

IN-COMMAND® First-In Tablet

User Manual



IN-COMMAND[®] First-In Tablet

User Manual

Table of Contents

NFPA 1982-2018ed. RF PASS Requirements	3
Tablet Requirements	4
Installing the IN-COMMAND Android App	6
Configuring the App for Operation	8
Working with Name Files	10
Programming Device IDs	14
Starting and Stopping an Incident	16
The Incident Display	20
The Incident Data Log	26
File Management	28
Incident Alarm Monitor Familiarization	30
Configuring the WIFI Access Point on the Incident Alarm Monitor	33
Configure the WIFI Connection	37

IN-COMMAND® First-In Tablet

Emergency Signaling Accountability System

System Components



**Customer
Tablet**

with

**In-Command®
First-In Tablet App**



Incident Command Monitor



TPASS®5



SuperCELL® SC500



TPASS® Micro Repeater

IMPORTANT!

NFPA-1982, 2018 edition, RF PASS Requirements:

The NFPA-1982, 2018 edition, includes minimum requirements for RF PASS systems. The use of the In-Command® software under its default installed-configuration is compliant with NFPA requirements for RF PASS systems.

The host Tablet running the In-Command® software must have its speakers enabled and volume turned up to a level that can be heard in loud fire ground environments.

The default installation of the In-Command® Tablet software uses audio files to activate or 'play' on the host Tablet's speakers for various functions including 'RF PASS alarm', 'RF PASS Evacuation alarm initiated' and 'loss-of-signal alarm'. The In-Command® Tablet software allows custom audio files to be used in place of the default audio files, however any change to these audio files may jeopardize NFPA compliance if they are not of a suitable nature.

Caution should be used if the default audio files are changed.

Tablet Requirements

Hardware:

- Android 10” Tablet
- ARM Cortex-A series processor
- ARMv7 Instructions
- Neon Technology
- Screen Resolution 1280x800 minimum recommended
- WIFI
- 2GB RAM (or greater) Required

** Not Compatible with Intel ATOM architecture.*

Operating Systems:

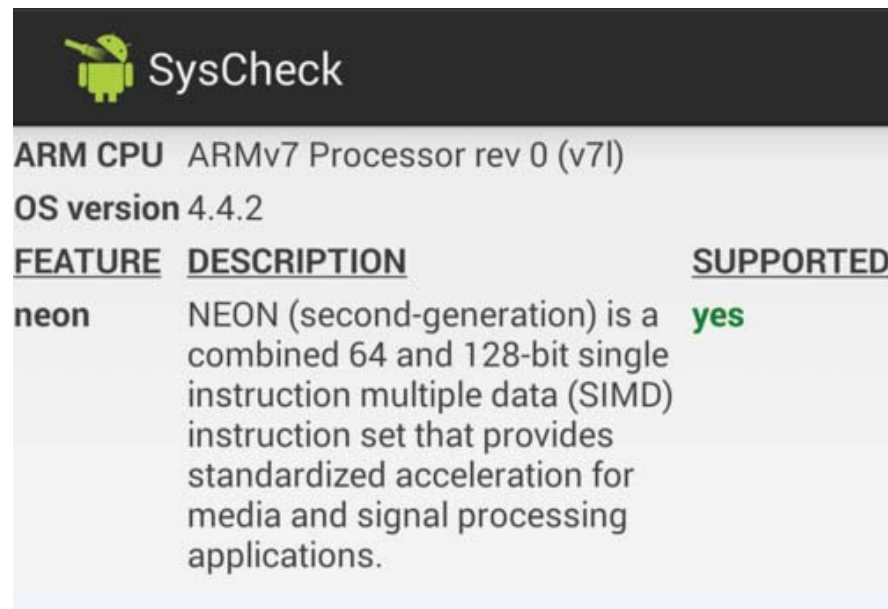
- Android 4.1.2 Jelly Bean or newer

Tablet Requirements

If you are unsure if your device has the required features, you can get SysCheck from the Google Play store and run it on your device:

NOTE: SysCheck is free, has no ads, and does not require special privileges to run.

You should see a screen similar to the following:



The screenshot shows the SysCheck app interface. At the top, there is a green Android robot icon and the text 'SysCheck'. Below this, the system information is displayed: 'ARM CPU ARMv7 Processor rev 0 (v7l)' and 'OS version 4.4.2'. A table follows with three columns: 'FEATURE', 'DESCRIPTION', and 'SUPPORTED'. The first row shows 'neon' as a feature, with a detailed description of NEON and 'yes' in green text in the 'SUPPORTED' column.

<u>FEATURE</u>	<u>DESCRIPTION</u>	<u>SUPPORTED</u>
neon	NEON (second-generation) is a combined 64 and 128-bit single instruction multiple data (SIMD) instruction set that provides standardized acceleration for media and signal processing applications.	yes

