# NXG-7002(-SIM) 4G Cellular and WiFi Router Module Installation Sheet

Product Summary

4G Cellular Modem

This module adds 4G cellular communication capabilities to the xGenConnect alarm panel, allowing alarm reporting and remote connections over the 4G mobile network via UltraSync Cloud.

In the event that the primary path (WiFi or Ethernet) from the customer's broadband internet is not working, the panel will automatically switch to the backup 4G cellular to provide seamless alarm reporting.
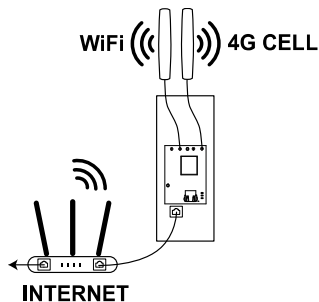

If 4G is unavailable, the module will switch to 2G where available. One SIM card may be pre-installed and should not be removed.

Only alarm traffic is routed to 4G, video from cameras is not.
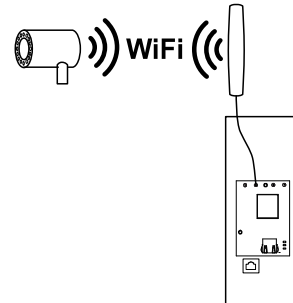
WiFi Client Mode

In client-mode, the WiFi Router can connect wirelessly to a customer's WiFi router which will provide the primary internet connection to the xGenConnect panel. This avoids having to install an Ethernet cable between the xGenConnect and the customer's router.
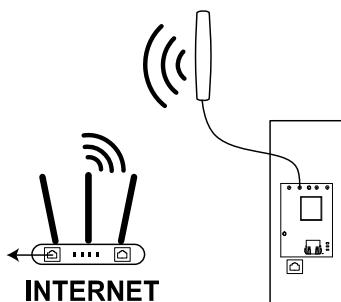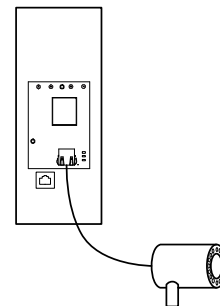

WiFi Access Point Mode

In access-point-mode, security devices such as WiFi cameras should be connected to the WiFi Router. It provides DHCP services to assign camera IP addresses and performs router functions for connected devices. This separates the cameras from the customer's network for better performance and security.
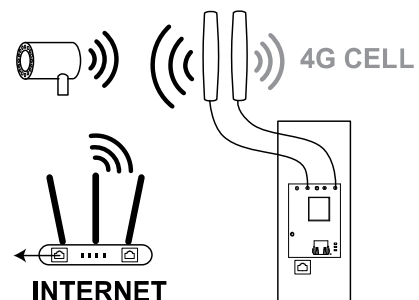

Wired LAN

The WiFi Router provides a wired Ethernet LAN for connecting one or more cameras. An ethernet switch may be connected to this Ethernet port.

Full Wireless Integration

Access Point and Client modes can operate simultaneously to allow flexible connection of equipment with 4G cellular backup.

Before You Begin

The xGenConnect panel must be provisioned before going to site. This allows the panel to connect to the servers so it can be programmed using the UltraSync+ app.

The module's SIM cards must be activated to provide internet to the panel. The cellular connection also allows initial programming of the module using the UltraSync+ app.

The xGenConnect panel should be configured to allow remote access. This requires the Web Access Passcode to be set, and the site added to the UltraSync+ app.

Pre-Installation Check

OpenSignal is a 3rd party app that can be used to check cellular signal levels, location of cell towers, and perform speed tests. It may assist installers in identifying a suitable location for the alarm panel.

If the alarm panel is installed in a location with poor cellular signal, it may report intermittent communication errors.

Contact OpenSignal for support on the app.

1. Download and install the OpenSignal app on your smart phone.

2. Open the app and check 4G signal level is three bars or more.

3. If signal level is poor, find an alternative location with three bars or more. Installing multiple or high gain antennas may assist.

