

OnCell G3470A-LTE User's Manual

Version 1.4, October 2019

www.moxa.com/product



© 2019 Moxa Inc. All rights reserved.

OnCell G3470A-LTE User's Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

© 2019 Moxa Inc. All rights reserved.

Trademarks

The MOXA logo is a registered trademark of Moxa Inc.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.

Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Moxa Americas

Toll-free: 1-888-669-2872
Tel: +1-714-528-6777
Fax: +1-714-528-6778

Moxa Europe

Tel: +49-89-3 70 03 99-0
Fax: +49-89-3 70 03 99-99

Moxa India

Tel: +91-80-4172-9088
Fax: +91-80-4132-1045

Moxa China (Shanghai office)

Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505

Moxa Asia-Pacific

Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Table of Contents

1. Introduction	1-1
Overview	1-2
Package Checklist	1-2
Product Features	1-2
Product Specifications	1-3
Functional Design	1-4
LED Indicators	1-5
Beeper.....	1-6
Reset Button.....	1-6
2. Getting Started	2-1
First-time Installation and Configuration	2-2
Step 1: Inserting a SIM Card	2-2
Step 2: Turning on the OnCell G3470A-LTE	2-2
Step 3: Connecting the OnCell G3470A-LTE to a Computer.....	2-2
Step 4: Configuring the Computer's IP Address	2-2
Step 5: Accessing the Web Console	2-3
Step 6: Establishing a Cellular Connection	2-3
Step 7: Verifying the Cellular Connection	2-4
3. Web Console Configuration	3-1
Accessing the Web Console	3-2
Configuration Menu Overview	3-3
Overview	3-4
Basic Settings	3-4
System Info Settings	3-4
Network Settings.....	3-5
Time Settings	3-5
Cellular Settings	3-6
Cellular WAN Settings	3-6
GuaranLink.....	3-8
Auto IP Report Settings.....	3-11
GPS Settings	3-12
OnCell Central Manager Setting.....	3-12
Advanced Settings	3-12
DHCP Server.....	3-13
DDNS	3-14
Packet Filters.....	3-14
SNMP Agent.....	3-16
Port Forwarding	3-18
VPN	3-19
Auto Warning Settings.....	3-27
System Log	3-27
Syslog	3-28
E-Mail	3-29
Relay	3-30
Trap	3-31
SMS.....	3-32
Status	3-34
DNS Information	3-34
SIM Status	3-34
Network Statistics	3-34
Routing Table	3-36
DHCP Client List.....	3-36
System Log	3-37
Relay Status	3-37
DI and Power Status.....	3-38
VPN Log	3-38
Maintenance	3-39
Console Settings	3-39
Ping	3-39
Firmware Upgrade.....	3-40
Config Import Export	3-40
Load Factory Default.....	3-41
Password.....	3-42
Misc. Settings	3-42
Manual SMS.....	3-42
Remote SMS Control.....	3-43
Save Configuration	3-43
Restart	3-44

Logout.....	3-45
4. Software Installation and Configuration	4-1
Overview	4-2
Wireless Search Utility.....	4-2
Installing the Wireless Search Utility	4-2
Configuring the Wireless Search Utility.....	4-5
A. Supporting Information	A-1
Firmware Recovery	A-2
DoC (Declaration of Conformity)	A-3
Federal Communication Commission Interference Statement	A-3
R&TTE Compliance Statement.....	A-4
B. Dynamic Domain Name Server	B-1
C. Well-Known Port Numbers	C-1

Introduction

The OnCell G3470A-LTE industrial cellular gateway is an ideal wireless solution for remote monitoring applications. With wide temperature support and power and antenna isolation design, the OnCell G3470A-LTE is rugged enough for any harsh industrial environment.

The following topics are covered in this chapter:

- ❑ **Overview**
- ❑ **Package Checklist**
- ❑ **Product Features**
- ❑ **Product Specifications**
- ❑ **Functional Design**
 - LED Indicators
 - Beeper
 - Reset Button

Overview

The OnCell G3470A-LTE industrial cellular gateway provides a higher cellular bandwidth and more reliable connection to your Ethernet network for cellular applications. With the integrated 4-port gigabit Ethernet switch and LTE support, the OnCell G3470A-LTE offers a faster cellular connection with a lower total cost of ownership. To enhance reliability, a key for industrial users, the OnCell G3470A-LTE features isolation design for both power and antenna inputs. Coupled with high-level EMS and wide-temperature support, the OnCell G3470A-LTE provides the highest level of device stability in any rugged environment. In addition, with dual SIM and dual power-input features, the OnCell G3470A-LTE supports network redundancy to ensure that your application's network connectivity is not interrupted.

Package Checklist

Moxa's OnCell G3470A-LTE is shipped with the following items. If any of these items is missing or damaged, please contact your customer service representative for assistance.

- OnCell G3470A-LTE
- 1 GPS connector terminator
- 2 2G/3G/4G omni-directional antennas, 2 dBi, SMA (male)
- 5 plastic RJ45 protective caps for serial console and Ethernet ports
- Quick installation guide (printed)
- Warranty card

NOTE The above items come with the standard OnCell G3470A-LTE model, but the package contents may vary for customized versions.

Product Features

- VPN support
- Multiple LTE band support:
 - EU Model: B1/B3/B7/B8/B20
 - US Model: B2/B4/B5/B13/B17/B25
- Universal cellular bands support for GSM/GPRS/HSPA
- Built-in 4-port Gigabit Ethernet switch for local network connectivity
- Virtual private responder/initiator support
- Industrial-grade design:
 - Dual power input for power redundancy
 - Dual-SIM support for cellular connection redundancy
 - Antenna isolation for 500V protection against radio interference
 - Power isolation for 500V power source insulation protection
 - -35°C to 70°C wide operating temperature (wide temperature support only applies to certain SKUs)

Product Specifications

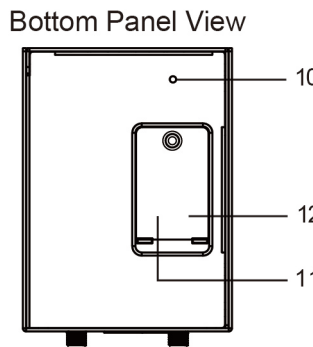
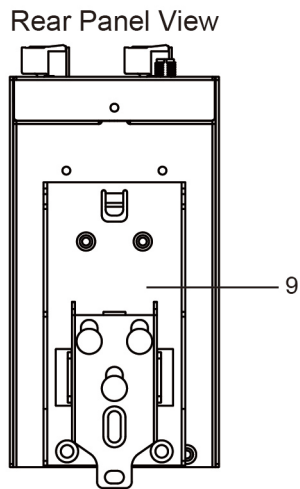
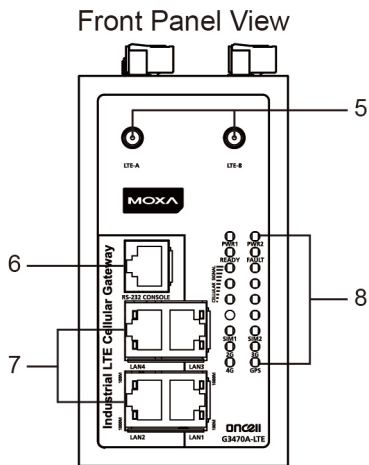
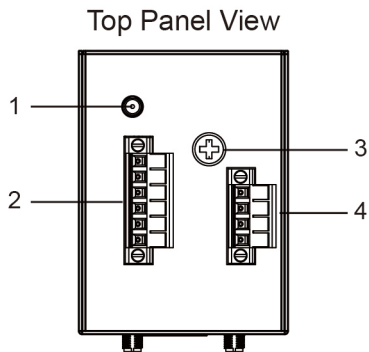
NOTE The latest specifications for Moxa's products can be found at <https://www.moxa.com>.



ATTENTION

- The OnCell G3470A-LTE is NOT a portable mobile device and should be located at least 20 cm away from the human body.
- The OnCell G3470A-LTE is NOT designed for the general public. A well-trained technician should be enlisted to ensure safe deployment of OnCell G3470A-LTE units, and to establish a wireless network.

Functional Design



1. GPS antenna connector (female SMA)
2. Terminal block (two digital input and one digital relay)
3. Grounding screw (M5)
4. Terminal block (PWR1 and PWR2)
5. 2x2 MIMO antenna ports for LTE (female SMA)
6. RS-232 serial console (RJ45)
7. 10/100/1000 BaseT(X) Ethernet ports (RJ45)
8. LED display
9. DIN-rail mounting kit
10. Reset button
11. Dual SIM - SIM1
12. Dual SIM - SIM2

LED Indicators

The LEDs on the front panel of the OnCell G3470A-LTE provide a quick and easy means of determining the current operational status and wireless settings.

The following table summarizes how to read the device's wireless settings from the LED displays. More information is available in Chapter 3 in the "Basic Wireless Settings" section.

LED	Color	State	Description
Front Panel LED Indicators (System)			
PWR1	Green	On	Power is being supplied from power input 1
PWR2	Green	On	Power is being supplied from power input 2
READY	Green	On	System startup is complete and the system is operating
		Blinking	Device has been located by the OnCell Search Utility
		Off	Power is off, or the system is booting up
FAULT	Red	On	System configuration error or a relay event has occurred
		Blink	IP address conflict
		Off	Power is off, or there is no error condition.
CELLULAR SIGNAL (3 LEDs)	Green	On	Number of LEDs to indicate cellular signal level when registered to a base station. Signal LED 1: $0 < \text{RSSI} \leq 12$ Signal LED 2: $12 < \text{RSSI} \leq 21$ Signal LED 3: $22 < \text{RSSI} \leq 31$
SIM1	Amber	On/Off	SIM 1 is active or inactive
		Blink	SIM 1 is not inserted or PIN code is incorrect
SIM2	Amber	On/Off	SIM 2 is active or inactive
		Blink	SIM 2 is not inserted or PIN code is incorrect
2G	Amber	On	Registered to a base station with cellular connection in GPRS or EDGE mode
3G	Amber	On	Registered to a base station with cellular connection in UMTS or HSPA mode
4G	Amber	On	Registered to a base station with cellular connection in LTE mode
GPS	Green	On	GPS has been located
		Blinking	Locating GPS or less than four satellites have been located.
		Off	GPS has not been located.
LAN Port LED Indicators (Port Interface)			
1000M	Green	On	1000Mbps link is active
		Blink	Data is being transmitted at 1000Mbps
		Off	1000Mbps link is inactive
10/100M	Amber	On	10/100Mbps link is active
		Blink	Data is being transmitted at 10/100Mbps
		Off	10/100Mbps link is inactive



ATTENTION

When the system fails to boot, the LEDs for **STATE** (Green), **FAULT**, and **WLAN** will all light up simultaneously and blink at one-second intervals. This may be due to improper operation or uncontrollable issues, such as an unexpected shutdown while updating the firmware. To recover the firmware, refer to the "Firmware Recovery" section in Chapter 6.

Beeper

The beeper emits two short beeps when the system is ready.

Reset Button

The **RESET** button is located on the bottom panel of the OnCell G3470A-LTE. You can reboot the OnCell G3470A-LTE or reset it to factory default settings by pressing the **RESET** button with a pointed object such as an unfolded paper clip.

- **System reboot:** Hold the RESET button down for under 5 seconds and then release.
- **Reset to factory default:** Hold the RESET button down for *over* 5 seconds until the **STATE** LED starts blinking green. Release the button to reset the OnCell G3470A-LTE.

Getting Started

This chapter explains how to install Moxa's OnCell G3470A-LTE for the first time, and quickly set up your wireless network and test whether the connection is running well. The Function Map discussed in the third section provides a convenient means of determining which functions you need to use.

The following topics are covered in this chapter:

▣ **First-time Installation and Configuration**

- Step 1: Inserting a SIM Card
- Step 2: Turning on the OnCell G3470A-LTE
- Step 3: Connecting the OnCell G3470A-LTE to a Computer
- Step 4: Configuring the Computer's IP Address
- Step 5: Accessing the Web Console
- Step 6: Establishing a Cellular Connection
- Step 7: Verifying the Cellular Connection

First-time Installation and Configuration

Before installing the OnCell G3470A-LTE, make sure that all items in the package checklist are in the box. In addition, you will need access to a notebook computer or PC equipped with an Ethernet port. The OnCell G3470A-LTE has a default IP address that you must use when connecting to the device for the first time.

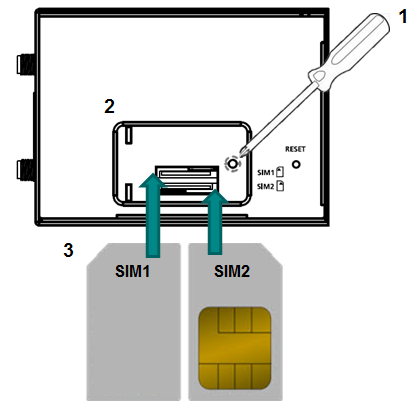
Step 1: Inserting a SIM Card

Insert one or two 2G/3G/4G SIM cards into the SIM slots located on the bottom of the OnCell G3470A-LTE.

Installing a SIM Card

The SIM card slots are inside the OnCell G3470A-LTE's housing. To install a SIM card, complete the following steps:

1. Turn off the OnCell G3470A-LTE.
2. Remove the screw to remove the SIM card slot cover.
3. Install a SIM card into a SIM card slot. Do the following:
 - a. For SIM 1, orient the gold contacts facing down and the cut-off edge to the left.
 - b. For SIM 2, orient the gold contacts facing up and the cut-off edge to the right.
4. Install the screw to secure the SIM card slot cover.



Step 2: Turning on the OnCell G3470A-LTE

Turn on the OnCell G3470A-LTE by connecting a power terminal block to a DC power source.

Step 3: Connecting the OnCell G3470A-LTE to a Computer

Since the OnCell G3470A-LTE supports MDI/MDI-X auto-sensing, you can use either a straight-through cable or crossover cable to connect the OnCell G3470A-LTE to a computer. If the LED indicator on the OnCell G3470A-LTE's LAN port lights up, it means a connection has been established.

Step 4: Configuring the Computer's IP Address

Set an IP address on the same subnet as the OnCell G3470A-LTE. Since the OnCell G3470A-LTE's default IP address is **192.168.127.254**, and the subnet mask is **255.255.255.0**, you should set the IP address of the computer to **192.168.127.xxx**.

