ACCESS360
ConnectBridge™ Gateway
Operational Guide

Table of Contents

Introduction

The ACCESS360 functions as a network controller and **Bluetooth®** gateway that facilitates bi-directional data transfer with CTC Connect Wireless Sensors within range.

ACCESS360 can accept an unlimited number of sensor inputs with 10 concurrent Bluetooth® connections at one time. Sensors communicating with the gateway should operate at a -20 to -75 dBm signal strength range to achieve a reliable connection.

Rated IP67, the ACCESS360 can withstand harsh environments including temperatures ranging from -4 °F to 158 °F (-20 °C to 70 °C). A cover featuring four self-tapping screws allows the box to be sealed from the elements. There is no need to remove the cover, except for if the SD card needs to be replaced. When the gateway is fully powered on, a green LED light will be visible through the clear lid.

Product Dimensions

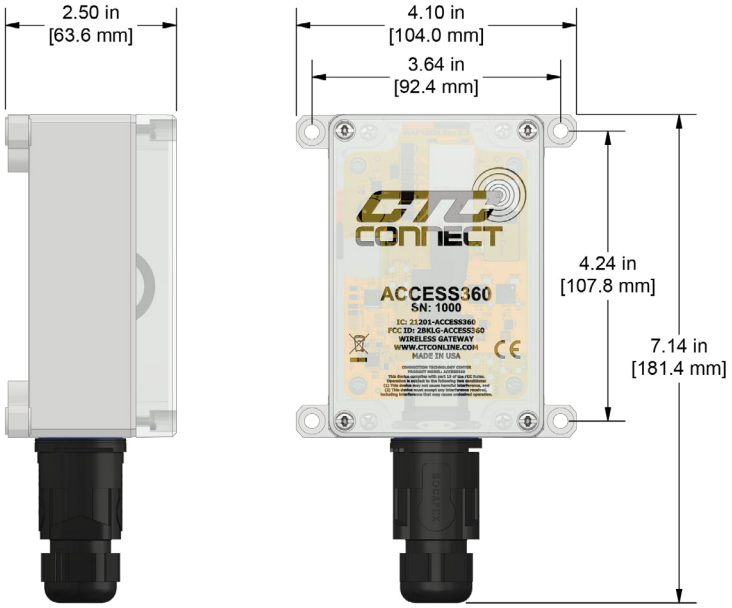


Figure 1. Dimensions

Figure 2. Diagram

ACCESS360 Network Requirements

Supported Network Configurations
ACCESS360 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

General Network Requirements

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

ACCESS360s should be installed on a **stable, business-class network** with sufficient uptime, bandwidth, and administrative controls.

Firewall & Security Requirements
The customer is responsible for allowing required outbound traffic:

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

Unsupported or Customer-Managed Configurations

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/5G 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.

Remote Management of 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 the use of DYNDNS (Dynamic DNS). Please note that the use of a static IP address is preferred for stability.

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

Mounting Instructions

Molded mounting brackets are included on the enclosure. Wall anchoring screws are not included.

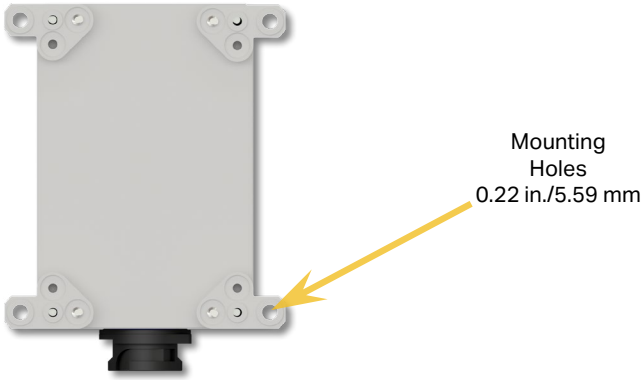


Figure 3. Gateway Rear View

Note: DO NOT mount the access point inside a metal enclosure.
Metal enclosures will significantly attenuate RF signals and can severely degrade wireless performance, range, and reliability.

Mounting the access point 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 access point.

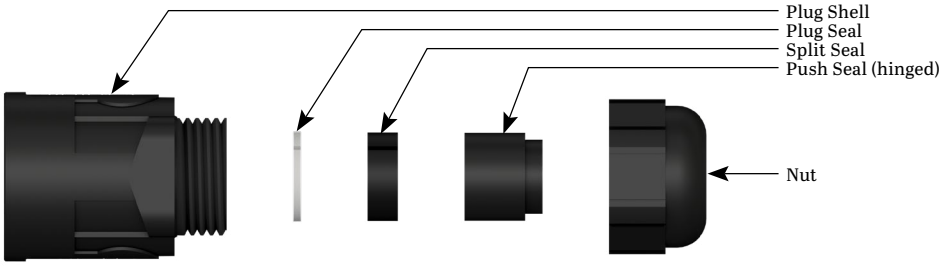
For optimal wireless performance, the access point should be mounted in an open environment with a clear RF path to the sensors.

Mount the gateway to a solid surface using mounting bolts as shown in Figure 4 below.

