iC Module™

INTERNET OF THINGS CONTROL MODULE

Part No. 1171600, 1171500

USER MANUAL

English

Control • Monitor • Analyze

Wireless + 10/100Base-T

ISO 9001 CERTIFIED

Made in the USA

GARRETT METAL DETECTORS

CUSTOMERS IN USA:

Garrett Metal Detectors
Security Division
1881 W. State Street
Garland, TX 75042-6797 USA
Email: security@garrett.com
Phone: 800.234.6151 *(US/Canada)*

INTERNATIONAL CUSTOMERS:

Garrett Metal Detectors
International Division
1881 W. State Street
Garland, TX 75042-6797 USA
Email: international@garrett.com
Phone: 1.972.494.6151

TABLE OF CONTENTS

1.0 IC MODULE PRODUCT OVERVIEW

Congratulations on selecting Garrett Metal Detectors' Internet of things Control (iC) Module. The iC Module is a multi-functional product designed to be used with specific Garrett Walk-Through Metal Detector products. When using the Garrett iC Module with the CMA Connect client software, users can create an Internet of things ecosystem to help control their walk-through metal detectors. This ecosystem provides the ability to have full control by allowing access to observe and examine multiple walk-through units remotely. Users have the ability to quickly respond to security events by changing settings to individual walk-throughs, groups of walk-throughs or all walk-throughs at once on their system. Statistics, such as historical graphs and data, allow users to better examine their security needs at checkpoints in the future.

Garrett Internet of Things Control Module (iC Module)

The iC Module *(see Figure 1-A)* contains memory and processing circuitry and allows connection to your network wirelessly or via a wired RJ45 Ethernet connection using a laptop or personal computer (PC).

Garrett CMAConnect Software

The CMAConnect software provides remote network access to data collection, alarm statistics and real-time detector events for monitoring and / or analyzing. When connected to a network, the walk-through unit can be remotely monitored and controlled from any location around the world.

Note: Prior to installation, please contact your network administrator to obtain an IP address (or range of IP addresses) to ensure a successful install.

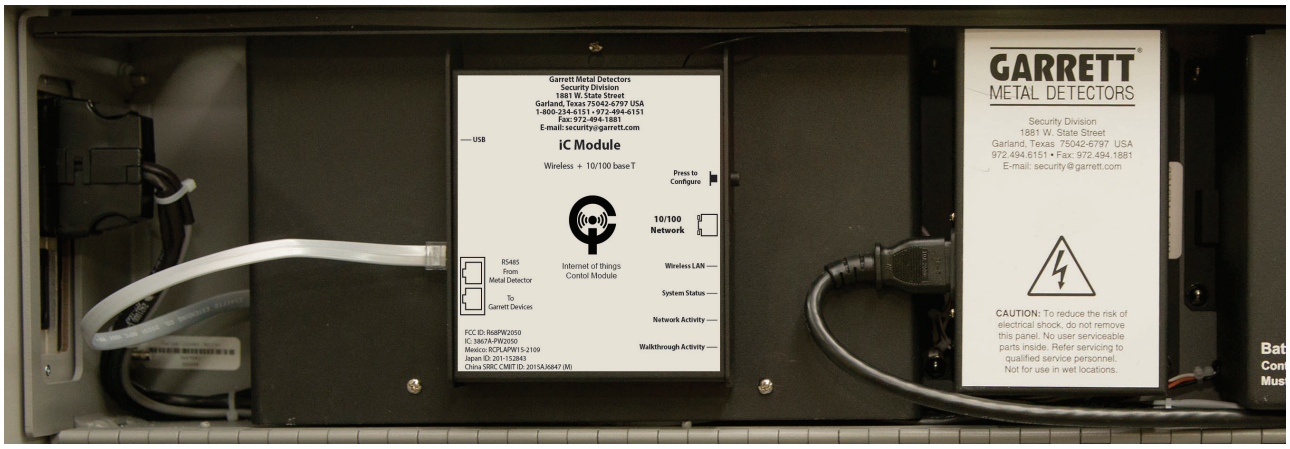


Figure 1-A

2.0 INSTALLATION TIPS

- The CMA Connect client software works with Java runtime V.7. This software is provided on the USB drive that is supplied with each iC Module.

- This product is shipped with a static Ethernet IP address of 192.168.0.192/32, but each device will ultimately require its own unique IP address. The Wireless IP address is set to DHCP by default to assist in first time set up. However, Garrett recommends that customers disable DHCP and assign a unique static IP addresses on each iC Module to ensure a stable connection with the CMA Connect software. Information about the product function, assigning the IP address, network and soft ware installation is included in this manual.

- The MAC address for each iC Module is provided to help when assigning IP addresses. A pre-assigned IP address can be reserved for each address when the module comes online.

- Software installation may require assistance from your System Administrator if your operating system is password protected. Network installation may require the assistance of your Network Administrator.

- Certain functions of the iC Module are password-protected.

LED Summary

Wireless LAN LED	Solid:	iC Module is connected to wireless LAN
System Status LED	(Nothing of interest)	
Network Activity LED	Off: Blinking 1x/second: Blinking 3x/second: Solid:	WEB interface is disabled WEB interface is enabled USB is being used. Do not unplug USB at this time USB operations have completed. Safe to unplug the USB
Walkthrough Activity LED	Flashing: Solid:	iC Module is starting up iC Module is running

Table 2.1

"Press to Configure" Button Functions

1 press	Enable/disable WEB interface
2 press	Enable Wireless Access Point and reboot.
3 press	Reboot immediately

Table 2.2

3.0 WIRELESS NETWORK CHECKLIST

Below is a checklist of information intended to be filled out and returned to Garrett if you would like to have your iC Module arrive pre-configured for your wireless network.

Wireless Network Infrastructure

1. Is the SSID used to connect the WTMD's accessible from ALL desired installation locations? Yes___ No ___
2. SSID Name: _____
   Key: _____
3. IP Block to use?
   FROM:_____ TO _____

Note: DHCP is not supported with Garrett Client SW. A wireless static IP address must be assigned for each iC Module.

4. Subnet Mask: _____
5. Gateway Address: _____

Wireless Security Information

1. What wireless encryption method will be used? WEP___ WPA___ WPA2___
   a. If WPA/WPA2 - PSK
      i. Key/Passphrase _____
   b. If Enterprise with 802.1x
      i. Username:_____
      ii. Password: _____

Note: Networks utilizing SSL certificates cannot be configured by Garrett prior to delivery and can only be configured at the end users location

2. Is broadcast traffic allowed on the wireless network? _____
   • If no, are there any protocols that could block traffic from repeated broadcast requests? _____
3. Is the desired SSID broadcasting (not hidden)? _____

Note: Broadcasting allows for iC Module to be discoverable in the Client SW when it first comes online. Otherwise, the IP address will need to be entered manually for it to be discovered. Broadcasting is only needed for initial setup.

4. Is a client isolation protocol enabled?

Note: Enabling isolation protocol prevents remote access to iC Module with the Client SW

   a. Yes___ If yes, is it global_____ or by SSID_____?
   b. No ___

Infrastructure Information

1. Can a contiguous block of IPv4 addresses be reserved for the iC Modules? _____

Note: DHCP is not currently supported when using Garrett Client SW

2. Is the SSID to be used connected to the same VLAN or Subnet that the Client PC will be connected to? _____
3. Is traffic allowed on ports 6876:TCP and 6877:TCP?
   Yes___ No ___

Note: If "No," these two ports must be opened for CMA Client to operate properly.

