SUPPORT REQUEST FORM