Installing the Module
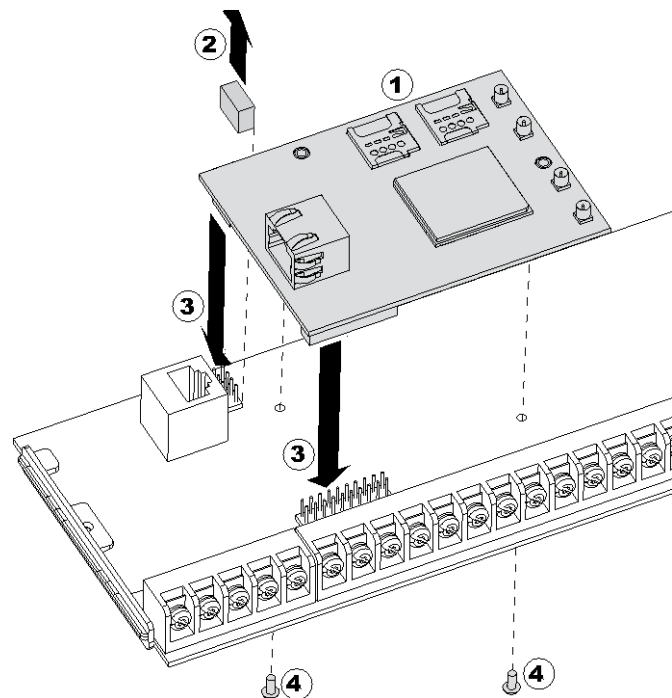
1. Check the SIM card is installed in the SIM1 slot.

2. Remove J14, an 8-way header on the xGenConnect located next to the Ethernet port. This connects the Ethernet WAN port pins to the panel or redirects them to the module.

3. Align the module to the 8-pin and 16-pin headers on the xGenConnect. Push down to attach the module. Take care not to bend the pins.

4. Attach the provided screws to the reverse side of the xGenConnect to secure the module. Do not overtighten screws.
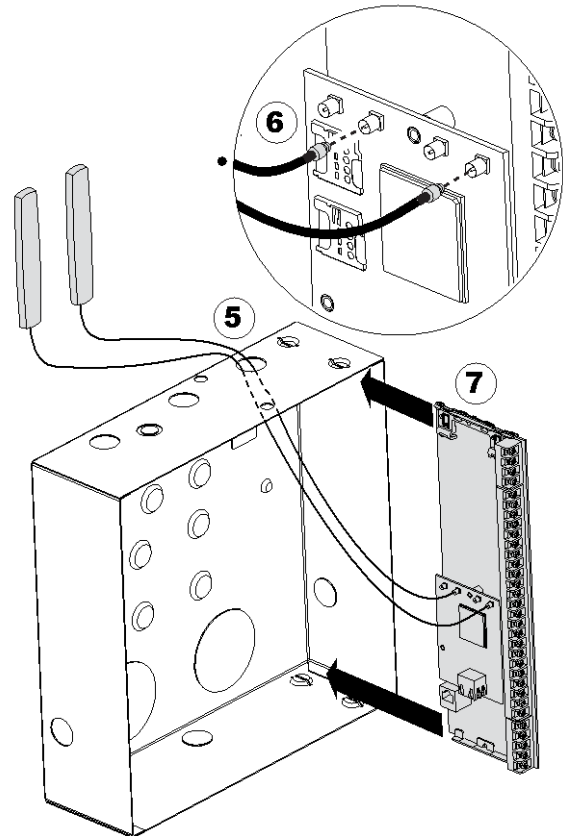
5. Remove knockouts as needed from metal box, then feed the two antennas through.

6. Connect the antennas to the MMCX jacks on the module labeled MAIN. Both supplied antennas are identical. Do not attach to wall yet.

