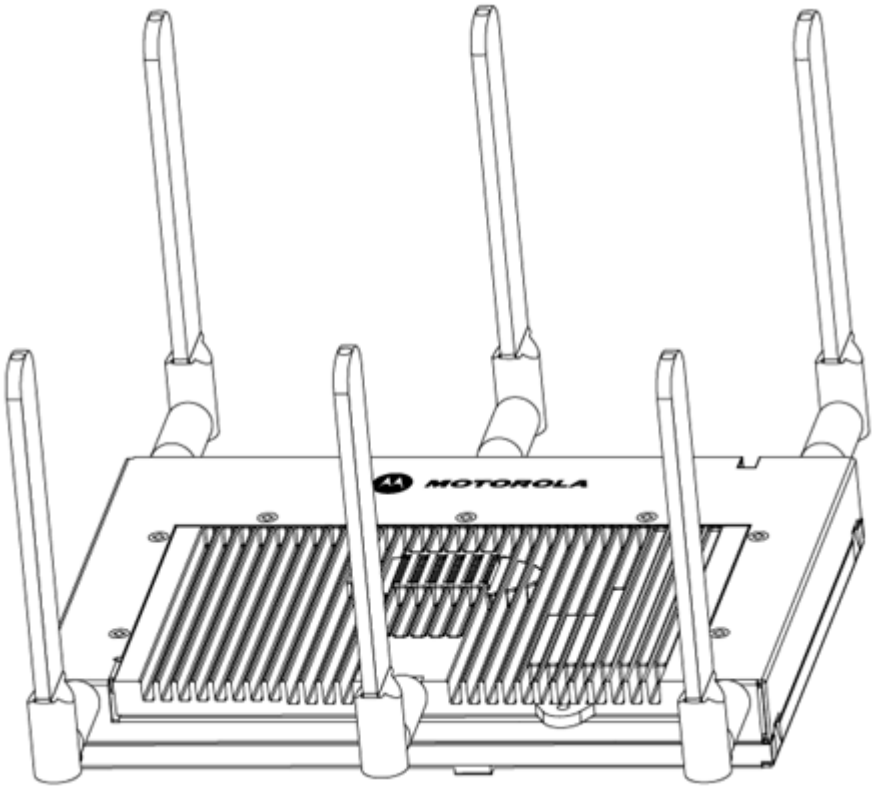
AP-7131N-FGR Access Point

Installation Guide



Contents

1 Introduction

As a standalone access point, an AP-7131N-FGR provides small and medium-sized businesses with a consolidated wired and wireless networking infrastructure, all in a single device. The integrated router, gateway, firewall, DHCP and *Power-over-Ethernet* (PoE) simplify and reduce the costs associated with networking by eliminating the need to purchase and manage multiple devices.

The access point is also designed to meet the needs of large, distributed enterprises by converging the functionality of a thick access point and thin access port into a single device. This mode enables the deployment of a fully featured intelligent access point that can be centrally configured and managed via a Motorola wireless switch in either corporate headquarters or a *network operations center* (NOC). In the event the connection between the access point and the wireless switch is lost, a *Remote Site Survivability* (RSS) feature ensures the delivery of uninterrupted wireless services at the local or remote site. All traffic between the adaptive access points and the wireless switch is secured though an IPSec tunnel. Additionally, compatibility with Motorola's *RF Management Suite* (RFMS) allows you to centrally plan, deploy, monitor and secure large deployments.

Beginning with the 4.x access point firmware baseline, Motorola is introducing an AP-7131N-FGR model access point as a compliment to the existing AP-7131 access point family. The new AP-7131N-FGR access point supports the same feature set as existing AP-7131and AP-7131N model access points. Unlike the AP-7131 and AP-7131N models however, an AP-7131N-FGR has specialized data protection mechanisms and prompts the user when secure information is displayed within the access point GUI applet.

The AP-7131N-FGR enables you to configure one radio for 802.11a/n support, and the other for 802.11b/g/n support.

The two models available to the AP-7131N-FGR series include:

- AP-7131N-66040-FGR (802.11an and 802.11bgn capable)
- AP-7131N-44040-FGR (802.11a and 802.11bg capable)

1.1 Document Conventions

The following graphical alerts are used in this document to indicate notable situations:

NOTE Tips, hints, or special requirements that you should take note of.

CAUTION Care is required. Disregarding a caution can result in data loss or equipment malfunction.

WARNING! Indicates a condition or procedure that could result in personal injury or equipment damage.

1.2 Warnings

- Read all installation instructions and site survey reports, and verify correct equipment installation before connecting the access point to its power source.
- Remove jewelry and watches before installing this equipment.
- Verify that the unit is grounded before connecting it to the power source.
- Verify that any device connected to this unit is properly wired and grounded.
- Connect all power cords to a properly wired and grounded electrical circuit.
- Verify that the electrical circuits have appropriate overload protection.
- Attach only approved power cords to the device.
- Verify that the power connector and socket are accessible at all times during the operation of the equipment.
- Do not work with power circuits in dimly lit spaces.
- Do not install this equipment or work with its power circuits during thunderstorms or other weather conditions that could cause a power surge.
- Verify there is adequate ventilation around the device, and that ambient temperatures meet equipment operation specifications.

1.3 Site Preparation

- Consult your site survey and network analysis reports to determine specific equipment placement, power drops, and so on.
- Assign installation responsibility to the appropriate personnel.
- Identify and document where all installed components are located.
- Provide a sufficient number of power drops for your equipment.
- Ensure adequate, dust-free ventilation to all installed equipment.
- Identify and prepare Ethernet and console port connections.
- Verify cable lengths are within the maximum allowable distances for optimal signal transmission.

2 Hardware Installation

An AP-7131N-FGR access point installation includes mounting the access point, connecting the access point to the network, connecting antennae and applying power. Installation procedures vary for different environments.

The AP-7131N-FGR model access point has the following port designations:

- GE1/POE - LAN port
- GE2 - WAN Port

2.1 Precautions

Before installing the AP-7131N-FGR, verify the following:

- Do not install in wet or dusty areas without additional protection. Contact a Motorola representative for more information.
- Verify the environment has a continuous temperature range between -20° C to 50° C.

2.2 Requirements

The minimum installation requirements for a single-cell, peer-to-peer network:

- An AP-7131N-FGR model access point (in either of its two available dual-radio models)
- 48 Volt Power Supply (50-14000-247R) or Power Injector (AP-PSBIAS-1P3-AFR)
- A power outlet
- Dual-band antennae or an antenna specifically supporting the AP's 2.4 or 5 GHz band

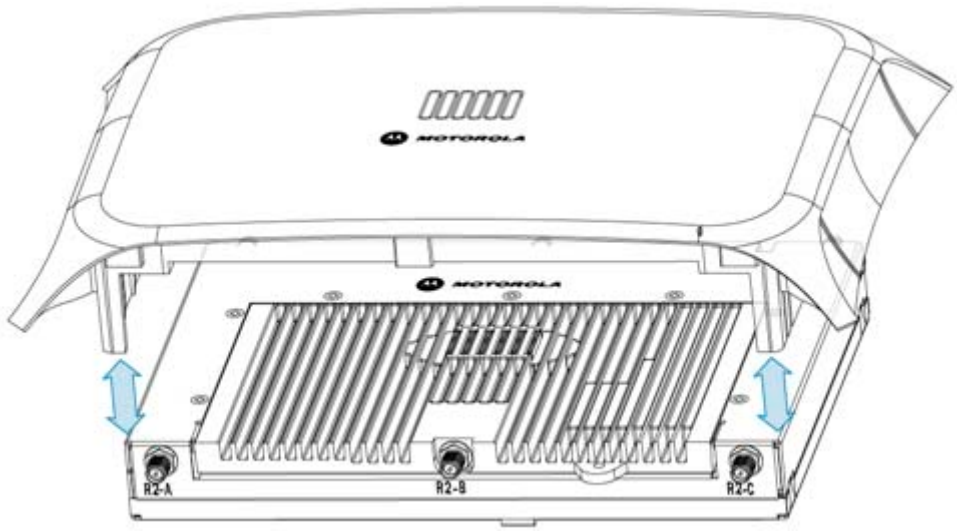
2.3 Package Contents

Check package contents for the correct model AP-7131N-FGR and applicable accessories. Each available configuration (at a minimum), contains:

- AP-7131N-FGR model access point (accessories dependent on SKU ordered)
- AP-7131N-FGR Install Guide (this guide)
- Wall mount screw and anchor kit
- Accessories Bag (4 rubber feet and a LED light pipe and badge with label for above the ceiling installations)

Contact the Motorola Support Center to report missing or improperly functioning items.

NOTE Some access points ship with a protective cover (facade) or a 6-element MIMO antenna. The cover disconnects from the access point as illustrated on the next page. When attached, LEDs continue to illuminate through the cover.



2.4 Access Point Placement

For optimal performance, install the AP-7131N-FGR away from transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators and other industrial equipment. Signal loss can occur when metal, concrete, walls or floors block transmission. Install the access point in an open area or add access points as needed to improve coverage.

Antenna coverage is analogous to lighting. Users might find an area lit from far away to be not bright enough. An area lit sharply might minimize coverage and create *dark areas*. Uniform antenna placement in an area (like even placement of a light bulb) provides even, efficient coverage.

Place the access point using the following guidelines:

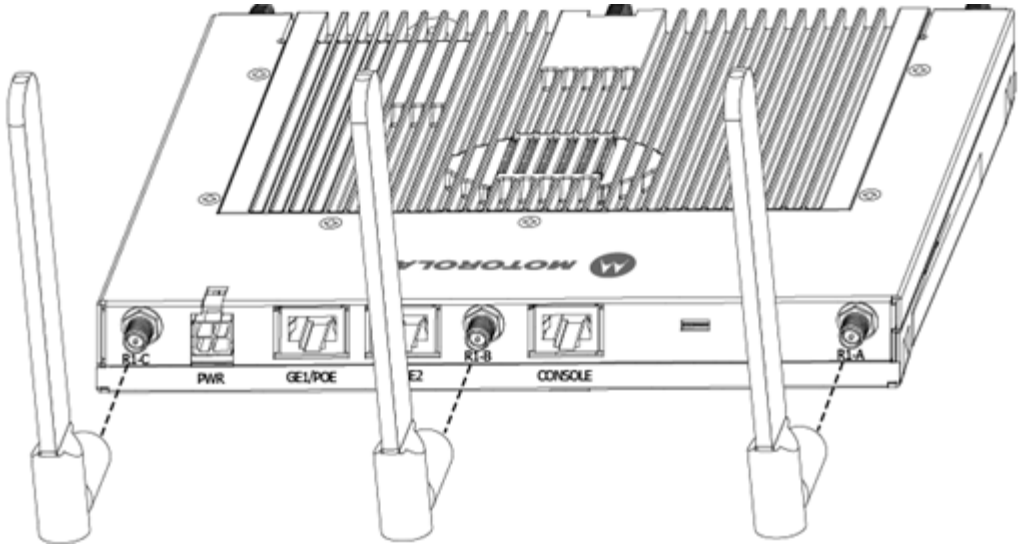
- Install the access point at an ideal height of 10 feet from the ground.
- Orient the access point antennas vertically for best reception.
- Point the access point antennas downward if attaching to the ceiling.

To maximize the access point's radio coverage area, Motorola recommends conducting a site survey to define and document radio interference obstacles before installing the access point.

2.4.1 Antenna Options

Motorola supports two antenna suites for AP-7131N-FGR. One antenna suite supporting the 2.4 GHz band and another antenna suite supporting the 5 GHz band. Select an antenna model best suited to the intended operational environment of your access point.