4.0 HARDWARE INSTALLATION

iC Module Components:

- iC Module
- Power/Data Cable
- CMA Connect USB drive
- User's Manual
- Transmitter ID Label

REQUIRED TOOL:

- Phillips screwdriver, #2
- 1/4" drill bit

Figure 4-A

IMPORTANT: Disconnect all power to the walk-through unit before installing the iC module!

Installation Steps

1. Open the access door.
   (see Figure 4-B)

Figure 4-B

2. Remove the 2 ft. power cord.
   (see Figure 4-C)

Figure 4-C

3. Remove the circuit board cover by removing the 3 screws.
   (see Figure 4-D)

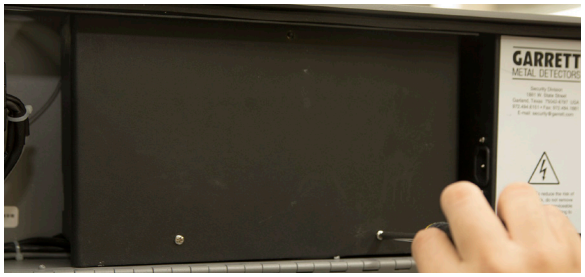


Figure 4-D

4. Follow the schematic drawing for models that do not already include drill hole indications (see Figure 4-E). Drill quarter-inch (.25″) hole in the detection housing top. Use caution to prevent any metal shavings from falling inside the unit during this step.

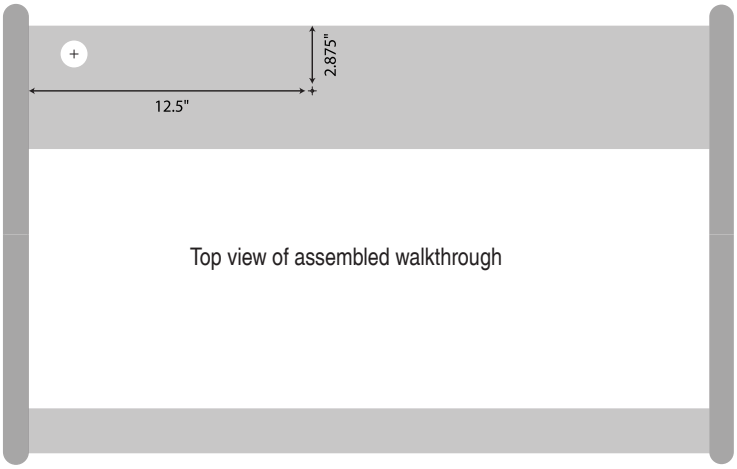
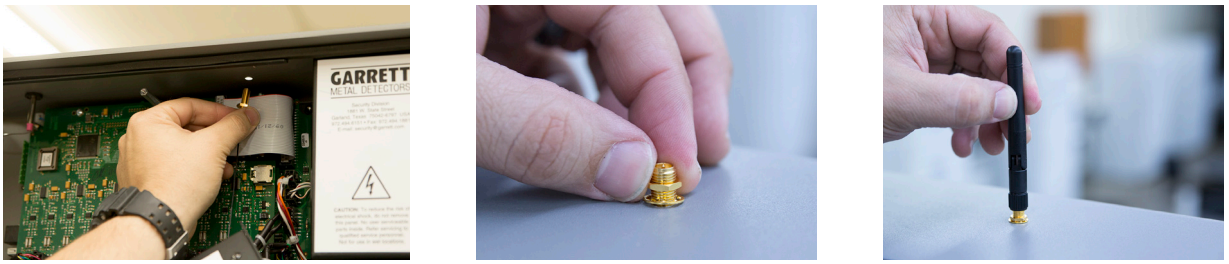


Figure 4-E

5. Mount the antenna through the top of the detector housing. Tighten washer and nut, then screw in the antenna. (see Figure 4-F)



Figures 4-F

6. Replace circuit board shield using the two bottom screws. Use the top screw to mount the new iC Module. (see Figure 4-G)

Figures 4-G

7. Plug one end of the power / data cable into the port on the controller circuit board. Listen for a click to ensure proper connection. (On earlier versions of the PD 6500*i*, it is necessary to remove the controller cover to make this connection). (see Figure 4-H)

Figures 4-H

8. Insert the free end of the Power/Data Cable into the port labeled "From Metal Detector" on the iC Module. Click to ensure proper connection. (see Figure 4-I)

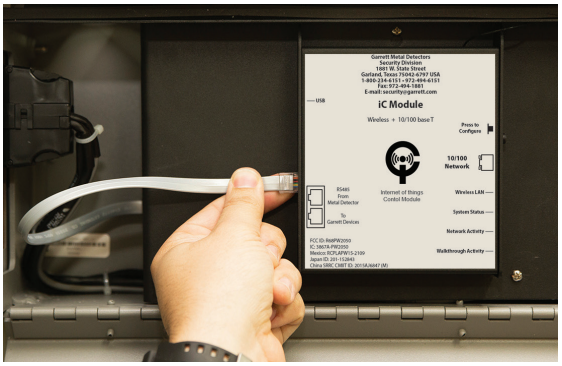


Figure 4-I

9. Add Transmitter ID label below the product label on the detection housing. (see Figure 4-J)

Figure 4-J

10. Replace the power cord. (see Figure 4-K)

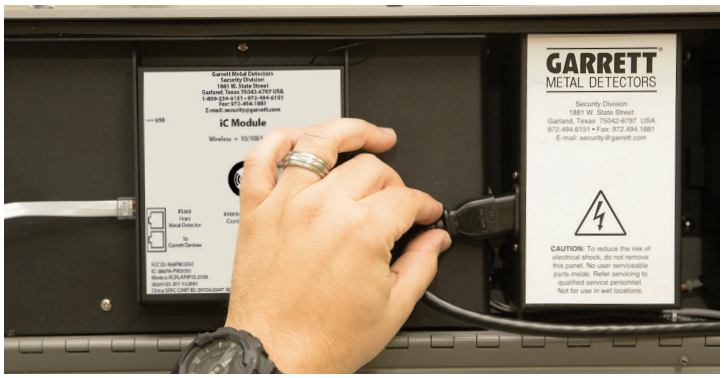


Figure 4-K

11. This concludes the hardware installation. The unit will be turned on in Section 6. Make note of the naming convention and location of connections and LEDs on the front of the unit as reference.

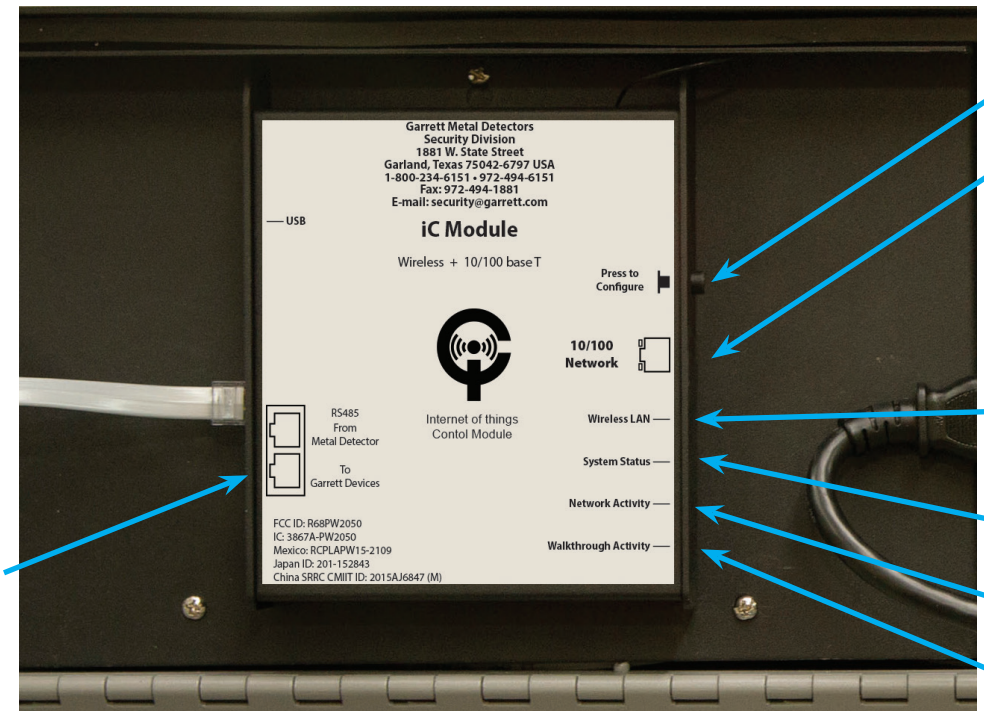


Figure 4-L

5.0 SOFTWARE INSTALLATION

Each iC Module ships with a USB drive that contains software needed for connecting and accessing the iC Module.