7. Slide the xGenConnect into the metal box.

8. Turn on power to xGenConnect. The LEDs on the module should light:
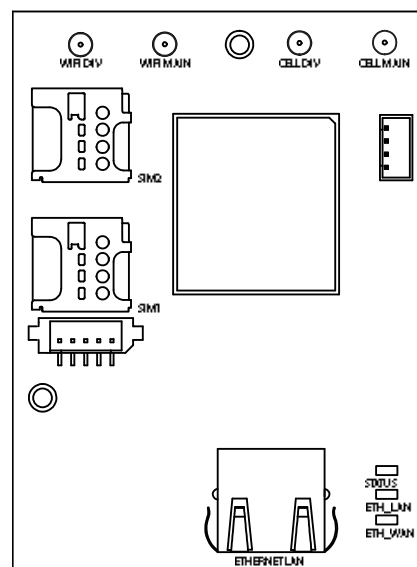
**STATUS**: on indicates power is connected to the module.

ETH_LAN: on indicates LAN cable plugged in to module, off indicates LAN cable not plugged in, blinking indicates activity on LAN port.

ETH_WAN: on indicates WAN cable plugged into panel, off indicates WAN cable not plugged in, blinking indicates activity on WAN port.

9. Check the signal level of the 4G and cellular (see following page).

10. The module supports "antenna diversity" to improve multipath reception. If signal level is not sufficient on either WiFi or cellular, then install extra antenna(s) by connecting them to the MMCX jack(s) labeled "DIV".

    For best reception, install the DIVersity antennas parallel to the MAIN antennas and at least 20cm apart. Antennas should be attached away from metal surfaces.

11. Once module is fully functioning, fix the antennas vertically to the wall. Surface should be clean and dry. The alarm panel should look like this once assembled:
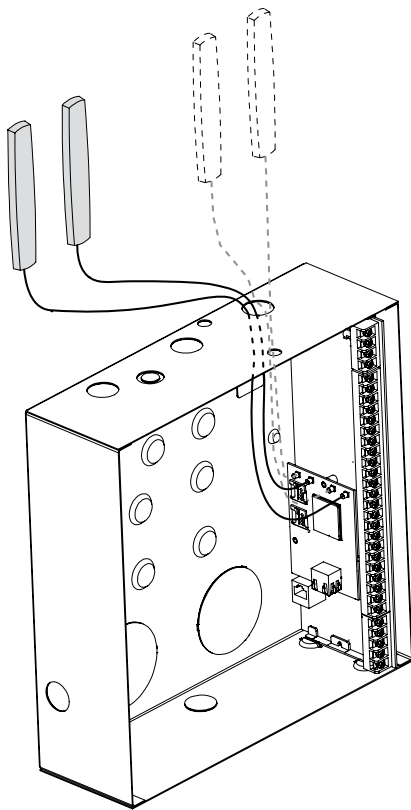
Single/Dual Path Reporting

If only single path cellular reporting is required, then follow steps to check signal level.

If dual path (cellular and WiFi/Ethernet) reporting is required, check signal level then complete steps to "Connect WiFi Router to Customer Router".

If single path WiFi/Ethernet reporting is required, skip to "Connect WiFi Router to Customer Router".

Note: Dual path is only available if the panel Ethernet reporting and the cellular module reporting are used.

Check Signal Strength Using NXG-1820 Keypad

1. Turn on power.

2. Wait 3 minutes for the module to boot and connect to the cellular network.

3. Enter a valid PIN on NXG-1820 keypad to get access to the main screen.

4. Press MENU, enter PIN, press ENTER, go to Settings > Status > Connection Status.

5. Check "UltraSync Status" shows "Connected".

6. Scroll Right ▶.

7. Check "Signal Strength" is acceptable.

Signal Strength

← Low →	← OK →

−121	−106	−105	−77	−76	−51
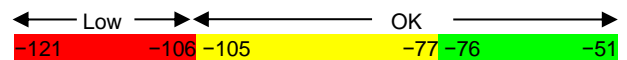
• If the reported value is −105 to −51 then the signal level is OK.

• If the reported value is −121 to −106 then installing an external high-gain antenna is recommended.