NOTE On dual-radio model AP-7131N-FGR access points, Radio 1 refers to the 2.4 GHz radio and Radio 2 refers to the 5 GHz radio. However, there could be some cases where a dual-radio access point is performing a Rogue AP detector function. In this scenario, the access point is receiving in either 2.4 GHz or 5 GHz over the Radio 1 or Radio 2 antennae depending on which radio is selected for the scan. Certain Rogue AP detection features use a radio to perform dual-band scanning. The dedicated radio should be connected to an appropriate dual-band dipole antenna (Part No. ML-2452-APA2-01)



R1 defines the access point's radio 1 antenna connectors and R2 defines radio 2 antenna connectors.

2.4.2 Power Injector System

The AP-7131N-FGR can receive power via an Ethernet cable connected to the GE1/POE (LAN) port.

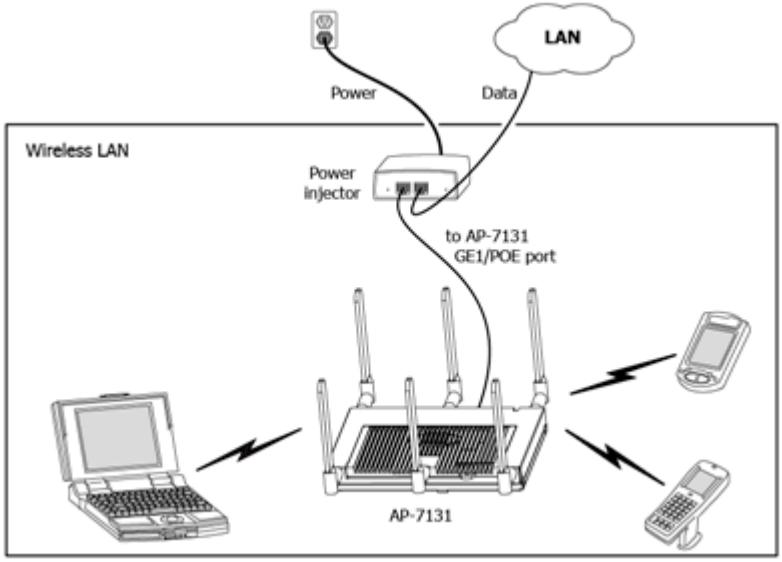
When users purchase a WLAN solution, they often need to place access points in obscure locations. In the past, a dedicated power source was required for each access point in addition to the Ethernet infrastructure. This often required an electrical contractor to install power drops at each access point location. The Power Injector merges power and Ethernet into one cable, reducing the burden of installation and allowing optimal access point placement in respect to the intended coverage area.

The Power Injector (Part No. AP-PSBIAS-1P3-AFR) is a high power POE Injector delivering up to 30 watts. The access point can only use a Power Injector when connecting the unit to the access point's GE1/POE port. The Power Injector is a separately ordered and not shipped with an AP SKU.

An AP-7131 and AP-7131N can also be used with the 3af power injector (AP-PSBIAS-1P2-AFR). However, AP functionality is limited when powered by an AP-PSBIAS-1P2-AFR, since the AP has Ethernet connectivity limited to only the GE1 port.

The Motorola access point Power Supply (Part No. 50-14000-247R) is not included with the access point and is orderable separately as an accessory. If the access point is provided both POE power over the GE1/POE connection, as well as the 50-14000-247R power supply concurrently, the access point will source power from the 50-14000-247R supply only. Disconnecting AC power from the 50-14000-247R, causes the AP to re-boot before sourcing power from the POE power injector. If the AP is operating using injector supplied power, the AP will not automatically reboot if an AC adapter is connected. The AP continues to operate with power supplied from the AC adapter without change to the AP operating configuration. If using AC adapter supplied power and a change to the AP's operating configuration is warranted (for example, if needing to access the GE2 port), the AP needs to be manually rebooted by the customer.

CAUTION The access point supports any standards-based compliant power source (including non-Motorola power sources). However, using the wrong solution (including a POE system used on a legacy Motorola access point) could either limit functionality or severely damage the access point and void the product warranty.



The Power Injector can be installed free standing, on an even horizontal surface or wall mounted using the power injector's wall mounting key holes. The following guidelines should be adhered to before cabling the Power Injector to an Ethernet source and an access point:

- Do not block or cover airflow to the Power Injector.
- Keep the Power Injector away from excessive heat, humidity, vibration and dust.
- The Power Injector isn't a repeater, and does not amplify the Ethernet signal. For optimal performance, ensure the Power Injector is placed as close as possible to the data port.

CAUTION To avoid problematic performance and restarts, disable POE from a wired switch port connected to an access point if mid-span *power sourcing equipment* (PSE) is used between the two, regardless of the manufacturer of the switch.

To install the Power Injector to an Ethernet data source and an access point:

CAUTION Ensure AC power is supplied to the Power Injector using an AC cable with an appropriate ground connection approved for the country of operation.

1. Connect the Power Injector to an AC outlet (110VAC to 220VAC).
2. Connect an RJ-45 Ethernet cable between the network data supply (host) and the Power Injector **Data In** connector.
3. Connect an RJ-45 Ethernet cable between the Power Injector **Data & Power Out** connector and the access point's GE1/POE port.

NOTE Cabling the Power Injector to WAN port (GE2) renders the AP non-operational. Only use a AP-PSBIAS-1P3-AFR (or AP-PSBIAS-1P2-AFR) Power Injector with the access point's GE1/POE (LAN) port.

Ensure the cable length from the Ethernet source (host) to the Power Injector and access point does not exceed 100 meters (333 ft).

The Power Injector has no On/Off power switch. The Injector receives power and is ready for device connection and operation as soon as AC power is applied. Refer to the *Installation Guide* shipped with the Power Injector for a description of the device's LEDs.

2.5 Mounting the Access Point

The AP-7131N-FGR can attach to a wall, mount under a suspended T-Bar or above a ceiling (plenum or attic) following the same installation instructions. Choose one of the following mounting options based on the physical environment of the coverage area. Do not mount the access point in a location that has not been approved in a site survey.

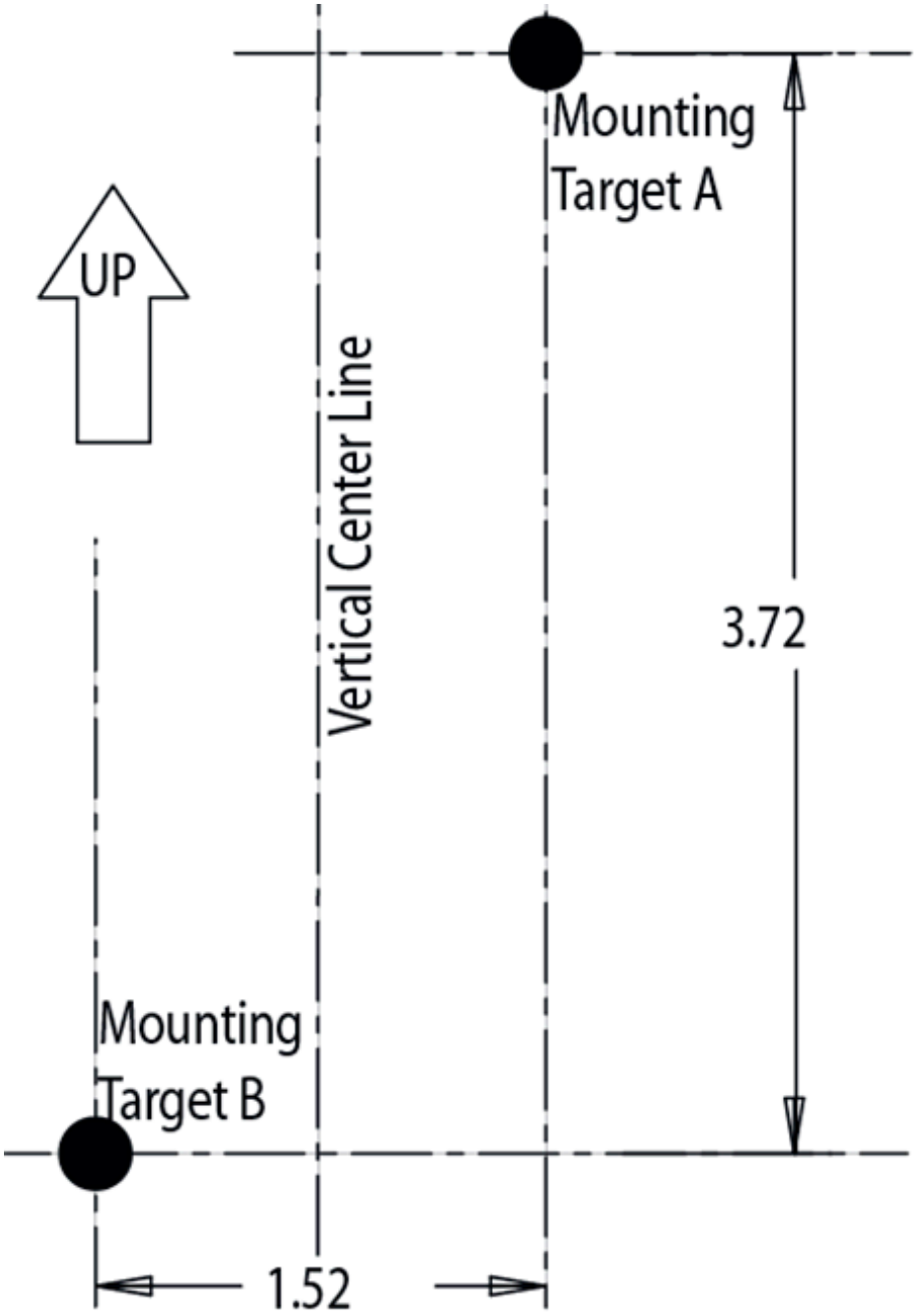
2.5.1 Wall Mounting

Wall mounting requires hanging the access point along its width (or length) using the pair of slots on the bottom of the unit and the access point mounting template (on the next page) for the screws.

CAUTION An access point should be wall mounted to concrete or plaster-wall-board (dry wall) only. Do not wall mount the access point to combustible surfaces.

The hardware and tools (customer provided) required to install the access point on a wall consists of:

- Two Phillips pan head self-tapping screws
  (ANSI Standard) #6-18 X 0.875in. Type A or AB Self-Tapping screw, or
  (ANSI Standard Metric) M3.5 X 0.6 X 20mm Type D Self-Tapping screw
- Two wall anchors
- Wall mount template (included on the next page)
- Security cable (optional third part provided accessory)


Mounting
Target A
UP
Vertical Center Line
3.72
Mounting
Target B
1.52

To mount the access point on a wall using the provided template:

1. Xerox copy the template (on the previous page) to a blank piece of paper. Do not reduce or enlarge the scale of the template.

CAUTION If printing the mounting template (on the previous page) from an electronic PDF, dimensionally confirm the template by measuring each value for accuracy.

2. Tape the template to the wall mounting surface.
   - If the installation requires the antenna be positioned vertically, the centerline reference (of the template) needs to be positioned vertically. The cabling shall exit the access point in a vertical direction.
   - If the installation requires the antenna be positioned horizontally, the vertical centerline (of the template) needs to be positioned horizontally. The cabling shall exit the access point in a horizontal direction.
3. At mounting targets A and B, mark the mounting surface through the template at the target center.
4. Discard the mounting template.
5. At each point, drill a hole in the wall, insert an anchor, screw into the anchor the wall mounting screw and stop when there is 1mm between the screw head and the wall.