Laptop / PC Requirements

- USB drive
- Network Interface Card (NIC)

Install Software

The following steps are required to install the Client Software on your laptop or desktop PC.

Install the Java file from the USB drive that ships with the product:

1. Insert USB drive into the Laptop/PC's USB port.
2. Locate the USB drive on your Laptop/PC.
3. Select the Java file, jxxxxx.exe > Click Open > Click Run and follow the setup instructions.

Copy CMA Connect Software to Local PC hard drive.

1. Access the files on the USB drive.
2. Copy the "CMA Connect" folder to your hard drive. This folder can go anywhere on your local hard drive (C:, D:). If you have a specific folder for all your software (e.g."Software"), it is a good idea to copy the CMA Connect folder to this folder. If not, you can copy it to the root of the chosen partition as well (C:\ or D:\). Note: Your computer's user security permissions and policies decide where you can or cannot copy the CMA Connect folder.
3. Close all windows and remove the CMA Connect USB drive from the Laptop/PC's USB port.
4. Right click on desktop > click New > Shortcut > Browse.
5. Select the CMA.jar in the CMA Connect folder you installed.
6 Click OK > Next > Finish. Shortcut is now located on the PC desktop.

Note: It is not necessary to reboot the computer to run this software.

6.0 ACCESSING THE IC MODULE DIRECTLY

Once all the hardware has been installed on the iC Module from Section 4.0 and the Client software from Section 5.0, the iC Module will need to be configured. In order to configure the module we will first need to access each iC Module discretely using a direct connection.

The connection to the iC Module includes the following tasks:

- Power on the walk-through and iC Module
- Connect to the iC Module
- Enable web configuration
- Access web page

Power on the Walk-Through and iC Module

Ensure that the Power/Data cable is connected and turn on power to the walk-through metal detector by pushing the "On-Operate-Test" button on the front of the control panel. This will power on the iC Module. Once ON, the iC Module will take a few minutes to boot up before it can be accessed. Once the "Walkthrough Activity" LED stays solid red, proceed to the next step.

Connect to the iC Module

Connecting directly to the iC Module will allow you to access the iC Module's web page and configure your wired or wireless connection settings needed to access the module on your network. Initially, each iC Module ships with a factory assigned IP address, 192.168.0.192/32. This IP address will be used to make a direct connection with the module using a Laptop for the first time.

The following steps will allow a direct connection from your laptop to the iC Module.

1. Disable your wireless network connection temporarily on your laptop.
2. Use an Ethernet cable to connect one end to the 10/100 Network connection on the iC Module and the other end to the Ethernet LAN connection on your laptop.

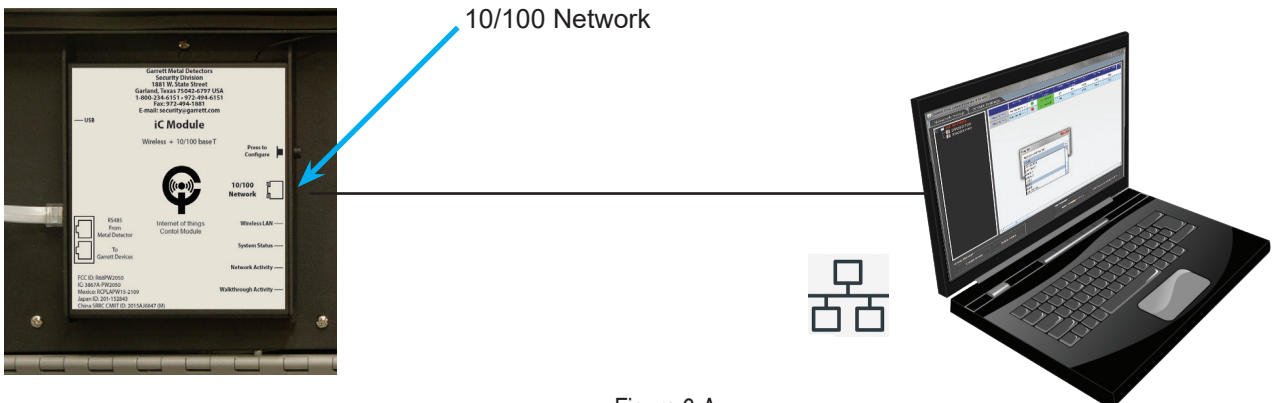


Figure 6-A

3. With the direct connection between the iC Module and the laptop, take note of your existing laptop settings and modify the laptop IP address so it is in the same network as the iC Module. For example, since the iC Module ships with an IP address of 192.168.0.192/32, Garrett suggests setting your laptop IP address to 192.168.0.10. It is critical this is done in order to proceed through the following sections. Please contact your local IT administrator for assistance in modifying your laptop's IP address. If this same laptop will be used to access the iC Module through the LAN, it will be necessary to modify the laptop back to its previous settings.

4. If the direct connection does not work, please reference section 8 "Troubleshooting Network Connectivity to iC Module", "Factory Reset".

Enable Web Configuration

Each iC Module has a web page for configuration that can be accessed through Google Chrome. The iC Module is shipped with the web page disabled for security reasons. In order to configure settings inside the module, the web page must be enabled first.

Press and release the "Press to Configure" button on the right side of the iC Module until the "Walkthrough Activity" LED flashes once to enable the Web Configuration page. This should only take a second for it to blink once. It may take up to 30 seconds for the configuration page to become available before your Google Chrome browser can access it. Reference Table 2.1 for LED Summary.

Once the "Network Activity" light on the side of the module blinks once per second, the web page is enabled and ready to be accessed.

Note: Pressing and releasing the button twice will enable the Wireless Access Point and reboot. Pressing and releasing the button three times will make the iC Module reboot immediately. Reference Table 2.2 for Button Function Summary.

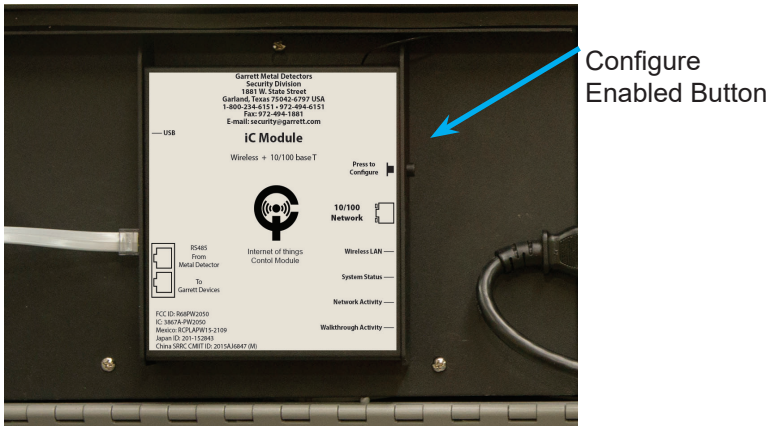


Figure 6-D

Access the Web Page

The web page will need to be accessed by logging into the page with credentials. Once logged into the page you will need to change the time server, change the time zone, and set the static IP address for your Ethernet network.