Note: Signal levels vary day to day and are not absolute values. Use the UltraSync Portal to track signal level performance over time.

Default the Module

If required, clear all the settings of the module back to factory default:

1. Launch the UltraSync+ app.

2. Click the site name to login to the panel.

3. Click the Menu button on the top left.

4. Click Advanced.

5. Click Shortcut.

6. Enter 24.910.

7. Press ENTER.

Connect WiFi Router to Customer Router

Method 1 – Scan for WiFi Router

1. Login to the panel.

2. Click Advanced > Communicator > IP Configuration > IP Options.

3. Tick "Enable WiFi / Disable Ethernet".

4. Click Save.

5. Click Logout to activate the change.

6. Login to the panel.

7. Click Settings > WiFi Setup.

8. Click "Scan for Wireless Networks".

9. Wait 30 sec for the router to complete searching for nearby WiFi access points.

10. Select the customer's WiFi router from the list.

11. Enter the Passphrase of the customer's WiFi router.

12. Click Logout.

13. Power cycle panel.

14. Click Settings > Connection Status.

15. Check "WiFi Status" shows "Connected" to the correct customer router SSID.

Method 2 – Manually enter SSID

1. Login to the panel.

2. Click Advanced > Communicator > IP Configuration > IP Options.

3. Tick "Enable WiFi / Disable Ethernet".

4. Click Save.

5. Click Logout to activate the change.

6. Login to the panel.

7. Click Settings > Network.

8. Enter the customer's WiFi router details (SSID, Security Type, and Passphrase).

9. Click Save.

10. Click Settings > Connection Status for connection details.

Method 3 – Use Ethernet cable

Alternatively, you may connect the Ethernet WAN port on the xGenConnect directly to the customer's router using an Ethernet cable. This will provide the most reliable primary path connection.

Connect Camera to WiFi Router

If the xGenConnect is installed without the WiFi Router Module, optional cameras would normally connect to the customer's WiFi broadband router.

With the WiFi Router Module installed, UltraSync cameras should be connected to the Access Point (AP) Mode on the WiFi Router Module.

Settings Selector

Network

Save

LAN configuration

IP Host Name

Enable DHCP ☑

IP Address	192	168	31	66
Gateway	192	168	31	1
Subnet	255	255	255	0
Primary DNS	192	168	31	1
Secondary DNS	0	0	0	0

WiFi Configuration

WiFi SSID

WiFi Security Type
WPA2-PSK

WiFi Password

WiFi Internal Access Point SSID
NXX_8_WZ_AU_113625466955

WiFi Internal Access Point Security Type
WPA2-PSK

WiFi Internal Access Point Password

1. Log in to the panel.

2. Click Click Settings > Network.

3. Configure "WiFi Internal Access Point. SSID" up to 31 alphanumeric characters.

4. Configure "WiFi Internal Access Point Security Type": WPA2-PSK.

5. Configure "WiFi Internal Access Point Password" between 8 and 63 alphanumeric characters.

6. Click Save then Logout. The Access Point will then be enabled.

7. Open UltraSync+ app.

8. Run "New Device Setup".

9. Enter the above SSID and password when prompted.

The cameras will then connect to the router.

Troubleshooting

The router cannot connect to home WiFi, Access Point SSID does not appear, or panel does not appear in DLX900 Network Discover

Cycle panel power to reboot the router.

Signal Strength is poor, unable to connect using app

If cellular reception is poor, and the panel is on cellular-only connection, then the app will be unable to connect. Provide

internet to the panel, so programming can be done using the app:

1. Connect an Ethernet cable to the Ethernet WAN port on the xGenConnect panel.

2. Connect the other end of the Ethernet cable to an available LAN port on the customer's router.

Panel should now connect to servers and app will be able to access programming menus.