   If pre-drilling a hole, the recommended hole size is 2.8mm (0.11in.) if the screws are going directly into the wall and 6mm (0.23in.) if wall anchors are being used.
6. If required, install and attach a security cable to the access point lock port.
7. Attach the antennas to their correct connectors.
8. For information on available antennas, see "**Antenna Options**" on page 5.
9. Place the large center opening of each of the mount slots over the screw heads.
10. Slide the access point down along the mounting surface to hang the mount slots on the screw heads.

CAUTION Ensure you are placing the antennas on the correct connectors to ensure the successful operation of the AP-7131N-FGR access point.

NOTE It is recommended the access point be mounted with the RJ45 cable connector oriented upwards or downwards to ensure proper operation.

11. Cable the access point using either the Power Injector solution or an approved line cord and power supply.

    For Motorola Power Injector installations:

    a. Connect a RJ-45 CAT5e (or CAT6) Ethernet cable between the network data supply (host) and the Power Injector **Data In** connector.
    b. Connect a RJ-45 CAT5e (or CAT6) Ethernet cable between the Power Injector **Data & Power Out** connector and the access point GE1/POE port.
    c. Ensure the cable length from the Ethernet source (host) to the Power Injector and access point does not exceed 100 meters (333 ft). The Power Injector has no On/Off power switch. The Power Injector receives power as soon as AC power is applied. For more information on using the Power Injector, see "**Power Injector System**" on page 7.

    For standard power adapter (non Power Injector) and line cord installations:

    a. Connect a RJ-45 CAT5e (or CAT6) Ethernet cable between the network data supply (host) and the access point's GE1/POE or GE2 port.
    b. Verify the power adapter is correctly rated according the country of operation.
    c. Connect the power supply line cord to the power adapter.
    d. Attach the power adapter cable into the power connector on the access point.
    e. Attach the power supply line cord to a power supply.

CAUTION Do not actually connect to the power source until the cabling portion of the installation is complete.

12. Verify the behavior of the access point LEDs. For more information, see "**LED Indicators**" on page 19.
13. The access point is ready to configure. For information on basic access point device configuration, see "**Configuring "Basic" Device Settings**" on page 25.

2.5.2 Suspended Ceiling T-Bar Installations

A suspended ceiling mount requires holding the access point up against the T-bar of a suspended ceiling grid and twisting the access point chassis onto the T-bar.

The mounting tools (customer provided) and hardware required to install the access point on a ceiling T-bar consists of:

- Safety wire (recommended and customer supplied)
- Security cable (optional and customer supplied)

To install the access point on a ceiling T-bar:

1. Motorola recommends you loop a safety wire — with a diameter of at least 1.01 mm (.04 in.), but no more than 0.158 mm (.0625 in.) — through the tie post (above the access point's console connector) and secure the loop.
2. If desired, install and attach a security cable to the access point lock port.
3. Attach the antennas to their correct connectors.

   For information on the antennas available to the access point, see "**Antenna Options**" on page 5.

CAUTION Ensure you are placing the antennas on the correct connectors to ensure the successful operation of the AP-7131N-FGR access point.

4. Cable the access point using either the Power Injector solution or an approved line cord and power supply.

   For Motorola Power Injector installations:

   a. Connect a RJ-45 CAT5e (or CAT6) Ethernet cable between the network data supply (host) and the Power Injector **Data In** connector.

   b. Connect a RJ-45 CAT5e (or CAT6) Ethernet cable between the Power Injector **Data & Power Out** connector and the access point's GE1/POE port.

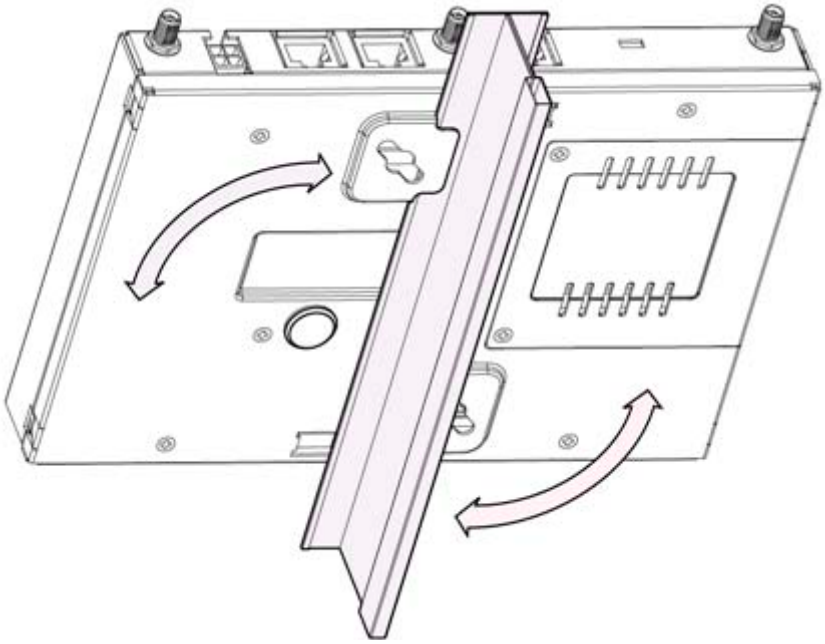
   c. Ensure the cable length from the Ethernet source (host) to the Power Injector and access point does not exceed 100 meters (333 ft). The Power Injector has no On/Off power switch. The Power Injector receives power as soon as AC power is applied. For more information, see "**Power Injector System**" on page 7.

   For standard power adapter (non Power Injector) and line cord installations:

a. Connect a RJ-45 Ethernet cable between the network data supply (host) and the access point's GE1/POE or GE2 port.
b. Verify the power adapter is correctly rated according the country of operation.
c. Connect the power supply line cord to the power adapter.
d. Attach the power adapter cable into the power connector on the access point.
e. Attach the power supply line cord to a power supply.

CAUTION Do not actually connect to the power source until the cabling portion of the installation is complete.

5. Verify the behavior of the access point LEDs. For more information, see "**LED Indicators**" on page 19.
6. Align the bottom of the ceiling T-bar with the back of the access point.
7. Orient the access point chassis by its length and the length of the ceiling T-bar.
8. Rotate the access point chassis 45 degrees clockwise.
9. Push the back of the access point chassis on to the bottom of the ceiling T-bar.
10. Rotate the access point chassis 45 degrees counter-clockwise. The clips click as they fasten to the T-bar.



11. The access point is ready to configure. For information on basic access point device configuration, see "**Configuring "Basic" Device Settings**" on page 25.

NOTE If the access point is utilizing remote management antennas, a wire cover can be used to provide a clean finished look to the installation. Contact Motorola for more information.

2.5.3 Above the Ceiling (Plenum) Installations

An above the ceiling installation requires placing the access point above a suspended ceiling and installing the provided light pipe under the ceiling tile for viewing the rear panel status LEDs of the unit. An above the ceiling installation enables installations compliant with drop ceilings, suspended ceilings and industry standard tiles from .625 to .75 inches thick.

NOTE The AP-7131N-FGR is Plenum rated to UL2043 and NEC1999 to support above the ceiling installations. To ensure UL compliance and proper operation within the Air Handling Plenum, the access point must be installed with the bottom surface of the unit in contact with the un-finished surface of the ceiling tile. This will facilitate the positioning of the light pipe (described in the following pages) through the ceiling tile.

CAUTION Motorola does not recommend mounting the access point directly to any suspended ceiling tile with a thickness less than 12.7mm (0.5in.) or a suspended ceiling tile with an unsupported span greater than 660mm (26in.). Motorola strongly recommends fitting the access point with a safety wire suitable for supporting the weight of the device. The safety wire should be a standard ceiling suspension cable or equivalent steel wire between 1.59mm (.062in.) and 2.5mm (.10in.) in diameter.

The mounting hardware required to install the access point above a ceiling consists of:

- Light pipe
- Badge for light pipe
- Decal for badge
- Safety wire (strongly recommended)
- Security cable (optional)

To install the access point above a ceiling:

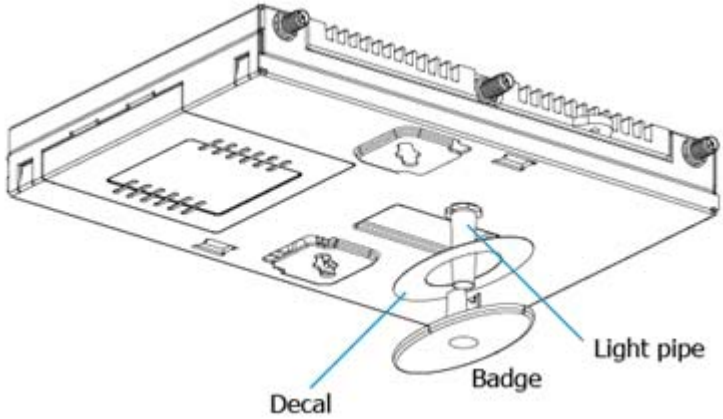
NOTE Remove the access point's facade and antennas before installing in an above the ceiling orientation. The access point is not certified for an above the ceiling installation with its accessories installed.

1. If possible, remove the adjacent ceiling tile from its frame and place it aside.
2. If required, install a safety wire, between 1.5mm (.06in.) and 2.5mm (.10in.) in diameter, in the ceiling space.
3. If required, install and attach a security cable to the access point's lock port.
4. Mark a point on the finished side of the tile where the light pipe is to be located.

5. Create a light pipe path hole in the target position on the ceiling tile.
6. Use a drill to make a hole in the tile the approximate size of the access point LED light pipe.

CAUTION Motorola recommends care be taken not to damage the finished surface of the ceiling tile when creating the light pipe hole and installing the light pipe.

7. Remove the light pipe's rubber stopper (from the access point) before installing the light pipe.
8. Connect the light pipe to the bottom of the access point. Align the tabs and rotate approximately 90 degrees. Do not over tighten.



9. Fit the light pipe into hole in the tile from its unfinished side.
10. Place the decal on the back of the badge and slide the badge onto the light pipe from the finished side of the tile.
11. Attach the antennas to their correct connectors.

    For information on the antennas available to the access point, see "**Antenna Options**" on page 5.

CAUTION Ensure you are placing the antennas on the correct connectors to ensure the successful operation of the AP-7131N-FGR access point.

12. Motorola recommends attaching safety wire to the access point safety wire tie point or security cable (if used) to the access point's lock port.

13. Align the ceiling tile into its former ceiling space.
14. Cable the access point using either the Power Injector solution or an approved line cord and power supply.

    For Motorola Power Injector installations:

    a. Connect a RJ-45 CAT5e (or CAT6) Ethernet cable between the network data supply (host) and the Power Injector **Data In** connector.
    b. Connect a RJ-45 CAT5e (or CAT6) Ethernet cable between the Power Injector **Data & Power Out** connector and the access point's GE1/POE port.
    c. Ensure the cable length from the Ethernet source (host) to the Power Injector and access point does not exceed 100 meters (333 ft). The Power Injector has no On/Off power switch. The Power Injector receives power as soon as AC power is applied. For more information on using the Power Injector, see "**Power Injector System**" on page 7.

    For standard power adapter (non Power Injector) and line cord installations:

    a. Connect a RJ-45 Ethernet cable between the network data supply (host) and the access point's GE1/POE or GE2 port.
    b. Verify the power adapter is correctly rated according the country of operation.
    c. Connect the power supply line cord to the power adapter.
    d. Attach the power adapter cable into the power connector on the access point.
    e. Attach the power supply line cord to a power supply.

