



ACCESS2000 Gateway Software Guide

TABLE OF CONTENTS

- Device Setup 3
- User Accounts..... 6
- Configuring NTP Settings.....12
- Performing a Software Update.....14
- Executing Functionality15
- Federal Communications Commission (FCC) Interference Statement20
- RF Exposure Warning20
- Maintenance21
- Warranty and Refund Information21



DEVICE SETUP

Consult your Network or IT Team for help deciding and configuring the best method for your environment. Below are some highlights of the differences between DHCP and Static IP schemas.

DHCP Overview

A **DHCP (Dynamic Host Configuration Protocol) lease** is a temporary, time-bound assignment of an IP address to a device (such as a phone, laptop, or smart TV) on a network.

Instead of permanently tying an IP address to a single machine, a network's DHCP server "rents" the address out for a specific duration. DHCP can be provided by a DHCP server or Network Router.

How the Lease Works

- The "Rental" Period: The DHCP server dictates how long the device can use the IP address. Once this time expires, the address returns to an available pool to be reused.
- Automatic Renewal: When 50% of the lease time passes, the device automatically attempts to renew its lease with the server. If it is successful, the timer resets and the device keeps the same IP address.

Why is it used?

- Efficient Management: In environments like corporate offices where hundreds of temporary devices connect, leases ensure that disconnected devices don't hoard IP addresses.
- Seamless Updates: If a network administrator changes network configurations (like updating DNS servers), the lease system forces devices to get updated settings when they renew.

Static IP Overview and Comparison

A static IP address is a permanent, manually assigned numerical identifier for a device on a network. Unlike dynamic IPs—which change periodically—a static IP never alters, acting as the digital equivalent of a fixed street address that devices and servers can consistently locate.

Why are Static IPs used?

- Reliable Remote Access: Essential for connecting to private corporate networks (VPNs).
- Hosting Servers: Necessary for running web, email, or cloud data servers so users and clients can always find the host without updating DNS records.
- Network Devices: Ideal for hardware like printers, security cameras, or media servers, ensuring devices in an office or home don't lose connection due to a shifting IP.

Static vs. Dynamic IP

Feature	Static IP	Dynamic IP
Stability	Remains fixed across sessions.	Changes periodically.
Setup	Manually configured in network settings or requested from an ISP.	Automatically assigned by a router using DHCP.
Best Used For	Servers, printers, remote access points.	Everyday browsing, streaming, and mobile devices.
Cost	Often comes with a premium fee or requires a business-tier internet plan.	Standard for almost all residential internet connections.

Configure for DHCP

Ensure the ACCESS2000 settings in the example below are configured to the local network:

 **Wired**

IP Allocation

DHCP

DNS1

192.168.0.110

DNS2

8.8.8.8

Configure for Static IP

Ensure the ACCESS2000 settings in the example below are configured to the local network:

 **Wired**

IP Allocation

Static

IP

192.168.1.242

Netmask

255.255.248.0

Gateway

192.168.0.1

DNS1

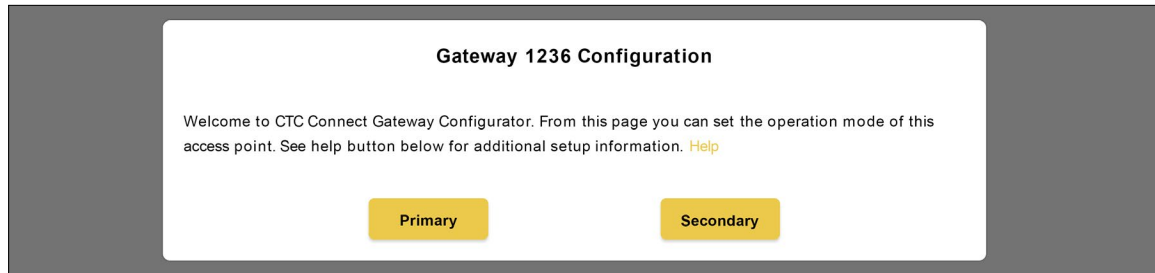
192.168.0.110

DNS2

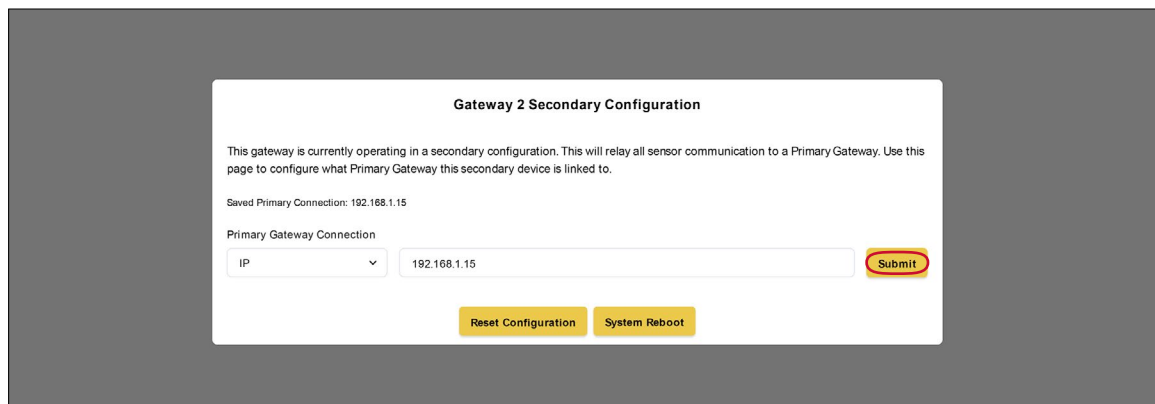
8.8.8.8

Configuring the Gateway

1. Prior to configuration setup on any gateway, it must be connected to the local network. For complete instructions on this process, refer to the ACCESS2000 Operational Guide, Section V: "Setup Bluetooth Router."
2. Following step seven of the above, open a browser on a local computer or laptop and navigate to the IP address of the gateway.



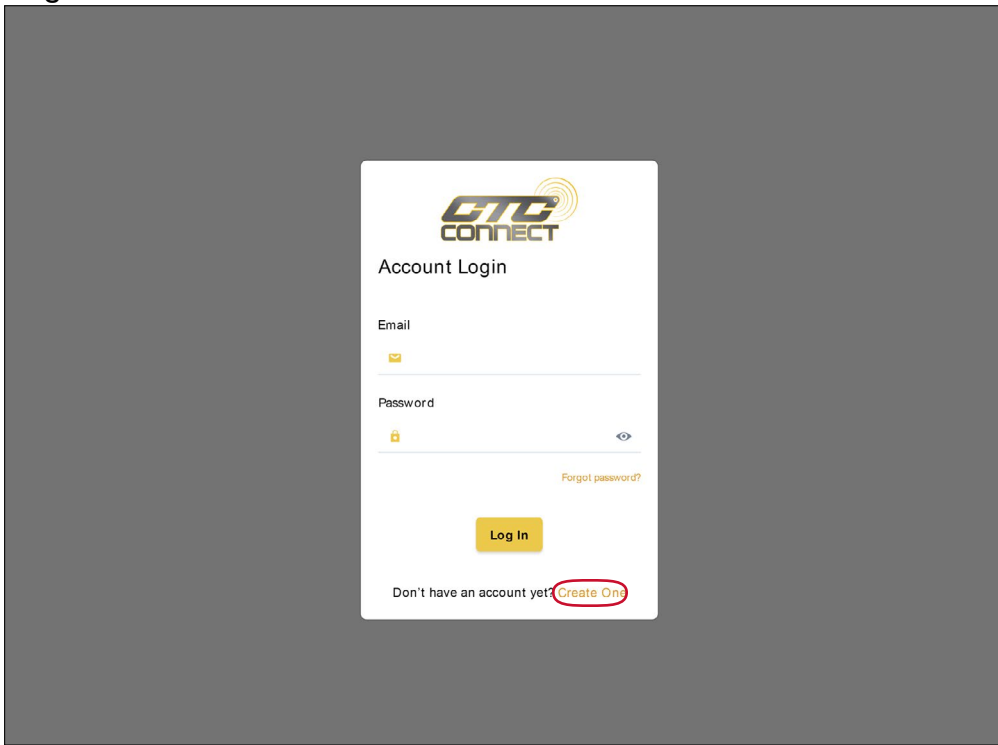
3. If the gateway is intended to be used as a primary connection point, click **Primary**. This will lead to the user login screen.
4. If the gateway is intended to be an intermediary connection point between a group of sensors and a primary gateway, click the **Secondary** button. This will lead to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