Check Signal Strength Using UltraSync+ App

1. Turn on power.

2. Log in to the panel using UltraSync+.

3. Click Settings > Connection Status.

4. Scroll down to Signal Strength.

5. Check whether Signal Strength is acceptable.

Check Signal Strength Using Web Server

1. Turn on power.

2. Connect device (smartphone or laptop) to customer's router.

3. On the keypad, go to the Installer menu and select Communicator > IP Configuration > IP Address, and note the IP address displayed.

4. Open web browser and enter panel IP address.

5. Log in to the panel.

6. Click Settings > Connection Status.

7. Scroll down to Signal Strength.

8. Check whether Signal Strength is acceptable.

WiFi Setup screen shows "WiFi Mode Not Enabled"

1. Click Advanced > Communicator > IP Configuration > IP Options.

2. Tick "Enable WiFi / Disable Ethernet".

3. Click Save.

4. Click Logout to activate the change.

Cell State does not show Connected, Cell Service is not showing a valid service

If SIM card(s) are preinstalled, no configuration is necessary. Check SIM cards are installed correctly, SIM1 is prioritized, try defaulting the module, and power cycling the system.

If SIM card(s) require custom settings:

1. Login to the panel (e.g. UltraSync+ app)

2. Click Advanced > Communicator > Cellular Configuration.

3. Click SIM1.

4. Enter the APN, Username, Password, as instructed by the carrier.

5. Click Save.

6. Click Settings > Connection Status.

7. Check SIM cards are connecting to their network.

Alarm Transmission Path and Alarm Transmission System Faults

See *xGenConnect Installation and Programming Guide*, section "Alarm Transmission Path and Alarm Transmission System Faults" for information.

Cannot access cameras

Alarm messages and video streaming require a functioning primary IP path. This is via the WiFi Client Mode or Ethernet cable to the customer router.

1. Check UltraSync Portal for camera state.

2. Check the primary IP path is connected and functioning.

3. Reboot the customer router and wait 5 minutes.

4. If still not working, power cycle panel and wait 5 minutes.

5. If still not working, power cycle camera(s) and wait 5 minutes.

Secondary cellular path is only for alarm delivery. Video features cannot be accessed via the cellular network.

Cannot scan WiFi cameras

1. Cameras must be added using the UltraSync+ app to activate them.

2. Check cameras are connected to access point SSID.

3. Camera password must not be default.

4. Default camera and re-add using UltraSync+ app.

5. Check antennas are in vertical orientation

6. Check antennas are connected to MAIN and not DIV.

Cannot scan Ethernet cameras

Managed PoE switches for Ethernet connected cameras are not advised. Use normal unmanaged PoE switch.

Switch LAN port should be plugged in to LAN port on router module, not WAN port on panel.

Devices on AP Mode not stable

Only cameras and touchscreens should be connected to the wireless access point. Do not connect any other device to the access point.

Typical range of WiFi signal is up to 30 m. Best performance is when devices are within 10m of the router. This is dependent on the environment and the obstructions (walls) between the router and the device.

Extend the range of the router WiFi network by connecting a mesh router supporting 802.11b/g/n to the LAN port on the router. Then install additional mesh nodes between the mesh router and cameras/touchscreens.

Client Mode frequently disconnects

Check connection log in UltraSync Portal. Disconnections or frequent path switching may indicate poor internet connection of customer router to ISP.

Best WiFi performance is when panel router is within 10m of customer's router.

Features

- Client Mode – router can connect to customer's broadband router as a client to report alarm messages and stream cameras. Alarm delivery and video is delivered over the primary IP path (WiFi to customer's broadband router).

- Access Point Mode – router can provide an access point to allow cameras and touchscreens to connect to the system. This separates security devices from end-user equipment.

- Cellular Backup – module can provide a secondary path over a cellular network to deliver alarm messages if the primary IP path is unavailable. Dual path or single path cellular reporting must be enabled in the UltraSync Portal.

- Camera Support – supports up to sixteen (16) UltraSync Gen 2 Bullet and Indoor Cube Cameras. Cameras must be activated using the UltraSync+ app or have a secure password set.

    Note: Doorbell camera is not supported.