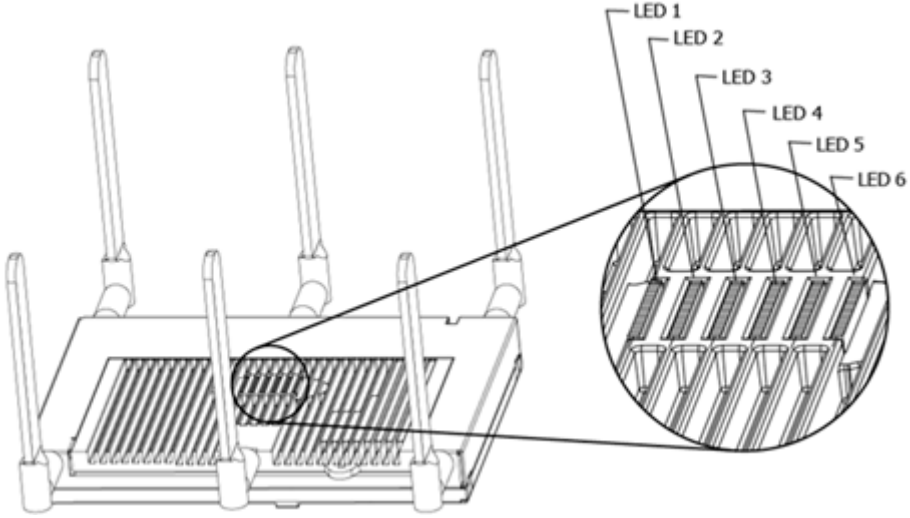
CAUTION Do not actually connect to the power source until the cabling portion of the installation is complete.

15. Verify the behavior of the access point LED light pipe. For more information, see "**LED Indicators**" on page 19.
16. Place the ceiling tile back in its frame and verify it is secure.
17. The access point is ready to configure. For information on basic access point device configuration, see "**Configuring "Basic" Device Settings**" on page 25.

2.6 LED Indicators

An AP-7131N-FGR access point has six LEDs on the top of the access point housing, and one optional LED light pipe at the bottom of the unit. However, an AP-7131N-FGR model access point does not use LED 6, as no third radio is available. Five LEDs illuminate (on top of the housing) for dual radio AP-7131N-FGR models.

The access point utilizes two (different colored) lights below each LED. Only one light displays within a LED at any given time. Every light within each LED is exercised during startup to allow the user to see if an LED is non-functional. The LEDs turn on and off while rotating around in a circle. Since two LEDs feed each light pipe, the pattern is from left to right, then right to left.



NOTE The LED blink rate is proportional to activity. The busiest traffic corresponds to the fastest blink, while the slowest traffic corresponds to slowest blink.

NOTE Depending on how the 5 GHz and 2.4 GHz radios are configured, the LEDs will blink at different intervals between amber and yellow (5 GHz radio) and emerald and yellow (2.4 GHz radio).

The LEDs on the top housing of the access point are clearly visible in wall and below ceiling installations. The top housing LEDs have the following display and functionality:

2.6.1 Dual Radio (2.4/5 Ghz) LEDs

A dual radio (2.4/5 Ghz) AP-7131N-FGR access point has the following unique LED behavior:

LED 1	***LED 2 (LAN)***	***LED 3 (WAN)***	***LED 4 - 5 GHz***	***LED 5 - 2.4 GHz***	***LED 6***
Blinking **Red** indicates booting. Solid **Red** defines the diagnostic mode. **White** defines normal operation.	**Green** defines normal GE1 operation.	**Green** defines normal GE2 operation.	Blinking **Amber** indicates 802.11a activity. A 5 second **Amber** and **Yellow** blink rate defines 802.11an activity. A 2 second **Amber** and **Yellow** blink rate defines 802.11an (40 MHz) activity. When functioning as a sensor, LED alternates between **Amber** and **Yellow**. The blink interval is 0.5 seconds. It's 1 second when no Server is connected.	Blinking **Emerald** indicates 802.11bg activity. A 5 second **Emerald** and **Yellow** blink rate defines 802.11bgn activity. A 2 second **Emerald** and **Yellow** blink rate defines 802.11bgn (40 MHz) activity. When functioning as a sensor, LED alternates between **Emerald** and **Yellow**. The blink interval is 0.5 seconds. It's 1 second when no Server is connected.	Not Used

2.6.2 Rear AP-7131N-FGR LED

The LED on the rear (bottom) of the access point is optionally viewed using a single (customer installed) extended light pipe, adjusted as required to suit above the ceiling installations. The LED light pipe has the following color display and functionality

LED 7
Blinking **Red** (160 msec) indicates a failure condition. Solid **Red** defines the diagnostic mode. **White** defines normal operation.

3 Basic Configuration

3.1 Configuring Your Browser for AP-7131N-FGR Support

An AP-7131N-FGR model access point is compliant with the FIPS140-2 standard. The AP-7131N-FGR is only accessible using browsers that support the TLS 1.0 protocol. The AP-7131N-FGR is not accessible by browsers supporting the SSL 2.0 or SSL 3.0 protocols. Additionally, ensure JRE (version 1.6 or above) is installed on the computer accessing the AP-7131N-FGR GUI applet. The following sections describe how to change your browser settings using either Internet Explorer or Mozilla Firefox in order to correctly launch and display the AP-7131N-FGR GUI applet. Without these browser modifications, you will not be able to access the AP-7131N-FGR GUI applet.

CAUTION With both the Internet Explorer and Mozilla Firefox browser configurations, screens may display stating Website certificates cannot be validated or have been certified by an unknown authority. Do not exit the browser configuration, as these messages will occur with only the initial AP-7131N-FGR browser configuration.

3.1.1 Accessing the AP-7131N-FGR Using Internet Explorer

To define the browser settings needed to access the AP-7131N-FGR using Windows Internet Explorer:

1. Open the Internet Explorer browser and open the **Tools** > **Internet Options** menu.
2. Select the **Advanced** tab.
3. Scroll down to the bottom of the Advanced tab and ensure the **Use TLS 1.0** option is selected. Remember, the AP-7131N-FGR does not support SSL 2.0 or SSL 3.0.

4. Enter the IP address of the AP-7131N-FGR within Internet Explorer. Select the **Continue to this Website (not recommended)** option. The default IP address of the WAN port is 10.1.1.1. Remember to use https (and not http) when you enter the IP address, as http is not supported with the AP-7131N-FGR.

   At this point in the browser configuration, a screen displays stating the Web site's certificate cannot be verified.

5. Click **Yes** to continue. The access point's login screen displays.
6. Log in using **admin** as the default User ID and **motorola** as the default password. If the default login is successful, the **Change Admin Password** window displays. It is strongly recommended you immediately change the password to optimize device security. For more information, see "**Configuring the Access Point**" on page 23.

3.1.2 Accessing the AP-7131N-FGR Using Mozilla Firefox

To define the browser settings needed to access the AP-7131N-FGR using Mozilla Firefox:

1. Open the Mozilla Firefox browser and open the **Tools** > **Options** menu (some versions of Firefox use Edit > Preferences).
2. Select the **Advanced** tab, then select either the **Encryption** or **Security** tab (they differ depending on the version of Firefox used).
3. Within the Protocols field, ensure the **Use TLS 1.0** option is selected. Remember, the AP-7131N-FGR does not support SSL 2.0 or SSL 3.0.
4. Enter the IP address of the AP-7131N-FGR. Remember to use https (and not http) when you enter the IP address, as http is not supported with the AP-7131N-FGR.

   A **Website Certified by an Unknown Authority** screen displays stating Firefox is unable to define a trusted site.

5. Select either the **Accept this certificate permanently** or **Accept this certificate temporarily for this session**. Click the **OK** button to continue.

   A **Security Error: Domain Name Mismatch** screen could display. Click **OK** to continue. At this point in the browser configuration, a screen displays stating the Web site's certificate cannot be verified.

6. Click **Yes** to continue. The access point's login screen displays.
7. Log in using **admin** as the default User ID and **motorola** as the default password. If the default login is successful, the **Change Admin Password** window displays. It is strongly recommended you immediately change the password to optimize device security. For more information, see "**Configuring the Access Point**" on page 23.

3.2 Configuring the Access Point

For the basic setup described in this guide, the Java-based Web UI will be used to configure the access point. The GE1/POE port's default setting is static (with a default IP address of 192.168.0.1). For this example, the access point's WAN interface will be used to connect to the access point. The default WAN IP address is 10.1.1.1. For optimal viewing of the Web UI, the screen resolution should be set to 1024 x 768 pixels or greater.

Remember, Internet Explorer and Mozilla Firefox require unique settings be defined in order for the browser to access the AP-7131N-FGR GUI applet. For instructions on configuring these browser settings, see "**Configuring Your Browser for AP-7131N-FGR Support**" on page 21.

NOTE For advanced configuration options beyond the scope of this guide, refer to the *AP-7131N-FGR Access Point Product Reference Guide*. The guide is available on the Motorola Web site, at *https://support.symbol.com/support/product/FIPS_and_CC_Compliant_Products.html*.

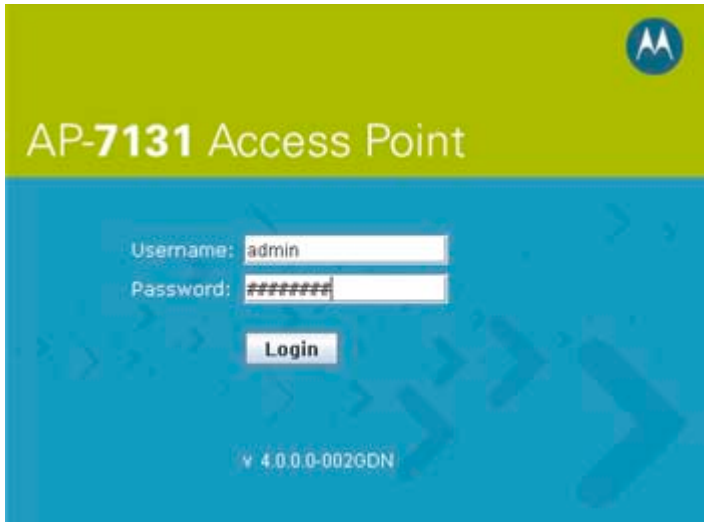
1. Start a browser and enter the following IP address in the address field:

   https://10.1.1.1

NOTE For optimum compatibility, use Sun Microsystems' JRE 1.6 or higher (available from Sun's Website), and be sure to disable Microsoft's Java Virtual Machine if installed.

NOTE The computer being used should be configured to use the same IP address and subnet mask as the access point.

   The login screen displays.



2. Log in using **admin** as the default User ID and **motorola** as the default password. If the default login is successful, the **Change Admin Password** screen displays.
3. Change the password to ensure the AP-7131N-FGR is using a secure password different from the default password. The new password must be at least 8 characters in length.

   Enter the current password and a new admin password in fields provided, and click **Apply**. Once the admin password has been updated, a warning message displays stating the access point could be operating illegally unless set to operate in the correct country. Proceed to "**Configuring "Basic" Device Settings**" on page 25 to validate the country setting.

NOTE Though the access point can have its basic settings defined using a number of different screens, Motorola recommends using the **AP-7131 Quick Setup** screen to define a minimum required configuration from one location.

3.3 Resetting the Access Point's Password

The access point has a means of restoring its password to its default value. Doing so also reverts the access point's security, radio and power management configuration to their default settings. Only an installation professional should reset the access point's password and promptly define a new restrictive password.

To contact Motorola Support in the event of a password reset requirement, go to *http://www.symbol.com/contactsupport*.

CAUTION Only a qualified installation professional should set or restore the access point's radio and power management configuration in the event of a password reset.

3.4 Configuring "Basic" Device Settings

Configure a set of minimum required device settings within the **Quick Setup** screen. The values (LAN, WAN etc.) can often be defined in other locations within the menu tree. When you change the settings in the Quick Setup screen, the values also change within the screen where these parameters also exist. Additionally, if the values are updated in these other screens, the values initially set within the Quick Setup screen will be updated.