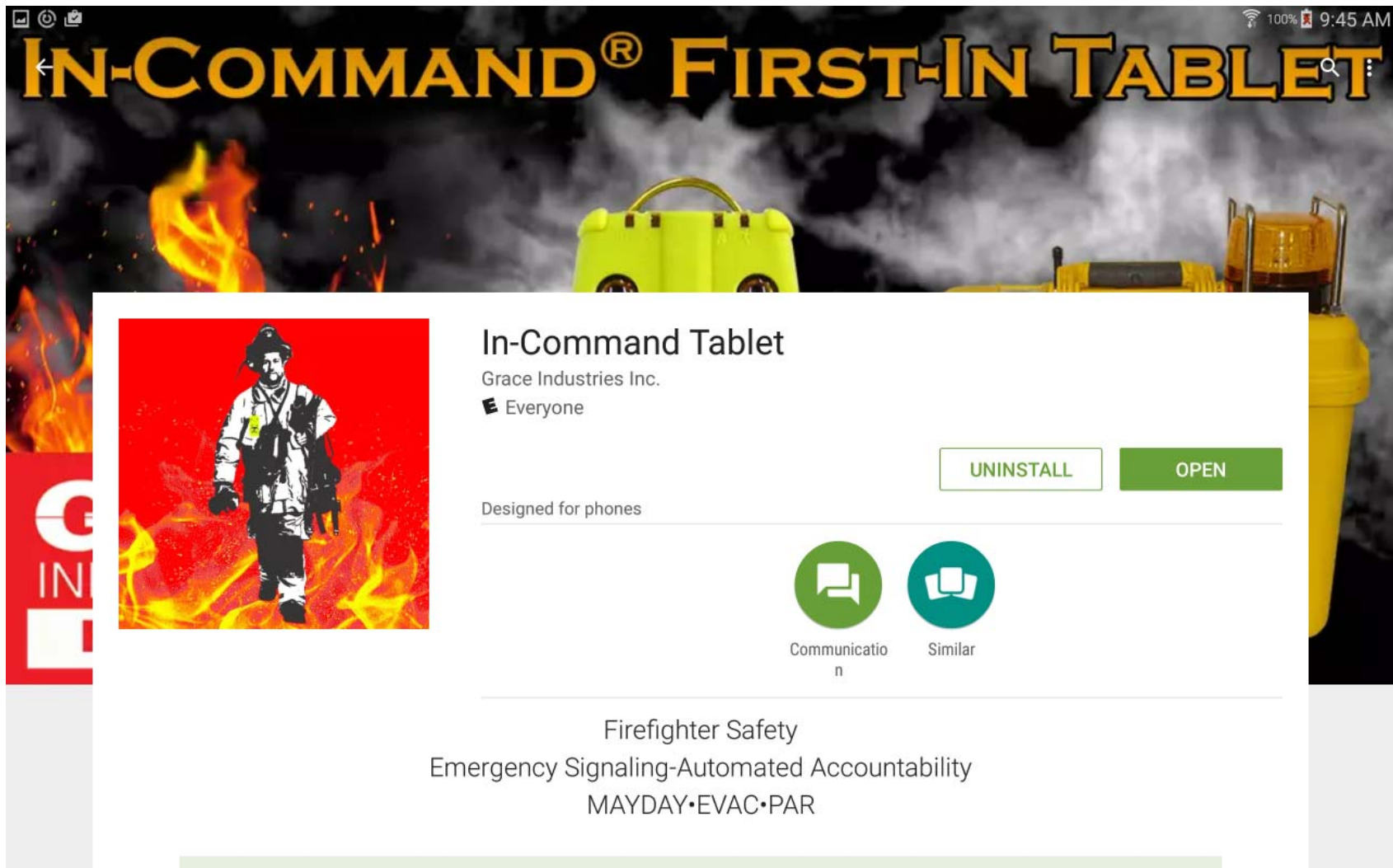
If you see:

- ARM CPU showing ARMv7
- OS Version listed above (or newer)
- NEON is listed as yes

Then the device should work.

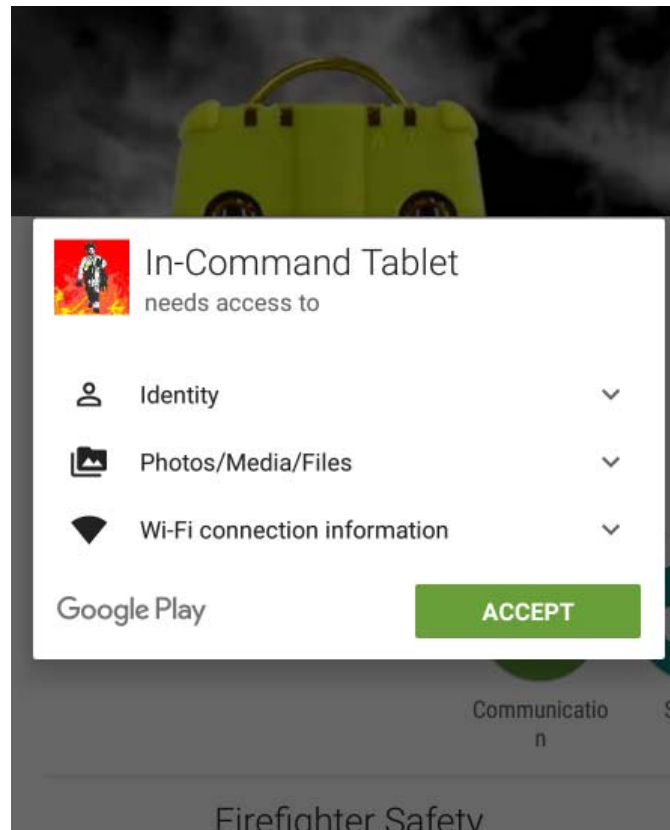
Installing the In-Command® First-In Tablet Android App

Search for “IN-COMMAND” in the Google Play store. Follow the play store instructions to complete the installation.



Installing the In-Command® First-In Tablet Android App

You will need to choose accept when prompted to allow special permissions to the app.



Configuring the App for Operation

TCP Connection

- Run the In-Command® First-In Tablet App and choose the Configuration Tab.
- Under the section TCP Connection, complete the Server IP Address and TCP Port fields using the settings that the Incident Command Monitor has been configured for.
- For More Information See: **Configuring the WIFI Access Point on the Incident Command Monitor.**

The screenshot shows the 'In-Command® First-In Tablet' app interface. The top status bar indicates 100% battery and 1:23 PM. The app title bar shows 'In-Command® First-In Tablet' and 'v1.0653'. The main menu has four tabs: INCIDENT, DATA LOG, NAMES, and CONFIGURATION (selected). The CONFIGURATION screen has a 'Configuration Settings' header. Under the 'TCP Connection' section, the 'Server IP Address' is set to 10.10.100.254 and the 'TCP Port' is 5001. Below this, there are settings for 'No-Signal' (checked) and 'Alarm Monitor' (checked). At the bottom, it shows 'Incident Stopped' and 'Users Online: 0'.

INCIDENT	DATA LOG	NAMES	CONFIGURATION
Configuration Settings			
TCP Connection			
Server IP Address The configured IP Address of the USR Dual Receiver 10 . 10 . 100 . 254			
TCP Port The configured TCP Port for the USR TCP Server 5001			
No-Signal			
Check For No-Signal Does not apply to TPASS5 or SuperPASS 5X 5 Minutes			
No-Signal Timeout Does not apply to TPASS5 or SuperPASS 5X 5 Minutes			
No-Signal Condition Causes Alarm Does not apply to TPASS5 or SuperPASS 5X 60 Seconds			
Alarm Monitor			
Mute Siren The number of seconds to mute the siren 60 Seconds			
Report Unmonitored Alarms			
Incident Stopped			
Users Online: 0			

Configuring the App for Operation

Configure a Name File entry for all of your PASS devices.

A name file entry must exist in order for a TPASS®, SuperCELL®, or Micro Repeater to be identified by the Incident display.

For more information, see: *Working with Name Files*.

Once you have configured TCP and created a name file, basic setup is complete and you can start an Incident. The following configuration items can be changed at any time to adjust the way an incident responds.

No Signal

- Check for No-Signal
This will toggle the No-Signal functionality on and off.
- No-Signal Timeout
When using the No-Signal feature, this setting will allow you to change the amount of time that must elapse before a no-signal condition is reported by the incident.
- No-Signal Condition Causes Alarm
When using the No-Signal feature, the no-signal status icon will always appear when a device meets the no-signal criteria. This setting will force the system to treat a no-signal as an alarm and put the system into an alarm state with visual and audible cues.