Figure 4. Mounted Gateway

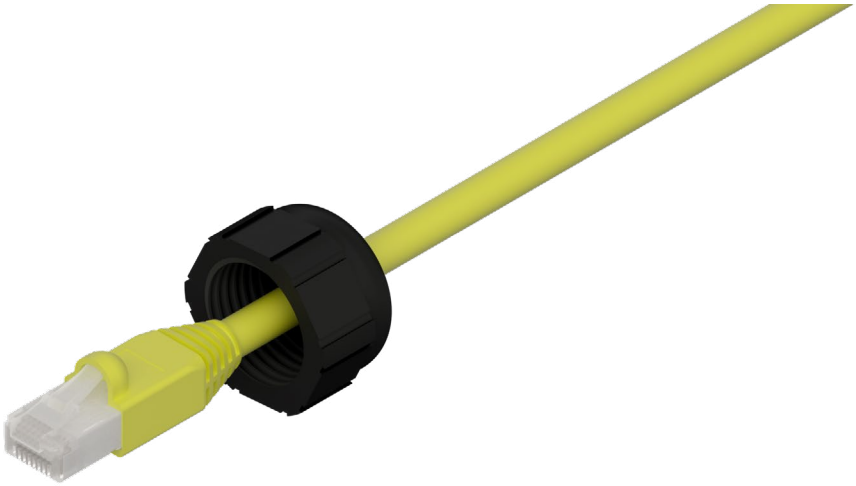
Ethernet Connection

Every ACCESS360 ships with a separate Ethernet cable backshell, which requires on site assembly. This backshell is mandatory to achieve the enclosure's IP67 rating. To prevent build up of condensation, ensure the ethernet cable entry point is facing downward.

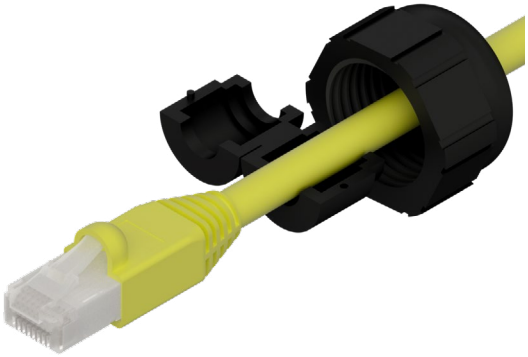


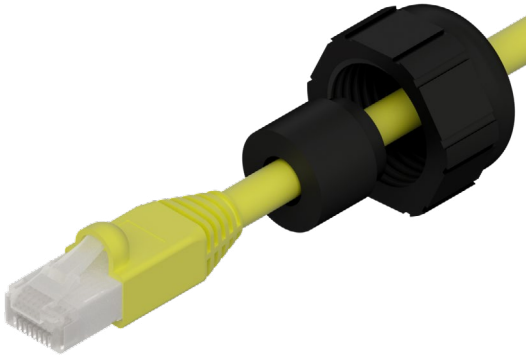
Note: The ACCESS360 requires power over ethernet to function. If your network is not capable of supplying power over ethernet, an external PoE injector supporting IEEE 802.3af or above is required.