USER ACCOUNTS

Creating a New Account

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

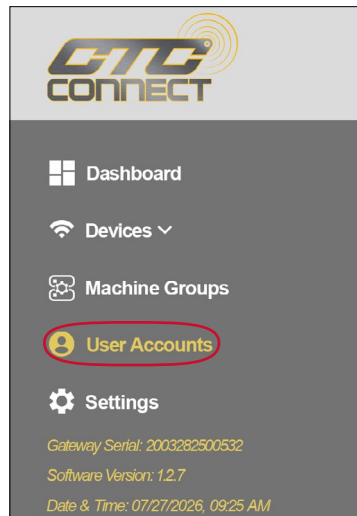


2. Enter the required user information: first and last name, email address, and password.
3. Click the **Details** button to view any additional information, if desired.
4. Click the **Register** button. The app will return to the login screen.
5. Login to the newly created account.
6. If prompted, check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

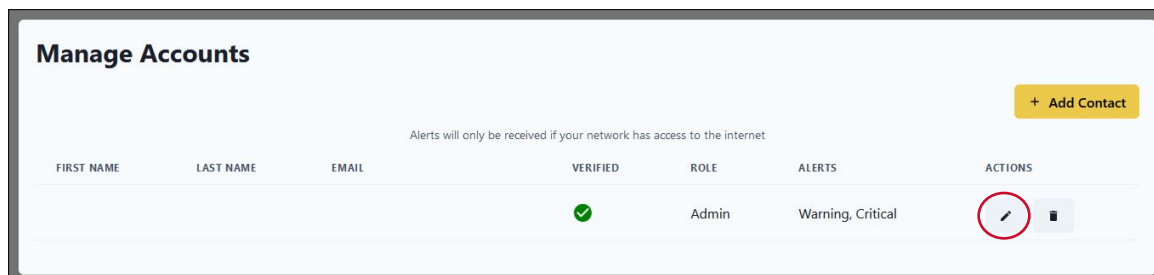
Note: The first account created on the network will automatically be assigned the Admin role. All subsequent users must have their roles elevated, as described in the following section.

Modifying User Accounts

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



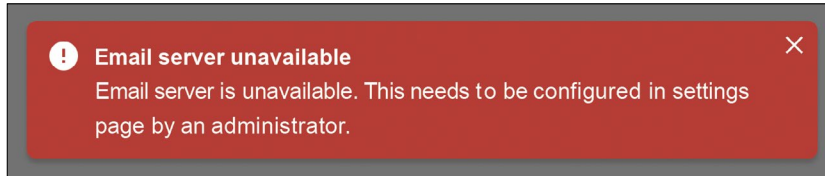
2. Select the user account you wish to edit.
3. Click the pencil icon.



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

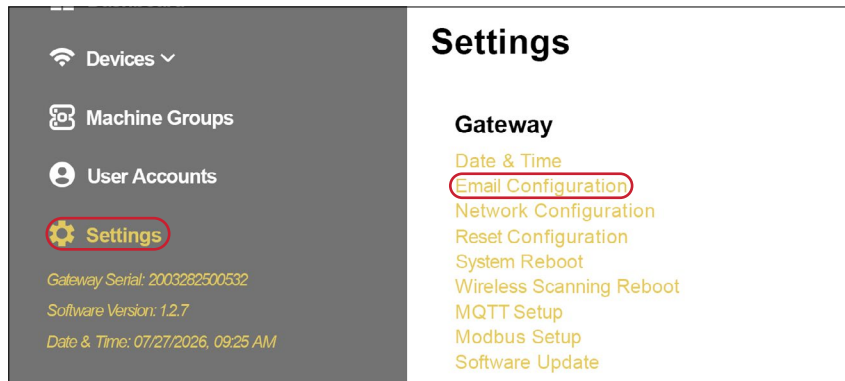
Configuring Email Alerts for User Accounts

Starting with Software Version 1.2.7 CTC Connect now allows users to configure their own email server for alerts as well as password recovery. If the user does not have their email server configured, they will not be able to perform a password recovery. They will instead receive the following error.