NOTE After you select **Maintenance > Load Factory Default** and click the **Submit** button, the OnCell G3470A-LTE will be reset to factory default settings and the IP address will be reset to **192.168.127.254**.

Step 5: Accessing the Web Console

To access the web console:

1. Open a web browser.
2. Enter http://192.168.127.254 in the address field.
3. A login screen appears. Enter the user name (the default is "admin") and password (the default is "moxa"); then, click **Login**.

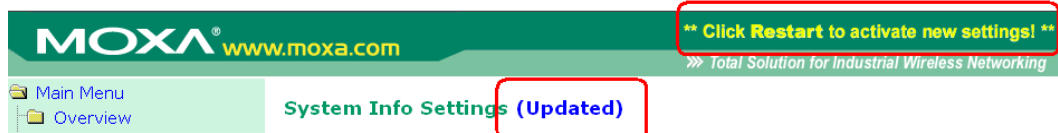


NOTE Default user name and password:

User Name: **admin**
 Password: **moxa**

For security reasons, we strongly recommend changing the default password. To do so, select **Maintenance > Password**, and then follow the on-screen instructions to change the password.

NOTE After you click **Submit** to apply changes the web page will refresh **(Updated)** will appear on the page and a blinking reminder will be shown on the upper-right corner of the web page:



To activate the changes click **Restart** and then **Save and Restart** after you change the settings. About 30 seconds are needed for the OnCell G3470A-LTE to complete the reboot procedure.

Step 6: Establishing a Cellular Connection

After installing a SIM card, obtain the SIM card PIN and APN (Access Point Name) information from your service provider and configure the cellular WAN settings.

To configure cellular WAN settings and establish a cellular connection:

1. Log into the web console.
2. Click **Cellular Settings > Cellular WAN Settings** and enter the SIM card PIN and APN values.
3. Restart the OnCell G3740A-LTE. The OnCell 3740A-LTE automatically establishes a cellular connection to the service provider.

Step 7: Verifying the Cellular Connection

You can use one of the following methods to verify the cellular connection:

1. Check the LED display.

Check the SIM 1, SIM2, 2G, 3G, and 4G LEDs on the front panel.

If a SIM LED is blinking, this indicates that a SIM card is not installed in the SIM slot or the SIM card PIN information is not configured in the web console.

If the installed SIM card supports 3G or 4G service but only the 2G LED is turned on, this indicates that the OnCell G3470A-LTE is connected to the cellular network but is not registered for 3G or 4G service. Make sure that you enter the correct APN information in the web console.

2. Check the Overview screen in the web console.

Log into the web console and display the Overview screen. Check the status for the Cellular RSSI, Cellular WAN IP address, and Cellular Mode fields to diagnose any connection problem.

For Cellular RSSI (Received Signal Strength Indication), make sure that the value is above 12 RSSI in order to maintain a stable connection.

If the Cellular WAN IP address is not available but the RSSI is more than 12, make sure that the APN configuration is correct. The service provider assigns a private address for the WAN IP address, which is not accessible externally.

3. Test cellular network access on your computer.

For users with public SIM cards, instead of SIM cards with MDVPN service enabled, you can test the connection to the Internet on your computer (assuming that your computer is connected to an Ethernet port on the OnCell G3470A-LTE). The following shows an example configuration.

- Laptop IP Address: 192.168.127.10 (on the same subnet as the OnCell gateway)
- Laptop Subnet Mask: 255.255.255.0 (on the same subnet as the OnCell gateway)
- Laptop Default Gateway: 192.168.17.254 (the OnCell gateway IP address)
- Laptop Primary DNS Server: 8.8.8.8 (test with Google's public DNS server)
- Laptop Primary DNS Server: 8.8.4.4 (test with Google's public DNS server)

After the configuration is complete, your computer will be able to access the Internet.

For information on testing the connection with a DHCP server, refer to Chapter 3.

Web Console Configuration

This chapter describes the web console that you can use to configure your OnCell G3470A-LTE and set up a wireless network.

The following topics are covered in this chapter:

- ❑ **Accessing the Web Console**
 - Configuration Menu Overview
- ❑ **Overview**
- ❑ **Basic Settings**
 - System Info Settings
 - Network Settings
 - Time Settings
- ❑ **Cellular Settings**
 - Cellular WAN Settings
 - GuaranLink
 - Auto IP Report Settings
 - GPS Settings
 - OnCell Central Manager Setting
- ❑ **Advanced Settings**
 - DHCP Server
 - DDNS
 - Packet Filters
 - SNMP Agent
 - Port Forwarding
 - VPN
- ❑ **Auto Warning Settings**
 - System Log
 - Syslog
 - E-Mail
 - Relay
 - Trap
 - SMS
- ❑ **Status**
 - DNS Information
 - SIM Status
 - Network Statistics
 - Routing Table
 - DHCP Client List
 - System Log
 - Relay Status
 - DI and Power Status
 - VPN Log
- ❑ **Maintenance**
 - Console Settings
 - Ping
 - Firmware Upgrade
 - Config Import Export
 - Load Factory Default
 - Password
 - Misc. Settings
 - Manual SMS
 - Remote SMS Control
- ❑ **Save Configuration**
- ❑ **Restart**
- ❑ **Logout**

Accessing the Web Console

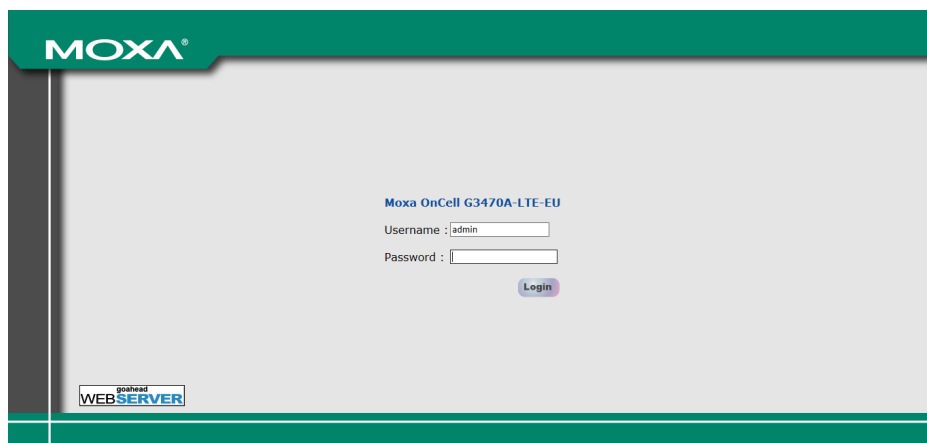
Moxa OnCell G3470A-LTE's web browser interface provides a convenient way to modify its configuration and access the built-in monitoring and network administration functions. The recommended web browser is Microsoft® Internet Explorer 7.0 or 8.0 with JVM (Java Virtual Machine) installed.

NOTE To use the OnCell G3470A-LTE's management and monitoring functions from a PC host connected to the same LAN as the OnCell G3470A-LTE, you must make sure that the PC host and the OnCell G3470A-LTE are on the same logical subnet.

The Moxa OnCell G3470A-LTE's default IP is **192.168.127.254**.

Follow these steps to access the OnCell G3470A-LTE's web-based console management interface.

1. Open your web browser (e.g., Internet Explorer) and type the OnCell G3470A-LTE's IP address in the address field; then, press [Enter].
2. The login page appears. Enter the password (the default username is "admin" and the default password is "moxa") and click **Login**.



It may take a few moments for the web page to load on your computer. Note that the Model name and IP address of your OnCell G3470A-LTE are both shown on the title bar of the web page. You can use this information to identify multiple OnCell G3470A-LTE units.

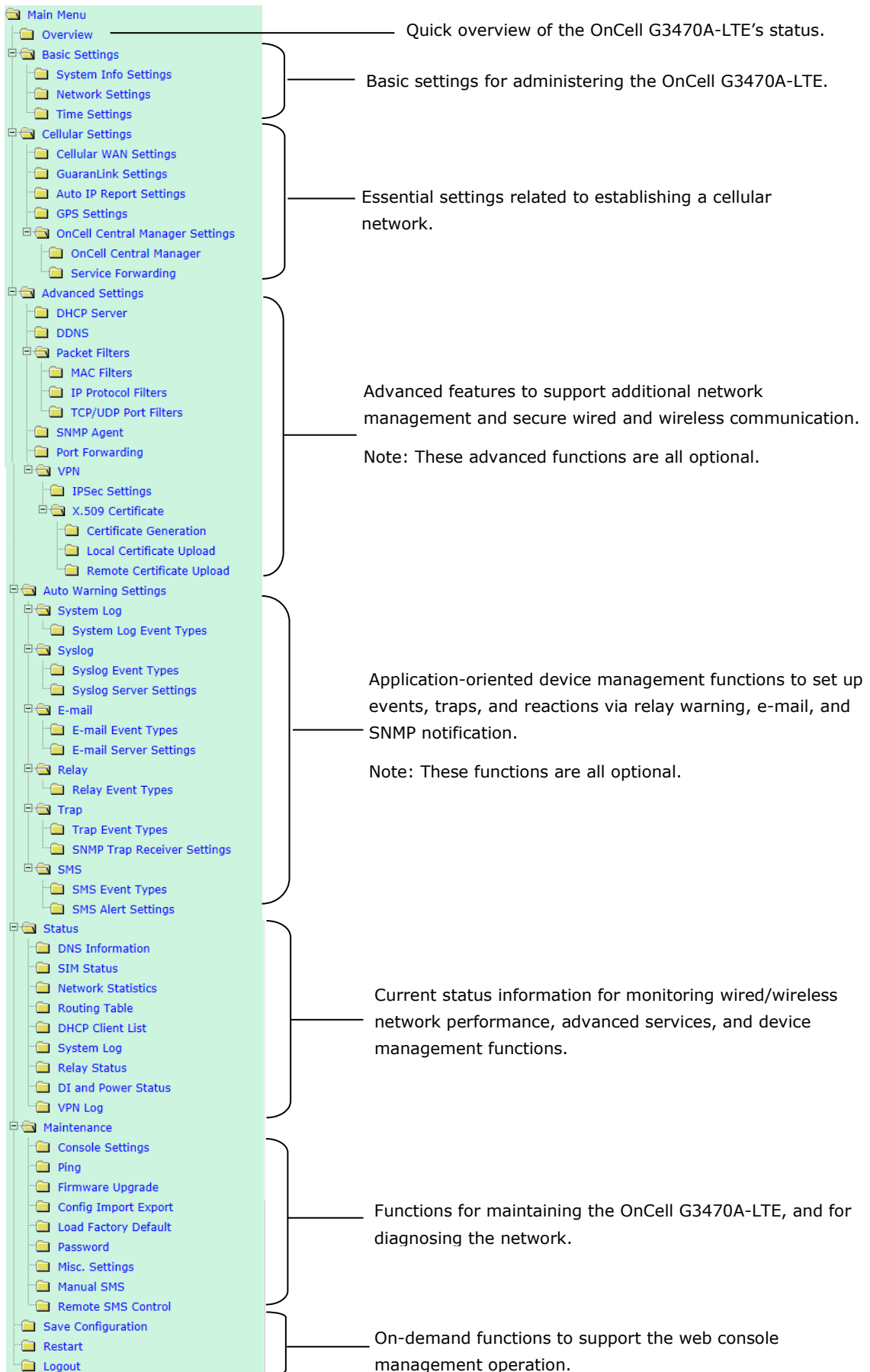
3. Use the menu navigation panel to access the configuration screens.



In the following sections, we describe each OnCell G3470A-LTE management function in detail. For an overview of the menus, refer to the "Function Map" section of Chapter 2.

NOTE The model name of the OnCell G3470A-LTE is shown as OnCell G3470A-LTE-XX, where XX indicates the country code. The country code indicates the OnCell G3470A-LTE version and which bandwidth it uses. Example figures shown in this document are for OnCell G3470A-LTE-US. The country code and model name that appear on your computer screen may be different than the one shown here.

Configuration Menu Overview



Overview

The **Overview** page provides a summary of the OnCell G3470A-LTE’s current status. The information is categorized into groups: **System Info**, **LAN Info**, and **Cellular Info**.

Overview	
All information on this page are active values.	
System Info	
Model name	OnCell G3470A-LTE-EU
Device name	OnCell G3470A-LTE_0000
Serial No.	0
System up time	0 days 00h:07m:49s
Firmware version	1.1 Build 15012914
LAN Info	
Device MAC address	00:90:E8:00:00:01
IP address	192.168.127.254
Subnet mask	255.255.255.0
Cellular Info	
Cellular RSSI	15
Cellular WAN IP address	10.195.156.219
Cellular mode	LTE
IMEI	356853050144221
IMSI	466924000081300

Basic Settings

The Basic Settings group includes the most commonly used settings required by administrators to maintain and control the OnCell G3470A-LTE.

System Info Settings

The **System Info** items, especially **Device name** and **Device description**, are displayed and included on the **Overview** page, in SNMP information, and in alarm emails. Setting **System Info** items makes it easier to identify the different OnCell G3470A-LTE units connected to your network.

System Info Settings	
Device name	<input type="text" value="OnCell G3470A-LTE_0000"/>
Device location	<input type="text"/>
Device description	<input type="text"/>
Device contact information	<input type="text"/>
<input type="button" value="Submit"/>	

Field	Description	Default setting
Device name	Enter a descriptive name (up to 31 characters). This option is useful for specifying the role or application of different OnCell G3470A-LTE units.	OnCell G3470A-LTE_ <i>[serial no]</i>
Device location	Specify the location (up to 31 characters) of the OnCell G3470A-LTE.	
Device description	Enter a description (up to 31 characters) for the OnCell G3470A-LTE.	
Device contact information	Enter the contact information (up to 31 characters) of the person responsible for maintaining this OnCell G3470A-LTE.	

Network Settings

You can use the Network Settings screen to configure TCP/IP settings.

Network Settings

LAN Settings

IP address

Subnet mask

Primary DNS server

Secondary DNS server

Field	Description	Default setting
IP address	Enter the unique IP address for the OnCell G3470A-LTE.	192.168.127.254
Subnet mask	Enter the subnet mask to specify the type of network to which the OnCell G3470A-LTE is connected.	255.255.255.0
Primary/Secondary DNS server	Enter the IP address of the primary or secondary DNS server. After you specify a DNS server, you can access a web site by entering its URL instead of the IP address.	

Time Settings

You can synchronize the system time on the OnCell G3470A-LTE based on an NTP (Network Time Protocol) server or user-specified date and time information. The OnCell G3470A-LTE includes the system time in system logs.