Incident Command Monitor

- Mute Siren
When the Incident Command Monitor is in an alarm condition, you can mute the audio on the Incident Command Monitor at any time by pressing the “Clear Alarm” button on the incident display “tools” menu. This configuration setting allows you to set the amount of time that the Incident Command Monitor will be muted for.
- Report Unmonitored Alarms
If a TPASS® goes into alarm but is not being monitored because a name file entry was not created, the Incident Command Monitor will go into alarm but the In-Command app will not. If you check this setting, the unmonitored alarm will be reported in the incident similar to the way a normal alarm is reported.

General

- Use Real Time Clock Set Message
The RadioH platform provides a means to synchronize the device clock for all devices in use. Check this option to use this feature.

System

- Use 24 Hour Clock
This will control the format that is used in the Incident Data Log. Turn this setting on to use the 24-hour clock format.

Working with Name Files

Every Grace PASS device is uniquely identified by assigning it a System and User ID.

- System ID's consist of a 2 character HEX based value where the first character is referred to as the Family and the second character is the Group.
- Family possible values range from 0-F Hex. (0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F).
- Group possible values range from 0-F Hex. (0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F).
- User ID possible values range from 1 to 99.
Values (101-109) are reserved for Micro-Repeaters.

A typical System/User ID combination would look something like this:

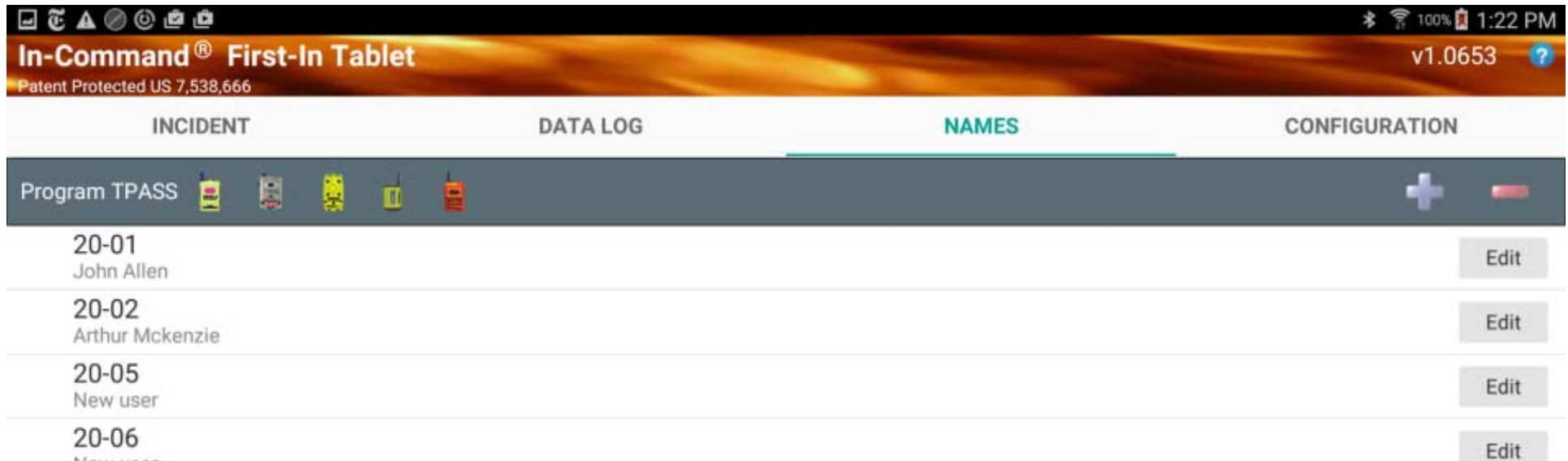
C0-01 Where C is the Family, 0 is the Group and 01 is the UserID.

Once a device's ID is programmed, the device will only ever transmit or respond to Grace messages which are identified by this ID.

In-Command® uses a Name File to identify all of the TPASS® users that it will monitor. If a user is not defined in the Name File, the user will not be monitored. You must create a Name entry in the Name File for every TPASS® device that you will use.

- * TPASS®, SuperCELL®, and Micro Repeaters are pre-programmed at the factory prior to shipment and are ready for use once the Tablet is properly configured.

Working with Name Files



To Manage Name Files, select the NAMES tab in the In-Command® App.

Adding Names

Press the “+” button on the Names toolbar to add a name. This will create a new entry in the Names list with a User ID of “00-00” and a default name of “New User”. Once a new entry has been created, you must edit it to modify the User ID and Name and assign the ID and Name of an actual TPASS® and User.

Deleting Names

Select the Name entry you would like to remove by tapping it one time. This will highlight the user. Once a user is selected, press the “-” button to delete the entry. You will be prompted to confirm deletion.

Editing Names

Press the Edit button next to the Name entry that you would like to modify. This will take you to the User Edit screen with the user details filled in.

Working with Name Files

The screenshot shows the 'In-Command First-In Tablet' interface with the 'NAMES' tab selected. The interface includes a top status bar with system icons and a bottom status bar with incident and user information.

INCIDENT DATA LOG NAMES CONFIGURATION

SAVE CANCEL

System ID

Family 2
Hexidecimal value representing the Family portion of the System ID (0-F)

Group 0
Hexidecimal value representing the Group portion of the System ID (0-F)

User Info

User ID 01
Decimal value (01-99)

User Full Name Tap To Edit John Allen

Detail

Device Type TPASS 3

Program TPASS ID Tap To Program

Incident Stopped Users Online: 0  

Editing Names in the User Edit Screen

Working with Name Files

Editing Names

Select the NAMES tab in the In-Command® App.

Press the Edit button next to the Name entry that you would like to modify. This will take you to the User Edit screen with the user details filled in. *(Example shown on previous page).*

- Change the Family and Group values by clicking the item popup boxes to the right of each field. Modifying these values will change the System ID. Family and Group combined make up the System ID. You should change these values to match the System ID of the TPASS® device you are modifying the Name entry for.
- Change the User ID of the Name entry by clicking the item popup box to the right of the User ID field. Modifying this value will change the User ID. You should change this value to match the User ID of the TPASS® device you are the Name entry for.
- Change the User Name by clicking the User entry field on the right side. This will allow editing of the User Name.
- Change the Device Type by clicking the item popup box to the right of the Device Type field then select the type of device that you are modifying the Name entry for.
- Once you have modified the Name entry record you can press the “Save” or “Cancel” buttons in the upper tool bar to complete the modification of the Name entry.