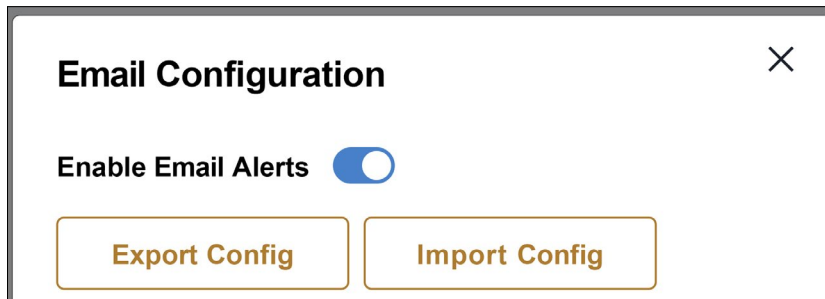


Configuration

1. From the main menu, select Settings, then Email Configuration.



2. Toggle on "Enable Email Alerts"



3. Follow the required configuration for the user's corporate SMTP server.

SMTP Server

Port

Sender Address

Username

Password
 

Email Subject Password for SMTP authentication

4. Click Save to commit the changes.

Email Subject Password for SMTP authentication

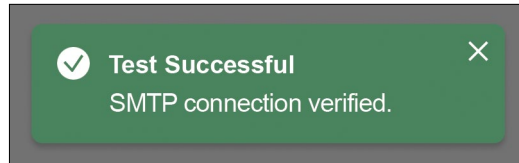
Test Configuration

1. To test the configuration, press the test button.

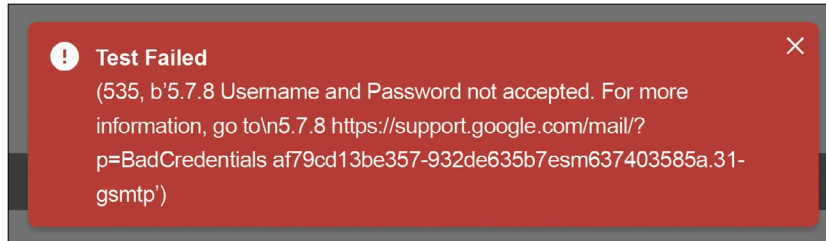
Email Subject

Subject line used for all alert emails

2. If the test passes, the following confirmation will display.

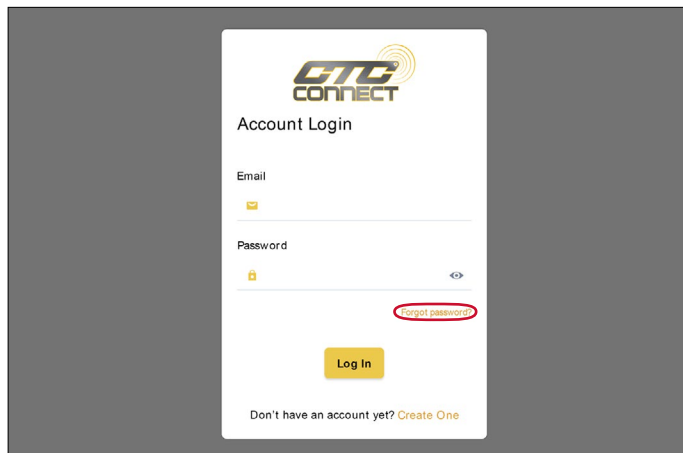


3. If the test fails, an error message will display with a discription of the failure.

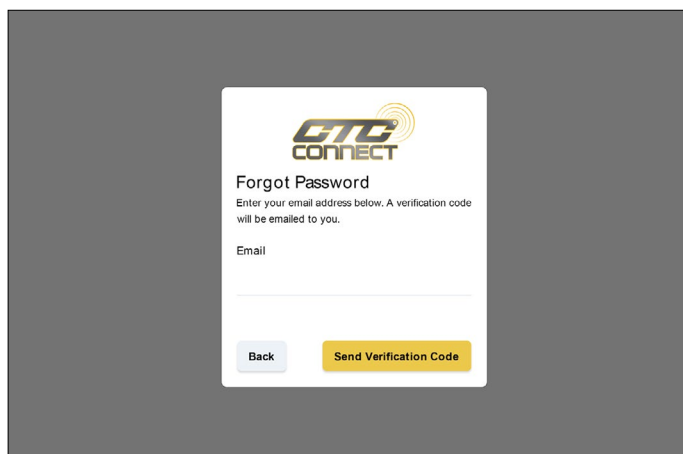


Resetting User Password

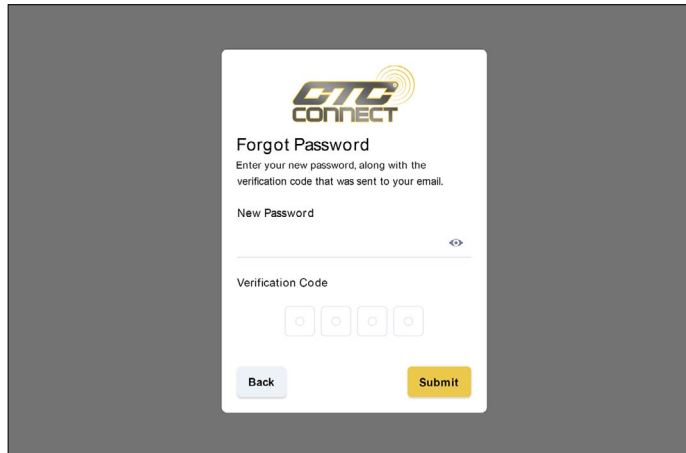
1. Ensure that the gateway is connected to a network with internet access.
2. From the login screen, select the **Forgot Password?** option.