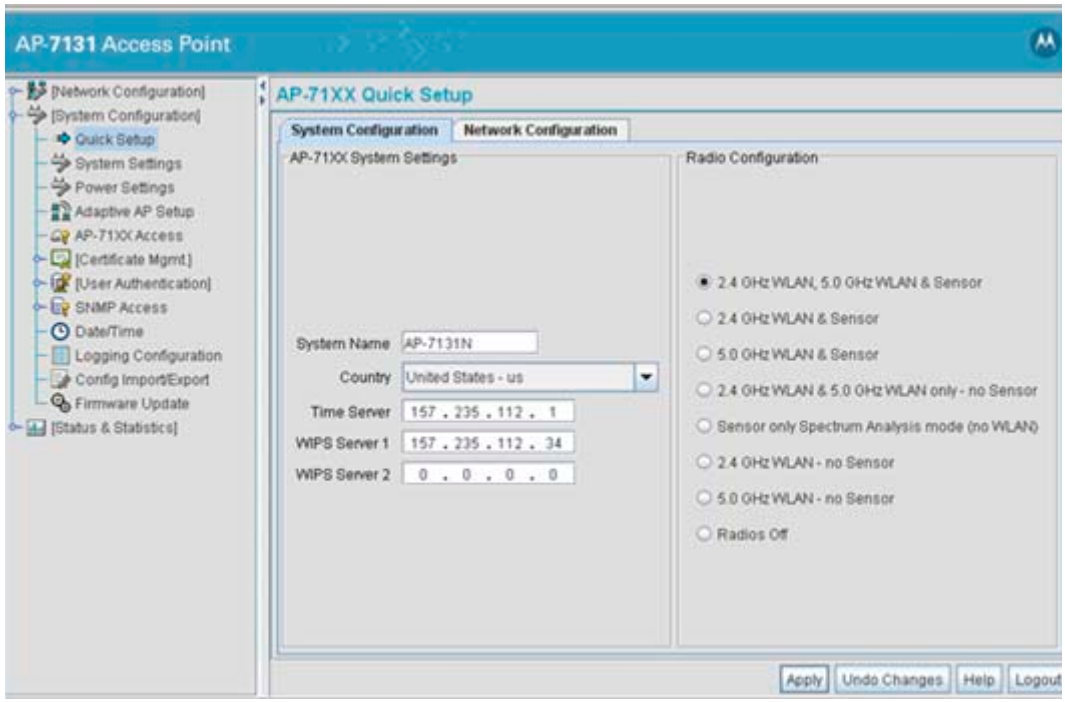
NOTE Beginning with the 4.0 release of the access point firmware, a new scheme for radio configuration and WIPS server management has been implemented within the Quick Setup GUI applet. These radio buttons define how WLAN and sensor functionality are supported amongst the radios available to the access point. The options available depend on the SKU supported (and are described within this section).

To define a basic access point configuration:

1. Select **System Configuration** -> **Quick Setup** from the menu tree, if the Quick Setup screen is not already displayed.

2. Select the **System Configuration** tab to define the access point's system, WIPS server and radio configuration.

NOTE The WIPS Server designation and radio configuration can be defined as part of the access point's quick setup. For a description of sensor functionality and how it relates to access point operation, refer to the *AP-7131N-FGR Access Point Product Reference Guide* available at https://support.symbol.com/support/product/FIPS_and_CC_Compliant_Products.html.



3. Refer to the **AP-71xx System Settings** field to define the following parameters:
   a. Assign a **System Name** to define a title for this access point. The System Name is useful if multiple devices are being administered.
   b. Select the **Country** for the AP-7131N-FGR's country of operation. The access point prompts for the correct country code on the first login. A warning message also displays stating an incorrect country setting may result in illegal radio operation. Selecting the

correct country is central to legally operating the access point. Each country has its own regulatory restrictions concerning electromagnetic emissions and the maximum RF signal strength that can be transmitted. To ensure compliance with national and local laws, set the country accurately.

c. Optionally enter the IP address of the server used to provide system time to the access point within the Time Server field. Once the IP address is entered, the access point's *Network Time Protocol* (NTP) functionality is engaged automatically. With the AP-7131N-FGR, a VPN tunnel is established using the NTP server.

d. Define a primary and alternate WIPS server IP Address for WIPS Server 1 and 2. These are the addresses of the primary and secondary WIPS console server. WIPS support requires a Motorola AirDefense WIPS Server on the network. WIPS functionality is not provided by the access point alone. The access point works in conjunction with the dedicated WIPS server(s).

NOTE The System Name and Country are also configurable within the **System Settings** screen. Refer to the *AP-7131 Series Product Reference Guide* to optionally set a system location and admin email address for the access point or to change other default settings.

4. Refer to the new **Radio Configuration** field to define how WLAN and WIPS are supported by the access point's radio(s).

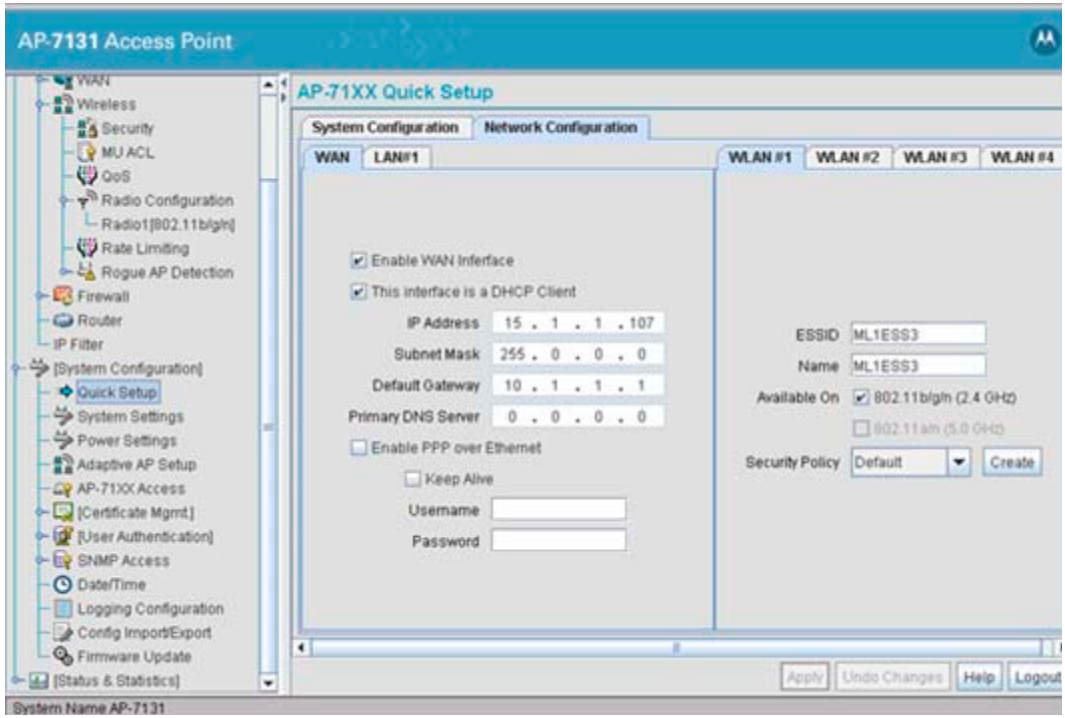
   A dual radio AP-7131N-FGR access point displays 7 configuration options. Refer to the following table for the options available to AP-7131N-FGR models.

Radio Button	***AP-7131N-FGR Dual Radio SKU***
2.4 GHz WLAN, & Sensor	Radio1 WLAN, Radio 2 WIPS
5.0 GHz WLAN & Sensor	Radio 1 WIPS, Radio 2 WLAN
2.4 GHz WLAN & 5.0 GHz WLAN only - no Sensor	Radio 1 WLAN, Radio 2 WLAN
Sensor only Spectrum Analysis mode (no WLAN)	Radio 1 WIPS, Radio 2 WIPS
2.4 GHz WLAN - no Sensor	Radio1 WLAN, Radio 2 Disabled

Radio Button	***AP-7131N-FGR Dual Radio SKU***
5.0 GHz WLAN - no Sensor	Radio1 Disabled, Radio 2 WLAN
Radios Off	Radios 1 and 2 Disabled

CAUTION Only a qualified installation professional should set the access point's radio and power management configuration.

5. Select the Quick Setup screen's **Network Configuration** tab to define a minimum set of WAN or LAN configuration values. The WAN tab displays by default.



a. Select the **Enable WAN Interface** checkbox to enable a connection between the access point and a larger network or outside world through the WAN port. Disable this option to effectively isolate the access point's WAN connection. No connections to a larger network or the Internet will be possible. MUs cannot communicate beyond the configured subnets.

b. Select the **This Interface is a DHCP Client** checkbox to enable DHCP for the access point WAN connection. This is useful, if the target corporate network or *Internet Service Provider (ISP)* uses DHCP. DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these parameters are IP address, network mask, and gateway.

NOTE Motorola recommends the WAN and LAN ports should not both be configured as DHCP clients.

c. Specify an **IP address** for the access point's WAN connection. An IP address uses a series of four numbers expressed in dot notation, for example, 190.188.12.1.

d. Specify a **Subnet Mask** for the access point's WAN connection. This number is available from the ISP for a DSL or cable-modem connection, or from an administrator if the access point connects to a larger network. A subnet mask uses a series of four numbers expressed in dot notation. For example, 255.255.255.0 is a valid subnet mask.

e. Specify a **Default Gateway** address for the access point's WAN connection. The ISP or a network administrator provides this address.

f. Specify the address of a **Primary DNS Server**. The ISP or a network administrator provides this address.

g. Optionally, use the **Enable PPP over Ethernet** checkbox to enable *Point-to-Point Protocol over Ethernet (PPPoE)* for a high-speed connection that supports this protocol. Most DSL providers are currently using or deploying this protocol. PPPoE is a data-link protocol for dialup connections. PPPoE will allow the access point to use a broadband modem (DSL, cable modem, etc.) for access to high-speed data networks.

h. Select the **Keep Alive** checkbox to enable occasional communications over the WAN port even when client communications to the WAN are idle. Some ISPs terminate inactive connections, while others do not. In either case, enabling Keep-Alive maintains the WAN connection, even when there is no traffic. If the ISP drops the connection after the idle time, the access point automatically reestablishes the connection to the ISP.

i. Specify a **Username** entered when connecting to the ISP. When the Internet session begins, the ISP authenticates the username.

j. Specify a **Password** entered when connecting to the ISP. When the Internet session starts, the ISP authenticates the password.

6. Click the **LAN#1** tab to set a minimum set of parameters to use the access point LAN interface.

a. Select the **Enable LAN Interface** checkbox to forward data traffic over the access point LAN connection. The LAN connection is enabled by default.

b. Use the **This Interface** drop-down menu to specify how network address information is defined over the LAN connection. Select **DHCP Client** if the larger corporate network uses DHCP. DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these parameters are IP address, network mask, and gateway. Select **DHCP Server** to use the access point as a DHCP server over the LAN connection. Select the **Bootp client** option to enable a diskless system to discover its own IP address.