Programming Device ID's

When setting up your system for the first time or when purchasing new devices, it may become necessary to change the System and User ID assigned to the TPASS® device. To reprogram the TPASS® ID assignment, select the “NAMES” tab in the In-Command® app. On the upper left side of the toolbar you will see the button called “Program TPASS”. Pressing this button will open the programming screen.

Note: To use the programming feature, you must be connected to the Incident Command Monitor WIFI and have TCP configured in the App. See “Configuring the In-Command® App for Operation” for more information.

When the programming screen opens, you will see “Connection Ready” in the bottom toolbar. If you see anything other than this, you will not be able to program ID's until the configuration issue is addressed. Exit the programming screen, address the connection issue and reenter to retest the connection.

The screenshot shows the 'In-Command® First-In Tablet' app interface. At the top, there's a status bar with icons and the time '1:23 PM'. Below it, the app title 'In-Command® First-In Tablet' and 'Patent Protected US 7,538,666' are visible. The main menu has four tabs: 'INCIDENT', 'DATA LOG', 'NAMES' (which is selected and highlighted in green), and 'CONFIGURATION'. Below the tabs is a 'Back' button. The 'NAMES' section is divided into two parts. The first part, 'TPASS Current ID', has a subtitle 'Use Discover To Determine Current TPASS ID' and contains three dropdown menus for 'Family', 'Group', and 'User ID'. To the right of these are 'Discover' and 'Call' buttons. The second part, 'TPASS ID Program', has a subtitle 'NAME: John Allen' and contains three dropdown menus for 'Family' (set to 2), 'Group' (set to 0), and 'User ID' (set to 01). To the right of these is a 'Program' button. At the bottom of the screen, there's a status bar with 'Connection Ready' on the left, 'Incident Stopped' in the middle, and 'Users Online: 0' on the right, along with a globe icon.

Programming Device ID's

TPASS® Current ID (top section)

Step 1: Discover

Press the Discover button and the system will listen for radio traffic from the TPASS® device. It is best to do this when there is limited radio traffic in the system. To force the TPASS® to produce radio traffic, you can press the side buttons or even put the TPASS® into alarm. Once the discovery is complete, you will see the ID fields have been populated and the Call button will be enabled.

Step 2: Call

Press the Call button to send notice to the TPASS® device that was just discovered. This is a valuable feature that will help ensure you have identified the TPASS® correctly. The device will begin sounding an audible alert. Press the side buttons on the device to clear the alert. If you do not receive the audible alert, it most likely means the device discovered is not the device you are working with and you should redo the discovery process.

TPASS® ID Program (bottom section)

Step 1: ID Fields

The ID fields represent the ID values you would like to program your TPASS® to. These fields may be automatically populated when the programming screen is opened from the user edit screen. Otherwise, these fields must be manually populated by using the dropdowns provided. Once populated, the Program button will become enabled.

Step 2: Program

Press the program button to begin sending programming messages to the device.

Once completed, you will receive a message confirming the ID was successfully programmed. If you receive an error, ensure that WIFI is connected, TCP is correctly configured and the device is turned on.

Starting and Stopping an Incident

On the Incident tab you will find the Start Incident button in the upper left side of the toolbar. The button is color coded red meaning the incident is currently stopped.

The screenshot displays the 'In-Command First-In Tablet' interface. At the top, the status bar shows 'In-Command First-In Tablet', 'Patent Protected US 7,538,666', 'v1.0653', and a help icon. Below this is a navigation bar with four tabs: 'INCIDENT' (selected), 'DATA LOG', 'NAMES', and 'CONFIGURATION'. The 'INCIDENT' tab contains a red button labeled 'Incident Stopped Press To Start' and a 'Select All' checkbox. The main area is a table with the following columns: SYSTEM ID, DEVICE TYPE, NAME, ON TIME, and STATUS. The table lists eight users, all with 'ON TIME' of '00:00:00' and 'STATUS' of 'OFF'. The bottom status bar shows 'Incident Stopped', 'Users Online: 0', and icons for 'Mute Alarm Monitor' and 'Details'.

SYSTEM ID	DEVICE TYPE	NAME	ON TIME	STATUS
20-01	TPASS 3	John Allen	00:00:00	OFF
20-02	TPASS 3	Arthur Mckenzie	00:00:00	OFF
20-05	TPASS 5	New user	00:00:00	OFF
20-06	TPASS 5	New user	00:00:00	OFF
20-07	SuperCELL 500	New user	00:00:00	OFF
20-08	SuperCELL 500	New user	00:00:00	OFF
20-09	SuperCELL 500	New user	00:00:00	OFF
20-16	SuperCELL 500	Martin Clement	00:00:00	OFF
20-17	SuperCELL 500	Neil Levelle	00:00:00	OFF

Starting an Incident

Pressing the Start Incident button will display the Incident Details screen where you can provide location and details about the incident.

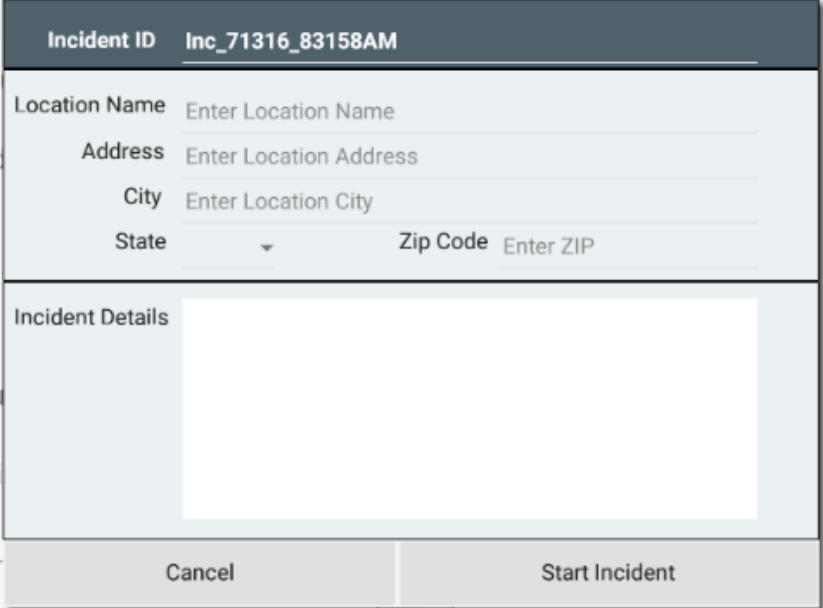
This screen can be displayed at any time by pressing the Details button on the right side of the bottom toolbar. This is convenient for entering incident details at any time and lets you start an incident without delay because you can go back to the details screen after the incident is started and provide more detail.

Initially, the Incident will not be started until you press the Start Incident button on the detail screen.