3. Enter the user's email address.



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



The screenshot shows a web form titled "GTC CONNECT" with the heading "Forgot Password". Below the heading is a sub-header: "Enter your new password, along with the verification code that was sent to your email." The form contains two input fields: "New Password" with a toggle icon (an eye) to its right, and "Verification Code" with four individual input boxes. At the bottom of the form are two buttons: a grey "Back" button and a yellow "Submit" button.

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

CONFIGURING NTP SETTINGS

An NTP server (Network Time Protocol server) is a system that distributes exact time to computers and devices across a network. By functioning as a central timekeeper, it ensures that all connected devices share the exact same time.

Why are they important?

- **Security & Auditing:** Accurate timestamps ensure that security logs, event histories, and system updates can be reliably cross-referenced during investigations.
- **System Stability:** They prevent failures in distributed databases, automated software tasks, and network authentication systems that rely on time-sensitive operations.
- **Data Consistency:** They stop files from having conflicting creation or modification dates, which is crucial for version control and backups.

System & Network Requirements

An Internet Connection is required to establish a time sync on the gateway to standard NTP servers. CTC Connect Gateways use 2 very common NTP Server Pools by default.

0.pool.ntp.org

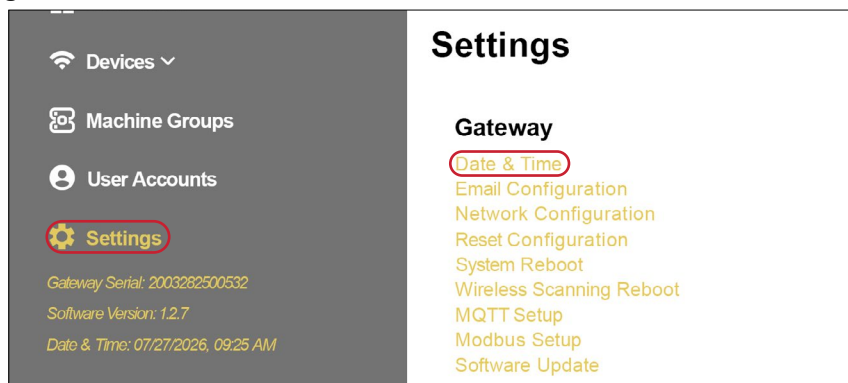
1.pool.ntp.org

UDP port 123 is exclusively used by the Network Time Protocol (NTP). It allows devices (computers, servers, routers, and IoT devices) to communicate with time servers across a network and perfectly synchronize their internal clocks.

If connectivity to the NTP servers is unsuccessful, ensure the network firewall allows outbound UDP traffic on port 123 for time synchronization.

Configuration of NTP on CTC Connect Gateways

1. Log into the Web Interface of the CTC Connect Gateway.
2. Select Settings, then Date & Time.



3. If the Gateway NTP is showing Inactive, that means the sync is disabled. To enable the sync, press the enable button.

Two side-by-side screenshots of the "Gateway Date and Time Select" dialog box. The left screenshot shows the "Gateway NPT: Inactive (Enable)" status with a red box around the "Enable" button. The right screenshot shows the "Gateway NPT: Inactive (Enable)" status with a green checkmark next to the "Enable" button. Both screenshots show the "Computer" and "Gateway" times, a "Manually Set Gateway Date/Time" section with date and time pickers, and "Apply" and "Auto Sync" buttons.

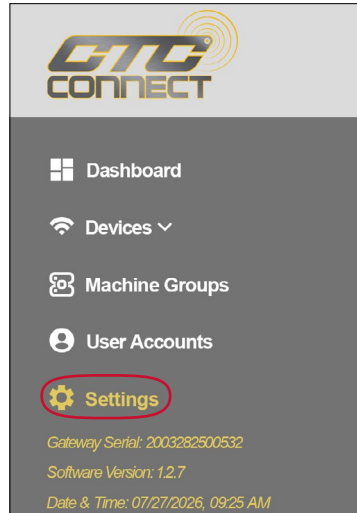
4. The sync can take up to a minute to complete. Once completed the sync status will change to Active. Close the box to complete, **do not** hit the apply button.