1. Slide the nut over the connector and onto the cable.

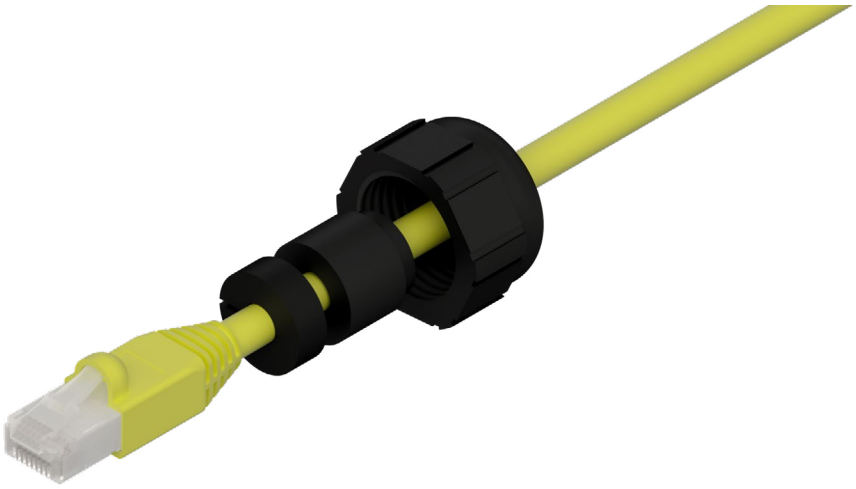


2. Place the push seal on the cable and close.

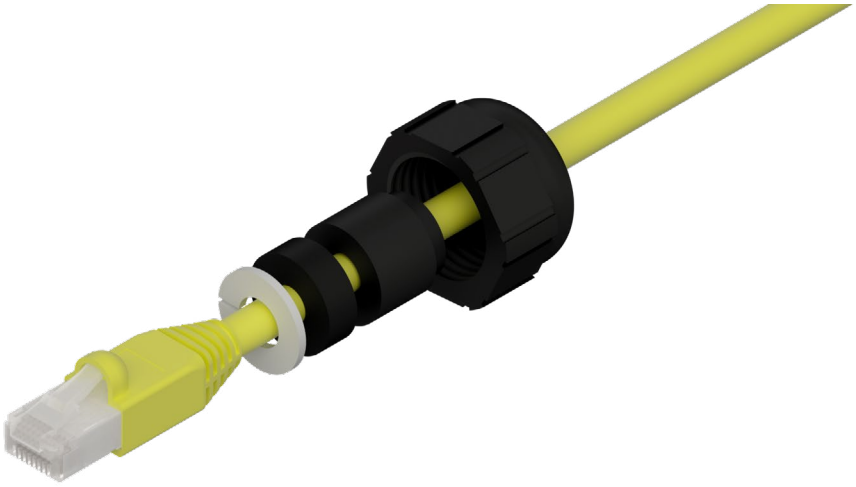




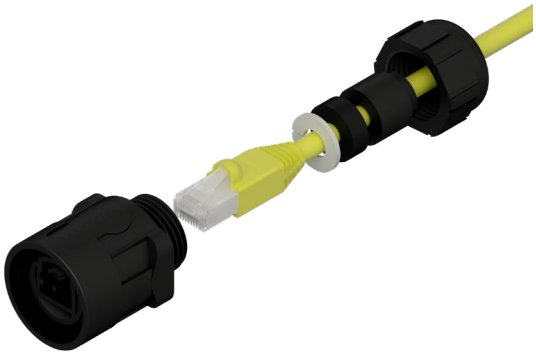
3. Attach the split seal around the cable.

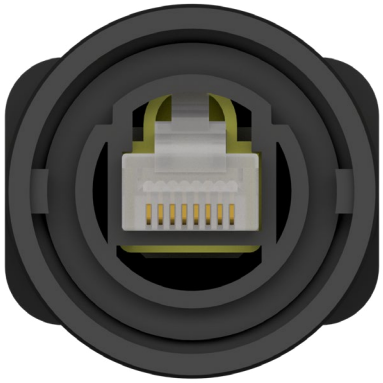


4. Attach the plug seal around the cable.

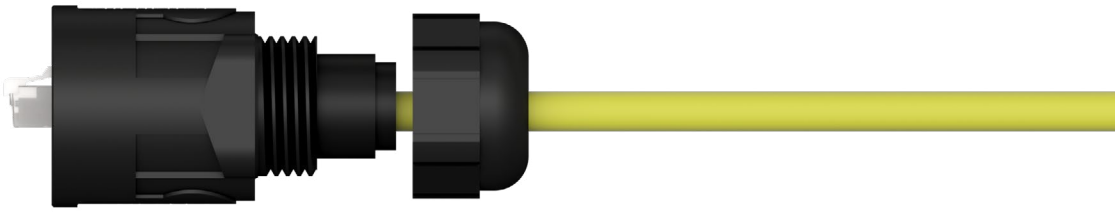


5. Slide the plug shell over the ethernet connector until the RJ45 plug latch is fixed in place.





6. Slide the assembly together and thread the nut onto the plug shell



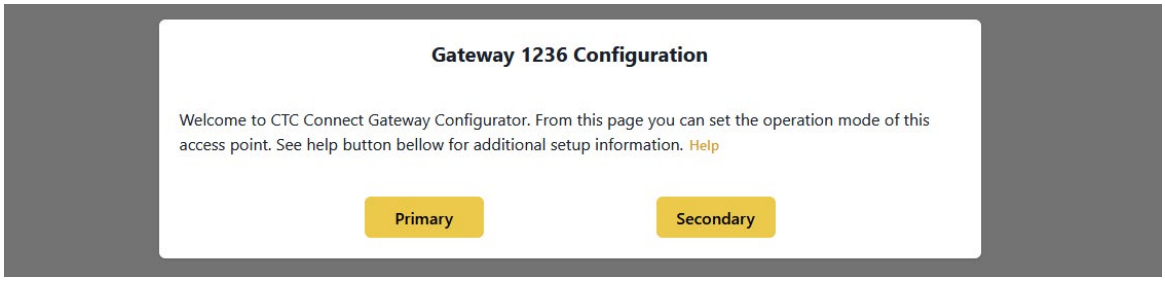
7. Tighten the nut to 2.2 lb-ft (3 N-m).

8. Insert the Ethernet cable into the port on the ACCESS360. Slide the dust protector up onto the mating collar and twist clockwise to lock into place.