After the incident is started, the button on the details screen will display Done, and the Start Incident button on the main screen will display “Stop Incident”.

- Incident ID: This is an auto generated field used to uniquely identify the incident. The Incident ID is used as the filename when generating the incident log file. The file type of the incident log will be .txt. The current date and time values at the time the incident is started are used to generate this value. It uses the following format and cannot be changed: [Prefix]_[Date]_[Time].
[Prefix: Prefix will always be 'Inc']_[Date: mmddyy]_[Time: hhmmss followed by AM or PM]
- Location Name: This is a free text region that allows you to enter a Name for the incident.
- Location Address, City, State and Zip Code should be entered as they relate to the incident.
- Incident Details: This is a free text region that allows you to enter details about the incident such as time, weather, personnel, etc.

Again, this information can be entered before or any time after the incident is started.



Incident ID Inc_71316_83158AM	
Location Name	Enter Location Name
Address	Enter Location Address
City	Enter Location City
State	Zip Code Enter ZIP
Incident Details	
Cancel	Start Incident

Starting an Incident

Once an incident is started, you will see the bottom status bar will display “Incident Running”, and the main incident toolbar will be revealed from the right of the screen.

The incident is now running and busy listening for traffic from TPASS® units, logging activity and working to ensure the connection to the Incident Alarm Monitor is maintained.

Incident Toolbar buttons can be used by selecting one or more active incident users and clicking the appropriate incident tool button. For example, to clear a users alarm status, select the user you want to clear and press the Clear Alarm button.

All activity during the incident is recorded for display while the incident is active. This information will also be saved at 1 minute intervals to an incident log file using the Incident ID which was automatically generated by the system.

Reference previous page for explanation of the Incident Details screen. .



Incident Toolbar

Stopping an Incident

The incident can be stopped at any time by pressing the “Stop Incident” button on the left side of the upper toolbar. This button is green indicating that the incident is currently running.

When an incident is stopped, a final save of the incident log takes place.

All of the information gathered during the incident: Incident Data Log, Incident Details, Alarm Box information and radio traffic details are packaged and saved to a log file using the auto generated name that was displayed as the Incident ID on the details screen.

The Incident Display

The screenshot shows the 'In-Command First-In Tablet' interface. At the top, the status bar displays '100%' battery, signal strength, and the time '1:40 PM'. Below this, the app title 'In-Command First-In Tablet' and version 'v1.0653' are shown. The main interface has four tabs: 'INCIDENT' (selected), 'DATA LOG', 'NAMES', and 'CONFIGURATION'. A green button labeled 'incident Running Press To Stop' is in the top left of the main area. A 'Select All' checkbox is in the top right. The central table lists incident data with columns for SYSTEM ID, DEVICE TYPE, NAME, ON TIME, and STATUS. To the right of the table is a 'Command Tools' panel with buttons for 'SEND EVAC', 'CALL FOR PAR', 'CLEAR ALARM', 'CLEAR EVAC', 'CLEAR PAR', and 'CLEAR NO SIGNAL'. At the bottom, a status bar shows 'Incident Running.', 'Users Online: 5', 'Mute Alarm Monitor', and 'Details'. Various icons for connectivity and status are also present.

Annotations:

- Tab Pages
- Start / Stop Incident
- User Details
- Incident Running.
- Incident Status
- Tablet Battery Status
- App Version and Help
- Select All
- Command Tools
- User Status
- Incident Details
- Users Online
- Alarm Monitor Mute
- Internet Connectivity Status
- TCP Connectivity Status

SYSTEM ID	DEVICE TYPE	NAME	ON TIME	STATUS
20-09	TPASS 3	Ward Mchanley	00:00:56	ON
20-16	TPASS 5	Martin Clement	00:00:59	ON
90-01	MicroCELL AES-1	John Allen	00:00:06	ON
90-02	MicroCELL ERT-1	Equip 10	00:00:27	ON
20-R6	Micro Repeater	Repeater 6	00:00:54	ON
20-05	TPASS 5	New user	00:00:00	OFF
20-06	TPASS 5	New user	00:00:00	OFF
20-07	SuperCELL 500	New user	00:00:00	OFF
20-08	SuperCELL 500	New user	00:00:00	OFF

The Incident Display

Tab Pages

The main tabs of the application. Incident, Data Log, Names and Configuration. Used to navigate the app.

Start/Stop Incident

The incident start and stop button. Used for starting and stopping the incident.

User Details

The user detail section contains the User ID, Device Type, and User Name as defined in the Name File. The online time is controlled by an active incident and represents the time elapsed since the user first came online.

Incident Status

This will display brief information about the incident. Running, Stopped and Connection errors.

Tablet Battery Status

Indicates tablet battery level remaining.

App Version and Help

The version of the app.

Help button  opens user manual for In-Command® First-In Tablet App.

Select All

Used to select all users. This is helpful when issuing incident commands such as PAR and EVAC.

Command Tools

Collection of tools for issuing and clearing commands.

User Status (of personnel wearing TPASS®)

This portion of the User Details section is used to display images representing TPASS® and SuperCELL® user status such as: On/Off, Alarms, Low Battery, No-Signal, etc.

Incident Details

Button used to open the incident details entry screen.

Connectivity Status

Two status icons used to indicate connectivity to Internet and TCP connection to Incident Command Monitor.

Alarm Monitor Mute

This button is a convenient way to temporarily silence the alarm on the Incident Command Monitor. The length of the mute can be managed under the configuration tab.

Users Online

Always displays the number of active users on the system.

TPASS® Status Display

Once an incident is running, users will begin coming online as the system receives transmissions from their TPASS® devices. As conditions change for each user in the incident, these changes will be reflected in the Incident view.

Each type of user status has a corresponding image to give a quick visual of their status.

SYSTEM ID	DEVICE TYPE	NAME	ON TIME	STATUS
10-03	SuperCELL 500-IC	David Crosby	00:17:12	

ONLINE: The green “ON” image indicates that this device is turned on. The amount of time the unit has been turned on begins counting. On units will be sorted to the top of the incident display.

10-02	TPASS 3	John Abrahms	00:06:50	
-------	---------	--------------	----------	---

OFFLINE: Grey “OFF” image indicates the device is turned off. Online time indicates the unit was turned on at one time during this incident. When turned off, the counter will not be active. The grey background is also an indicator that the unit is not active. Off units will be sorted to the bottom of the display.

10-02	TPASS 3	John Abrahms	00:06:50	
-------	---------	--------------	----------	---

REHAB: Blue “Rehab” image indicates the device is offline with the Rehab key in place.

TPASS[®] Status Display

C0-18

TPASS 3

Joan Klingensmith

00:07:55



ALARM: Alarm condition status images are displayed to the right of On/Off Status



PANIC ALARM: The Alarm has been manually pressed on this TPASS[®] device.