With the Laptop IP address in the same network as the IP address of the iC Module, the IP address of the iC Module will be used to access the devices web page. It is recommended that the Wi-Fi access to the laptop is disabled temporarily.

Logging into Web Page

Once the device's configuration web page has been enabled, you can access the device's settings by navigating to its IP address using Google Chrome. While still directly connected to the device with an Ethernet cable, type in the IP address (iC Module default IP address 192.168.0.192) into your address bar and press enter. The web page will display an authentication window to log in.

The default credentials to log in are:

Username: admin
Password: PASS

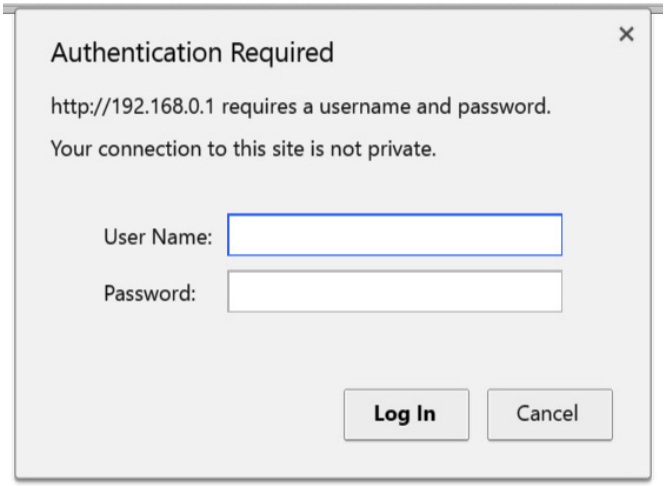


Figure 6-E

Once all configuration settings have been set in the following sections, it is recommended to return to this section and change this to a User Name and Password per your local IT Administrator guidelines.

Note: If the page does not load or appears unavailable, verify that Google Chrome is the web browser and repeat step. Also verify that the "Network Activity" LED is blinking once per second indicating that the web page is ready to be accessed. If it is not blinking once per second, refer to previous section on **Enable Web Configuration** to access the web page. Reference Table 2.1 for LED Summary.

7.0 CONFIGURATION - WIRED OR WIRELESS CONNECTION

The iC Module requires some configuration prior to use such as time server setting, disabling DHCP, setting static IP address and creating a profile if operating for wireless.

Change Time Server / Change Time Zone
On the web configuration page, navigate to:
Administration (on top menu) ⊚ Clock (on left)
(see Figure 7-A)
To change date and time, enter your preferred network time server information into the box labelled "NTP Server". If you do not have a preferred network time server, then "pool.ntp.org" is used by default.

To change the time zone, use the drop down to select region first, then your location.

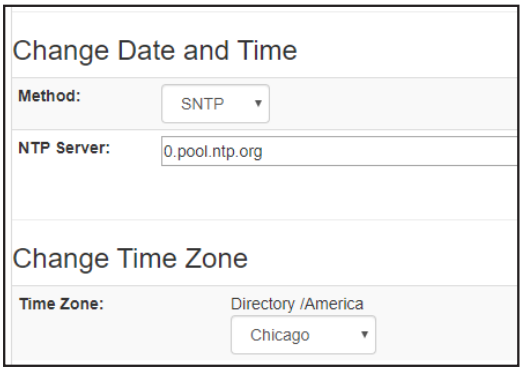


Figure 7-A

Configuration for Wired 10/100Base-T Operation

Disabling Wired DHCP
The current Garrett Client software does not support DHCP so a static IP address must be assigned. DHCP must be Off for wired connections.

Disable wired DHCP from the web page, navigate to:
Network (top menu) ⊚ Wired Network ⊚ Interface ⊚ Configuration (left side)
Set DHCP Client to "OFF"

Figure 7-B

Setting Wired Static IP Address
A static IP address will be required to access the iC Module for wired and wireless operation.

Navigate to: Network (top menu) ⊙ Wired Network ⊙ Interface ⊙ Configuration (left side)
To set the static IP address, enter your desired IP Address and Default Gateway.
To set the subnet mask, use CIDR format in the IP Address field.
For example:

For desired IP Address 192.168.0.10 and the Subnet Mask 255.255.255.0
Enter 192.168.0.10/24 in the IP Address field with the Default Gateway 192.168.0.1 as shown in Figure 7-C.

Figure 7-C

Make sure that the IP Address and Default Gateway are on the same network, otherwise the device will become unreachable and requires a factory reset. **Once all changes have been made, scroll to the bottom of the page and select the "Submit" button to save changes.**

Note: If the desire is to operate the module using only a wired connection, then the wireless feature of the iC Module can simply be disabled.
Navigate to: Network (top menu) ⊙ Wireless Network ⊙ Interface ⊙ Configuration (left side)
To disable wireless, select the "Disabled" radio button and select the "**Submit**" button to save changes.

Rebooting the iC Module
Once all the changes have been made (date and time, the time zone, disabling DHCP, setting the static IP address, and disabling wireless) the device will need to be rebooted.

On the web configuration page, navigate to:
Administration (top menu)
To reboot the device, select "Reboot" under the
Reboot Device header.

Figure 7-D

Note: Rebooting the iC Module will disable access to the web page. To access the web page of the module, reference **Enable Web Configuration in** Section 6.0.

Configuration for Wireless LAN Operation

Disabling Wireless DHCP

The current Garrett Client software does not support DHCP so a static IP address must be assigned. By default, the iC Module ships with wireless DHCP enabled. DHCP should be Off for wireless connections unless a static IP address is reserved by the network for each MAC address where the IP address is same every time.

Disable wireless DHCP from the web page, navigate to:
Network (top menu) ⊚ Wireless Network ⊚ Interface ⊚ Configuration (left side)
Set DHCP Client to "OFF"

Setting Wireless Static IP Address

The process for setting up the IP address for a wireless network is identical as the wired network with the exception of the menu location.
Navigate to: Network (top menu) ⊚ Wireless Network ⊚ Interface ⊚ Configuration (left side)
To set the static IP address, enter your desired IP Address and Default Gateway.
To set the subnet mask, use CIDR format in the IP Address field.
For example:

> For desired IP Address 192.168.0.10 and the Subnet Mask 255.255.255.0
> Enter 192.168.0.10/24 in the IP Address field with the Default Gateway 192.168.0.1 as shown in Figure 7-C.

Make sure that the IP Address and Default Gateway are on the same network, otherwise the device will become unreachable and requires a factory reset. **Once all changes have been made, scroll to the bottom of the page and select the "Submit" button to save changes.**

Setting up for Wireless Network Connection

In order to set up the iC Module for use in a wireless network, a profile must be established.
Navigate to: Network (top menu) ⊚ WLAN Profiles (left side)
Add a new profile name into the empty section titled "Name:" and click submit.