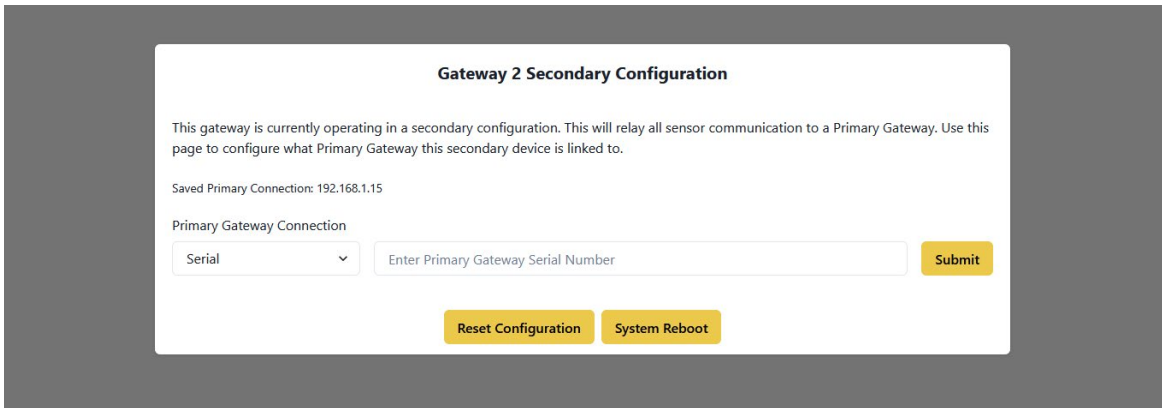
Device Setup

Connecting to a Network

1. Establish a physical connection between the gateway and the local network using the ethernet port and a Category 5 or higher ethernet cable. The gateway will power on automatically and two indicator LEDs will begin to blink, one orange and one green.
2. Wait until the orange LED remains solidly lit.
3. On a computer connected to the network, open a browser and navigate to http://ctcap-**XXXX**, where **XXXX** is the serial number of your gateway. The following screen will be displayed.

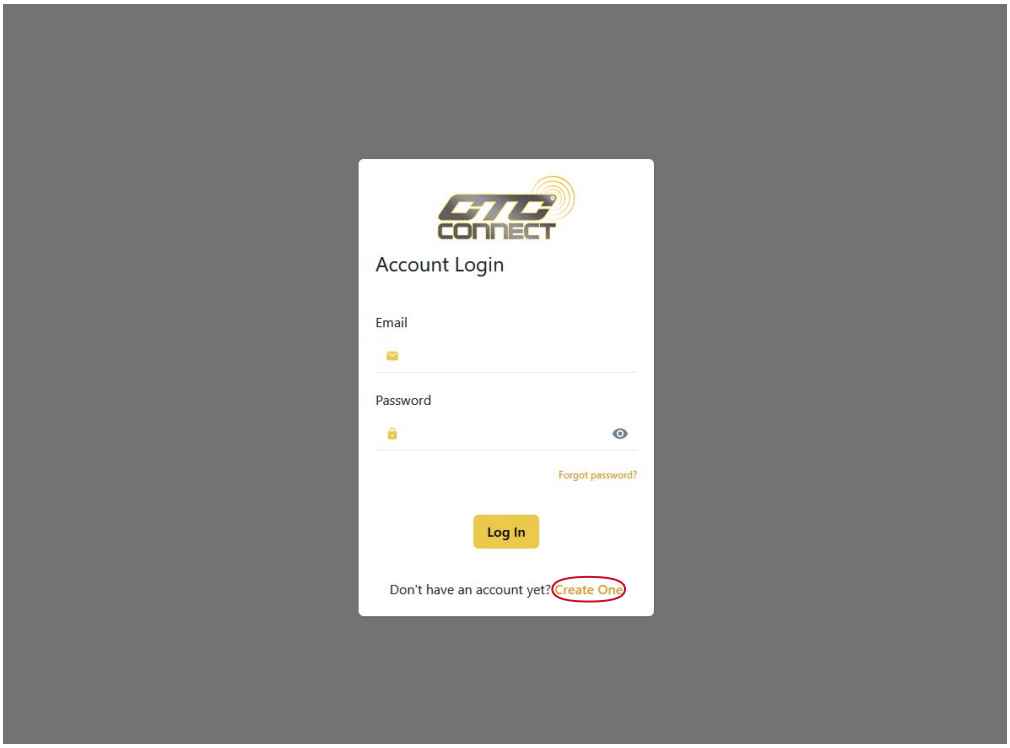


4. If the gateway is intended to be used as a primary connection point, click **Primary**. This will lead to the user login screen.
5. If the gateway is intended to be an intermediary connection point between a group of sensors and a primary gateway, click the **Secondary** button. This will lead to an additional setup screen.
6. Select Serial from the Primary Gateway Connection dropdown menu. Enter the serial number of the primary gateway into the text field. Use the Submit button to begin a connection between the two gateways.



Creating a New Account

1. From the login screen, click the **Create** button on the bottom of the window.

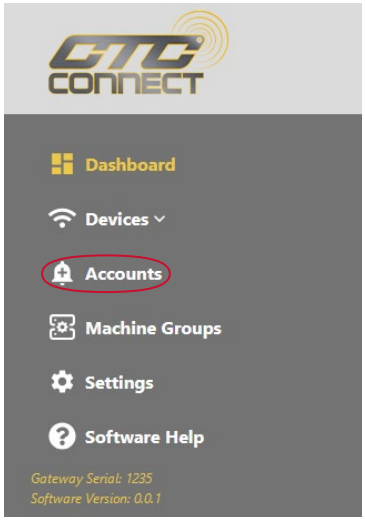


2. Enter the required user information: first and last name, email address, and password.
3. Click the **Details** button to view any additional information, if desired.
4. Click the **Register** button. The app will return to the login screen.
5. Login to the newly created account.
6. If prompted, check the associated email address for a verification email.