NOTE The OnCell G3470A-LTE includes a built-in real time clock (RTC). We strongly recommend that you update the **Current local time** for the OnCell G3470A-LTE after the initial setup or a long-term shutdown, especially when the network does not have an Internet connection for accessing the NTP server or if there is no NTP server on the LAN.

Time Settings

Date (YYYY/MM/DD)
Time (HH:MM:SS)

Current local time / / : :

Time zone

Daylight saving time Enable

Time server 1

Time server 2

Query period (600~9999 seconds)

Field	Description	Default setting
Current local time	The fields indicate the current system time on the OnCell G3470A-LTE. Enter the date and time in the format <code>yyyy/mm/dd hh:mm:ss</code> . To make the changes take effect, click Set Time . An "Updated" text appears to indicate that the change is complete. Note: Set the time zone before you configure the current local time.	

Field	Description	Default setting
Time zone	Select a time zone from the drop-down list. The default option is GMT (Greenwich Mean Time). Note: Changing the time zone automatically changes the Current local time . We strongly recommend that you set the time zone before you set the Current local time .	
Daylight saving time	Select Enable to activate daylight saving time (DST) or summer time. When Daylight saving time is enabled, the following fields appear: <ul style="list-style-type: none"> • Starts at: The date that daylight saving time begins. • Stops at: The date that daylight saving time ends. • Time offset: Indicates how many hours forward the clock should be advanced. 	
Time server 1/2	Enter the IP address or the domain name of the primary or secondary NTP server.	time.nist.gov
Query period	Specify how many seconds (1 to 9999) the OnCell G3470A-LTE is to wait before requesting updates from the NTP server.	600

Cellular Settings

This section describes the screens you can use to configure cellular connection settings on the OnCell G3470A-LTE:

- **Cellular WAN Settings**—Configure this screen to establish a cellular connection.
- **GuaranLink Settings**—Use this screen to configure Moxa’s proprietary 3-tire link protection to ensure reliable network connectivity.
- **Auto IP Report Settings**—If your service provider assigns a dynamic WAN IP address, you can configure this screen to set the OnCell G3470A-LTE to automatically send its WAN IP address to the specified host.
- **GPS Settings**—Configure this screen to enable the built-in GPS sensor to locate your OnCell G3740A-LTE.
- **OnCell Central Manager Settings**—Configure this screen to allow Moxa OnCell Central Manager to connect to and manage your OnCell G3740A-LTE.

Cellular WAN Settings

Configure the fields in the **Cellular WAN Settings** screen to establish a 2G/3G/4G connection to a service provider.

If you install two SIM cards in the OnCell G3470A-LTE, you can select Dual SIM mode and enable the GuaranLink feature set the OnCell G3470A-LTE to regularly check connection quality and perform an automatic switchover in case a cellular connection is down. This setting ensures operator-level redundancy.

Cellular WAN Settings

Cellular WAN Configuration

Used SIM: SIM 1 Please ensure inserting SIM card into right slot.

SIM 1 Configuration

SIM 1 PIN: Auto
Manual

SIM 1 band:

<input checked="" type="checkbox"/> GSM 1800 MHz	<input checked="" type="checkbox"/> E-GSM 900 MHz	<input checked="" type="checkbox"/> P-GSM 900 MHz	<input checked="" type="checkbox"/> GSM 850 MHz	<input checked="" type="checkbox"/> GSM 1900 MHz
<input checked="" type="checkbox"/> WCDMA 2100 MHz (BAND 1)	<input checked="" type="checkbox"/> WCDMA 1900 MHz (BAND 2)	<input checked="" type="checkbox"/> WCDMA 850 MHz (BAND 5)	<input checked="" type="checkbox"/> WCDMA 800 MHz (BAND 6)	<input checked="" type="checkbox"/> WCDMA 900 MHz (BAND 8)
<input checked="" type="checkbox"/> LTE 2100 MHz (BAND 1)	<input checked="" type="checkbox"/> LTE 1800 MHz (BAND 3)	<input checked="" type="checkbox"/> LTE 2600 MHz (BAND 7)	<input checked="" type="checkbox"/> LTE 900 MHz (BAND 8)	<input checked="" type="checkbox"/> LTE 800 MHz (BAND 20)

SIM 1 username:

SIM 1 password:

SIM 1 APN:

SIM 1 authentication type: AUTO
PAP
CHAP

Warning: When plugging in GSM/GPRS/EDGE SIM card, please select related band to get better performance!

Field	Description	Default setting
Used SIM	Select a connection mode from the drop-down list. SIM 1 – Select this option to establish a cellular connection using the SIM card installed in the SIM 1 slot. SIM 2 – Select this option to establish a cellular connection using the SIM card installed in the SIM 2 slot. Dual SIM – Select this option to set the system to automatically establish a cellular connection using either SIM card. To ensure optimum link quality and operator-level redundancy, enable the GuaranLink feature.	SIM 1
SIM 1/2 PIN	If provided, enter the PIN (4 digits) to unlock the SIM card. Note: A SIM card becomes locked if you enter an incorrect PIN more than three times.	
SIM 1/2 band	Select Auto to have the OnCell device automatically negotiate with the base station for the optimum cellular band frequency. Select Manual to set the OnCell device to use the selected cellular band frequency. Note: The OnCell device does not establish a cellular connection if your service provider does not support any of the bands you have selected.	Auto
SIM 1/2 username	If provided, enter the username for authentication with your service provider.	
SIM 1/2 password	If provided, enter the password for authentication with your service provider.	
SIM 1/2 APN	Your service provider may use access point network (APN) information to provide different service levels. If provided, enter the access point network (APN) information.	

Field	Description	Default setting
SIM 1/2 Authentication Type	<p>Select Auto if you want the OnCell device to automatically select either PAP or CHAP authentication method when setting up a data session.</p> <p>Select PAP (Password Authentication Protocol) to send user name and password to the server and verify that the user name and password match with the server database.</p> <p>Select CHAP (Challenge-Handshake Authentication Protocol) if the identifiers are changed frequently and if authentication can be requested by the server at any time. CHAP provides more security than PAP.</p> <p>Note: This technique is vulnerable to eavesdroppers who may try to obtain the password by listening in on the serial line, and to repeated trial and error attacks. If you select CHAP (Challenge Handshake Authentication Protocol), the authenticator (i.e., the server) sends a randomly generated "challenge" string to the OnCell device along with its host name. The OnCell device uses the host name to look up the appropriate secret, combines it with the challenge, and encrypts the string using a one-way hashing function.</p>	Auto

GuaranLink

A number of factors can contribute to connection failures for cellular communications, including loss of cellular signal, interference, and termination by the operator for unknown reasons. Moxa's proprietary GuaranLink feature, which is different from the basic heartbeat function, enables reliable connectivity with 4-tier intelligent connection checks without sending excessive and costly cellular packets.

GuaranLink Recovery Process for Dual SIM Connections

The GuaranLink feature in OnCell G3470A-LTE automatically tries to re-establish a connection when a connection failure occurs by performing one of the following actions depending on the number of SIM cards enabled in the device:

- One SIM card: Resets the cellular module without rebooting the device to force negotiation between the OnCell G3470A-LTE and the base station.
- Dual SIM cards: Resets the cellular module without rebooting the device and establishes a cellular connection using the second SIM card account.

GuaranLink Settings

In the navigation panel, click **Network Settings** → **GuaranLink Settings** to display the configuration screen.

GuaranLink Settings

GuaranLink Enable Disable

Common Settings

Register to network timeout (10 - 600 mins)

Data session retry count (1 - 5/per 3 mins)

DNS/Ping remote host 1

DNS/Ping remote host 2

Warning: "DNS/Ping remote host" are only for "Cellular connection alive check"/"Packet-level connection check".

GuaranLink Check Settings

ISP initial connection check Enable Disable

Cellular connection alive check Enable Disable

Cellular connection alive check interval (1 - 600 mins)

Cellular connection alive check retry count (1 - 5/per 15 secs)

Packet-level connection check Enable Disable

Packet-level connection check action ▼

Packet-level connection check interval (1 - 600 mins)

Packet-level connection check retry count (1 - 5/per 15 secs)

Transmission connection check Enable Disable

Transmission connection alive check interval (1 - 600 mins)

The following table describes the fields.

Field	Description	Default setting
GuaranLink	Select Enable to activate the GuaranLink feature. For operator-level redundancy, enable GuaranLink with Dual SIM mode to set the OnCell G3470A-LTE to regularly check connection quality and perform an automatic switchover in case a cellular connection is down. Select Disable to deactivate the GuaranLink feature.	Disable
Register to network timeout	This field is used for ISP initial connection check. Enter the time (10 – 600 minutes) the OnCell G3470A-LTE is to wait before terminating connection to an ISP and starts the GuaranLink recovery process.	10
Data session retry count	Enter the number of times (1 to 5; default is 3) the OnCell G3470A-LTE is to request an IP address from the ISP. If the OnCell G3470A-LTE fails to obtain an IP address after 3 tries (default value), it starts the GuaranLink recovery process.	3
DNS/Ping remote host 1/2	This field is used for cellular connection alive and packet-level connection checks. Enter the IP address or domain name of a remote host to ping or for DNS lookup test.	

Field	Description	Default setting
ISP initial connection check	Select Enable to set the OnCell G3470A-LTE to complete the registration process to a base station before the timeout specified in the Register to network timeout field. If the OnCell G3470A-LTE fails to register to the base station within the timeout period, it starts the GuaranLink recovery process. Select Disable to allow the OnCell G3470A-LTE to wait until base station registration is successful.	Disable
Cellular connection alive check	Depending on your ISP, cellular connection is terminated if there is no active data transmission for a period of time. Select Enable to set the OnCell G3470A-LTE to keep the cellular connection alive by performing a DNS lookup or remote host Ping if no data is transmitted within the timeout period. If the connection check fails after the number of retries specified in the Cellular connection alive retry count field, the OnCell G3470A-LTE starts the GuaranLink recovery process.	Disable
Cellular connection alive check interval	Enter the time (between 1 to 600 minutes) the OnCell G3470A-LTE is to wait before performing a connection check.	5
Cellular connection alive check retry count	Enter the number of times the OnCell G3470A-LTE is to try the connection check in a 15-second time interval. If the connection check fails, the OnCell G3470A-LTE starts the GuaranLink recovery process.	3
Packet-level connection check	Select Enable to check whether the cellular network is accessible using DNS lookup and remote host ping, regardless of any existing data transmission. If the connection check fails after the number of retries specified in the Packet-level connection check retry count field, the OnCell G3470A-LTE starts the GuaranLink recovery process.	Disable
Packet-level connection check action	Select one of the following options to determine if the connection check is successful: <ul style="list-style-type: none"> • DNS and Ping – Response from both the DNS server and remote host. • DNS or Ping – Response from either the DNS server or the remote host. 	DNS and Ping
Packet-level connection check interval	Enter the time (between 1 to 600 minutes) the OnCell G3470A-LTE is to wait before performing a connection check.	5
Packet-level connection check retry count	Enter the number the OnCell G3470A-LTE is to try the connection check in 15 seconds before re-establishing the connection.	3
Transmission connection check	If a remote system regularly monitors connection to the OnCell G3470A-LTE, select Enable to set the OnCell G3470A-LTE to receive polling information from the remote system at regular intervals. If no polling information is received within the timeout period, the OnCell G3470A-LTE starts the GuaranLink recovery process.	Disable
Transmission connection alive check interval	Enter the time (between 1 to 600 minutes) the OnCell G3470A-LTE is to wait for polling information from a remote system before starting the GuaranLink recovery process.	5

Auto IP Report Settings

In MDVPN (mobile data virtual private network) applications where service providers set up private VPNs for enterprise customers, a cellular gateway must be assigned IP address that is visible to a remote host in a central office. In cases where a service provider assigns dynamic IP addresses, you can configure the **Auto IP Report Settings** screen to set the OnCell G3470A-LTE to regularly send its WAN IP address to a remote host.

Auto IP Report Settings

Configuration

Auto IP report to host

Report to UDP port

Report period (1 - 65535 mins)

The following table describes the fields.

Field	Description	Default setting
Auto IP report to host	Enter the IP address of a remote host to which the OnCell G3470A-LTE is to send the WAN IP address information.	
Report to UDP port	Enter the listing port number on the remote host.	63100
Report period	Enter the number of minutes the OnCell G3470A-LTE is to wait before sending WAN IP address information.	99

The following figure shows the Auto IP report format.

Auto IP Report Format

"Moxa", 4 bytes	Info[0]	Info[1]	...	Info[n]
-----------------	---------	---------	-----	---------

Info [n]

Field	ID	Length	Data
Length	a	1	Variable, Length is "Length Field"

ID List

ID Value	Description	Length	Note
1	Server Name	Variable	ASCII char
2	Hardware ID	2	Little-endian
3	MAC Address	6	6-byte MAC address. If the MAC address is "00-90-E8-01-02-03" then MAC[0] is 0, MAC[1] is 0x90(hex), MAC[2] is 0xE8(hex), etc.
4	Serial Number	4, DWORD	Little-endian
5	IP Address	4, DWORD	Little-endian (LAN IP)
9	AP ID	4, DWORD	Little-endian
10	IP Address2	4, DWORD	Little-endian (WAN IP)
11	Signal Level	1	Unsigned char
12	RSSI	1	Unsigned char

AP ID & Hardware ID Mapping Table

AP ID	Hardware ID	Product
0x80005260	0x5061	5004-HSPA
0x80005260	0x5061	5104-HSPA

GPS Settings

You can activate the GPS module function under GPS Settings, and then enable GPS serial mode under Real COM mode or Reverse Real COM mode. OnCell Central Manager provides the current location, including latitude and altitude information.

GPS Settings

GPS Enable ▾

GPS Serial Mode

Enable Disable ▾

Serial operation mode RealCOM ▾

TCP alive check time 7 (0 - 99 min)

Setting	Description	Factory Default
GPS	Activate GPS module	Disable
Enable	Enable GPS Serial Mode	Disable
Serial Operation mode	Use OCM to get the location information under Real COM or Reverse Real COM serial mode.	Real COM
TCP alive check time	This field specifies how long the OnCell G3470A-LTE will wait for a response to "keep alive" packets before closing the TCP connection. The OnCell G3470A-LTE checks the connection status by sending periodic "keep alive" packets. If the remote host does not respond to the packet within the time specified in this field, the OnCell G3470A-LTE will force the existing TCP connection to close. For socket and device control modes, the OnCell G3470A-LTE will listen for another TCP connection from another host after closing the connection. If TCP alive check time is set to 0, the TCP connection will remain open but will not send any "keep alive" packets.	7 min

OnCell Central Manager Setting

For OnCell Central Manager settings, refer to the *OnCell Central Manager User's Manual*, which can be downloaded from www.moxa.com.