- Touchscreen Support – supports up to four (4) WiFi Secondary Touchscreens.

- Access Point SSID – can be configured up to 31 alphanumeric characters.

- Access Point Password – can be configured between 8 to 63 alphanumeric characters. Default is blank which disables the Access Point feature.

- Authentication – WPA2-PSK (AES) is default and recommended. WPA and WPA/WPA are supported.

- DHCP Server – security devices connecting to the router can be allocated an IP address using DHCP.

- DHCP IP Address Range – 192.168.33.100 to 192.168.33.250

- IP Address Range – for devices configured with a static IP address, use 192.168.33.10 to 192.168.33.250

- Lease Period – 12 hours.

- DNS – fixed at 192.168.33.1.

- Gateway – fixed at 192.168.33.1.

Specifications

Compatible alarm receivers (RCT)	UltraSync Receiver, OH NetRec Receiver
Voltage	13.8 VDC (provided by panel)
Current	
Maximum	200 mA at 13.8 V
Quiescent	118 mA at 13.8 V
Average	138 mA at 13.8 V
Frequency band	GSM/GPRS/EDGE: 900 / 1800 MHz
	LTE: 800 MHz (B20) / 900 MHz (B8) / 1800 MHz (B3) / 2100 MHz (B1)
Transmit power	EGSM900: Class 4 (+32.5 dBm ±2 dB)
	GSM1800: Class 1 (+30 dBm ±2 dB)
	GSM900 8-PSK: Class E2 (+26.5 dBm ±3 dB)
	GSM1800 8-PSK: Class E2 (+26 dBm +3/−4 dB)
	LTE800, LTE FDD B20, LTE900, LTE FDD B8, LTE1800, LTE FDD B3, LTE2100, LTE FDD B1: Class 3 (+23 dBm ±2 dB)

External connector	MMCX
Dimensions (W × H × D)	136 x 80 x 5 mm
Storage temperature	−34° to 60°C (−30° to 140°F)
Weight	150 g
Operating environment	
Temperature	−10° to 55°C (14° to 131°F)
Relative humidity	maximum 90% noncondensing
Environmental class	II

Regulatory information

Manufacturer	Placed on the market by: Carrier Fire & Security Americas Corporation, Inc. 13995 Pasteur Blvd Palm Beach Gardens, FL 33418, USA Authorized EU manufacturing representative: Carrier Fire & Security B.V. Kelvinstraat 7, 6003 DH Weert, Netherlands
Product warnings and disclaimers	THESE PRODUCTS ARE INTENDED FOR SALE TO AND INSTALLATION BY QUALIFIED PROFESSIONALS. CARRIER FIRE & SECURITY CANNOT PROVIDE ANY ASSURANCE THAT ANY PERSON OR ENTITY BUYING ITS PRODUCTS, INCLUDING ANY "AUTHORIZED DEALER" OR "AUTHORIZED RESELLER", IS PROPERLY TRAINED OR EXPERIENCED TO CORRECTLY INSTALL FIRE AND SECURITY RELATED PRODUCTS. For more information on warranty disclaimers and product safety information, please check https://firesecurityproducts.com/policy/product-warning/ or scan the QR code.
Certification	EN 50136-2:2013, EN 50131-10:2014 SP3 and SP4 (GSM/GPRS) DP2/DP3 (GSM/GPRS with control panel IP) Tested and certified by Telefication B.V. $C \epsilon$
European Union directives	Carrier Fire & Security hereby declares that this device is in compliance with the applicable requirements and provisions of all applicable rules and regulations, including but not limited to the Directive 2014/53/EU. For more information see: firesecurityproducts.com
REACH	Product may contain substances that are also Candidate List substances in a concentration above 0.1% w/w, per the most recently published Candidate List found at ECHA Web site. Safe use information can be found at https://firesecurityproducts.com/en/content/intrusion-intro
	2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: recyclethis.info.

Contact information

www.firesecurityproducts.com/en/page/caddx