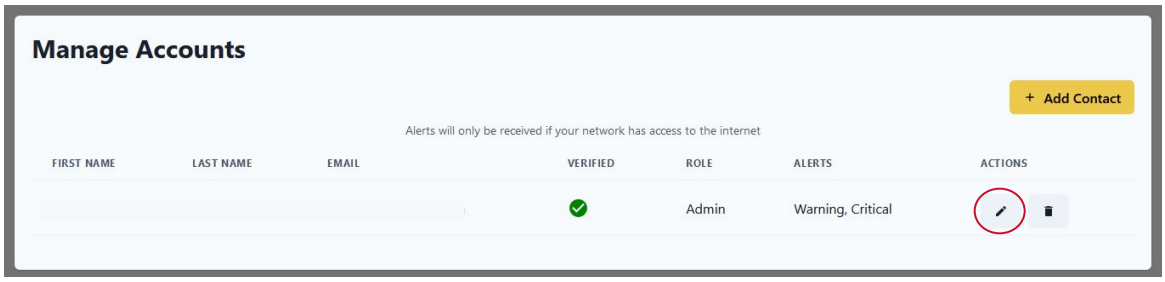
Note: The first account created on the network will automatically be assigned the Admin role. All subsequent users must have their roles elevated, as described in the following section.

Modifying User Accounts

1. While logged into an account with Admin privileges, click the **Accounts** button on the left side of the dashboard.



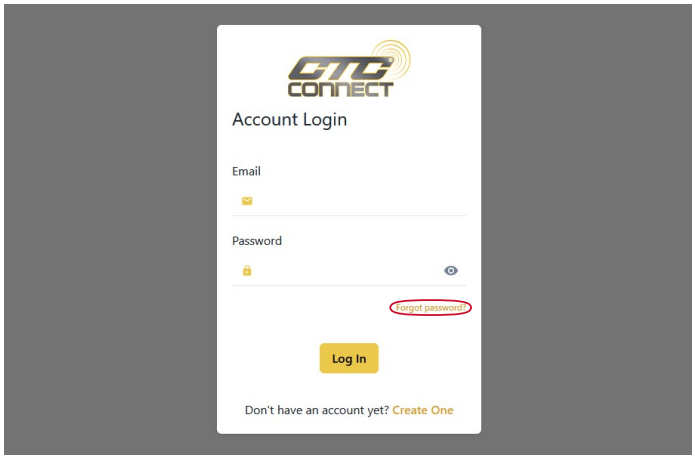
2. Select the user account you wish to edit.
3. Click the pencil icon.



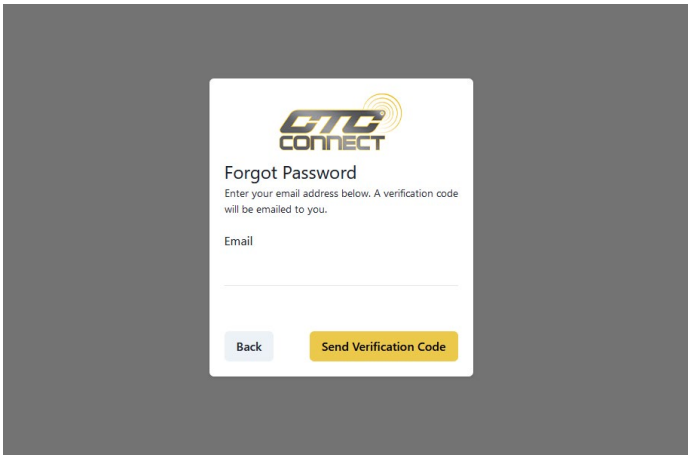
4. Modify account information as desired.
5. Click the **Save** button to complete.

Resetting User Password

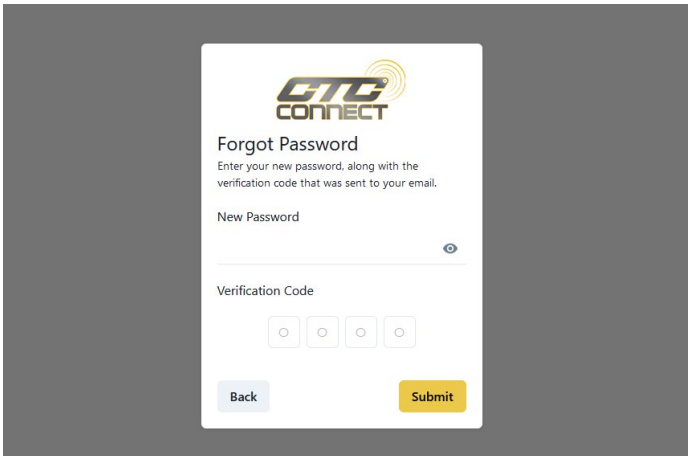
1. Ensure that the gateway is connected to a network with internet access.
2. From the login screen, select the **Forgot Password?** option.