MOTION ALARM: The device has gone into an alarm state because of lack of motion.



HEAT ALARM: The device's internal heat monitoring threshold has been exceeded.

C0-18

TPASS 3

Joan Klingensmith

00:07:55



Additional status images will be displayed to the right of the Alarm Indicator.

Additional Status Images:



Low Battery: The TPASS[®] device is reporting a low battery condition.



No Signal: In-Command has not received any signal from the device within the configured time.

TPASS® Status Display

EVAC



EVAC Commanded:

When first commanding an EVAC, Selected devices will momentarily show this image.



EVAC Sent:

Once the app sends the EVAC message to selected devices, this image will be displayed.



EVAC Received:

When a device receives the EVAC message, it will automatically respond. When the app receives the response, this image will be displayed.



EVAC Acknowledged:

Once the user manually presses the side buttons of a device being evacuated, this image will be displayed.

PAR



PAR Commanded:

When first commanding a PAR, Selected devices will momentarily show this image.



PAR Sent:

Once the app sends the PAR message to selected devices, this image will be displayed.



PAR Received:

When a device receives the PAR message, it will automatically respond. When the app receives the response, this image will be displayed.



PAR Acknowledged:

Once the user manually presses the side buttons of a device being PARRED, this image will be displayed.

TPASS® Status Display

Sort Priority

The order in which users are displayed in the incident view is determined by the following rules:

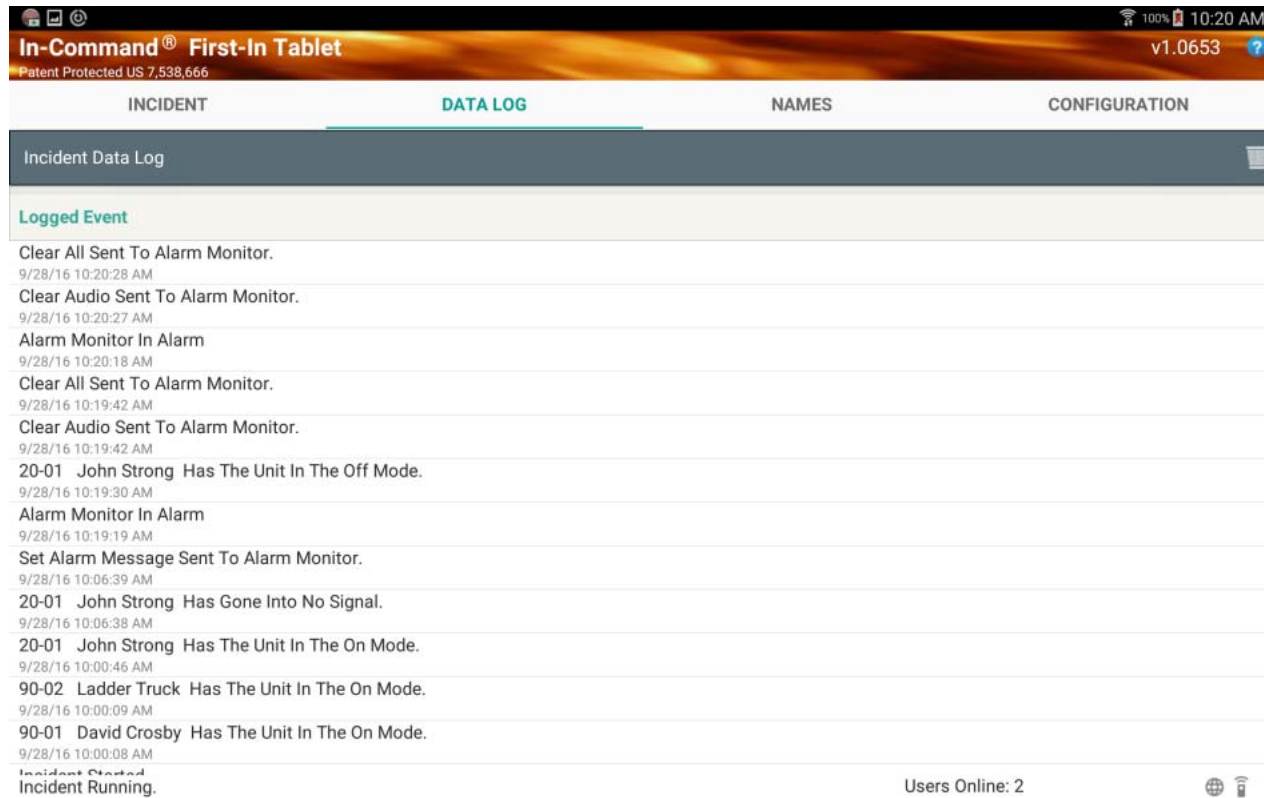
Alarms: Highest priority. Alarms are sorted to the top of the display.

Evacuation: Second highest priority. Evacuation conditions are sorted to the top just below any alarm conditions.

Par: Par conditions are the third highest priority. Users in a PAR condition will be sorted below alarms and evacuations.

- Users ID value is always the default sort order within any given status.
- MicroCELL devices have a less significant sort value than any other device except for Repeaters.
- Repeater devices will always have the least significant sort value and would be found at the bottom of the user status display.

Incident Data Log



The screenshot shows the 'In-Command® First-In Tablet' interface. At the top, there's a status bar with icons for signal, battery, and time (10:20 AM). Below the status bar, the text 'In-Command® First-In Tablet' and 'Patent Protected US 7,538,666' are visible. The main interface has four tabs: 'INCIDENT', 'DATA LOG' (which is selected and highlighted in green), 'NAMES', and 'CONFIGURATION'. Below the tabs, there's a header 'Incident Data Log' with a trash icon. The main content area is titled 'Logged Event' and lists a series of incident events in chronological order, with the most recent event at the top. The events include 'Clear All Sent To Alarm Monitor.', 'Clear Audio Sent To Alarm Monitor.', 'Alarm Monitor In Alarm', and 'Set Alarm Message Sent To Alarm Monitor.' for various units like '20-01 John Strong' and '90-02 Ladder Truck'. At the bottom right, it says 'Users Online: 2' and has a globe icon.