Advanced Settings

Several advanced functions are available to increase the functionality of your OnCell G3470A-LTE and wireless network system. The DHCP server helps you deploy wireless clients efficiently. Packet filters provide security mechanisms, such as firewalls, in different network layers. Moreover, SNMP support can make network management easier.

DHCP Server

DHCP (Dynamic Host Configuration Protocol) is a networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

The OnCell G3470A-LTE can act as a DHCP server and assign IP addresses to your DHCP clients by responding to DHCP requests from the clients. The IP-related parameters you set on this page will also be sent to the client.

You can also assign a static IP address to a specific client by entering its MAC address. The OnCell G3470A-LTE provides a **Static DHCP mapping** list with up to 16 entities. Be reminded to check the **Active** check box for each entity to activate the setting.

You can check the IP assignment status in the **DHCP Client List** screen (click **Status > DHCP Client List**).

DHCP Server

DHCP server

Default gateway

Subnet mask

Primary DNS server

Secondary DNS server

Start IP address

Maximum number of users

Client lease time (2~14400 minutes)

Static DHCP mapping

No	<input type="checkbox"/> Active	IP Address	MAC Address
1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
5	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

The following table provides the field descriptions.

Field	Description	Default setting
DHCP server	Select Enable to set the OnCell G3470A-LTE as a DHCP server. Select Disable to set the OnCell G3470A-LTE as a DHCP client.	Disable
Default gateway	Enter the IP address of the default gateway that connects to an outside network.	
Subnet mask	Enter the subnet mask to specify the type of network for the DHCP clients.	
Primary/Secondary DNS server	Enter the IP address of the primary or secondary DNS server. After you specify a DNS server, you can access a web site by entering its URL instead of the IP address.	
Start IP address	Enter the starting IP address in the IP address pool.	
Maximum number of users	Enter the number (between 1 and 999) of IP address to assign to DHCP clients.	
Client lease time	Enter the lease time (between 2 and 14400 minutes) for an assigned IP address. The IP address expired after the lease time.	

DDNS

If a DHCP server assigns an IP address to the OnCell G3470A-LTE, you can configure dynamic DNS (DDNS) setting on the OnCell G3470A-LTE to allow remote servers to access the OnCell G3470A-LTE using its domain name instead of IP address. For more information on DDNS, see *Appendix C*.

Click **Advanced Settings > DDNS** to display the configuration screen.

DDNS

Enable Disable ▾

Service provider no-ip.org ▾

Host name

Username

Password

The following table provides the field descriptions.

Field	Description	Default setting
Enable	Select Enable to activate the DDNS feature.	Disable
Service provider	Select an option from the drop-down list.	
Host name	Enter the host name you created with the service provider.	
Username	Enter the username for update authentication.	
Password	Enter the password for update authentication.	

Packet Filters

The OnCell G3470A-LTE includes various filters for **IP-based** packets going through LAN and WLAN interfaces. You can set these filters as a firewall to help enhance network security.

MAC Filter

The OnCell G3470A-LTE’s MAC filter is a policy-based filter that can allow or filter out IP-based packets with specified MAC addresses. The OnCell G3470A-LTE provides 8 entities for setting MAC addresses in your filtering policy. Remember to check the **Active** check box for each entity to activate the setting.

MAC Filters

Enable Disable ▾

Policy Drop ▾

No	<input type="checkbox"/> Active	Name	MAC address
1	<input type="checkbox"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
2	<input type="checkbox"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
3	<input type="checkbox"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>

Field	Description	Default setting
Enable	Select Enable to enable MAC filtering.	Disable
Policy	Select Accept to allow packets that meet the specified criteria. Select Drop to deny packets that meet the specified criteria.	Drop



ATTENTION

Be careful when you enable the filter function:

Drop + "no entity on list is activated" = all packets are **allowed**

Accept + "no entity on list is activated" = all packets are **denied**

IP Protocol Filter

The OnCell G3470A-LTE’s IP protocol filter is a policy-based filter that can allow or filter out IP-based packets with specified IP protocol and source/destination IP addresses.

The OnCell G3470A-LTE provides 8 entities for setting IP protocol and source/destination IP addresses in your filtering policy. Four IP protocols are available: **All**, **ICMP**, **TCP**, and **UDP**. You must specify either the Source IP or the Destination IP. By combining IP addresses and netmasks, you can specify a single IP address or a range of IP addresses to accept or drop. For example, "IP address 192.168.1.1 and netmask 255.255.255.255" refers to the sole IP address 192.168.1.1. "IP address 192.168.1.1 and netmask 255.255.255.0" refers to the range of IP addresses from 192.168.1.1 to 192.168.255. Remember to check the **Active** check box for each entity to activate the setting.

IP Protocol Filters

Enable

Policy

No	<input type="checkbox"/> Active	Protocol	Source IP	Source netmask	Destination IP	Destination netmask
1	<input type="checkbox"/>	All	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="checkbox"/>	All	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="checkbox"/>	All	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Field	Description	Default setting
Enable	Select Enable to enable IP protocol filtering.	Disable
Policy	Select Accept to allow packets that meet the specified criteria. Select Drop to deny packets that meet the specified criteria.	Drop



ATTENTION

Be careful when you enable the filter function:

Drop + "no entity on list is activated" = all packets are **allowed**.

Accept + "no entity on list is activated" = all packets are **denied**.

TCP/UDP Port Filter

The OnCell G3470A-LTE’s TCP/UDP port filter is a policy-based filter that can allow or filter out TCP/UDP-based packets with a specified source or destination port.

The OnCell G3470A-LTE provides 8 entities for setting the range of source/destination ports of a specific protocol. In addition to selecting TCP or UDP protocol, you can set either the source port, destination port, or both. The end port can be left empty if only a single port is specified. Of course, the end port cannot be larger than the start port.

The **Application name** is a text string that describes the corresponding entity with up to 31 characters. Remember to check the **Active** check box for each entity to activate the setting.

TCP/UDP Port Filters

Enable

Policy

No	<input type="checkbox"/> Active	Source port	Destination port	Protocol	Application name
1	<input type="checkbox"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	TCP	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	TCP	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	TCP	<input type="text"/>

Field	Description	Default setting
Enable	Select Enable to enable TCP/UDP port filtering.	Disable
Policy	Select Accept to allow packets that meet the specified criteria. Select Drop to deny packets that meet the specified criteria.	Drop



ATTENTION

Be careful when you enable the filter function:

Drop + "no entity on list is activated" = all packets are **allowed**

Accept + "no entity on list is activated" = all packets are **denied**

SNMP Agent

The OnCell G3470A-LTE supports SNMP V1/V2c/V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the community string *public/private* (default value). SNMP V3, which requires you to select an authentication level of MD5 or SHA, is the most secure protocol. You can also enable data encryption to enhance data security.

The OnCell G3470A-LTE’s MIB can be found in the software CD and supports reading the attributes via SNMP. (Only **get** method is supported.)

SNMP security modes and security levels supported by the OnCell G3470A-LTE are shown in the following table. Select the security mode and level that will be used to communicate between the SNMP agent and manager.

Protocol Version	Setting on UI web page	Authentication Type	Data Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Use a community string match for authentication
	V1, V2c Write/Read Community	Community string	No	Use a community string match for authentication
SNMP V3	No-Auth	No	No	Use account with admin or user to access objects
	MD5 or SHA	Authentication based on MD5 or SHA	No	Provides authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.

Protocol Version	Setting on UI web page	Authentication Type	Data Encryption	Method
	MD5 or SHA	Authentication based on MD5 or SHA	Data encryption key	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication and encryption.

The following parameters can be configured on the **SNMP Agent** page.

SNMP Agent

Enable Disable ▾

Remote management Disable ▾

Read community

Write community

SNMP agent version V1, V2c ▾

Admin authentication type No Auth ▾

Admin privacy type Disable ▾

Privacy key

Private MIB information

Device object ID enterprise.8691.15.7

Field	Description	Default setting
Enable	Select Enable to activate SNMP agent.	Disable
Remote management	Select Enable to allow remote management via SNMP agent.	Disable
Read community	Enter the community string or password (up to 31 characters long) for an SMNP agent to access objects with read-only permission.	public
Write community	Enter the community string or password (up to 31 characters long) for an SMNP agent to access objects with read-write permission.	private
SNMP agent version	Select the SNMP protocol version used to manage the OnCell G3470A-LTE.	V1, V2c
Admin authentication type	Select No Auth to use an administrator account to access objects without authentication. Select MD5 to authenticate using HMAC-MD5 algorithms where the minimum requirement is to use an 8-character password. Select SHA to authenticate using HMAC-SHA algorithms where the minimum requirement is to use an 8-character password.	No Auth
Admin privacy type	Select Disable for no data encryption. Select DES to use DES-based data encryption. Select AES to use AES-based data encryption.	Disable
Privacy key	Enter the key (up to 63 characters) for data encryption.	

Field	Description	Default setting
Private MIB information Device object ID	The object ID (OID) is the enterprise value for the OnCell G3470A-LTE. This value is not configurable.	

Port Forwarding

You can configure port forwarding settings on the OnCell G3470A-LTE to redirect specific packets from a remote host on the WAN to a server on the LAN. This feature hides the IP address of a local server and prevents remote hosts from accessing the local server directly.

The OnCell G3470A-LTE filters out unrecognized packets to protect your LAN network when computers connected to the OnCell G3470A-LTE are not visible to the WAN.

NOTE You can make LAN computers accessible from the Internet by enabling Virtual Server.

You can also configure port forwarding on the OnCell G3470A-LTE to redirect traffic to a specific port on a LAN computer.

To access the **Port Forwarding** screen, click **Advanced Settings → Port Forwarding**. The OnCell G3470A-LTE supports a total of 32 port forwarding rules.

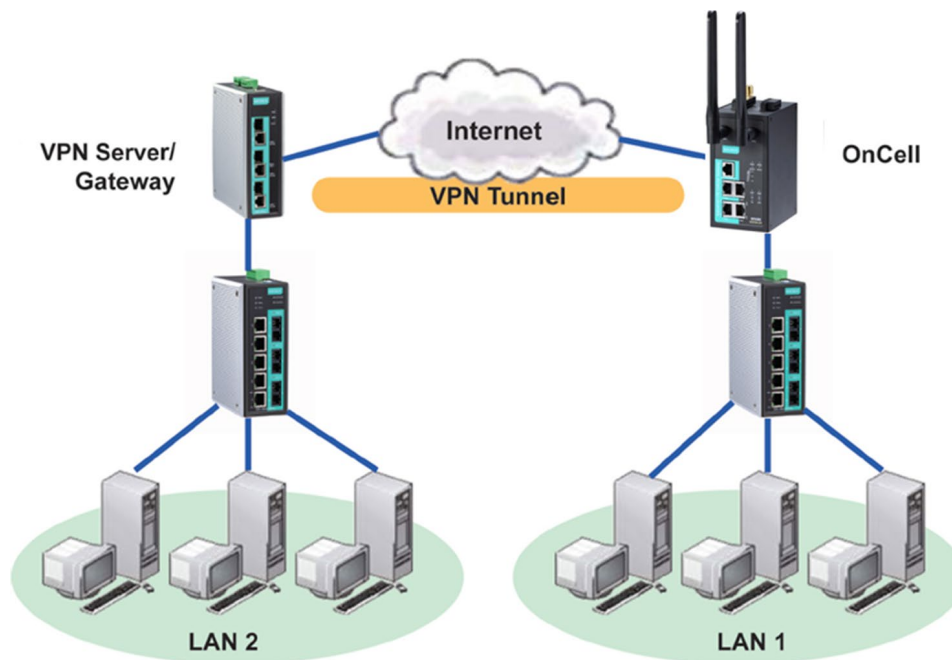
The following table includes the field descriptions.

Field	Description	Factory Default
Enable	Select Enable to activate the port forwarding feature.	Disable
Active	Select this check box to activate the port forwarding entry.	
Protocol	Select an option from the drop-down list.	
Public Port	Enter the public port number. Make sure that the port number specified is not already used by OP modes.	
Internal IP	Enter the IP address of a LAN device to receive the redirected traffic.	
Internal Port	Enter the port number on a LAN device to which to redirect traffic.	

VPN

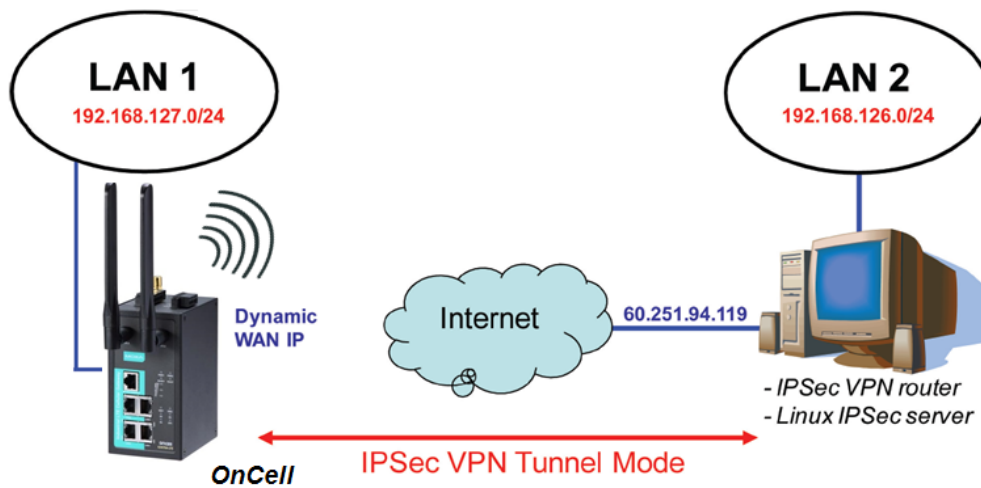
Computers that are part of a virtual private network (VPN) use a second, "virtual" IP address to connect to the Internet. Instead of running across a single private network, some of the links between nodes that are part of a VPN use open network connections or virtual circuits on a larger network, such as the Internet. With the help of VPNs, cellular devices acting as a VPN client can initiate a connection with a VPN server. Once the connection is established, cellular devices can communicate with other network devices on the same private network.