3. Enter the user's email address.



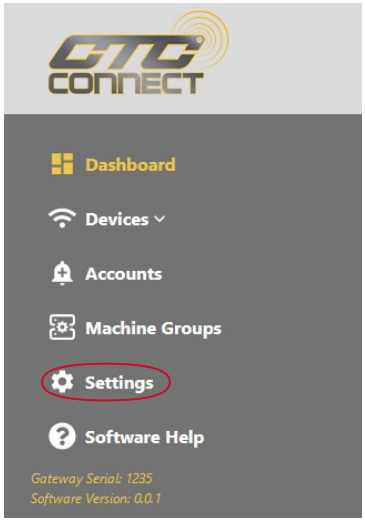
4. Create a new password, and enter the verification code sent via email. Click **Submit**.



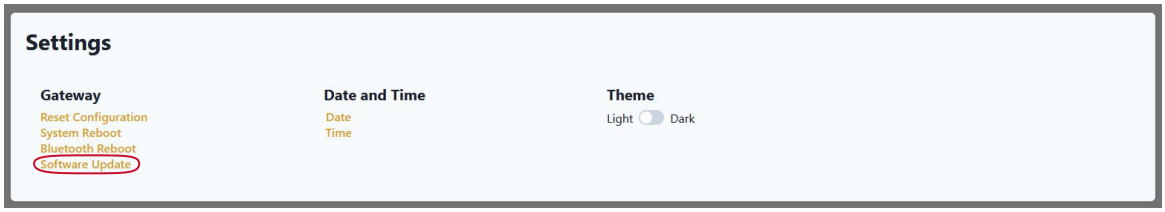
5. The user will be returned to the login screen, where they will be able to log in with the new credentials.

Performing a Software Update

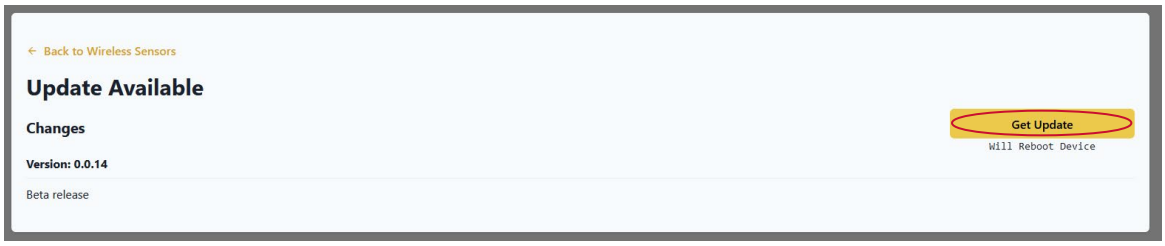
1. Ensure that the gateway is connected to a network with internet access.
2. While logged into an account with Admin privileges, click the **Settings** button on the left side of the dashboard.



3. Select the **Software Update** option.



4. If an update is available, it will be shown on this page. Click the **Get Update** button to update the software.

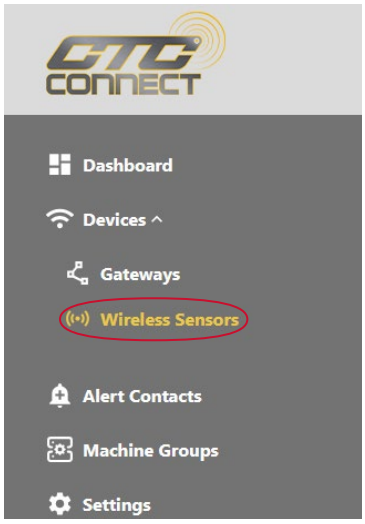


Executing Functionality

Note: Proceeding with any of the following requires the user to have either Analyst or Admin privileges.

Connecting a Sensor

1. Unscrew the sensor cap and plug in the battery.
2. From the dashboard, click the **Devices** dropdown on the left then click on **Wireless Sensors**.

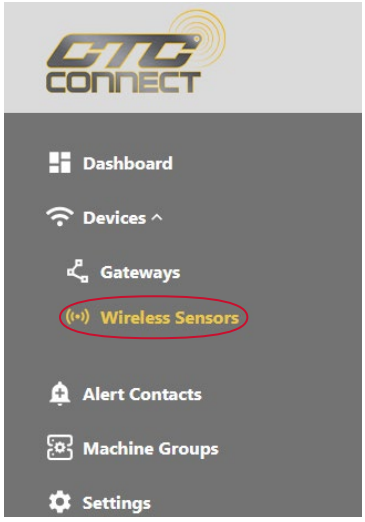


3. The sensor will automatically connect, and will show in the list of available sensors.

Note: Sensor connection status will also appear in notifications.