NOTE Motorola recommends that the WAN and LAN ports should not be configured as DHCP clients at the same time.

c. Enter the network-assigned **IP Address** of the access point. DNS names are not supported as a valid IP address for the access point. The user is required to enter a numerical IP address.

d. The **Subnet Mask** defines the size of the subnet. The first two sets of numbers specify the network domain, the next set specifies the subset of hosts within a larger network. These values help divide a network into subnetworks and simplify routing and data transmission.

e. If using the static or DHCP Server option, enter a **Default Gateway** to define the numerical IP address of a router the access point uses on the Ethernet as its default gateway

f. If using a static or DHCP Server, enter the **Primary DNS Server** numerical IP address.

g. If using DHCP Server, use the **Address Assignment Range** parameter to specify a range of IP address reserved for mapping clients to IP addresses. If a manually (static) mapped IP address is within the IP address range specified, that IP address could still be assigned to another client. To avoid this, ensure all statically mapped IP addresses are outside of the IP address range assigned to the DHCP server.

NOTE For additional access point port configuration options, as well as radio, WLAN and *Quality of Service* (QoS) options, refer to the *AP-7131N-FGR Access Point Product Reference Guide* available at *https://support.symbol.com/support/product/FIPS_and_CC_Compliant_Products.html*.

7. Select the **WLAN #1** tab (WLANs 1 - 4 are available within the Quick Setup screen) to define its ESSID security scheme for basic operation.

NOTE A maximum of 16 WLANs are configurable within the access point Wireless Configuration screen. The limitation of 16 WLANs exists regardless of the number of radios supported.

   a. Enter the *Extended Services Set Identification (ESSID)* and name associated with the WLAN.

   b. Use the **Available On** checkboxes to define whether the target WLAN is operating over the 802.11a/n or 802.11b/g/n radio. Ensure the radio selected has been enabled (see step 8).

8. Once the WLAN's radio designations have been made, the radio must be configured in respect to intended 2.4 or 5 GHz radio traffic and the antennas used. Refer to **Network Configuration** -> **Wireless** -> **Radio Configuration** -> **Radio1 (or Radio2)**, and configure the Radio Settings field (at a minimum). If you know the radio's Properties, Performance and Beacon Settings, those fields can also be defined at this time.

   Define the Channel Settings, Power Level and 802.11 mode in respect to the 2.4 or 5 GHz 802.11b/g/n or 802.11a/n radio traffic and anticipated gain of the antennas.

CAUTION Only a qualified wireless network administrator should set the access point radio configuration. Refer to the *AP-7131N -FGR Access Point Product Reference Guide* for an understanding of the configurable values involved and their implications. To access the guide, go to *https://support.symbol.com/support/product/FIPS_and_CC_Compliant_Products.html*.

NOTE Even an access point configured with minimal values must protect its data against theft and corruption. A security policy should be configured for WLAN1 as part of the basic configuration outlined in this guide. A security policy can be configured for the WLAN from within the Quick Setup screen. Policies can be defined over time and saved to be used as needed as the access point's security requirements change. Motorola recommends you familiarize yourself with the security options available on the access point before defining a security policy.

9. Click **Apply** to save any changes to the Quick Setup screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost, unless you use the **Un-applied Changes** pop-up window to overwrite the current settings.

10. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Quick Setup screen to the last saved configuration.

3.4.1 Configuring Basic Security

For testing basic connectivity, there is no reason to configure a server supported authentication scheme. WPA2/CCMP is described in this guide as a basic security scheme sufficient to protect the AP-7131N-FGR's initial transmissions. For details on configuring other authentication and encryption options available to the access point, refer to the *AP-7131N-FGR Access Point Product Reference Guide*. The guide is available on the Motorola Web site, at https://support.symbol.com/support/product/FIPS_and_CC_Compliant_Products.html.

NOTE A VPN tunnel must also be established to ensure the access point is using a secure connection to the external server providing NTP, syslog or Radius resources. For more information, see "**Defining an IPSec VPN Tunnel**" on page 34.

To configure WPA2/CCMP:

1. From the Quick Setup screen, click the **Create** button to the right of the Security Policy item.

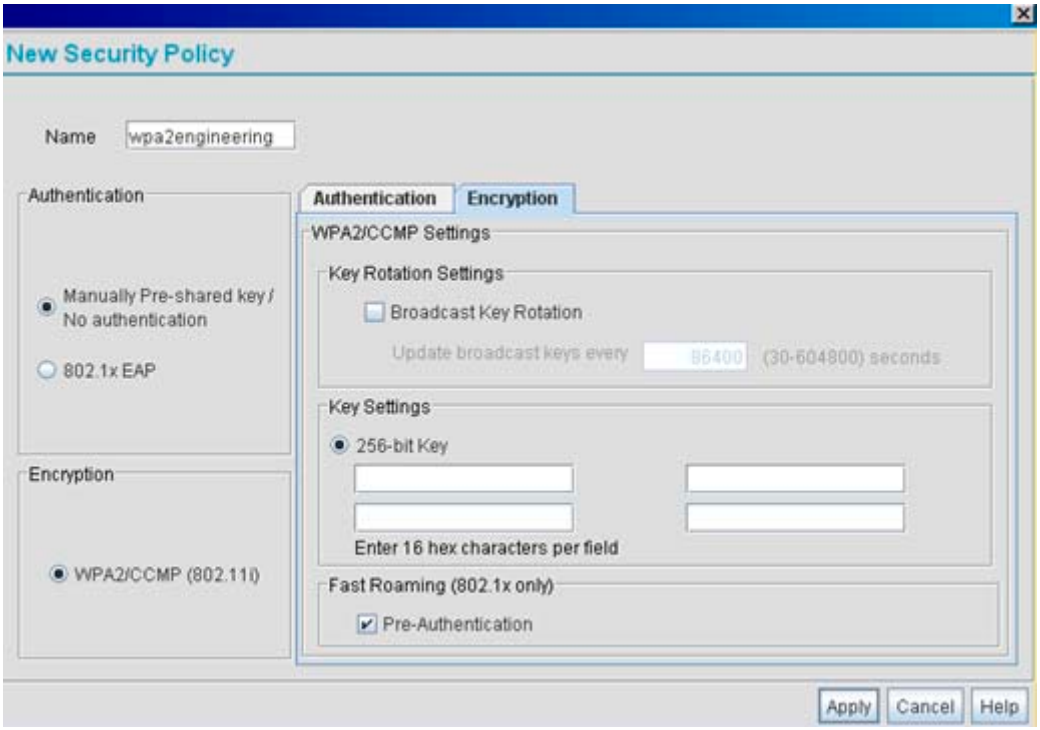
   The **New Security Policy** screen displays with the **Manually Pre-shared key/No authentication** and **No Encryption** options selected. Naming and saving such a policy (as is) would provide no security and might only make sense in a guest network wherein no sensitive data is either transmitted or received. Consequently, at a minimum, a basic security scheme (in this case, WPA2/CCMP is recommended.

NOTE For information on configuring other encryption and authentication options available to the access point, refer to the *AP-7131N-FGR Access Point Product Reference Guide*. The guide is available on the Motorola Web site, at https://support.symbol.com/support/product/FIPS_and_CC_Compliant_Products.html.

2. Ensure the **Name** of the security policy suits the intended configuration of the policy.

   Multiple WLANs can share the same security policy, so be careful not to name security policies after specific WLANs or risk defining a WLAN to single policy. Motorola recommends naming the policy after the attributes of the authentication or encryption type selected.

3. Select the **WPA2/CCMP (802.11i)** option.



4. Configure the **Key Rotation Settings** as required to set Broadcast Key Rotation and the update interval.

Broadcast Key Rotation	Select the **Broadcast Key Rotation** checkbox to enable or disable broadcast key rotation. When enabled, the key indices used for encrypting/decrypting broadcast traffic will be alternatively rotated on every interval specified in the Broadcast Key Rotation Interval. Enabling broadcast key rotation enhances the broadcast traffic security on the WLAN. This value is disabled by default.
Update broadcast keys every (300-604800 seconds)	Specify a time period in seconds to rotate the key index used for the broadcast key. Set the interval to a shorter duration like 3600 seconds for tighter broadcast traffic security on the wireless LAN. Set the interval to a longer duration like 86400 seconds for less broadcast traffic security requirements. Default value is 86400 seconds.

5. Configure the **Key Settings** as needed to set a 256-bit key.

   256-bit Key — Enter 16 hexadecimal characters into each of the four fields.

   Default (hexadecimal) 256-bit keys for WP2A/CCMP include:

   1011121314151617

   18191A1B1C1D1E1F

   2021222324252627

   28292A2B2C2D2E2F

6. Configure the **Fast Roaming (802.1x only)** field as required to enable additional roaming and key caching options. This feature is applicable only when using 802.1x EAP authentication with WPA2/CCMP.

   Pre-Authentication — Selecting this option enables an associated MU to carry out an 802.1x authentication with another access point before it roams to it. The access point caches the keying information of the client until it roams to the other access point. This enables the roaming client to start sending and receiving data sooner by not having to do 802.1x authentication after it roams. This feature is only supported when 802.1x EAP authentication is enabled.

NOTE PMK key caching is enabled internally by default when 802.1x EAP authentication is enabled.

7. Click the **Apply** button to save the security policy and return to the **AP-71XX Quick Setup** screen.

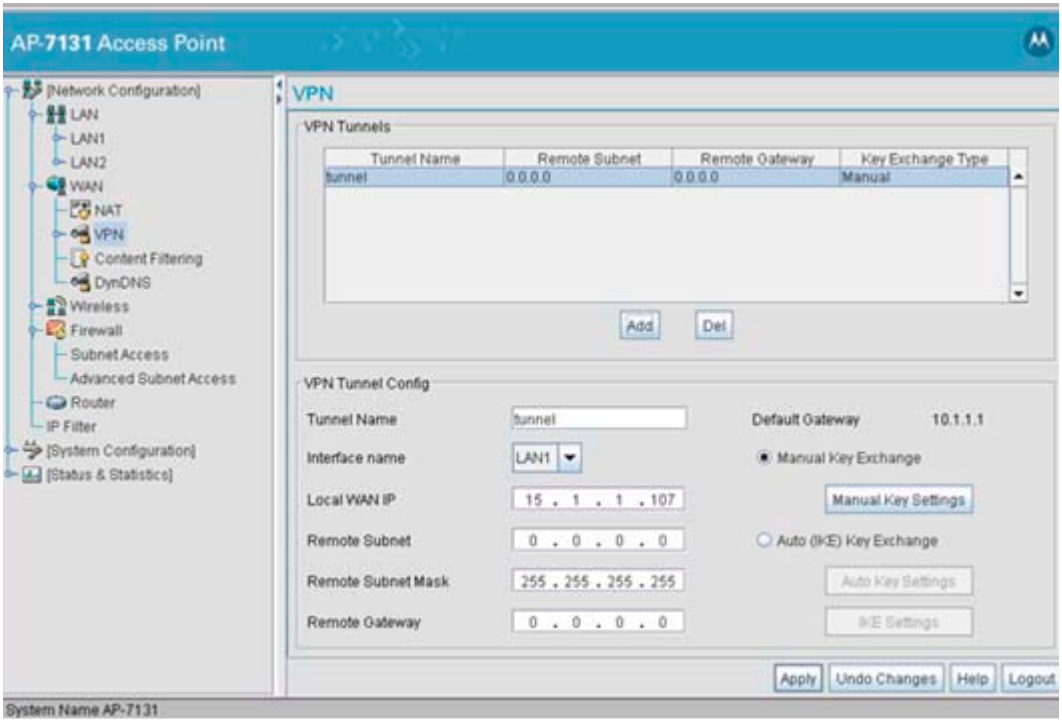
   At this point, you can either restrict specific MU access to the access point (using the ACL) or test the access point for MU interoperability.

3.4.2 Defining an IPSec VPN Tunnel

A secure IPSec VPN tunnel must be established between the AP-7131N-FGR and the external server providing the access point's external NTP, syslog or Radius resources. Ensure the IP address of the external NTP, syslog or Raidus resource is known, as it must be supplied to the access point for the access point to properly access and communicate with the external resource.