The following figure shows a network example.



OnCell G3470A-LTE VPN Feature Overview

- The OnCell G3470A-LTE IPsec provides security in a network with Gateway-to-gateway topology as illustrated in the following figure.
- The OnCell G3470A-LTE initiates a VPN connection to a VPN Server.
- The OnCell G3470A-LTE IPsec operates in Tunnel mode with **IPsec VPN tunnel**.
 - Manual Key/ESP, IKE/PSK
 - DES/3DES/AES128 encryption
 - MD5/SHA1 authentication
- IPsec NAT traversal and PFS (Perfect Forwarding Secrecy).



IPSec Settings

You can enable or disable the IPsec and NAT traversal functions and configure up to five VPN tunnels in the **IPSec Settings** screen (click **Advanced Settings > VPN > IPsec Settings**).

IPSec Settings (AP only)

IPSec setting enable Disable ▾

NAT traversal Disable ▾

Enable	Name	Remote Endpoint	Local Subnet	Remote Subnet	Action
Disable					Edit Delete
Disable					Edit Delete
Disable					Edit Delete
Disable					Edit Delete
Disable					Edit Delete

The following table provides the field descriptions.

Field	Description	Factory Default
IPSec setting enable	Select Enable to activate the IPsec feature.	Disable
NAT Traversal	Select Enable to activate the NAT traversal feature that allows IPsec traffic to traverse through NAT-enabled devices. Make sure that the remote VPN device supports this feature.	Disable
Action	Click Edit to configure a VPN tunnel. Click Delete to remove the selected VPN tunnel.	

Configuring a VPN Tunnel

To configure a VPN tunnel, click **Edit** in the **IPSec Settings** screen.

Tunnel Setting	
IPSec enable	Enable ▾
Connection name	Test (Must begin with an alphabet)
Connection type	Site to Site ▾
Startup mode	Start in Initial ▾
Remote VPN gateway	162.10.10.1
Local network	10.10.10.1
Local netmask	255.255.255.0
Local ID	10.10.10.1
Remote network	16.10.10.1
Remote netmask	255.255.255.0
Remote ID	16.10.10.1
Key Exchange (Phase1)	
Operation mode	Main ▾
Authentication mode	Pre-shared Key ▾ test
Encryption algorithm	DES ▾
Hash algorithm	MD5 ▾
DH group	DH-2 ▾
Negotiation times	0 (0:forever)
IKE life time	60 min.
Rekey expire time	9 min.
Rekey fuzz percentage	100 %
Data Exchange (Phase2)	
Perfect forward secrecy	Disable ▾
SA life time	480 min.
Encryption algorithm	DES ▾
Hash algorithm	MD5 ▾
Dead Peer Detection	
DPD action	Disable ▾
DPD delay	30 seconds
DPD timeout	120 seconds
Submit	

The following table provides the field descriptions.

Field	Description	Factory Default
IPSec enable	Select Enable to activate the VPN tunnel.	Disable
Connection name	Enter a descriptive name for the VPN tunnel.	
Connection type	Select one of the following connection types: <ul style="list-style-type: none"> Site-to-Site – Select this option to create a VPN tunnel for static local and remote subnets. Site-to-Site(any) – Select this option to create a VPN tunnel between a static local subnet and a dynamic remote subnet. 	Site-to-Site
Startup mode	Select Start in Initial to set the OnCell G3470A-LTE to initiate a connection with the remote VPN gateway. Select Wait for Connecting to set the OnCell G3470A-LTE to wait for a remote VPN gateway to initiate a connection.	Start in Initial
Remote VPN gateway	Enter the WAN IP address of the remote VPN gateway.	
Local network	Enter the remote VPN server subnet IP of the local network.	
Local netmask	Enter the remote VPN server subnet netmask of the local network.	
Local ID	Enter an ID (IP/FQDN/User_FQDN) to identify and authenticate the local VPN gateway.	
Remote network	Enter the remote VPN server subnet IP of the remote network.	
Remote netmask	Enter the remote VPN server subnet netmask of the remote network.	

Field	Description	Factory Default
Remote ID	Enter an ID (IP/FQDN/User_FQDN) to identify and authenticate the remote VPN endpoint.	
Key Exchange (Phase1)		
Operation mode	Select main mode or aggressive mode to configure the standard negotiation parameters for IKE Phase 1 of the VPN Tunnel.	Main
Authentication mode	Select Pre-shared key, RSA Signature or X.509 authentication mode to for phase 1 key exchange. The configuration fields vary depending on the authentication mode you select. For information on configuring each authentication mode, refer to the following sections.	Pre-shared key
Encryption algorithm	Select the DES, 3DES or AES128 algorithm for the VPN ISAKMP phase 1 encryption mode.	DES
Hash algorithm	Select the MD5 or SHA-1 VPN key exchange phase 1 hash mode.	MD5
DH group	Select the DH-2(1024) or DH-5(1536) VPN key exchange phase 1 Diffie-Hellman group. As the Diffie-Hellman Group number increases, the higher the level of encryption implemented for PFS.	DH-2
Negotiation time	The number of allowed reconnect times when startup mode is initiated. If the number is 0, this tunnel will always try connecting to the remote gateway when the VPN tunnel is not created successfully.	0
IKE life time	Enter the number of minutes for the VPN IKE SA phase 1 Lifetime. This is the period of time to pass before establishing a new IPSec security association (SA) with the remote endpoint.	60
Rekey expire time	Enter the number of minutes for the Start to Rekey before IKE lifetime expired.	9
Rekey fuzz percent	The rekey expire time will change randomly to enhance the security. Rekey fuzz percent is the maximum random change margin of the Rekey expire time. 100% means the rekey expire time will not change randomly.	100%
Data Exchange (phase2)		
Perfect forward secrecy	Enable or disable the Perfect Forward Secrecy. PFS is an additional security protocol.	Disable
SA life time	Enter the number of seconds for the VPN ISAKMP phase 2 Lifetime. This is the period of time to pass before establishing a new IPSec security association (SA) with the remote endpoint.	480
Encryption algorithm	Select the DES, 3DES, or AES128 algorithm for the VPN ISAKMP phase 1 encryption mode.	DES
Hash algorithm	Select the MD5 or SHA-1 VPN ISAKMP phase 1 authentication mode.	MD5
Dead Peer Detection		
DPD action	When you enable the Dead Peer Detection (DPD) feature, the OnCell G3470A-LTE performs one of the following actions when connection to a remote IPSec tunnel is down: <ul style="list-style-type: none"> • Hold: Keep the VPN tunnel • Clear: Clear the VPN tunnel • Restart: Re-establish the VPN tunnel on Start in Initial mode. 	Disable

Field	Description	Factory Default
	<ul style="list-style-type: none"> Restart by Peer: Re-establish the VPN tunnel on Wait for connecting mode. 	
DPD delay	The period of dead peer detection messages.	30
DPD timeout	Timeout to check if the connection is alive or not.	120

Configuring Pre-shared Key Settings

To configure pre-shared key authentication mode in phase 1 key exchange, in the **Tunnel settings** screen, select **Pre-shared key** from the **Authentication mode** drop-down list. Then, enter a key in the text field.

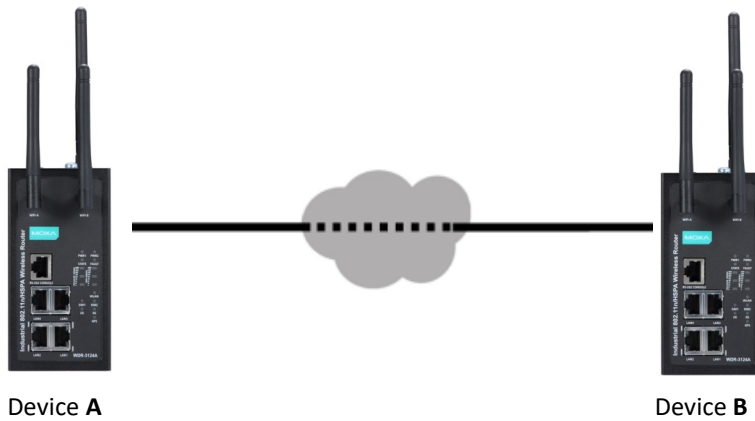
Make sure that you configure the same key on the OnCell G3470A-LTE and the remote VPN gateway.

Configuring RSA Signature Settings

To configure RSA signature settings, complete the following steps:

- In the Tunnel Settings screen, select RSA Signature from the Authentication mode drop-down list.
- Generate or import a local private key. Perform one of the following actions:
 - Click **Generate Local Private Key**. The OnCell G3470A-LTE creates a private key and displays the key information in the **Local private key** field.
 - Click **Import Local Private Key** and select a key file to import. After the OnCell G3470A-LTE successfully imports the selected key, the system displays the key information in the **Local private key** field.
- Generate or import a remote private key. Perform one of the following actions:
 - Click **Generate Remote Public Key**. The OnCell G3470A-LTE creates a public key and displays the key information in the **Remote public key** field.
 - Click **Import Remote Public Key** and select a key file to import. After the OnCell G3470A-LTE successfully imports the selected key, the system displays the key information in the **Remote public key** field.

The following figure shows the certificate generation and certificate export/import example.



1. Generate Root CA
2. Generate Local Certificate
3. Click **PKCS#12 Export** to export the local certificate (*local_CA_A.p12*)
4. Click **Certificate Export** to export the local certificate file (*local_CA_A.pem*)
5. Click **VPN > X.509 > Local Certificate Upload** and import the local certificate (*local_CA_A.p12*).
6. Click **VPN > X.509 > Remote Certificate Upload** to import the remote certificate (*local_CA_B.pem*).

1. Generate Root CA
2. Generate Local Certificate
3. Click **PKCS#12 Export** to export the local certificate (*local_CA_B.p12*)
4. Click **Certificate Export** to export the local certificate file (*local_CA_B.pem*)
5. Click **VPN > X.509 > Local Certificate Upload** and import the local certificate (*local_CA_B.p12*).
6. Click **VPN > X.509 > Remote Certificate Upload** to import the

X.509 Settings

NOTE Before you configure X.509 settings, make sure that you have imported local and remote certificates in the **Local/Remote Certificate Upload** screen (click **Advanced Settings > VPN > X.509 Certificate > Local/Remote Certificate Upload**).

In the **Tunnel Settings** screen, select **X.509** from the **Authentication mode** drop-down list and select a certificate from the **Local certificate** and **Remote certificate** drop-down lists.

Certificate Generation

X.509 is a digital certificate method commonly used for IPsec authentication. You can generate a self-signed root CA or local certificate on the OnCell G3470A-LTE and import or export the certificate on a remote VPN gateway.

To display the **Certificate Generation** screen, click **Advanced Settings > VPN > X.509 Certificate > Certificate Generation**.

Certificate Generation

Root Certificate Generation

Certificate days: 365

Certificate password (4 to 63 characters):

Country name (2 letter code): TW

State or province name (full name): Taiwan

Locality name (eg, city): Taipei

Organization name (eg, company): MOXA

Organizational unit name (eg, section): IW

Common name (e.g. server FQDN or your name): WDR-3124

Email address: info@moxa.com

Generate Root CA Export Root CA

Name	Subject	Action
Root CA		Delete
Trusted CA1		Choose File No file chosen Import Delete
Trusted CA2		Choose File No file chosen Import Delete

Local Certificate Setting

Certificate days:

Certificate password (4 to 63 characters):

Organizational unit name (eg, section):

Certificate name:

Email address:

Generate Local Certificate

Name	Certificate Days	Certificate Password	Organizational Unit Name	Certificate Name	Email Address	Action
Local certificate 1						Certificate Export PKCS#12 Export Delete
Local certificate 2						Certificate Export PKCS#12 Export Delete
Local certificate 3						Certificate Export PKCS#12 Export Delete
Local certificate 4						Certificate Export PKCS#12 Export Delete
Local certificate 5						Certificate Export PKCS#12 Export Delete

To generate a root CA certificate, complete the following steps:

1. In the **Certificate Generation** screen, enter information in the fields under **Root Certificate Generation**.

Field	Description
Certificate days	Enter the number of days the certificate is valid for.
Certificate password	Enter a password to create a password-protected certificate.
Country name	Enter the country.
State or province name	Enter the state or the province.
Locality name	Enter the city.
Organization name	Enter the name of the organization.
Organization unit name	Enter the unit or section in the organization.
Common name	Enter a name (such as a server name or your name).
Email address	Enter an email address.

2. Click **Generate Root CA**.

After you have generated the root CA certificate, generate a local certificate and export the key files. Complete the following steps:

1. In the **Certificate Generation** screen, enter information in the fields under **Local Certificate Settings**.

Field	Description
Certificate days	Enter the number of days the certificate is valid for.
Certificate password	Enter a password to create a password-protected certificate.

Field	Description
Organization unit name	Enter the unit or section in the organization.
Common name	Enter a name (such as a server name or your name).
Email address	Enter an email address.

2. Click **Generate Local Certificate**.
3. Click **Certificate Export** to export the public key file for the certificate that you import on a remote VPN gateway.
4. Click **PKCS#12 Export** to export the private key file for local certificates on the OnCell G3470A-LTE. You can import the local certificate in the **Local Certificate Upload** screen.

Local Certificate Upload

If you configure X.509 authentication mode for VPN tunnel setup, you must import a local certificate on the OnCell G3470A-LTE.

You can add or delete a local certificate in the **Local Certificate Upload** screen.

Local Certificate Upload

PKCS#12 upload No file chosen

Import password

Name	Password	Subject	Action
			<input type="button" value="Delete"/>
			<input type="button" value="Delete"/>
			<input type="button" value="Delete"/>
			<input type="button" value="Delete"/>
			<input type="button" value="Delete"/>

1. Click **Advanced Settings > VPN > X.509 Certificate > Local Certificate Upload**.
2. In the **PKCS#12 upload** field, click **Browse** to select a local certificate.
3. In the **Import password** field, enter the certificate password.
4. Click **Import**.

NOTE You can generate a local certificate in the **Certificate Generation** screen.

Remote Certificate Upload

You can add or delete a certificate from the remote VPN gateway in the **Remote Certificate Upload** screen.