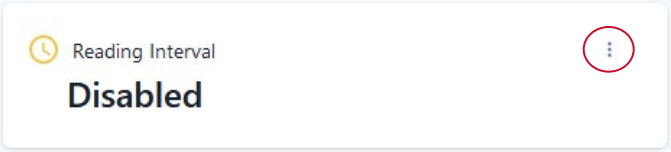
Programming a Dynamic Sensor

1. From the dashboard, click the **Devices** dropdown on the left then click on **Wireless Sensors**.



2. Select the desired sensor from the list.

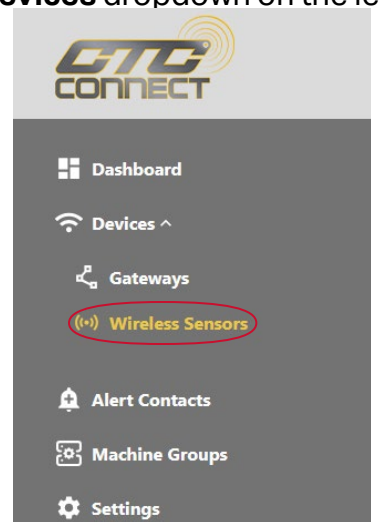
3. Modify any sensor setting by using the 3-dot button located in its field.



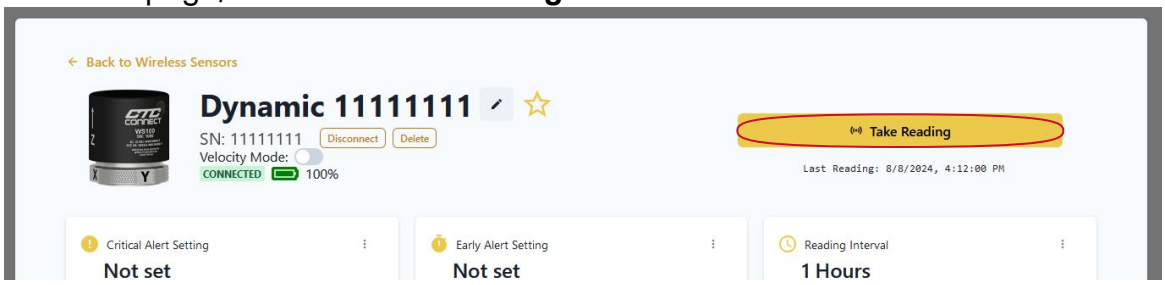
Note: WS100 Series sensors are not field reprogrammable.

Taking a Reading

1. From the dashboard, click the **Devices** dropdown on the left then click on **Wireless Sensors**.



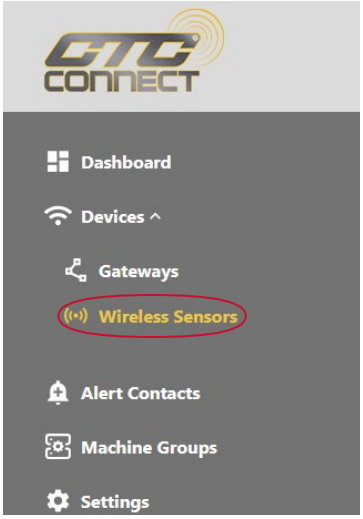
2. Find the desired dynamic sensor among the list of connected devices and click on it.
3. On the sensor page, click the **Take Reading** button.



Once the reading is complete, the page will automatically refresh with the resulting data capture.

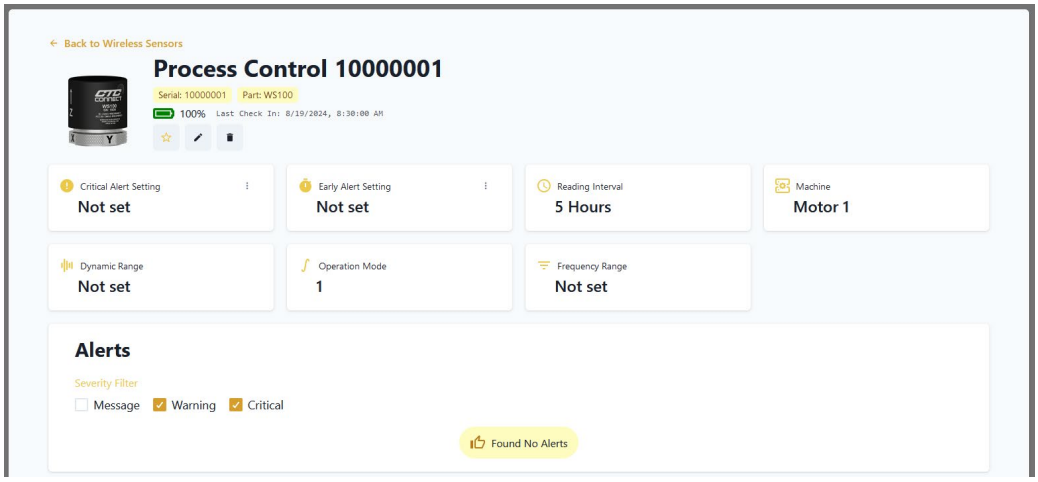
Viewing Process Control Sensors

1. From the dashboard, click the **Devices** dropdown on the left then click on **Wireless Sensors**.



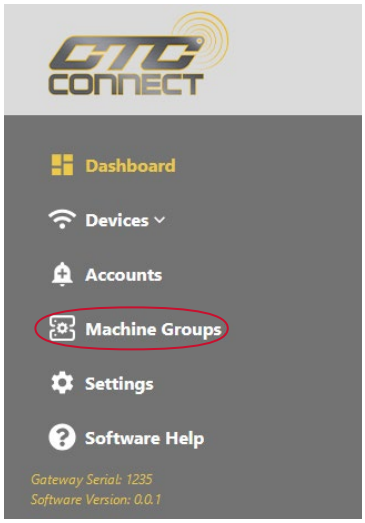
2. Find the desired sensor among the list of connected devices and click on it.