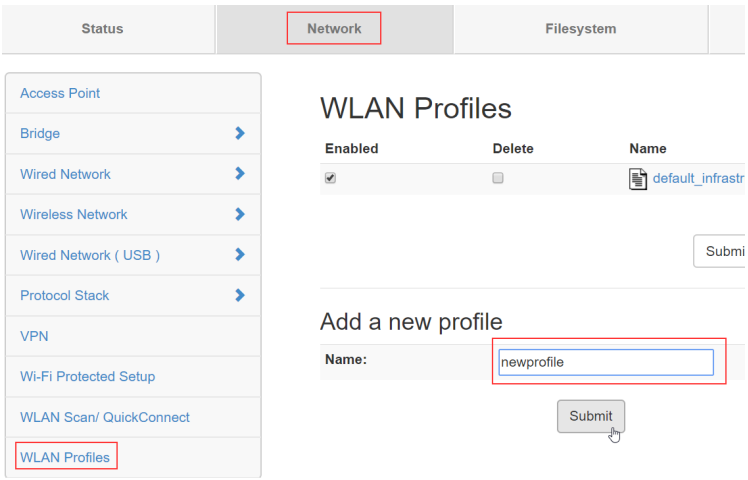


Figure 7-E

The name will appear in the "WLAN Profiles" section as a link located just above "Add a new profile" section. Select the new name link that was created (in our example we have used "new-profile" as the name) and a new page will show up (see Figure 7-F). Setup the SSID, Security Configuration and Passphrase as needed and click "**Submit**".

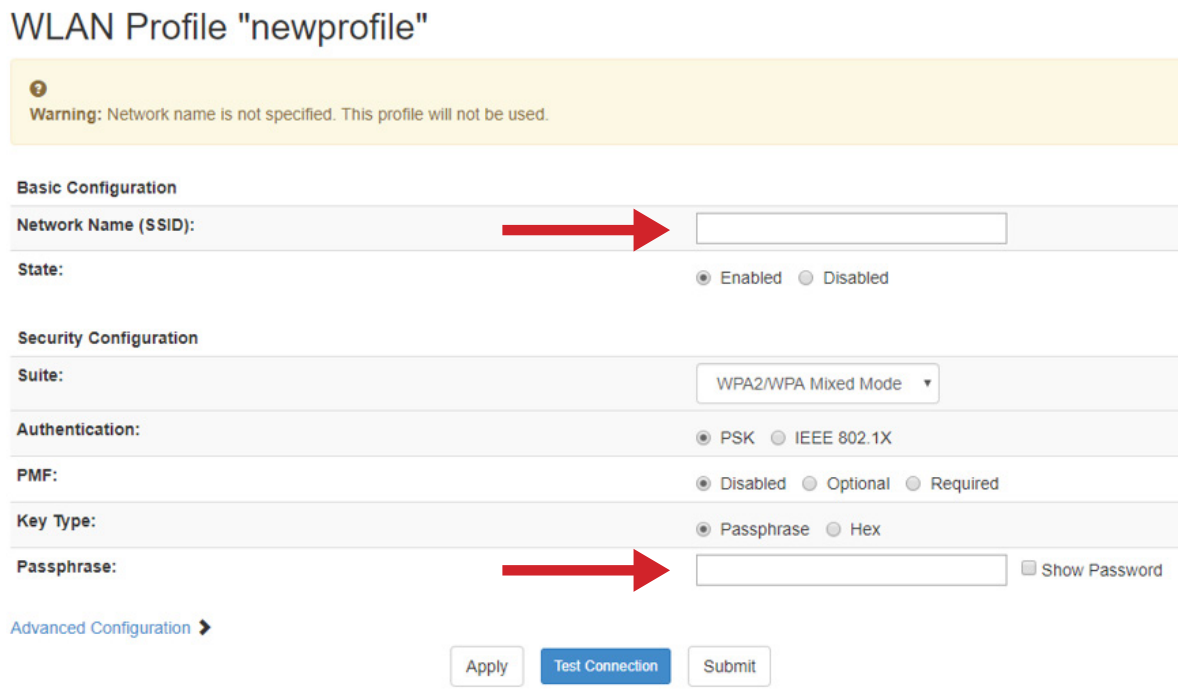


Figure 7-F

Rebooting the iC Module

Once all the changes have been made (date and time, the time zone, ensure DHCP is disabled, setting the static IP address, and disabling wireless) the device will need to be rebooted.

On the web configuration page, navigate to:
Administration (top menu)
To reboot the device, select "Reboot" under the Reboot Device header.

Figure 7-G

The "Walkthrough Activity" LED will turn solid red when the device is done rebooting.
Once the device is rebooted, the Wireless LAN LED on the side of the module should be solid red indicating that a wireless network connection has been successfully established between the iC Module and your network. The following section 8.0 will help to find the device on your network using the Client Software. Reference Table 2.1 for LED Summary.

Note: Rebooting the iC Module will disable access to the web page. To access the web page of the module, reference **Enable Web Configuration** in Section 6.0.

Exporting a Profile

For setting up multiple iC Modules, it is possible to export the profile of a single iC Module and import that profile into additional iC Modules to expedite the configuration process for individual units.

Navigate to: Administration (top menu) ◎ XML ◎ Export Configuration (left side)
Select the "Download (from link)" radio button.
Under Groups to Export section select the "Clear All" button.
Check the "Clock" group
Check the WLAN profile group with the profile name created earlier in the **Setting up for Wireless Network** section. Our example name was "newprofile" so select "WLAN Profile: newprofile" group.
Select the "Export" button and save the file to a file location. The file name will be clone.xcr and should not be modified.

Importing a Profile

Before an exported profile can be imported, it must first be modified. For security reasons, the passphrase that was entered in the previous section does not export and needs to be reentered. Open the clone.xcr file using windows Notepad and search for the SSID that was created in the previous section. In our example we will use "garrett-net" as an example SSID with "WTMD-123" as the passphrase. Once you've found the SSID, you will find that a few lines down the passphrase was replaced with the following text, "<!-- configured and ignored -->", as seen in Figure 7-H.

```
<configitem name = "basic">
    <value name = "network name">garrett-net</value>
    <value name = "state">enable</value>
</configitem>
<configitem name = "advanced">
    <value name = "tx power maximum">31 dBm</value>
    <value name = "power management">disable</value>
</configitem>
<configitem name = "security">
    <value name = "suite">WPA2-WPA Mixed</value>
    <value name = "key type">Passphrase</value>
    <value name = "passphrase"><!-- configured and ignored -->
</value>
    <value name = "wep authentication">Open</value>
    <value name = "wep key size">40</value>
```

Figure 7-H

Simply delete this phrase and replace it with the correct passphrase, which is “WTMD-123” in this example.

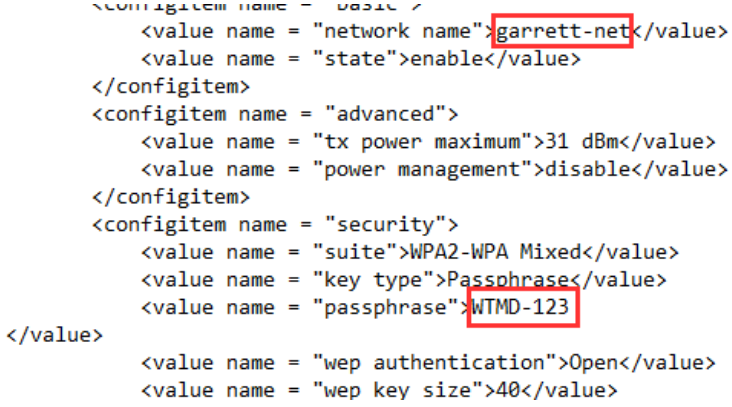


Figure 7-I

Once the file is modified with the correct passphrase, save the file (do not change the file name, “clone.xcr”) and close Notepad.