To define the attributes of the VPN tunnel:

1. Select **Network Configuration** -> **WAN** -> **VPN** from the access point menu tree.



2. Select the **Add** button from within the **VPN Tunnels** field to define the attributes of a new tunnel to provide secure access to the access point's external NTP, syslog or Radius resources.
3. Refer to the **VPN Tunnel Config** field and define the following attributes for the VPN tunnel:

Tunnel Name	Enter a name to define the VPN tunnel. The tunnel name is used to uniquely identify each tunnel.
Interface name	Use the drop-down menu to specify the LAN1, LAN2 or WAN connection used for routing VPN traffic. Remember, only one LAN connection can be active on the access point Ethernet port at a time.
Local WAN IP	Enter the WAN's numerical (non-DNS) IP address in order for the tunnel to pass traffic to a remote network.
Remote Subnet	Specify the numerical (non-DNS) IP address for the Remote Subnet.

Remote Subnet Mask	Enter the subnet mask for the tunnel's remote network for the tunnel. The remote subnet mask is the subnet setting for the remote network the tunnel connects to.
Remote Gateway	Enter a numerical (non-DNS) remote gateway IP address for the tunnel. The remote gateway IP address is the gateway address on the remote network the VPN tunnel connects to.

4. Select the **Auto (IKE) Key Exchange** checkbox and the **IKE Settings** button.

   IKE provides an automatic means of negotiation and authentication for communication between two or more entities.

5. Configure all the parameters within the **IKE Settings** screen.The IKE Authentication Passphrase must be shared by the external NTP, syslog or Radius resource.
6. From back within the VPN screen, select the **Auto (IKE) Key Exchange** checkbox and the **Auto Key Settings** button.

   Use the **Auto Key Settings** screen to specify the type of encryption and authentication used with the tunnel.

7. Configure all the parameters within the **Auto Key Settings** screen.

   For additional information on configuring either IKE Settings or Auto Key Settings, refer to the *AP-7131N-FGR Access Point Product Reference Guide* available at *https://support.symbol.com/support/product/FIPS_and_CC_Compliant_Products.html*.

8. Click **Apply** to save the configuration of the new tunnel.

   External NTP, syslog and Radius resources are now reachable from the access point's secure VPN tunnel. However, you must supply the access point with the IP address of the NTP, syslog or Radius server for the access point to connect to those external resources. For information on configuring external NTP, syslog and Radius server support, refer to the *AP-7131N-FGR Access Point Product Reference Guide* available at *https://support.symbol.com/support/product/FIPS_and_CC_Compliant_Products.html*.

3.4.3 Excluding MUs from Association

Optionally, use the access point *Access Control List ACL* to specify which MUs can or cannot gain access to an access point managed WLAN. By default, all mobile units can gain access. For specific information on configuring (restricting) MU access, refer to the *AP-7131N-FGR Access Point Product Reference Guide*. The guide is available on the Motorola Web site, at *https://support.symbol.com/support/product/FIPS_and_CC_Compliant_Products.html*.

3.4.4 Testing Mobile Unit Connectivity

Verify the access point's link with an MU by sending *Wireless Network Management Protocol* (WNMP) ping packets to the associated MU. Use the **Echo Test** screen to specify a target MU and configure the parameters of the ping test. The WNMP ping test only works with Motorola MUs. Only use a Motorola MU to test connectivity using WNMP.

To ping a specific MU to assess its connection with an access point:

NOTE Before testing for connectivity, the target MU needs to be set to the same ESSID as the access point. Since WPA2/CCMP has been configured for the access point, the MU also needs to be configured for WPA2/CCMP and use the same keys. Ensure the MU is associated with the access point before testing for connectivity.

1. Select **Status and Statistics** - > **MU Stats** from the menu tree.
2. Select the **Echo Test** button from within the **MU Stats Summary** screen.
3. Define the following ping test parameters:

Station Address	The station address is the IP address of the target MU. Refer to the **MU Stats Summary** screen for associated MU information.
Number of ping	Specify the number of ping packets to transmit to the target MU. The default is 100.
Packet Length	Specify the length of each data packet transmitted to the target MU during the ping test. The default is 100 bytes.

4. Click the **Ping** button to begin transmitting ping packets to the MU address specified.

   Refer to the **Number of Responses** to assess the number of responses from the target MU versus the number of pings transmitted by the access point. Use the ratio of packets sent versus packets received to assess the link quality between MU and the access point.

   Click the **Ok** button to exit the Echo Test screen and return to the MU Stats Summary screen.

   With basic access point and associated MU connectivity verified, the access point is now ready to operate as defined within this guide or have its more advanced features configured.

3.5 Where to Go From Here?

Once basic connectivity has been verified, the access point can be fully configured to meet the needs of the network and the users it supports. The sections referenced below are located within the *AP-7131N-FGR Access Point Product Reference Guide.* The guide is available on the Motorola Web site, at *https://support.symbol.com/support/product/FIPS_and_CC_Compliant_Products.html*.

- Refer to Chapter 4 to define System Settings (beyond the scope of the Quick Setup screen), configure access point device access, set SNMP values, log system events, set the access point system time and import device firmware and configuration files.
- See Chapter 5 for information on configuring the access point LAN and WAN ports, define up to 16 individual WLANs and their QoS policies and configure access point router settings.
- Refer to Chapter 6 for detailed information on configuring specific encryption (WPA2/CCMP) and authentication (802.1x EAP) security schemes, as well as VPN tunnel configuration and use case information.
- See Chapter 7 for information on accessing statistics helpful in monitoring the connection between the access point and its connected devices.
- Refer to Chapter 8 for information on using the access point *Command Line Interface (CLI),* as accessed through the serial port or Telnet.
- See Appendix A for device specifications for both the AP-7131N-FGR.

4 Specifications

4.1 Physical Characteristics

An AP-7131N-FGR access point has the following physical characteristics:

Dimensions	5.50 in. Depth x 7.88 in. Width x 1.38 in. Height 14 cm Depth x 20.32 cm Width x 3.5 cm Height
Housing	Metal, plenum-rated housing (UL2043)
Weight	2.7 lbs
Operating Temperature	-4°F to 122°F/-20°C to 50°C
Storage Temperature	-40°F to 158°F/-40°C to 70°C
Humidity	5 to 95% RH non-condensing
Electrostatic Discharge	15kV air, 8kV contact

4.2 Electrical Characteristics

The AP-7131N-FGR access point has the following electrical characteristics:

Operating Voltage	48VDC (compatible with POE .3af/.3at Draft)
Operating Current	Not to exceed 750mA @ 48VDC
Power	48VDC, 0.75A

4.3 Radio Characteristics

An AP-7131N-FGR has the following radio characteristics:

Operating Channels	All channels from 4920 MHz to 5825 MHz except channel 52 -64 Channels 1-13 (EU), Channels 1-11 (US/Canada) Channel 14 (2484 MHz) Japan only Actual operating frequencies depend on regulatory
Data Rates Supported	802.11g: 1,2,5.5,11,6,9,12,18,24,36,48, and 54Mbps 802.11a: 6,9,12,18,24,36,48, and 54Mbps 802.11n: MCS 0-15 up to 300Mbps
Wireless Medium	*Direct Sequence Spread Spectrum* (DSSS), *Orthogonal Frequency Division Multiplexing* (OFDM) *Spatial multiplexing* (MIMO)
Network Standards	802.11a, 802.11b, 802.11g, 802.3, 802.11n (Draft 2.0)
Maximum Available Transmit Power	Maximum available conducted transmit power per chain: 2.4Ghz: + 23dBm Maximum available conducted transmit power all chains: 2.4GHz: + 27.7dBm Maximum available conducted transmit power per chain: 5.2Ghz: + 20 dBm Maximum available conducted transmit power all chains: 5.2GHz: + 24.7dBm
Transmit Power Adjustment	1dB increments
Antenna Configuration	2x3 or 3x3

5 Regulatory Compliance

This device is approved under the Symbol Technologies brand; Symbol Technologies, Inc., is the Enterprise Mobility business of Motorola, Inc ("Motorola").

All Motorola devices are designed to be compliant with rules and regulations in locations they are sold and will be labeled as required. Any changes or modifications to Motorola equipment, not expressly approved by Motorola, could void the user's authority to operate the equipment.

Local language translations are available at the following website:
http://support.symbol.com/support/product/manuals.do.

Motorola's devices are professionally installed, the Radio Frequency Output Power will not exceed the maximum allowable limit for the country of operation.

Antennas: Use only the supplied or an approved replacement antenna. Unauthorized antennas, modifications, or attachments could cause damage and may violate regulations.

Country Approvals

Regulatory markings are applied to the device signifying the radio (s) are approved for use in the following countries: United States, Canada, Australia, Japan and Europe.

Please refer to the *Declaration of Conformity* (DoC) for details of other country markings. This is available at *http://www2.symbol.com/doc/*.

Note 1: For 2.4GHz Products: Europe includes, Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovak Republic, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

Operation of the device without regulatory approval is illegal.

Health and Safety Recommendations

Warnings for the use of Wireless Devices

Please observe all warning notices with regard to the usage of wireless devices.

Potentially Hazardous Atmospheres

You are reminded of the need to observe restrictions on the use of radio devices in fuel depots, chemical plants etc. and areas where the air contains chemicals or particles (such as grain, dust, or metal powders).

Safety in Hospitals

Wireless devices transmit radio frequency energy and may affect medical electrical equipment. When installed adjacent to other equipment, it is advised to verify that the adjacent equipment is not adversely affected.

RF Exposure Guidelines

Safety Information

The device complies with Internationally recognized standards covering human exposure to electromagnetic fields from radio devices.

Reducing RF Exposure—Use Properly

Only operate the device in accordance with the instructions supplied.

Remote and Standalone Antenna Configurations

To comply with FCC RF exposure requirements, antennas that are mounted externally at remote locations or operating near users at stand-alone desktop of similar configurations must operate with a minimum separation distance of 20 cm from all persons.

Power Supply

Use only a Motorola approved power supply output rated at 48Vdc and minimum 0.75A. The power supply shall be Listed to UL/CSA 60950-1; and certified to IEC60950-1 and EN60950-1 with SELV outputs.

Use only a Motorola approved power supply. Use of alternative power supply will invalidate any approval given to this device and may be dangerous.

Wireless Devices - Countries

Country Selection

Select only the country in which you are using the device. Any other selection will make the operation of this device illegal.

Operation in the US

The use on UNII (Unlicensed National Information Infrastructure) Band 1 5150-5250 MHz is restricted to indoor use only, any other use will make the operation of this device illegal.

The available channels for 802.11 b/g operation in the US are Channels 1 to 11. The range of channels is limited by firmware.

Radio Frequency Interference Requirements—FCC

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Radio Transmitters (Part 15)

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.

Radio Frequency Interference Requirements – Canada

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Devices using the 5.470 – 5.725 GHz band shall not be capable of transmitting in the band 5.60-5.65 GHz in Canada, make sure that Canada is the country selected during setup to ensure compliance.

Radio Transmitters

This device complies with RSS 210 of Industry & Science Canada. 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.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that permitted for successful communication.

This device has been designed to operate with the antennas listed in this guide, and having a maximum gain of 13.9 dBi (2.4 GHz) and 13 dBi (5 GHz) for radios one and two. Antennas not included in this list, or having a gain greater than 13.9 dBi (2.4 GHz) and 13 dBi (5 GHz) for radios one and two, are prohibited for use with this device. This device has been designed to operate with the antennas listed in this guide, and having a maximum gain of 3.03 dBi (2.4 GHz) and 4.06 dBi (5 GHz) for radio three. Antennas not included in this list, or having a gain greater than 3.03 dBi (2.4 GHz) and 4.06 dBi (5 GHz) for radio three, are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

Label Marking: The Term "IC:" before the radio certification signifies that Industry Canada technical specifications were met.