3. The resulting screen will display all available information about the sensor.

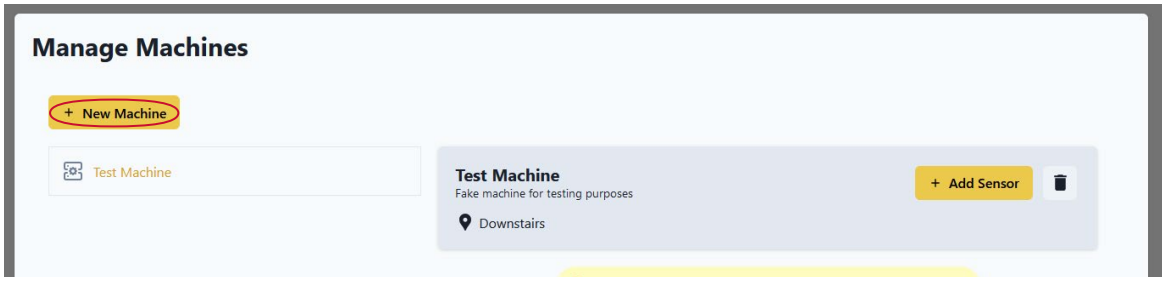


Create a Machine Group

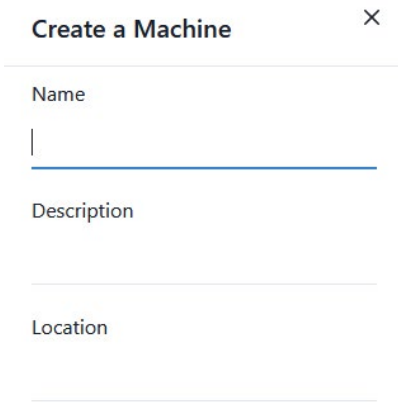
1. From the dashboard, click the **Machine Groups** button on the left.



2. Click the **New Machine** button.



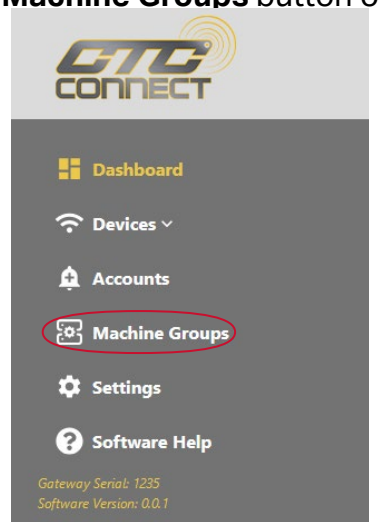
3. Enter machine information: name, description, and location.



4. Click the **Save** button to complete.

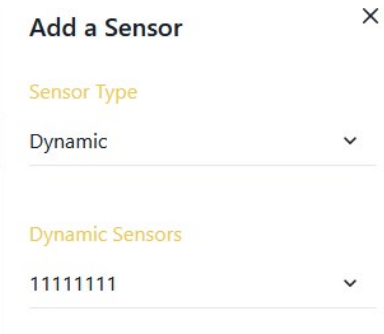
Add Sensor to a Machine Group

1. From the dashboard, click the **Machine Groups** button on the left.



2. Select the desired machine from the available list.
3. Press the **Add Sensor** button.

4. From the drop-down menu, select any desired sensor from the list of available options.



5. Press the **Submit** button to complete.

FCC Compliance Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CAUTION: The grantee is not responsible for any changes or modifications not expressly approved by the party responsible for compliance. Such modifications could void the user's authority to operate the equipment. NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

RF exposure statement

This equipment complies with the FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and any part of your body.

Canadian Compliance Statement

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada license-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1. L'appareil ne doit pas produire de brouillage;
2. L'appareil doit accepter tout brouillage radio électrique subi, même si le brouillage est susceptible d'encompromettre le fonctionnement.

RF exposure statement

This equipment meets the exemption from the routine evaluation limits in section 2.5 of RSS-102. It should be installed and operated with a minimum distance of 20 cm between the radiator and any part of your body.

Cet équipement est conforme à l'exemption des limites d'évaluation habituelle de la section 2.5 de la norme RSS-102. Il doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et toute partie de votre corps.

Maintenance

Once the system has been installed, it requires minimal maintenance. Basic checks to ensure system integrity should be made periodically.

Visual inspection should include examinations for the following:

1. No visible electrical burns or smoke inside the enclosure.
2. No moisture or condensation is present inside the enclosure.

Warranty and Refund

Please visit www.ctconline.com to view a complete recapitulation of our warranty and refund policies.

Disclaimer

The ACCESS360 contains software and firmware proprietary to CTC. Use of the ACCESS360 is, at all times, subject to the CTC's then current Software End User License Agreement available at www.ctconline.com. All data and information provided by, or collected from, you is subject to CTC's Privacy Policy available at www.ctconline.com.

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