Now that the exported profile has been modified, there are two ways to import the file into other units; manual import using the web page or auto import using a USB thumb drive. We recommend that you try to import using the web page first with the clone.xcr file you just modified. Use the same unit name where the file was exported. This will ensure the file was exported and modified correctly before loading onto other units.

Manual import using web page

You will first need to establish a connection to a new iC Module following the same steps in Section 6.0 **Accessing the iC Module Directly**. Once the web page has been accessed on the new module, you will need to import the file that was just recently modified in the previous section.

Navigate to: Administration (top menu) ⊚ XML ⊚ Import Configuration (left side), Select the “Configuration from External file” radio button in the “Import” section and click “Choose File” in the “Import configuration from (entire) external XCR file:” section. Navigate to the file that was exported, click OK and click the “Import” button to import.

Repeat the process for additional iC Modules that will be accessed with the same network credentials. Each individual iC Module will still have to have a new IP address assigned (reference Figure 7-C).

Auto import using USB drive

This method is extremely useful when updating multiple walk-throughs. Once it’s been verified that the exported clone file is good and can be used, copy the clone.xcr file onto a USB drive. We recommend using the USB drive that shipped with the product and saving the file in the top level folder. Reference Table 2.1 for LED Summary.

Use the following steps to configure a new walk-through with a USB:

1. Find the next walk-through you want to configure and turn on power by pushing the "On-Operate-Test" button on the front of the control panel.
2. Open the back door of the detector head and find the iC Module. Locate the "Walkthrough Activity" LED on the right side of the iC Module. Wait for the "Walkthrough Activity" LED to turn and stay solid red before proceeding.
3. Once the "Walthrough Activity" LED turns solid red, insert the USB drive into the left side of the iC Module.

Note: If the USB drive is inserted before the LED is solid red, the operation will not execute correctly and you will need to start over at step 1.

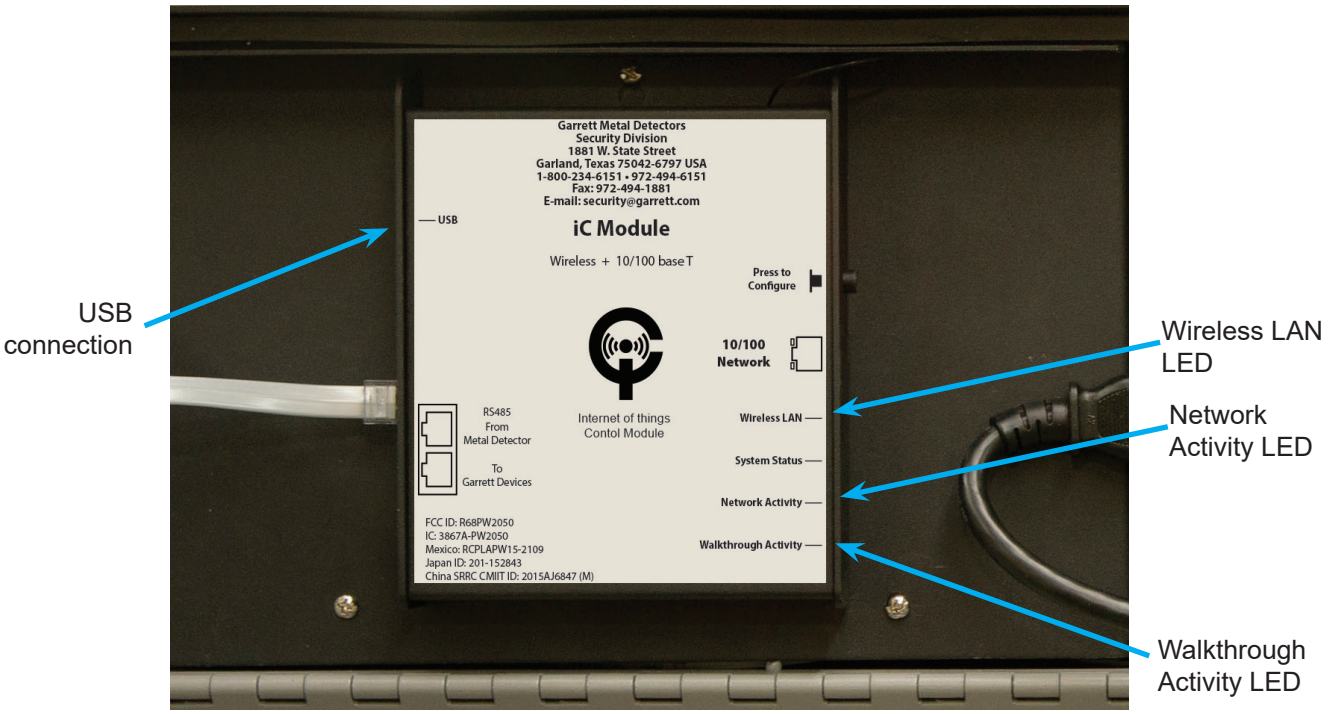


Figure 7-J

4. The "Network Activity" LED will start to blink 3x/second which means the USB is being used to upload the clone file into the iC Module. Do not unplug the USB at this time.
5. Once the "Network Activity" LED turns solid, the USB operation is complete and the clone file has been uploaded into the iC Module. It is now safe to unplug the USB drive.
6. To configure additional walk-through units, repeat steps 1-5.

If the file loaded successfully, the "Wireless LAN" LED will light up and turn solid indicating that a connection to the wireless network has been established. If it does not turn solid, then check that the wireless network is functioning and in range. Refer to Section 8. **Troubleshooting Network Connectivity to iC Module** for further troubleshooting techniques.

8.0 FINDING THE IC MODULE ON THE NETWORK

Now that the iC Module has been configured to be discoverable on your Local Area Network, we can verify that the module is discoverable through the network using the CMA Client software which was installed earlier in Section 5.0 of this User Manual.

Using the Client to Find iC Module

The following steps will allow you to find the iC Module using the CMA Connect Client

1. Disconnect the Ethernet cable from your iC Module that was connected to your laptop.
2. Launch the CMA Connect client software from your laptop or desktop PC. If using the same laptop that connected directly to the iC Module in Section 5 for configuration, make sure to put back in the place the previous network settings if they were changed prior to modifying the IP address.
3. Enter the Client using Full Access with Password "admin"
4. From the Network Setup tab, select "Find WTMDs" from the left side. The iC Module will show up in the "Known WTMDs" section of this tab.
5. If the iC Module does not show up, it may be possible to add it manually using the "Add WTMD" button on the left and entering the IP address.