INCIDENT	DATA LOG	NAMES	CONFIGURATION
Incident Data Log			
Logged Event			
Clear All Sent To Alarm Monitor. 9/28/16 10:20:28 AM			
Clear Audio Sent To Alarm Monitor. 9/28/16 10:20:27 AM			
Alarm Monitor In Alarm 9/28/16 10:20:18 AM			
Clear All Sent To Alarm Monitor. 9/28/16 10:19:42 AM			
Clear Audio Sent To Alarm Monitor. 9/28/16 10:19:42 AM			
20-01 John Strong Has The Unit In The Off Mode. 9/28/16 10:19:30 AM			
Alarm Monitor In Alarm 9/28/16 10:19:19 AM			
Set Alarm Message Sent To Alarm Monitor. 9/28/16 10:06:39 AM			
20-01 John Strong Has Gone Into No Signal. 9/28/16 10:06:38 AM			
20-01 John Strong Has The Unit In The On Mode. 9/28/16 10:00:46 AM			
90-02 Ladder Truck Has The Unit In The On Mode. 9/28/16 10:00:09 AM			
90-01 David Crosby Has The Unit In The On Mode. 9/28/16 10:00:08 AM			
Incident Started. Incident Running.			

Users Online: 2

The Data Log tab shows a chronological history of incident events with the most recent event displayed at the top. The Data Log is automatically saved to the android file system when the Incident is stopped. During an incident it will be updated every minute. The Data Log can be a valuable tool when it becomes necessary to investigate and reconstruct what happened in an incident.

Incident Data Log

Once an incident is started, the system will begin recording system, user and monitor events as they occur. Each event will be tagged with Date and Time corresponding with when the event was processed.

Every action taken by the incident commander is recorded in the data log. Here are some examples of commanded events:

- Incident Started
- Cleared Alarms
- Initiated Par and Evacuation

Every status change received from a PASS device will be recorded in the log. Some examples are:

- Device turned on
- Panic Alarm
- Low Battery

Incident Command Monitor activity is also recorded. Some examples are:

- Incident Command Monitor In Alarm
- Clear Alarm Sent To Incident Command Monitor
- Incident Command Monitor Low Battery

Event Type

The event type is displayed in bold and is a description of the event that occurred. E.g. Incident Started, Incident Command Monitor In Alarm etc.

Date and Time Stamp

The date and time are also recorded with each event. Time format can be changed to use 12 or 24 format. See “Configuring the App for Operation”.

File Management

File Management

Files used and created by the In-Command® First-In Tablet app are stored on the Android device in the Public storage area for the In-Command® First-In Tablet app. This storage location is accessible by the end user when using any file management app on the device or by connecting the device to a computer running the Windows operating system. Regardless of the way files are accessed, the location of the files remains the same. File types and usage are described below.

File location

From Windows Explorer, the location will look something like this.

Computer\[device name]\Android\data\com.graceindustries.GraceICT\files\GraceData

From the device, the location will look like this.

Device Storage\Android\data\com.graceindustries.GraceICT\files\GraceData

Files

- ConfigICT.txt

This is the configuration file for the app. The values defined within the content of this file should never have to be manually edited. Use the app configuration pages to make changes to this file.

- Names.xml

This is the data file for the Names database. It is in an xml format and is managed by the app by using the Names Editing features of the app. The xml structure of this file is very specific and can easily become corrupt when manually edited although it is possible to manually create and change name files by managing multiple versions of this file. You could have multiple name files and change the names being used by the app by replacing this file. Manual changes to this file should only ever be attempted when the app is closed.

(continued)

File Management

Files (continued)

- Alarm.wav

This is the audio file used when the system has an alarm condition. You can customize the alarm audio by replacing this file with your own wav file with the same name. **Alarm.wav must always exist and its name cannot change.**

- Evac.wav

This is the audio file used when the system is in an evacuation condition. You can customize the evacuation audio by replacing this file with your own wav file with the same name. **Evac.wav must always exist and its name cannot change.**

!!Caution should be used if the default audio files are changed!!

- Devices.txt

This is the device translation file. RadioH platform devices transmit a device type. This file is used as a lookup to identify the device. You should never make changes to this file.

- Log Files

Data log files will also be stored in this same location. Log files have the potential to use up large amounts of disk space. In-Command will warn you when disk space is running low. To avoid filling up internal disk space with log files it is recommended to remove or delete old files periodically or move the storage location to an external disk.

External storage of log files

It is possible in Android to move the application to an external disk (SD card). When doing this, all of the configuration files used by the system will continue to be stored on the internal storage of the device with the exception of Data log files. In this case, those file will be stored on the external disk in a location that looks something like this: SD card\Android\data\com.graceindustries.GraceICT\files\GraceData

Incident Command Monitor Familiarization



IMPORTANT NOTE:

Incident Command Monitor must be turned ON to send, receive, and repeat Emergency Signals. Always Test Incident Command Monitor For Proper Operation Before Use.

Incident Command Monitor is an important component used in the In-Command® First-In system.

Turn ON and strategically place the Incident Command Monitor on the Fire Ground to receive EMERGENCY Alarm Signals from compatible Grace TPASS® and SuperCELL® devices.

OPERATING INSTRUCTIONS

Turn ON Incident Command Monitor:

- Insert On/Off Security Key and turn to ON position.
- Remove key for security.
- Incident Command Monitor will be armed in thirty (30) seconds and ready to receive and respond to Emergency Alarm signals.

Reset Alarm:

- To momentarily silence the sirens activated by an Emergency Alarm, press the Reset button, located on the front of unit.
- This will silence the sirens for thirty (30) seconds.

Turn OFF Incident Command Monitor:

- Insert On/Off Security Key, turn to OFF position.

EVAC or Evacuate Button:

- Press and HOLD EVAC push-button for three seconds to send a Global Evacuation signal to all telemetry devices on the fire ground. EVAC Indicator will flash.
- To Clear EVAC press and Hold EVAC push-button for 3 seconds. EVAC Indicator will cease flashing.

Muting Control:

- To Mute or un-mute the sirens, momentarily press Alarm Reset button on front of the unit. Mute LED will show the MUTE Status.
- Solid Red LED: Sirens are MUTED.
- NO Red LED: Sirens are ENABLED.
- **NOTE:** Sirens can be temporarily muted (for up to 90 seconds) from the In-Command First-In Tablet Application.

Incident Command Monitor Familiarization

Specifications

Alarm Display: Dual sirens and bright flashing strobe light activated as Alarm signals are received from TPASS® or SuperCELL®

Siren Audio Output: 120 dBA at 1 meter.

Controls: ON/OFF Key Switch for enhanced security.

Global EVAC: Push-button. To EVAC or Clear an Evac - Press and Hold push-button for 3 seconds.

Global EVAC Indicator:

EVAC Active: LIGHT Flashing

EVAC Cleared: LIGHT Off

Safety Yellow Case: rugged, impact and weather resistant plastic

Size: 16" High, 16 1/2" Wide, 8 3/4" Deep

Weight: 12 lbs

Power: Internal 12 Volt rechargeable lead-acid battery; External 120VAC or 12VDC power with included power adapters. *Available international power adapters rated for 100-240VAC input, with UL, FCC, CE,  safety ratings.*

Hours of Operation in Standby: 24 hrs

Hours in Alarm, minimum at low battery: 2 hours

Long Term Battery Life: 3 to 5 years

Wifi Hub: 802.11 b/g/N.