Remote Certificate Upload

Remote certificate upload No file chosen

Name	Subject	Action
		<input type="button" value="Delete"/>
		<input type="button" value="Delete"/>
		<input type="button" value="Delete"/>
		<input type="button" value="Delete"/>
		<input type="button" value="Delete"/>

1. Click **Advanced Settings > VPN > X.509 Certificate > Remote Certificate Upload**.
2. In the **Remote certificate upload** field, click **Browse** to select a local certificate.
3. Click **Import**.

Auto Warning Settings

Since industrial-grade devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that these devices, including wireless APs or clients, must provide system maintainers with real-time alarm messages. Even when system administrators are out of the control room for an extended period, they can still be informed of the status of devices almost instantaneously when exceptions occur.

In addition to logging these events, the OnCell G3470A-LTE supports different approaches to warn engineers automatically, such as SNMP trap, e-mail, and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarms by email and relay output.

System Log

System Log Event Types

Detail information for grouped events is shown in the following table. You can select the **Enable log** check box to enable the selected event types. All default values are enabled (checked). The log for system events can be seen in **Status > System Log**.

Syslog Event Types

Event Group	Enable Log
System-related events	<input checked="" type="checkbox"/>
Network-related events	<input checked="" type="checkbox"/>
Config-related events	<input checked="" type="checkbox"/>
Power events	<input checked="" type="checkbox"/>
DI events	<input checked="" type="checkbox"/>
VPN events	<input checked="" type="checkbox"/>

The following table describes the types of system logs.

System-related events	Event is triggered when...
-----------------------	----------------------------

System restart (warm start)	The OnCell G3470A-LTE is rebooted, such as when its settings are changed (IP address, subnet mask, etc.).
Network-related events	Event is triggered when...
LAN link on	The LAN port is connected to a device or network.
LAN link off	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Config-related events	Event is triggered when...
Configuration Changed	A configuration item has been changed.
Configuration file import via Web Console	The configuration file is imported to the OnCell G3470A-LTE.
Console authentication failure	An incorrect password is entered.
Firmware upgraded	The OnCell G3470A-LTE's firmware is updated.
Power events	Event is triggered when...
Power 1/2 transition (On -> Off)	The OnCell G3470A-LTE is powered down in PWR1/2.
Power 1/2 transition (Off -> On)	The OnCell G3470A-LTE is powered via PWR1/2.
DI events	Event is triggered when ...
DI1/2 transition (On -> Off)	Digital Input 1/2 is triggered by on to off transition.
DI1/2 transition (Off -> On)	Digital Input 1/2 is triggered by off to on transition.

Syslog

This function provides the event logs for the Syslog server. The function supports up to three configurable Syslog servers and Syslog server UDP port numbers. When an event occurs, the event will be sent as a Syslog UDP packet to the specified Syslog servers.

Syslog Event Types

Detail information for the grouped events is shown in the following table. You can the **Enable log** check box to enable the selected event types. All default values are enabled (checked).

For information on the event types, refer to the *System Log Event Types* section.

Syslog Event Types	
Event Group	Enable Log
System-related events	<input checked="" type="checkbox"/>
Network-related events	<input checked="" type="checkbox"/>
Config-related events	<input checked="" type="checkbox"/>
Power events	<input checked="" type="checkbox"/>
DI events	<input checked="" type="checkbox"/>
VPN events	<input checked="" type="checkbox"/>

Submit

Syslog Server Settings

You can configure the parameters for your Syslog server on the **Syslog Server Settings** screen.

Syslog Server Settings

Syslog server 1

Syslog port

Syslog server 2

Syslog port

Syslog server 3

Syslog port

Field	Description	Factory Default
Syslog server 1/2/3	Enter the IP address of the 1st/ 2nd/ 3rd Syslog Server	
Syslog port	Enter the UDP port for the syslog server.	514

E-Mail

E-Mail Event Types

Select the **Active** checkbox to enable an event item. By default, all values are deactivated (unchecked).

E-mail Event Types	
Event	<input type="checkbox"/> Active
Cold start	<input type="checkbox"/>
Warm start	<input type="checkbox"/>
Power 1 transition (On-->Off)	<input type="checkbox"/>
Power 1 transition (Off-->On)	<input type="checkbox"/>
Power 2 transition (On-->Off)	<input type="checkbox"/>
Power 2 transition (Off-->On)	<input type="checkbox"/>
Configuration changed	<input type="checkbox"/>
IP changed	<input type="checkbox"/>
Password changed	<input type="checkbox"/>
Console authentication failure	<input type="checkbox"/>
DI 1 transition (On-->Off)	<input type="checkbox"/>
DI 1 transition (Off-->On)	<input type="checkbox"/>
DI 2 transition (On-->Off)	<input type="checkbox"/>
DI 2 transition (Off-->On)	<input type="checkbox"/>
LAN 1 link on	<input type="checkbox"/>
LAN 1 link off	<input type="checkbox"/>
LAN 2 link on	<input type="checkbox"/>
LAN 2 link off	<input type="checkbox"/>
LAN 3 link on	<input type="checkbox"/>
LAN 3 link off	<input type="checkbox"/>
LAN 4 link on	<input type="checkbox"/>

E-mail Server Settings

The E-mail server settings determine how e-mail warnings are sent for system and serial port events. You may configure up to 4 e-mail addresses to receive automatic warnings.

E-mail Server Settings

Mail server (SMTP)

User name

Password

From e-mail address

To e-mail address 1

To e-mail address 2

To e-mail address 3

To e-mail address 4



ATTENTION

Consult your Network Administrator or ISP for the proper mail server settings. The Auto warning function may not work properly if it is not configured correctly. The OnCell G3470A-LTE's SMTP AUTH supports LOGIN, PLAIN, and CRAM-MD5 (RFC 2554).

Mail server

Setting	Description	Factory Default
Mail server	This field is for your mail server's domain name or IP address. .	None

User name

Setting	Description	Factory Default
User name	This field is for your mail server's user name, if required.	None

Password

Setting	Description	Factory Default
Password	This field is for your mail server's password, if required.	None

From e-mail address

Setting	Description	Factory Default
From e-mail address	This is the e-mail address from which automatic e-mail warnings will be sent.	None

To e-mail address 1 to 4

Setting	Description	Factory Default
To e-mail address 1 to 4	This is the e-mail address or addresses to which the automatic e-mail warnings will be sent.	None

Relay

Relay Event Types

Select **Active** to enable the event types.

For information on the event types, refer to the *System Log Event Types* section.

Relay Event Types	
Event	Active
Power 1 transition (On-->Off)	<input type="checkbox"/>
Power 2 transition (On-->Off)	<input type="checkbox"/>
DI 1 transition (On-->Off)	<input type="checkbox"/>
DI 1 transition (Off-->On)	<input type="checkbox"/>
DI 2 transition (On-->Off)	<input type="checkbox"/>
DI 2 transition (Off-->On)	<input type="checkbox"/>
LAN 1 link on	<input type="checkbox"/>
LAN 1 link off	<input type="checkbox"/>
LAN 2 link on	<input type="checkbox"/>
LAN 2 link off	<input type="checkbox"/>
LAN 3 link on	<input type="checkbox"/>
LAN 3 link off	<input type="checkbox"/>
LAN 4 link on	<input type="checkbox"/>
LAN 4 link off	<input type="checkbox"/>

Submit

Trap

Traps can be used to signal abnormal conditions (notifications) to a management station. This trap-driven notification can make your network more efficient.

Because a management station usually takes care of a large number of devices that have a large number of objects, it will be overloading for the management station to poll or send requests to query every object on every device. It would be better if the managed device agent could notify the management station by sending a message known as a trap for the event.

Trap Event Types

Trap Event Types	
Event	<input type="checkbox"/> Active
Cold start	<input type="checkbox"/>
Warm start	<input type="checkbox"/>
Power 1 transition (On-->Off)	<input type="checkbox"/>
Power 1 transition (Off-->On)	<input type="checkbox"/>
Power 2 transition (On-->Off)	<input type="checkbox"/>
Power 2 transition (Off-->On)	<input type="checkbox"/>
Configuration changed	<input type="checkbox"/>
Console authentication failure	<input type="checkbox"/>
LAN link on	<input type="checkbox"/>
LAN link off	<input type="checkbox"/>

Submit

SNMP Trap Receiver Settings

SNMP traps are defined in SMIV1 MIBs (SNMPv1) and SMIV2 MIBs (SNMPv2c). The two styles are basically equivalent, and it is possible to convert between the two. You can set the parameters for SNMP trap receivers through the web page.

SNMP Trap Receiver Settings

1st Trap version

1st Trap server IP/name

1st Trap community

2nd Trap version

2nd Trap server IP/name

2nd Trap community

Field	Description	Default setting
Trap version	Select the SNMP version for SNMP traps.	V1
Trap server IP/name	Enter the IP address or domain name of the SNMP trap server.	
Trap community	Enter the community string or password (up to 31 characters) for authentication.	alert

SMS

SMS Event Types

Select **Active** to enable the event types. For information on the event types, refer to the *System Log Event Types* section.

SMS Event Types

Event	<input type="checkbox"/> Active
Cold start	<input type="checkbox"/>
Warm start	<input type="checkbox"/>
Power 1 transition (On-->Off)	<input type="checkbox"/>
Power 1 transition (Off-->On)	<input type="checkbox"/>
Power 2 transition (On-->Off)	<input type="checkbox"/>
Power 2 transition (Off-->On)	<input type="checkbox"/>
Configuration changed	<input type="checkbox"/>
IP changed	<input type="checkbox"/>
Password changed	<input type="checkbox"/>
Console authentication failure	<input type="checkbox"/>
DI 1 transition (On-->Off)	<input type="checkbox"/>
DI 1 transition (Off-->On)	<input type="checkbox"/>
DI 2 transition (On-->Off)	<input type="checkbox"/>
DI 2 transition (Off-->On)	<input type="checkbox"/>
LAN 1 link on	<input type="checkbox"/>
LAN 1 link off	<input type="checkbox"/>
LAN 2 link on	<input type="checkbox"/>
LAN 2 link off	<input type="checkbox"/>
LAN 3 link on	<input type="checkbox"/>
LAN 3 link off	<input type="checkbox"/>
LAN 4 link on	<input type="checkbox"/>
LAN 4 link off	<input type="checkbox"/>
Cellular close temperature range	<input type="checkbox"/>

Submit

SMS Alert Settings

You can set the OnCell G3470A-LTE to send SMS notifications to up to four phone numbers and select a message encoding format in the **SMS Alert Settings** screen.

SMS Alert Settings

To phone number 1

To phone number 2

To phone number 3

To phone number 4

Encode format

Submit

Field	Description	Factory Default
To phone number 1/2/3/4	Enter the phone numbers to which the OnCell G3470A-LTE sends SMS notifications.	
Encode format	Select an encoding format from the drop-down list. <ul style="list-style-type: none"> Text ASCII (7 bits) – Encode SMS messages in 7-bit format (160 bytes per packet). 	Text ASCII (7 bits)

Status

DNS Information

The DNS information screen displays the DNS server to which the OnCell G3470A-LTE is connected and the DNS server information.

DNS Information	
<input checked="" type="checkbox"/> Auto refresh	
No	DNS Server
DNS server 1	
DNS server 2	
DNS server 3	
DNS server 4	

SIM Status

The SIM Status screen displays the current SIM card in use and the status of the SIM cards installed in the OnCell G3470A-LTE.

SIM Status	
SIM	Information
Used SIM	SIM 1
SIM 1	Wrong PIN code or SIM absent
SIM 2	Not in-use

Network Statistics

The **Network Statistics** screen displays information on the network interfaces of the device and protocols used along with the packets received and transmitted.

Network Statistics						
<input checked="" type="checkbox"/> Auto refresh						
LAN	Received	2947			Sent	248
CWAN	Received	0			Sent	0
IP	Received	2986			Sent	2017
	RDiscard	0	SNoRoute	0	SDiscard	0
	ErrHeader	0	ErrProto	0	ErrAddr	0
ICMP	Received	964			Sent	964
	REchoReq	0			SEchoReq	0
	REchoRply	0			SEchoRply	0
UDP	Received	5			Sent	969
	ErrHeader	0	ErrPorts	964		
TCP	Received	85			Sent	84
	ErrHeader	0	ErrPorts	0	ReSent	0
	CurrEstab	1	Opens	0		

The network statistic parameters and values are described in the following tables:

Interface	Action	Description
LAN	Received	The number of packets the device received through the LAN interface
	Sent	The number of packets the device sent through the LAN interface
CWAN	Received	The number of packets the device received through the CWAN interface
	Sent	The number of packets the device sent through the CWAN interface
Protocol	Actions	Description
IP	Received	The total number of input IP datagram packets that the device received from all interfaces
	Sent	The total number of output IP datagram packets that the device sent from all interfaces
	RDiscard	The input IP datagram packets discarded for various reasons (e.g.: Lack of buffer space)
	SDiscard	The output IP datagram packets discarded for various reasons (e.g.: Lack of buffer space)
	ErrAddr	The input IP datagram packets received with invalid IP addresses
	Errproto	The input IP datagram packets received with incorrect protocol.(i.e., a protocol other than TCP, UDP, and ICMP)
	ErrHeader	The input IP datagram packets received with invalid headers. (e.g., bad checksum, version number mismatch, and time-to-live period exceeded)
	SNoRoute	The input IP datagram packets received with incorrect routes
ICMP	Received	The total number of ICMP messages that the device received
	Sent	The total number of ICMP messages that the device sent
	REchoReq	The ICMP request packets that the device received (e.g., Ping requests received)
	REchoRply	The ICMP reply packets that the device received (e.g., Ping replies received)
	SEchoReq	The ICMP request packets that the device sent (e.g., Ping requests sent)
	SEchoRply	The ICMP reply packets that the device received. (e.g., Ping replies received)
UDP	Received	The total number of input UDP datagram packets received by the device
	Sent	The total number of output UDP datagram packets received by the device
	ErrHeader	The input UDP datagram packets received with invalid headers
	ErrPorts	The input UDP datagram packets received with incorrect port numbers
TCP	Received	The total number of input TCP segment packets received by the device
	Sent	The total number of output TCP segment packets received by the device
	ErrHeader	The input TCP segment packets received with invalid headers (e.g., bad checksum)
	ErrPorts	The input TCP segment packets received with the wrong port number
	ReSent	The output TCP segment packets retransmitted
	CurrEstab	The number of TCP connections established (e.g. status is ESTABLISHED or CLOSE-WAIT)
	Opens	The number of TCP connections to be opened (e.g. status is SYNC-sent, SYNCRCBD, SYNC_RCVD)

System Log

Triggered events are recorded in System Log. You can export the log contents to an available viewer by clicking **Export Log**. You can use the **Clear Log** button to clear the log contents and the **Refresh** button to refresh the log.