A screenshot of the "Gateway Date and Time Select" dialog box. The "Gateway NPT" status is now "Active (Disable)". The "Apply" button is crossed out with a red X, and the "Auto Sync" button is visible. The "Computer" and "Gateway" times are updated, and the "Manually Set Gateway Date/Time" section shows the date and time.

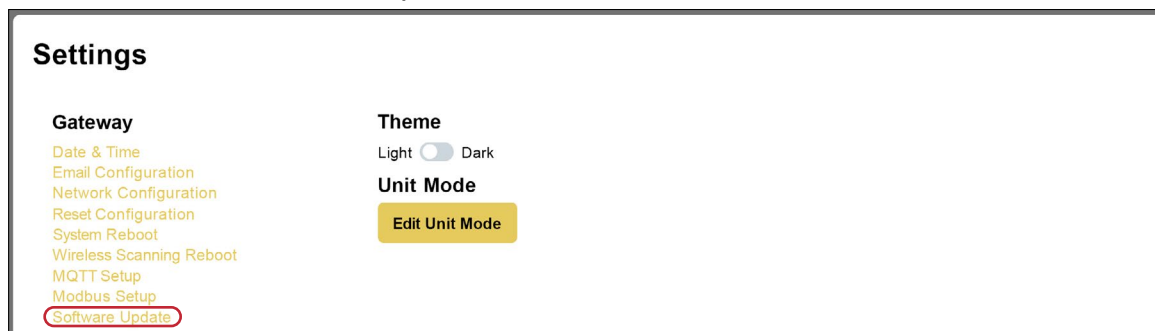
5. Double check the time on the gateway and to ensure the sync has completed and the time is correct.

PERFORMING A SOFTWARE UPDATE

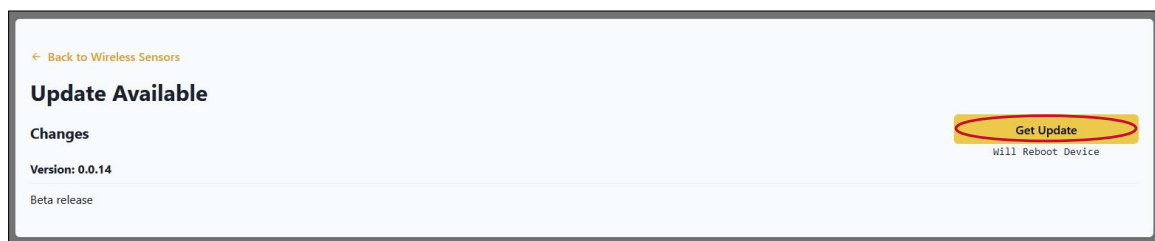
1. Ensure that the gateway is connected to a network with internet access.
2. While logged into an account with Admin privileges, click the **Settings** button on the left side of the dashboard.



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.



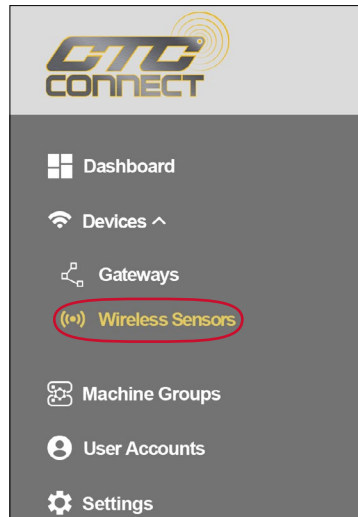
Note: Any updates must be allowed to complete before rebooting or resuming normal use of the gateway. It is recommended to allow for 30 to 60 minutes of downtime, depending on internet connection.

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**.

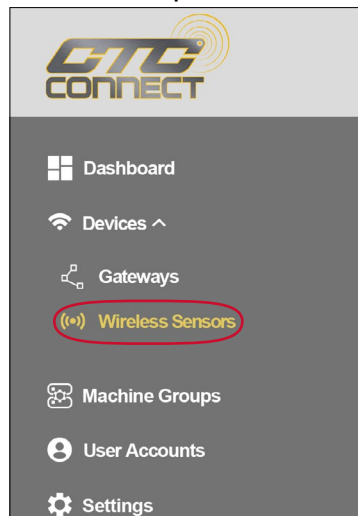


3. The sensor will automatically connect, and will show in the list of available sensors.

Note: Sensor connection status will also appear in notifications.