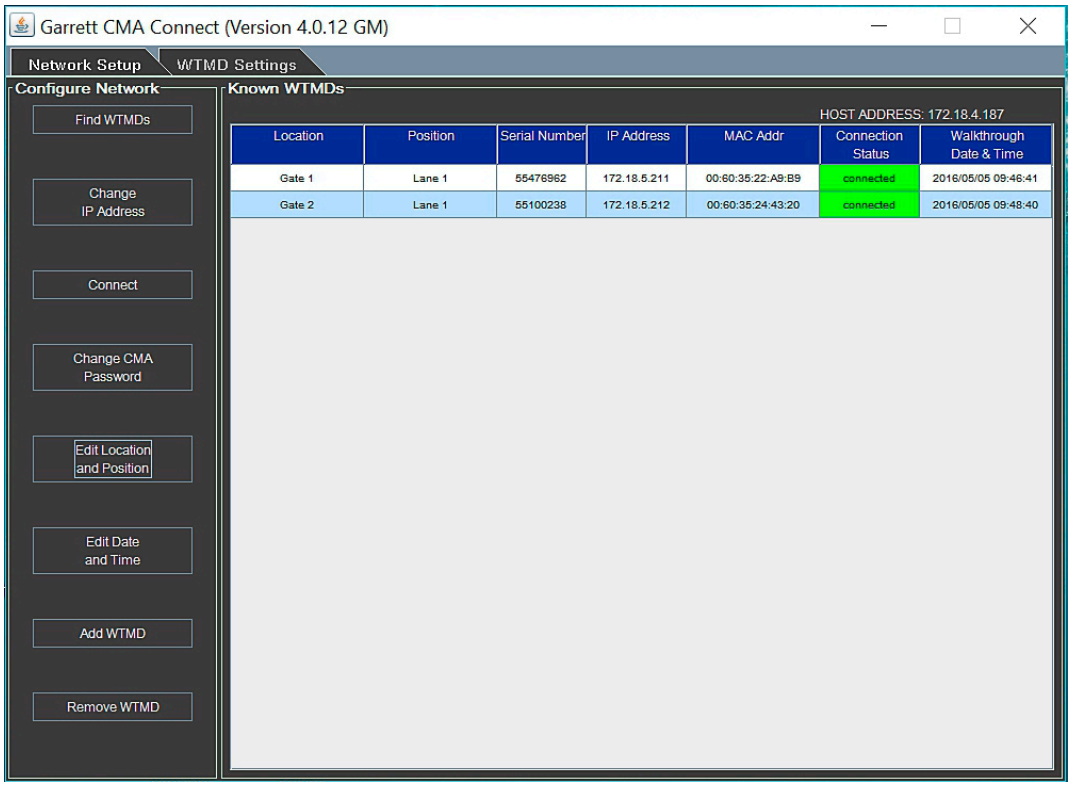


Figure 8-A

Troubleshooting Network Connectivity to iC Module

Garrett is responsible for helping establish a connection from the iC Module to the customer network. However, it is the responsibility of the customer to establish a connection from a laptop or desktop PC to the iC Module through their network. Some possible issues that may arise are listed below:

Factory Reset - If the direct Ethernet connection is not connecting to the iC Module, a factory reset may be required. Performing this operation will clear all log files on the iC Module. On an empty flash drive, create a blank text file and name it "factory_reset.txt". Power on the iC Module and wait until the Walkthrough Activity LED is solid red, then plug in the flash drive. Remove the flash drive when the Walkthrough Activity LED is blinking. Now, the Ethernet IP address is reset to 192.168.0.192 and the Wireless IP address is reset back to DHCP enabled with no IP address.

Wireless Connection - For wireless connection, always check if the Wireless LAN LED on the side of the iC Module is solid red. If it is not solid red, then reference the profile created in Section 7.0 Setting up for Wireless Network Connection and check that the SSID and Passphrase were entered correctly. If the LED is solid red, but you cannot connect using the Client, then the device is connected to the wireless network, but something in the network is preventing the Client from discovering the device. Below are some network related instances that may contribute this issue.

Matching SSID - Often times the laptop with the CMA Connect client is connected to a different VLAN / subnet of the network than the iC Module. Either move the CMA client software files to a laptop or desktop PC that uses the same VLAN / subnet and same SSID as the iC Module or reconnect the laptop or desktop to the same network with the same VLAN / subnet and SSID as the iC Module.

Verify IP Address and Default Gateway - It is possible the IP address and Default Gateway were typed in incorrectly and are not on the same network. Verify settings from the web page.

Broadcasting - Our client software uses broadcasting to communicate with the iC Module. If this is disabled, the unit will not show up on the client when the "Find WTMDs" button is used unless its IP address is manually added using the "Add WTMD".

Routing Across Networks - It is possible to have your iC Modules on a separate VLAN / subnet as the laptop or desktop PC from which you plan to run the Client. However, in this scenario you must ensure that this computer has a route to the IP addresses of your iC Modules. Furthermore, you will not be able to automatically discover your devices on the host device, using the "Find WTMDs" button. Rather, you will need to manually enter the IP addresses of your iC modules using the "Add WTMD" button on the client.

Blacklisted Device - If a MAC address is not registered on the network, it may be blacklisted and unable to communicate to the network, contact your IT department to help resolve this by providing the MAC address assigned to the iC Module. The MAC address is located on the top of the module where "E:" designates the Ethernet MAC address and the "W:" designates the wireless MAC address.

Swapping Out iC Module - If swapping out or replacing an iC Module where the same IP address will be reused for the new module, make sure to reassign the new MAC address to that IP address in your network configuration.

9.0 REGULATORY INFORMATION

Garrett Metal Detector Compliance

Changes or modifications not expressly approved by Garrett Metal Detectors for compliance 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 A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This Class A digital apparatus complies with Canadian ICES-003.
Cet appareil numerique de la classe A est conforme a la norme.

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-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 radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

To satisfy FCC RF Exposure requirements for mobile and base station transmission devices, a separation distance of 20 cm or more should be maintained between the antenna of this device and persons during operation. To ensure compliance, operation at closer than this distance is not recommended. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

EU Declaration of Conformity

Company name Garrett Metal Detectors
Postal address: 1881 W. State St.
Postcode and City: 75042 Garland, TX, USA
Telephone number: 972-494-1881
E-Mail address: bobp@garrett.com

Declare that the DoC is issued under our sole responsibility and belongs to the following product:

Apparatus model/Product: iC Module Interface
Type: Wireless + 10/100Base T

Object of the declaration (identification of apparatus allowing traceability; it may include a colour image of sufficient clarity where necessary for the identification of the apparatus):
iC Module Interface Wireless + 10/100Base-T

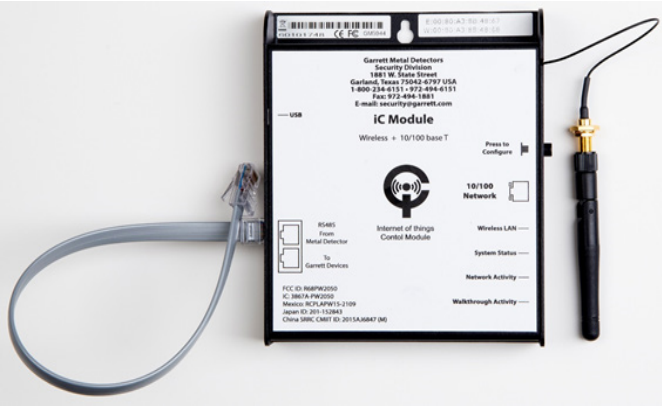


Figure 9-A

The object of the declaration described above is in conformity with the relevant Union harmonisation legislation:

Safety: EN 60950-1, 3rd edition (2012) - Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use.
RoHS 2011/65/EU
EMC Directive 2014/30/EU
Radio Equipment Directive 2014/53/EU

The following harmonised standards and technical specifications have been applied:

Title, Date of standard/specification:
ETSI EN 300 328 V2.1.1:2016
ETSI EN 301 489-1 V2.1.1 (2017-02)
ETSI EN 301 489-17 v:2017
Notified body (where applicable):
Intervention of notified body: None