(Wifi-SSID and Password provided on rear label)

Model Compatibility with Grace Telemetry Products

- **Model 45S-HWT** is designed for operation with the In-Command® Tablet Application* and is compatible with Grace Telemetry products operating on the RadioH platform. This model meets NFPA requirements for RF PASS
- In-Command® First-In Tablet application requires customer-provided Android tablet.

Incident Command Monitor Familiarization

FCC Statements

FCC ID: J5MXHEM - Meets FCC Part 15

Changes or modifications not expressly approved by the party responsible 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.

Industry Canada Notices

IC: 5916A-MXHEM - Complies with Canadian ICES-003

This Class A digital apparatus complies with Canadian ICES-003. This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device. Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada. (select the class for your device). Le présent appareil est conforme aux CNR d'Industrie 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, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Australia / New Zealand:

Compliant to ACMA AS/NZS CISPR22:2006, Class A Digital Apparatus | AS/NZS 4268:2012 for Intentional Radiators.

EMC93142C-ACMA

EMC93142C-AS/NZS 4268



Configuring WIFI Access Point on the Incident Command Monitor

The Incident Command Monitor will come preconfigured to broadcast a WIFI connection when turned on. A label on the rear of the Incident Command Monitor will include the SSID and password set by the factory. It is required that the tablet WIFI is connected prior to running the In-Command® app.

In order to connect to the TCP Server in the Incident Command Monitor, the In-Command® First-In Tablet app must be configured to connect to the default IP address 10.10.100.254 and default TCP Port of 5001.

The Incident Command Monitor SSID, security, default IP and TCP Port can be configured using the built in web interface.

- Connect to the Incident Command Monitor WIFI
- Using a web browser enter the IP Address. 10.10.100.254
- Enter the default username and password when prompted. admin/admin
- The following screen will be displayed. *(see next page)*.

Configuring WIFI Access Point on the Incident Command Monitor

Network SSID and Security can be modified on the Quick Configuration Page section 1F.

The screenshot displays the 'Quick Configure' interface of the Incident Command Monitor. On the left is a sidebar with navigation links: Quick Configure, Mode Selection, AP Interface Setting, STA Interface Setting, Application Setting, Ethernet Setting, HTTPD Client Mode, WEB IO, Advanced, and Device Management. The main area is titled 'Quick Configure' and contains several sections. The first section, '1F WI-FI Setting', is highlighted with a red '1F' and includes a 'Modify' link. It contains a table with the following settings: 'Wifi Mode' (AP Mode), 'Network Name(SSID)' (PAB_03), 'BSSID' (AC:CF:23:3A:03:24), and 'Security Mode' (Disable). The 'Network Name(SSID)' and 'Security Mode' fields are circled in red. Below this table are 'Apply' and 'Cancel' buttons. The subsequent sections are '2F Ethernet Ports Setting', '3F Uart Setting', '4F Network Setting', and '5F Device Management'. The '5F Device Management' section includes a 'Restart Module' button.

Wifi Mode	
Mode	AP Mode

Wireless configuration	
Network Name(SSID)	PAB_03
BSSID	AC:CF:23:3A:03:24
Security Mode	Disable

Apply Cancel

2F Ethernet Ports Setting [Modify](#)

3F Uart Setting [Modify](#)

4F Network Setting [Modify](#)

5F Device Management

Restart Module	
Restart Module	Restart

Configuring WIFI Access Point on the Incident Command Monitor

TCP Port can be changed on the Quick Configuration Page section 4F.

The screenshot displays the 'Quick Configure' interface of the Incident Command Monitor. On the left is a sidebar with navigation links: Quick Configure, Mode Selection, AP Interface Setting, STA Interface Setting, Application Setting, Ethernet Setting, HTTPD Client Mode, WEB IO, Advanced, and Device Management. The main area is titled 'Quick Configure' and contains several sections: 1F WI-FI Setting, 2F Ethernet Ports Setting, 3F Uart Setting, and 4F Network Setting. The '4F Network Setting' section is expanded, showing 'Network A Setting' with fields for Mode (Server), Protocol (TCP), Port (5001), Server Address (10.10.100.100), MAX TCP Num. (1~32), TCP Time out (0), and TCP connection password authentication (Disable). The 'Port' field is circled in red. Below the network settings are 'Apply' and 'Cancel' buttons. At the bottom, the '5F Device Management' section includes a 'Restart Module' button.

Quick Configure

1F WI-FI Setting [\[Modify\]](#)

2F Ethernet Ports Setting [\[Modify\]](#)

3F Uart Setting [\[Modify\]](#)

4F Network Setting [\[Modify\]](#)

Network A Setting

Mode	Server
Protocol	TCP
Port	5001
Server Address	10.10.100.100
MAX TCP Num.(1~32)	32
TCP Time out (小于600 秒)	0
TCP connection password authentication	Disable

Apply Cancel

5F Device Management

Restart Module

Restart Module	Restart
----------------	---------

Configuring WIFI Access Point on the Incident Command Monitor

IP Address can be changed on the AP Interface Settings page.

AP Interface Setting

AP Interface Setting such as SSID, Security...

Wireless Network	
Network Mode	11b/g/n mixed mode
Network Name(SSID)	PAB_03 ☐ Hidden
BSSID	AC:CF:23:3A:03:24
Frequency (Channel)	AutoSelect

Apply Cancel

PAB_03	
Security Mode	Disable

Apply Cancel

LAN Setup	
IP Address(Default DHCP Gateway)	10.10.100.254
Subnet Mask	255.255.255.0
DHCP Type	Server

Apply Cancel

Configuring WIFI Access Point on the Incident Command Monitor

It is also possible using this interface to configure the WIFI module to connect to an existing network. This is done by changing the WIFI mode from AP to STA and configuring the modules network settings on the STA Interface Settings page. When using this mode, the tablet WIFI can connect directly to your network and In-Command® will access the TCP of the Incident Command Monitor via the configured TCPIP and TCP Port.

Detailed configuration documentation for the WIFI module can be found at:

http://www.usriot.com/download/WIFI/USR-WIFI232-B2_User_Manual-V6.0.pdf

Configure the WIFI connection

- Go into Android device/settings on the tablet and configure the WIFI connection to connect to the SSID being broadcast by the Incident Command Monitor.



305 Bend Hill Road
Fredonia, PA 16124 U.S.A.
724-962-9231
www.graceindustries.com