System Log

```
( 985) 2015/02/04,09h:36m:44s Cellular WAN IP is Changed
( 986) 2015/02/04,09h:36m:44s Console authentication failure
( 987) 2015/02/04,10h:17m:04s Firmware upgraded from 1.1 Build 15012914 to 1.1 Build 15020416
( 988) 2015/02/04,10h:17m:29s Power 1 transition (Off -> On)
( 989) 2015/02/04,10h:17m:36s LAN 1 link on
( 990) 2015/02/04,10h:17m:38s System warm start, restarted by console
( 991) 2015/02/04,10h:18m:07s Cell. module gets an IP 10.192.115.194
( 992) 2015/02/04,10h:18m:07s Cellular WAN IP is Changed
( 993) 2015/02/04,10h:43m:30s LAN 1 link off
( 994) 2015/02/05,09h:47m:35s LAN 1 link on
( 995) 2015/02/05,09h:49m:46s Firmware upgraded from 1.1 Build 15020416 to 1.2 Build 15020517
( 996) 2015/02/05,09h:50m:31s Power 1 transition (Off -> On)
( 997) 2015/02/05,09h:50m:38s LAN 1 link on
( 998) 2015/02/05,09h:50m:40s System warm start, restarted by console
( 999) 2015/02/05,09h:51m:08s Cell. module gets an IP 10.199.135.33
(1000) 2015/02/05,09h:51m:08s Cellular WAN IP is Changed
```

↑
↓

Export Log Clear Log Refresh

Relay Status

The status of user-configurable events can be found under **Relay Status**.

If an event is triggered, the event is included on this list.

After you have addressed an event, click **Acknowledge Event**.

Relay Status

Auto refresh

Relay Status		
Power 1 transition (On-->Off)	---	Acknowledge Event
Power 2 transition (On-->Off)	---	Acknowledge Event
DI 1 transition (On-->Off)	---	Acknowledge Event
DI 1 transition (Off-->On)	---	Acknowledge Event
DI 2 transition (On-->Off)	---	Acknowledge Event
DI 2 transition (Off-->On)	---	Acknowledge Event
LAN 1 link on	---	Acknowledge Event
LAN 1 link off	---	Acknowledge Event
LAN 2 link on	---	Acknowledge Event
LAN 2 link off	---	Acknowledge Event
LAN 3 link on	---	Acknowledge Event
LAN 3 link off	---	Acknowledge Event
LAN 4 link on	---	Acknowledge Event
LAN 4 link off	---	Acknowledge Event

DI and Power Status

You can view the digital input (DI) and power input information in the **DI and Power Status** screen.

DI and Power Status	
<input checked="" type="checkbox"/> Auto refresh	
Input Status	On / Off
Power 1 status	Off
Power 2 status	On
DI 1 status	Off
DI 2 status	Off

VPN Log

The **VPN Log** screen displays VPN connection information.

<pre>"sandiago2"[1] 49.216.148.168 #12: NAT-Traversal: Result using draft-ietf-ipsec-nat-t-ike (MacOS X): peer is NATed "sandiago2"[1] 49.216.148.168 #12: transition from state STATE_MAIN_R1 to state STATE_MAIN_R2 "sandiago2"[1] 49.216.148.168 #12: STATE_MAIN_R2: sent MR2, expecting MI3 "sandiago2"[1] 49.216.148.168 #12: Main mode peer ID is ID_IPV4_ADDR: '192.168.127.253' match_id a=192.168.127.253 b=192.168.127.253 results matched "sandiago2"[1] 49.216.148.168 #12: transition from state STATE_MAIN_R2 to state STATE_MAIN_R3 "sandiago2"[1] 49.216.148.168 #12: new NAT mapping for #12, was 49.216.148.168:57473, now 49.216.148.168:57474 "sandiago2"[1] 49.216.148.168 #12: STATE_MAIN_R3: sent MR3, ISAKMP SA established {auth=OAKLEY_PRESHARED_KEY cipher=oakley_des_cbc_64 prf=oakley_md5 group=modp1024} "sandiago2"[1] 49.216.148.168 #12: the peer proposed: 192.168.128.0/24:0/0 -> 192.168.127.0/24:0/0 "sandiago2"[1] 49.216.148.168 #12: find_client_connection starting with sandiago2 "sandiago2"[1] 49.216.148.168 #12: looking for 192.168.128.0/24:0/0 -> 192.168.127.0/24:0/0 "sandiago2"[1] 49.216.148.168 #12: concrete checking against sr#0 192.168.128.0/24 -></pre>
<div style="display: flex; justify-content: space-between;"> Export Log Clear Log Refresh </div>

VPN System log

The following table lists the system logs for the VPN feature. [VPN name] indicates the name of the VPN tunnel you have created on the OnCell G3470A-LTE.

System log	Description
[VPN name] mismatch of PSK	Pre-shared key mismatch.
[VPN name] Phase 1 start	VPN tunnel phase 1 start.
[VPN name] Phase 1 pass	VPN tunnel phase 1 pass.
[VPN name] Phase 2 start	VPN tunnel phase 2 start.
[VPN name] Phase 2 pass	VPN tunnel phase 2 pass.
[VPN name] received Delete ISAKMP SA	Remote VPN tunnel request to delete ISAKMP SA.
[VPN name] no Preshared Key Found	No pre-shared key is found.
[VPN name] policy doesn't allow PRESHARED KEY	The encryption algorithm does not allow pre-shared key.
[VPN name] policy doesn't allow RSASIG	VPN encrypt algorithm does not allow RSA or X.509.
[VPN name] DPD timeout - declaring peer dead	No response from a peer. PDP timeout.
[VPN name] DPD: Hold connection	Clear the remote VPN SA and keep the peer routing table status.
[VPN name] DPD: Clearing Connection	Clear the remote VPN SA and peer routing table status.

System log	Description
[VPN name] DPD: Restarting Connection	Renegotiate VPN SA immediately.
[VPN name] encrypt alg is different	VPN encryption mismatch.
[VPN name] hash alg is different	VPN hash mismatch.
[VPN name] DH group is different	VPN Diffie-Hellman group mismatch.
[VPN name] Ignore initial Aggr message	Ignore aggressive requests from a remote VPN gateway.
[VPN name] Maybe ID format error	Invalid local or remote VPN ID format.
[VPN name] we require peer ID differ from peer declares ID	Remote ID mismatch.
[VPN name] no suitable connection for peer	No corresponding VPN connection for a remote peer from the VPN responder.
[VPN name] connect_fail_log:ip_port	Fail to route VPN connection to [IP address].
[VPN name] send payload name	Send "VPN INVALID_KEY_INFORMATION, INVALID_CERTIFICATE or..." to a remote VPN gateway.
[VPN name] receive payload name	Receive "VPN INVALID_KEY_INFORMATION , INVALID_CERTIFICATE or ..." from a remote VPN gateway.

Maintenance

Maintenance functions provide the administrator with tools to manage the OnCell G3470A-LTE and wired/wireless networks.

Console Settings

You can enable or disable access permissions to the device through a LAN or WAN for the following consoles: HTTP, HTTPS, Telnet, and SSH. For greater security, we recommend only allowing access to the two secure consoles, HTTPS and SSH..

Console Settings

LAN Console Setting

- HTTP console Enable Disable
- HTTPS console Enable Disable
- Telnet console Enable Disable
- SSH console Enable Disable

WAN Console Setting

- HTTP console Enable Disable
- HTTPS console Enable Disable
- Telnet console Enable Disable
- SSH console Enable Disable

Submit

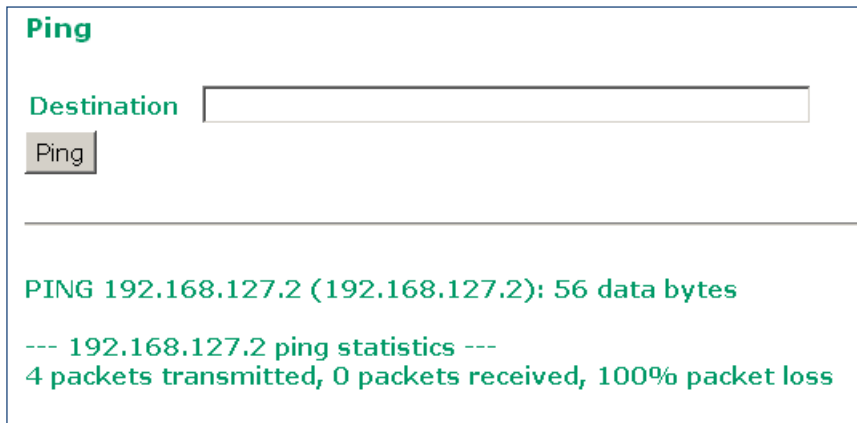
Ping

Ping helps to diagnose the integrity of wired or wireless networks. By inputting a node's IP address in the **Destination** field, you can use the **ping** command to make sure it exists and whether or not the access path is available.

Ping

Destination

If the node and access path are available, you will see that all packets were successfully transmitted with no loss. Otherwise, some, or even all, packets may get lost, as shown in the following figure.



Ping

Destination

PING 192.168.127.2 (192.168.127.2): 56 data bytes

--- 192.168.127.2 ping statistics ---

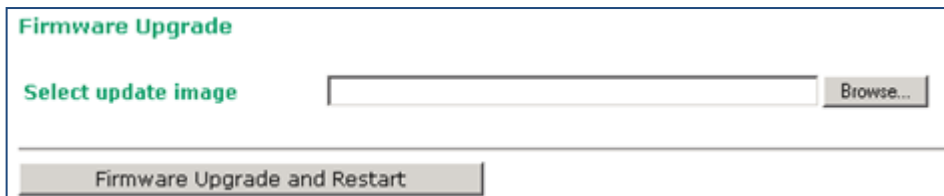
4 packets transmitted, 0 packets received, 100% packet loss

Firmware Upgrade

The OnCell G3470A-LTE can be enhanced with more value-added functions by installing firmware upgrades. The latest firmware is available at Moxa's download center.

Before running a firmware upgrade, make sure the OnCell G3470A-LTE is off-line. Click the **Browse** button to specify the firmware image file and click **Firmware Upgrade and Restart** to start the firmware upgrade. After the progress bar reaches 100%, the OnCell G3470A-LTE will reboot itself.

When upgrading your firmware, the OnCell G3470A-LTE's other functions are forbidden.



Firmware Upgrade

Select update image



ATTENTION

Please make sure the power source is stable when you upgrade your firmware. An unexpected power breakup may damage your OnCell G3470A-LTE.

Config Import Export

You can use the Config Import Export screen to back up or restore the following information:

- Configuration settings on the OnCell G3470A-LTE
- ABC-01 configuration
- MIB

In the **Config Import** section, click **Choose File** to select a configuration file and click **Config Import** button to begin importing configuration.

To save the configuration file to a storage media, click **Config Export**. The configuration file is a text file and you can view and edit it with a general text-editing tool.

For MIBs, click **MIB Export** to save the MIB file to a storage media. The configuration file is a .my file and you can import it with a general SNMP tool to remote control or set OnCell G3470A-LTE.

Config Import Export	
Config Import Select configuration file	<input type="button" value="Choose File"/> No file chosen
<input type="button" value="Config Import"/>	
Config Export	
<input type="button" value="Config Export"/>	
ABC-01 Import	
<input type="button" value="Config Import"/>	
ABC-01 Export	
<input type="button" value="Config Export"/>	
SNMP MIB File Export	
<input type="button" value="MIB Export"/>	

To download the configuration to the OnCell G3470A-LTE, complete the following steps:

1. Turn off the OnCell G3470A-LTE.
2. Connect ABC-01 to the OnCell G3470A-LTE's RS-232 console.
3. Turn on the OnCell G3470A-LTE.
4. The OnCell G3470A-LTE detects ABC-01 during the boot up process and automatically downloads the configuration from ABC-01. After the configuration is downloaded and if the configuration format is correct, the OnCell G3470A-LTE emits three short beeps before continuing the boot up process.
5. After the boot up process is complete, the OnCell G3470A-LTE emits two beeps, and the **Ready** LED turns solid green.

Load Factory Default

Use this function to reset the OnCell G3470A-LTE and roll all settings back to the factory default values. You can also reset the hardware by pressing the reset button on the top panel of the OnCell G3470A-LTE.

Load Factory Default
Reset to Factory Default
Click Activate to reset all settings, including the console password, to the factory default values. The system will be restarted immediately.
<input type="button" value="Activate"/>

Password

Use the **Password** function to change the administrative password of existing user accounts. First input the **Current password**, and then type the new password in the **New password** and **Confirm password** input boxes. To maintain a higher level of network security, do not use the default password (*moxa*), and be sure to change all user account passwords regularly.

Password

Current password

New password

Confirm password

Misc. Settings

Additional settings to help you manage your OnCell G3470A-LTE, are available on this page.

Misc. Settings

Reset button Always enable Disable 'restore to default function' after 60 sec

Select one of the following **Reset button** options:

- **Always enable**—Set the reset button to perform a factory restore on the OnCell G3470A-LTE. This is the default option.
- **Disable 'restore to default function' after 60 sec**—Deactivate the factory reset function of the reset button 60 seconds after the OnCell G3470A-LTE restarts.

Manual SMS

The manual SMS feature allows you to send text messages through the web console.

In the Manual SMS screen, enter the phone number of the SMS recipient and the message content of your message; then click **Send** to send the text message.

After the SMS is sent, the screen displays the following information:

- The entry number
- The time the message was sent
- The destination phone number
- Whether the SMS was successfully sent

Manual SMS

Manual Sending SMS Settings

Phone number

SMS content
Max length is 160.
The remain length is 160.

Warning: For some characters (e.g. '^', '\', '|', '~', '[', ']', '{', and '}'), two bytes are required.

Remote SMS Control

In cases where the OnCell G3470A-LTE is installed in a location with limited GPRS service, you can use the remote SMS control feature to get the current status of the OnCell G3470A-LTE or restart the OnCell G3470A-LTE.

The **Command** field in the **Remote SMS Control** screen shows the SMS message format.