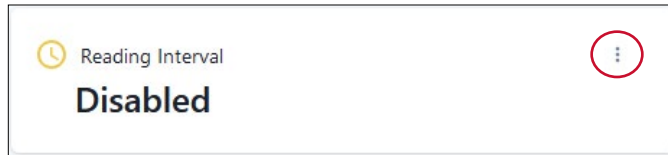
Programming a Dynamic Sensor

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



2. Select the desired sensor from the list.

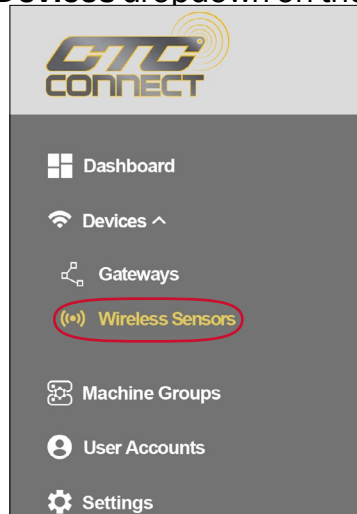
3. Modify any sensor setting by using the 3-dot button located in its field.



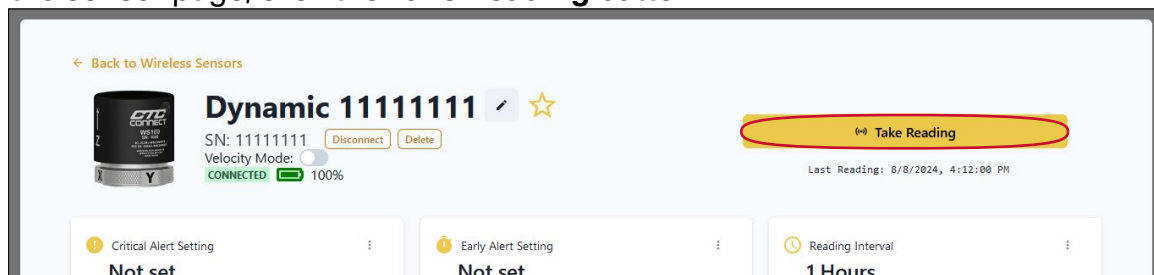
Note: WS100 Series sensors are not field reprogrammable.

Taking a Reading

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



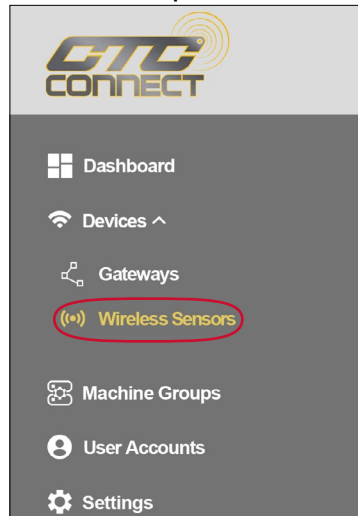
2. Find the desired dynamic sensor among the list of connected devices and click on it.
3. On the sensor page, click the **Take Reading** button.



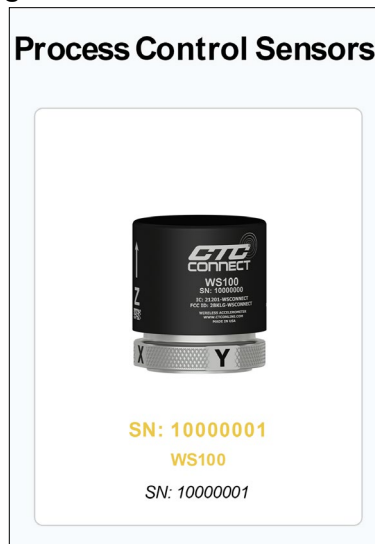
Once the reading is complete, the page will automatically refresh with the resulting data capture.