This device has been designed to operate with the antennas listed in the *Enterprise Wireless LAN Antenna Specification Guide*. Refer to the guide at http://support.symbol.com/support/product/manuals.do.

CE Marking and European Economic Area (EEA)

The use of 2.4GHz RLAN's, for use through the EEA, have the following restrictions:

- Maximum radiated transmit power of 100 mW EIRP in the frequency range 2.400 -2.4835 GHz.
- France outside usage, the equipment is restricted to 2.400-2.45 GHz frequency range.
- Italy requires a user license for outside usage.

Statement of Compliance

Motorola hereby, declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. A Declaration of Conformity may be obtained from *http://www2.symbol.com/doc/*.

Japan (VCCI) - Voluntary Control Council for Interference

Class B ITE

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

Korea Warning Statement for Class B

기 종 별	사 용 자 안 내 문
B 급 기기 (가정용 방송통신기기)	이 기기는 가정용 (B 급) 으로 전자파적합등록을 한 기기로서 주로 가정에서 사용하는 것을 목적으로 하며 , 모든 지역에서 사용할 수 있습니다 .
Class B (Broadcasting Communication Device for Home Use)	This device obtained EMC registration mainly for home use (Class B) and may be used in all areas.

Other Countries

Autstralia

Use of 5GHz RLAN's in Australia is restricted in the following band 5.50 – 5.65GHz.

Brazil

Regulatory declarations for AP7131N - BRAZIL

Note: The certification mark applied to the AP7131N is for Restrict Radiation Equipment. This equipment operates on a secondary basis and does not have the right for protection against harmful interference from other users including same equipment types. Also this equipment must not cause interference to systems operating on primary basis.

For more information consult the website *www.anatel.gov.br*

Declarações Regulamentares para AP7131N - Brasil

Nota: A marca de certificação se aplica ao Transceptor, modelo AP-7131N. Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário. Para maiores informações sobre ANATEL consulte o site: *www.anatel.gov.br*

Chile

Este equipo cumple con la Resolución No 403 de 2008, de la Subsecretaria de telecomunicaciones, relativa a radiaciones electromagnéticas.

This device complies with the Resolution Not 403 of 2008, of the Undersecretary of telecommunications, relating to electromagnetic radiation.

Mexico

Restrict Frequency Range to: 2.450 – 2.4835 GHz.

Taiwan

NOTICE!

According to: Administrative Regulations on Low Power Radio Waves Radiated Devices

Article 12

Without permission granted by the DGT, any company, enterprise, or user is not allowed to change frequency, enhance transmitting power or alter original characteristic as well as performance to a approved low power radio-frequency devices.

Article 14

The low power radio-frequency devices shall not influence aircraft security and interfere legal communications; If found, the user shall cease operating immediately until no interference is achieved. The said legal communications means radio communications is operated in compliance with the Telecommunications Act. The low power radio-frequency devices must be susceptible with the interference from legal communications or ISM radio wave radiated devices.

臺灣

低功率電波輻射性電機管理辦法

第十二條
經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電通信。
低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

限制頻率範圍是：2.400 - 2.4835 GHz。　最大發射功率：27dBm
5.250 - 5.350 GHz。　最大發射功率：17dBm
5.725 - 5.850 GHz。　最大發射功率：24dBm

2.4GHz：11個通道
5GHz：　8個通道

Wireless device operate in the frequency band of 5.25-5.35 GHz, limited for Indoor use only.

在 5.25-5.35 秭赫頻帶內操作之無線資訊傳輸設備，限於室內使用

Korea

For a radio equipment using 2400~2483.5MHz or 5725~5825MHz, the following two expression should be displayed;

1. This radio equipment can be interfered during operation.

당해 무선설비는 운용 중 전파혼신 가능성이 있음

2. This radio equipment cannot provide a service relevant to the human life safety.

당해 무선설비 는전파혼 신 가능성이 있으므로 인명안전과 관련된 서비스는 할 수 없습니다 .

6 Waste Electrical and Electronic Equipment (WEEE)

English: For EU Customers: All products at the end of their life must be returned to Symbol for recycling. For information on how to return product, please go to: http://www.symbol.com/environmental_compliance.

Čeština: Pro zákazníky z EU: Všechny produkty je nutné po skončení jejich životnosti vrátit společnosti Symbol k recyklaci. Informace o způsobu vrácení produktu najdete na webové stránce: http://www.symbol.com/environmental_compliance.

Dansk: Til kunder i EU: Alle produkter skal returneres til Symbol til recirkulering, når de er udtjent. Læs oplysningerne om returnering af produkter på: http://www.symbol.com/environmental_compliance.

Deutsch: Für Kunden innerhalb der EU: Alle Produkte müssen am Ende ihrer Lebensdauer zum Recycling an Symbol zurückgesandt werden. Informationen zur Rücksendung von Produkten finden Sie unter http://www.symbol.com/environmental_compliance.

Eesti: EL klientidele: kõik tooted tuleb nende eluea lõppedes tagastada taaskasutamise eesmärgil Symbol'ile. Lisainformatsiooni saamiseks toote tagastamise kohta külastage palun aadressi: http://www.symbol.com/environmental_compliance.

Español: Para clientes en la Unión Europea: todos los productos deberán entregarse a Symbol al final de su ciclo de vida para que sean reciclados. Si desea más información sobre cómo devolver un producto, visite: http://www.symbol.com/environmental_compliance.

Ελληνικά: Για πελάτες στην Ε.Ε.: Όλα τα προϊόντα, στο τέλος της διάρκειας ζωής τους, πρέπει να επιστρέφονται στην Symbol για ανακύκλωση. Για περισσότερες πληροφορίες σχετικά με την επιστροφή ενός προϊόντος, επισκεφθείτε τη διεύθυνση http://www.symbol.com/environmental_compliance στο Διαδίκτυο.

Français : Clients de l'Union Européenne : Tous les produits en fin de cycle de vie doivent être retournés à Symbol pour recyclage. Pour de plus amples informations sur le retour de produits, consultez : http://www.symbol.com/environmental_compliance.

Italiano: per i clienti dell'UE: tutti i prodotti che sono giunti al termine del rispettivo ciclo di vita devono essere restituiti a Symbol al fine di consentirne il riciclaggio. Per informazioni sulle modalità di restituzione, visitare il seguente sito Web: http://www.symbol.com/environmental_compliance.

Latviešu: ES klientiem: visi produkti pēc to kalpošanas mūža beigām ir jānogādā atpakaļ Symbol otrreizējai pārstrādei. Lai iegūtu informāciju par produktu nogādāšanu Symbol, lūdzu, skatiet: http://www.symbol.com/environmental_compliance.

Lietuvių: ES vartotojams: visi gaminiai, pasibaigus jų eksploatacijos laikui, turi būti grąžinti utilizuoti į kompaniją „Symbol“. Daugiau informacijos, kaip grąžinti gaminį, rasite: http://www.symbol.com/environmental_compliance.

Magyar: Az EU-ban vásárlóknak: Minden tönkrement terméket a Symbol vállalathoz kell eljuttatni újrahasznosítás céljából. A termék visszajuttatásának módjával kapcsolatos tudnivalókért látogasson el a http://www.symbol.com/environmental_compliance weboldalra

Malti: Għal klijenti fl-UE: il-prodotti kollha li jkunu waslu fl-aħħar tal-ħajja ta' l-użu tagħhom, iridu jiġu rritornati għand Symbol għar-riċiklaġġ. Għal aktar tagħrif dwar kif għandek tirritorna l-prodott, jekk jogħġbok żur: http://www.symbol.com/environmental_compliance.

Nederlands: Voor klanten in de EU: alle producten dienen aan het einde van hun levensduur naar Symbol te worden teruggezonden voor recycling. Raadpleeg http://www.symbol.com/environmental_compliance voor meer informatie over het terugzenden van producten.

Polski: Klienci z obszaru Unii Europejskiej: Produkty wycofane z eksploatacji należy zwrócić do firmy Symbol w celu ich utylizacji. Informacje na temat zwrotu produktów znajdują się na stronie internetowej http://www.symbol.com/environmental_compliance.

Português: Para clientes da UE: todos os produtos no fim de vida devem ser devolvidos à Symbol para reciclagem. Para obter informações sobre como devolver o produto, visite: http://www.symbol.com/environmental_compliance.

Slovenski: Za kupce v EU: vsi izdelki se morajo po poteku življenjske dobe vrniti podjetju Symbol za reciklažo. Za informacije o vraèilu izdelka obišèite: http://www.symbol.com/environmental_compliance.

Slovenščina: Pre zákazníkov z krajín EU: Všetky výrobky musia byť po uplynutí doby ich životnosti vrátené spoločnosti Symbol na recykláciu. Bližšie informácie o vrátení výrobkov nájdete na: http://www.symbol.com/environmental_compliance.

Suomi: Asiakkaat Euroopan unionin alueella: Kaikki tuotteet on palautettava kierrätettäväksi Symbol-yhtiöön, kun tuotetta ei enää käytetä. Lisätietoja tuotteen palauttamisesta on osoitteessa http://www.symbol.com/environmental_compliance.

7 Motorola's Enterprise Mobility Support Center

If you have a problem with your equipment, contact Enterprise Mobility support for your region. Contact information is available at: http://support.symbol.com/support/.

When contacting Enterprise Mobility support, please provide the following information:

- *Serial number of the unit*
- *Model number or product name*
- *Software type and version number*

Motorola responds to calls by email, telephone or fax within the time limits set forth in support agreements. If you purchased your Enterprise Mobility business product from a Motorola business partner, contact that business partner for support.

Customer Support Web Sites

Motorola's Support Central Web site, located at http://support.symbol.com/support/ provides information and online assistance including developer tools, software downloads, product manuals and online repair requests.

Manuals

For general Motorola Enterprise Wireless LAN releases:

http://support.symbol.com/support/product/manuals.do

For the AP-7131N-FGR:

https://support.symbol.com/support/product/FIPS_and_CC_Compliant_Products.html

General Information

Obtain additional information by contacting Motorola at:

Telephone (North America): 1-800-722-6234
Telephone (International): +1-631-738-5200
Website: http://www.motorola.com

8 ROHS Compliance

有毒有害物质或元素						
部件名称 **(Parts)**	铅 **(Pb)**	汞 **(Hg)**	镉 **(Cd)**	六价铬 **(Cr^{6+})**	多溴联苯 **(PBB)**	多溴二苯醚 **(PBDE)**
金属部件 (Metal Parts)	X	O	O	O	O	O
电路模块 (Circuit Modules)	X	O	O	O	O	O
电缆及电缆组件 (Cables and Cable Assemblies)	X	O	O	O	O	O
塑料和聚合物部件 (Plastic and Polymeric Parts)	O	O	O	O	O	O
光学和光学组件 (Optics and Optical Components)	O	O	O	O	O	O
电池 (Batteries)	O	O	O	O	O	O

O：表示该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T11363-2006 标准规定的限量要求以下。

X :表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 SJ/T11363-2006 标准规定的限量要求。

对销售之日的所售产品，本表表示，公司供应链的电子信息产品可能包含这些物质。注意：在所售产品中可能会也可能不会含有所有所列的部件。

This table was created to comply with China RoHS requirements for Motorola’s AP-7131N-FGR model access point.

MOTOROLA INC
1303 E. ALGONQUIN ROAD
SCHAUMBURG, IL 60196
http://www.motorola.com

72E-126726-01 Revision A
August 2009