Signed for and on behalf of:
Garrett Metal Detectors

Robert Podhrasky, Vice President
Garland, TX, USA
Place of issue 2019/11/26

Lantronic Transmitter Compliance

Country Certifications

Country	Specification
USA	FCC Part 15, Subpart B, Class B FCC Part 15, Subpart C 15.247 (WLAN) FCC Part 15, Subpart C 15.247 (BT) FCC Part 15, Supbart E 15.407 (DFS)
Canada	ICES-003:2012 Issue 5, Class B RSS-Gen, Issue 4, November 2014 RSS-102, Issue 5, March 2015 RSS-247, Issue 1, May 2015
Mexico	NOM-121-SCT1-2009
EU	RTTE Directives 1999/5/EC, 2004/108/EEC EN 300 328 V1.9.1 EN 301 489-1 V1.9.2 EN301 489-17 V2.2.1 EN 301 893 V1.8.1 EN 62311: 2008 EN 55022: 2011
Australia, New Zealand N11206	AS/NZS 4268: A1: 2013 AS/NZS 2772.2
Japan	ARIB STD-T66 (v3.7), MIC notice 88 Appendix 43 RCR STD-33 (v5.4), MIC notice 88 Appendix 44 ARIB STD-T71(v6.1), MIC notice 88 Appendix 45
China	SRRC CMIIT ID: 2015AJ6847 (M)

Country Transmitter IDs

Country	Specification
USA FCC ID	R68PW2050
Canada IC ID	3867A-PW2050
Mexico	RCPLAPW15-2109
Japan ID	201-152843
China SRRC	2015AJ6847 (M)

Safety

Country	Specification
World Wide CE0560	CB EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011 In accordance with the council directive 2006/95/EC
US, Canada	UL 60950-1 (2nd Edition)

Federal Communication Commission Interference 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.
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 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.

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

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

Radiation Exposure Statement:

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

Industry Canada statement:

This device complies with RSS-247 of the Industry Canada 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.
Ce dispositif est conforme à la norme CNR-247 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Caution:

(i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to cochannel mobile satellite systems;
(ii) the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit;
(iii) the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and
(iv) Users should also be advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Avertissement:

Le guide d'utilisation des dispositifs pour réseaux locaux doit inclure des instructions précises sur les restrictions susmentionnées, notamment :
(i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
(ii) le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5250 à 5 350 MHz et de 5470 à 5725 MHz doit être conforme à la limite de la p.i.r.e;

(iii) le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas;
(iv) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Europe – EU Declaration of Conformity

LANTRONIX

7535 Irvine Center Drive, Suite 100, Irvine, CA 92618

EU DECLARATION OF CONFORMITY

This declaration of conformity is issued under the sole responsibility of the manufacturer.

Object of the declaration			
Product Information	Product Name: PremierWave 2050		
	Model	SW Version (Radio FW)	HW Version
	PW 2050	6.37.42.9	11 (or later)

The object of the declaration described above is in conformity with the relevant Union harmonisation legislation:

- References to the relevant harmonised standards used or references to the technical specifications in relation to which conformity is declared

Radio Equipment Directive 2014/53/EU
EN 300 328 V2.1.1
EN 301 489-1 V2.1.1
EN 301 489-17 V3.1.1
EN 301 893-1 V2.1.1
EN 62311:2008
EN 60950-1:2006 + A1:2010 +A12:2011 +A2:2013

The notified body, TUV SUD BABT, performed a conformity assessment of the technical construction file and issued certificate BABT-RED000307 i02.01.

Signature: Daryl R. Miller **Date:** 8-29-17

Name: Daryl R. Miller

Title: VP of Engineering, Lantronix, Inc.

CE 0560

cs	Česky [Czech]	Lantronix tímto prohlašuje, že tento PremierWave 2050 enterprise Wi-Fi IoT module je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
da	Dansk [Danish]	Undertegnede Lantronix erklærer herved, at følgende udstyr PremierWave 2050 enterprise Wi-Fi IoT module overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
de	Deutsch [German]	Hiermit erklärt Lantronix, dass sich das Gerät PremierWave 2050 enterprise Wi- Fi IoT module in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
et	Eesti [Estonian]	Käesolevaga kinnitab Lantronix seadme PremierWave 2050 enterprise Wi-Fi IoT module vasta vust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakoha stele sätetele.
en	English	Hereby, Lantronix, declares that this PremierWave 2050 enterprise Wi-Fi IoT module is in com pliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
es	Español [Spanish]	Por medio de la presente Lantronix declara que el PremierWave 2050 enterprise Wi-Fi IoT module cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
el	Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Lantronix ΔΗΛΩΝΕΙ ΟΤΙ PremierWave 2050 enterprise Wi-Fi IoT module ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
fr	Français [French]	Par la présente Lantronix déclare que l'appareil PremierWave 2050 enterprise Wi-Fi IoT module est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
it	Italiano [Italian]	Con la presente Lantronix dichiara che questo PremierWave 2050 enterprise Wi- Fi IoT module è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
	Latviski [Latvian]	Ar šo Lantronix deklarē, ka PremierWave 2050 enterprise Wi-Fi IoT module atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
	Lietuvių [Lithuanian]	Šiuo Lantronix deklaruoja, kad šis PremierWave 2050 enterprise Wi-Fi IoT module atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
nl	Nederlands [Dutch]	Hierbij verklaart Lantronix dat het toestel PremierWave 2050 enterprise Wi-Fi IoT module in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
mt	Malti [Maltese]	Hawnhekk, Lantronix, jiddikjara li dan PremierWave 2050 enterprise Wi-Fi IoT module jik konforma mal‖tiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
hu	Magyar [Hungarian]	Alulírott, Lantronix nyilatkozom, hogy a PremierWave 2050 enterprise Wi-Fi IoT module meg felel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
pl	Polski [Polish]	Niniejszym Lantronix oświadcza, że PremierWave 2050 enterprise Wi-Fi IoT module jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
pt	Português [Portuguese]	Lantronix declara que este PremierWave 2050 enterprise Wi-Fi IoT module está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
sl	Slovensko [Slovenian]	Lantronix izjavlja, da je ta PremierWave 2050 enterprise Wi-Fi IoT module v skladu z bistveni mi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.

RoHS, REACH, and WEEE Compliance Statement

Please visit http://www.lantronix.com/legal/rohs/ for Lantronix's statement about RoHS, REACH and WEEE compliance.

10.0 WARRANTY AND SERVICE INFORMATION

Garrett Electronics, Inc. ("Garrett") warrants that each piece of security equipment manufactured by Garrett is protected by the following limited parts and labor warranty for a period of 24 (twenty-four) months (the "Warranty"). During this 24-month period, Garrett will inspect and evaluate all equipment returned to its authorized repair station or factory to determine if the equipment meets Garrett's performance specifications. Garrett will repair or replace at no charge to the owner all parts determined faulty. This Warranty does not cover batteries nor any and all failures caused by abuse, tampering, theft, failure due to weather, battery acid or other contaminants and equipment repairs made by an unauthorized party.

THIS WARRANTY IS EXPRESSLY IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING THE WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THE BUYER ACKNOWLEDGES THAT ANY ORAL STATEMENTS ABOUT THE MERCHANDISE DESCRIBED IN THIS CONTRACT MADE BY THE SELLERS' REPRESENTATIVES, IF ANY SUCH STATEMENTS WERE MADE, DO NOT CONSTITUTE WARRANTIES, SHALL NOT BE REPLIED UPON BY THE BUYER, AND ARE NOT A PART OF THIS CONTRACT FOR SALE. THE ENTIRE CONTRACT IS EMBODIED IN THIS WRITING. THIS WRITING CONSTITUTES THE FINAL EXPRESSION OF THE PARTIES' AGREEMENT AND IS A COMPLETE AND EXCLUSIVE STATEMENT OF THE TERMS OF THIS AGREEMENT.

The parties agree that the Buyers' sole and exclusive remedy against Seller shall be for the repair and replacement of defective parts. The Buyer agrees that no other remedy (including, but not limited to, incidental and consequential damages for lost sales, lost profits, injury to person or property) shall be available to him.