Viewing Process Control Sensors

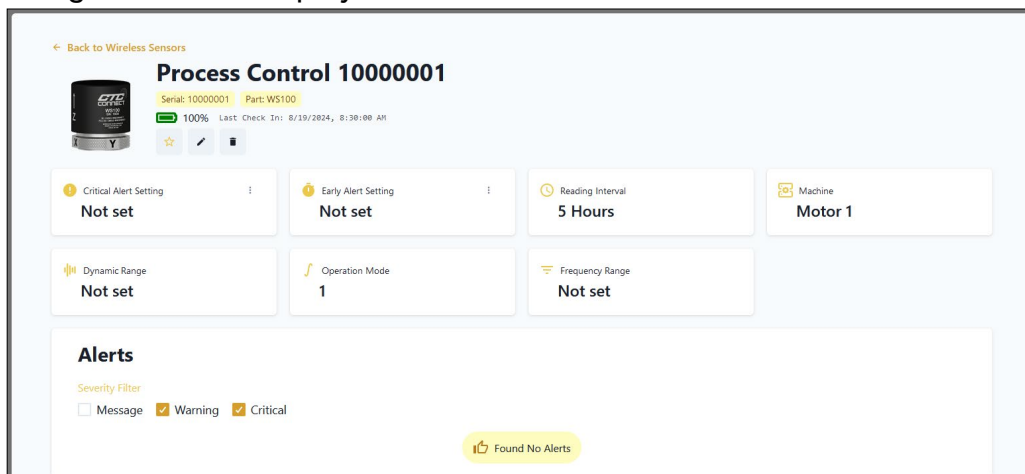
1. From the dashboard, click the **Devices** dropdown on the left then click on **Wireless Sensors**.



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

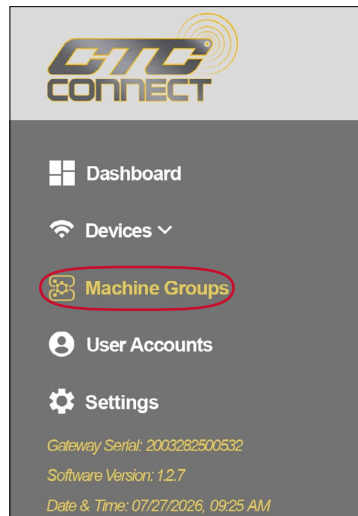


3. The resulting screen will display all available information about the sensor.

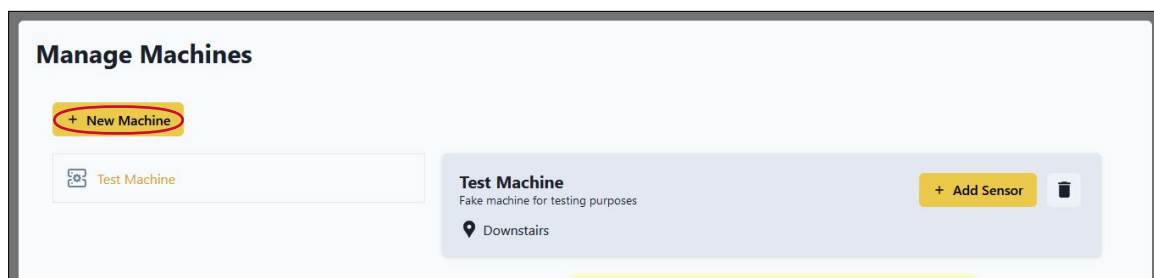


Create a Machine Group

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



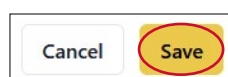
2. Click the **New Machine** button.



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

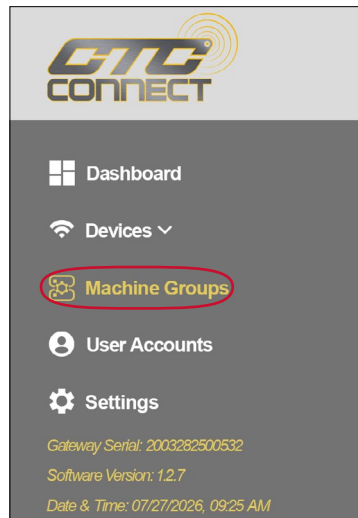
A screenshot of the 'Create a Machine' form. It has a title bar with a close button (X). The form contains three input fields: 'Name', 'Description', and 'Location'. Each field has a placeholder text and a blue underline.

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.



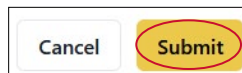
2. Select the desired machine from the available list.
3. Press the **Add Sensor** button.



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



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



FEDERAL COMMUNICATIONS COMMISSION (FCC) INTERFERENCE STATEMENT

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.

NOTE: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

For additional information, please go to: <https://www.cassianetworks.com>

RF EXPOSURE WARNING

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

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

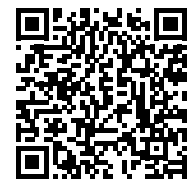
The ACCESS2000 contains software and firmware proprietary to CTC. Use of the ACCESS2000 is, at all times, subject to the CTC's then current Software End User License Agreement available at www.ctconline.com. All data and information provided by, or collected from, you is subject to CTC's Privacy Policy 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**

The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Connection Technology Center, Inc. (CTC) is under license. Other trademarks and trade names are those of their respective owners.