Remote SMS Control

Remote SMS Control Disable ▾

Remote SMS Control Configuration

Password
 Auth type None ▾
 Caller ID 1
 Caller ID 2
 Caller ID 3
 Caller ID 4

Item	Action	Acknowledge	Command
Restart	<input type="checkbox"/>	<input type="checkbox"/>	@password@restart
Cellular report	<input type="checkbox"/>	<input type="checkbox"/>	@password@cell.report

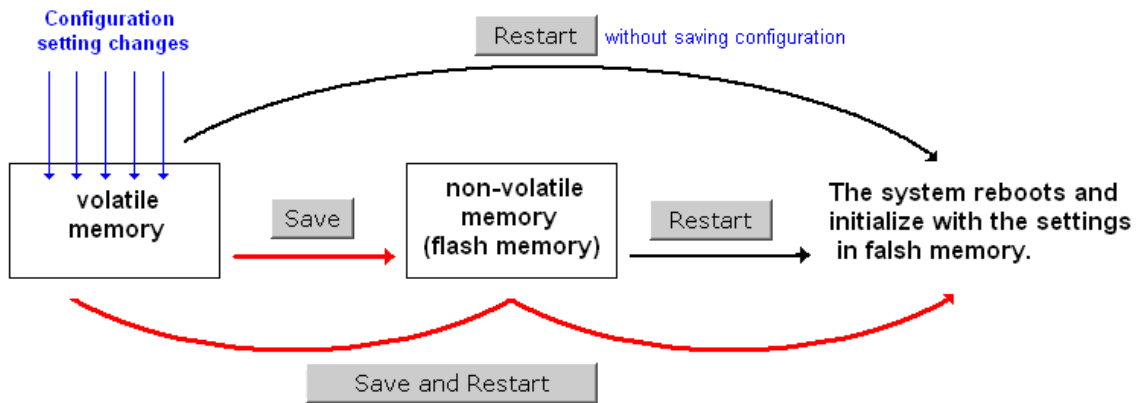
Field	Description	Default setting
Remote SMS Control	Select Enable to activate the remote SMS control feature.	Disable
Password	Enter a password (4 to 16 characters).	
Auth type	To restrict access to the OnCell G3470A-LTE, select the Caller ID authentication type.	None
Caller ID	If you use the caller ID authentication type, enter the caller ID number that can send SMS messages to control the OnCell G3470A-LTE.	
Action	Select this check box to perform the SMS control action.	
Acknowledge	Select this check box to send a reply to the SMS sender with an SMS message after the operation is completed.	

For example, if you enter "12345" for the password and send an SMS message with the content of "@12345@cell.report" to the OnCell G3470A-LTE, the OnCell G3470A-LTE sends an SMS message with the current status to the sender.

Save Configuration

The following figure shows how the OnCell G3470A-LTE stores the setting changes into volatile and non-volatile memory. All data stored in volatile memory will disappear when the OnCell G3470A-LTE is shutdown or rebooted unless they are **y**. Because the OnCell G3470A-LTE starts up and initializes with the settings stored in flash memory, all new changes must be saved to flash memory before restarting the OnCell G3470A-LTE.

This also means the new changes will not work unless you run either the **Save Configuration** function or the **Restart** function.



After you click on **Save Configuration** in the left menu box, the following screen will appear. Click **Save** if you wish to update the configuration settings in the flash memory at this time. Alternatively, you may choose to run other functions and put off saving the configuration until later. However, the new setting changes will remain in the non-volatile memory until you save the configurations.

Save Configuration

If you have submitted any configuration changes, you must save the changes and restart the system before they take effect. Click **Save** to save the changes in OnCell G3470A-LTE-EU's memory. Click **Restart** to activate new settings in the navigation panel.

Restart

If you submitted configuration changes, you will find a blinking string in the upper right corner of the screen. After making all your changes, click the **Restart** function in the left menu box. One of two different screens will appear.

If you made changes recently but did not save, you will be given two options. Clicking the **Restart** button here will reboot the OnCell G3470A-LTE directly, and all setting changes will be ignored. Clicking the **Save and Restart** button will apply all setting changes and then reboot the OnCell G3470A-LTE.

Restart

!!! Warning !!!

Click "Restart" to discard changes and reboot OnCell G3470A-LTE-EU directly.

Click "Save and Restart" to apply all setting changes and reboot OnCell G3470A-LTE-EU.

If you run the **Restart** function without changing any configurations or saving all your changes, you will see just one **Restart** button on your screen.

Restart

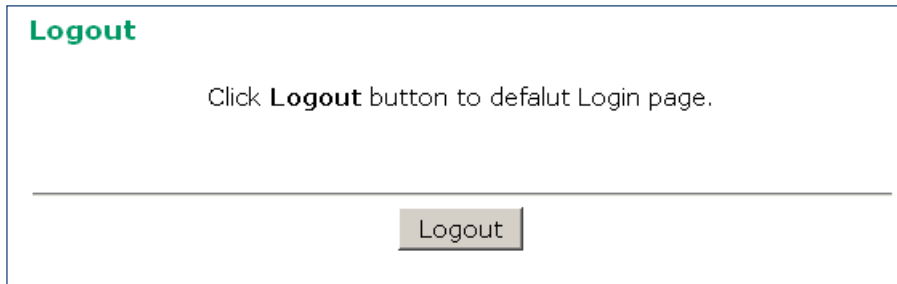
!!! Warning !!!

Clicking Restart will disconnect all Ethernet connections and reboot OnCell G3470A-LTE-EU.

You will not be able to run any of the OnCell G3470A-LTE's functions while the system is rebooting.

Logout

Logout helps users disconnect the current HTTP or HTTPS session and go to the Login page. For security reasons, we recommend you logout before quitting the console manager.



Software Installation and Configuration

The following topics are covered in this chapter:

- **Overview**
- **Wireless Search Utility**
 - Installing the Wireless Search Utility
 - Configuring the Wireless Search Utility

Overview

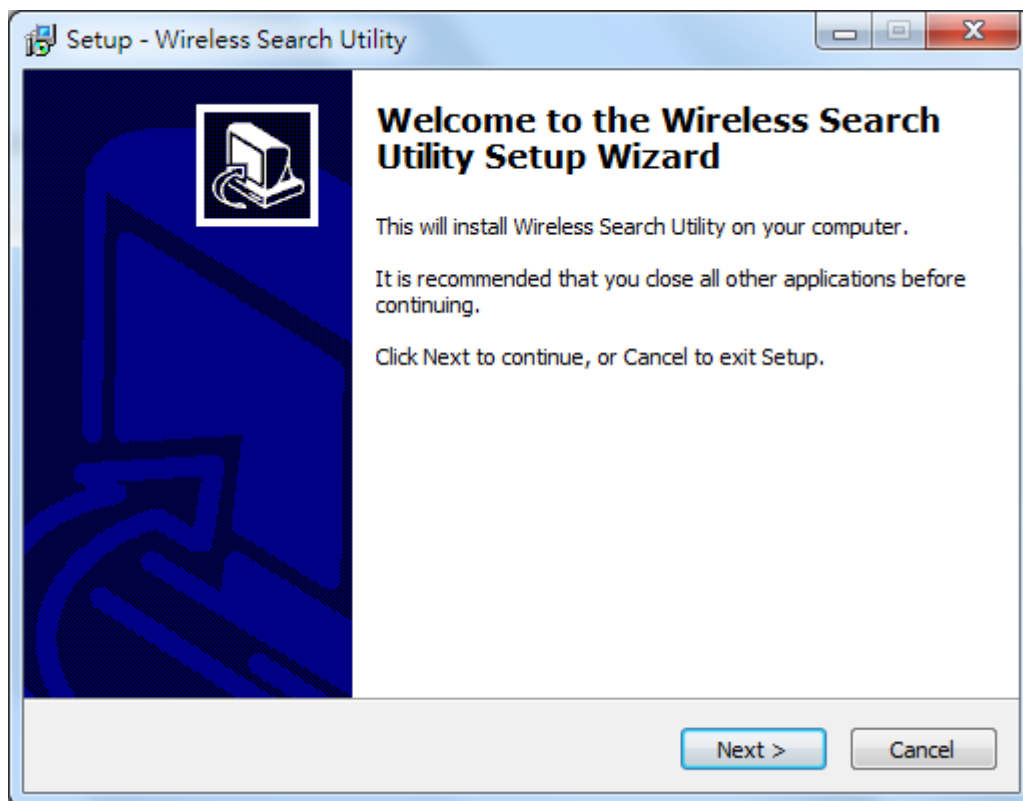
The Documentation & Software CD included with your OnCell G3470A-LTE is designed to make the installation and configuration procedure easy and straightforward. This auto-run CD includes the Wireless Search Utility (to broadcast search for all OnCell G3470A-LTE units accessible over the network), the OnCell G3470A-LTE User's Manual, and Quick Installation Guide.

Wireless Search Utility

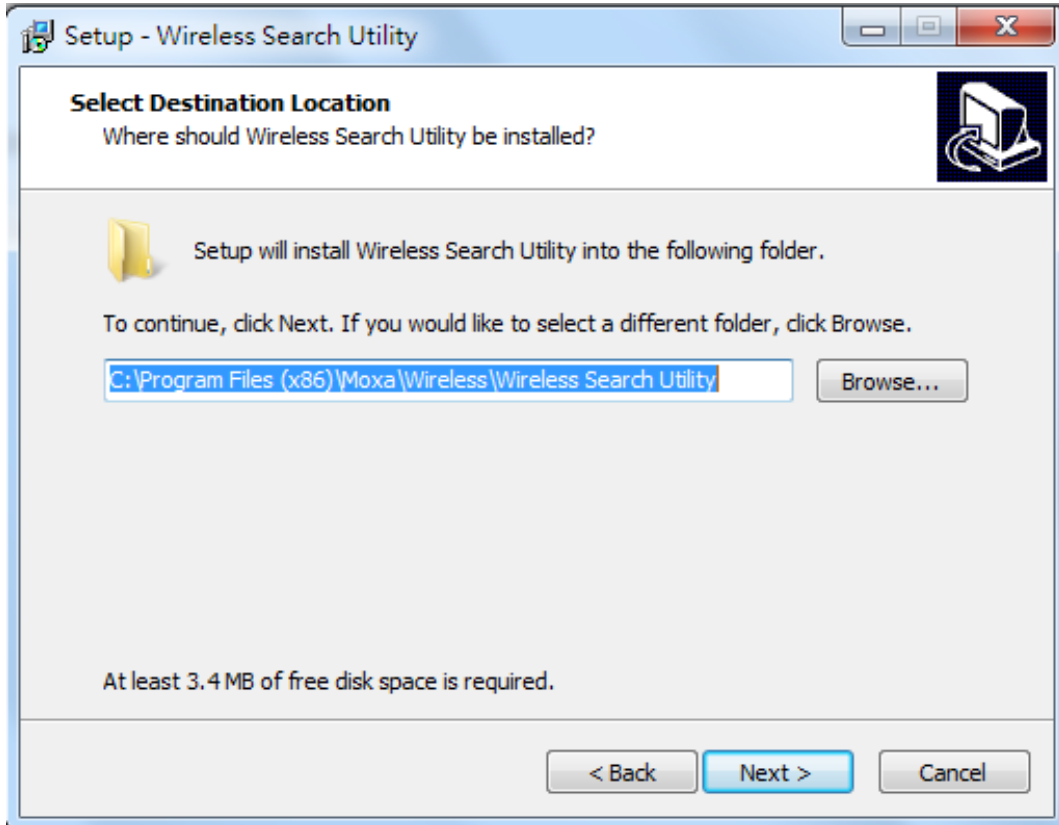
Installing the Wireless Search Utility

Click **INSTALL UTILITY** in the OnCell Installation CD auto-run window to install the Wireless Search Utility. Once the program starts running, click **Yes** to proceed.

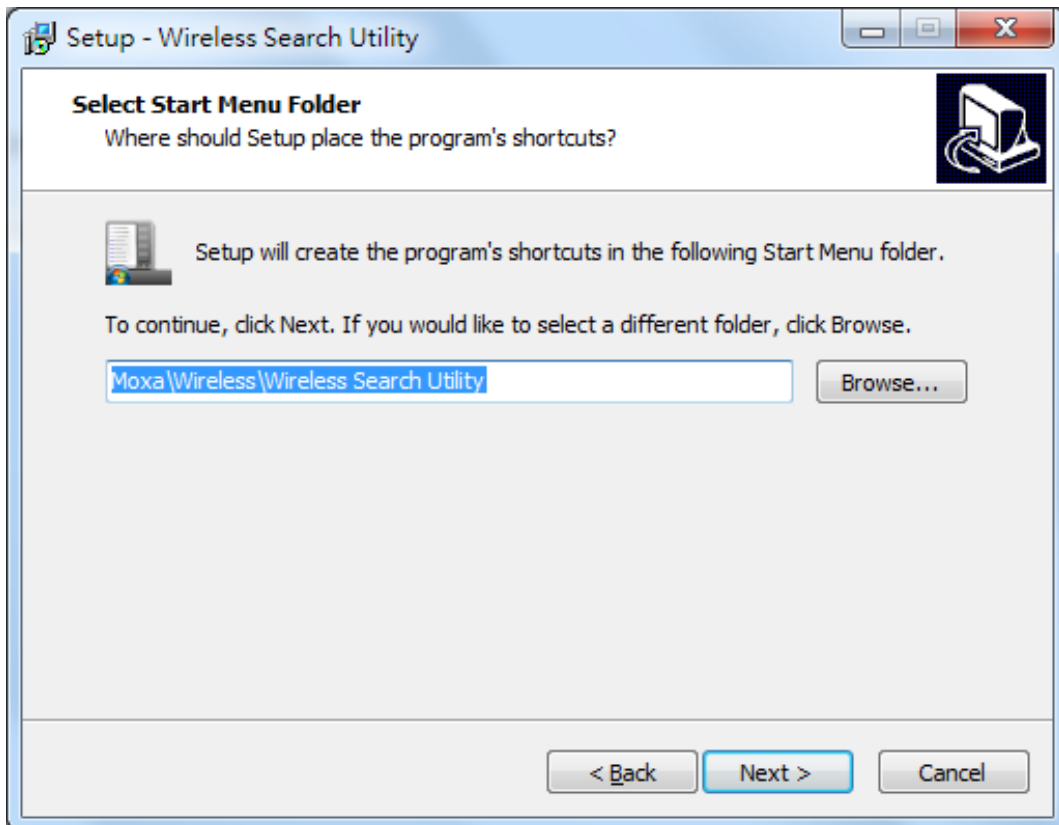
1. Click **Next** when the **Welcome** screen opens to proceed with the installation.



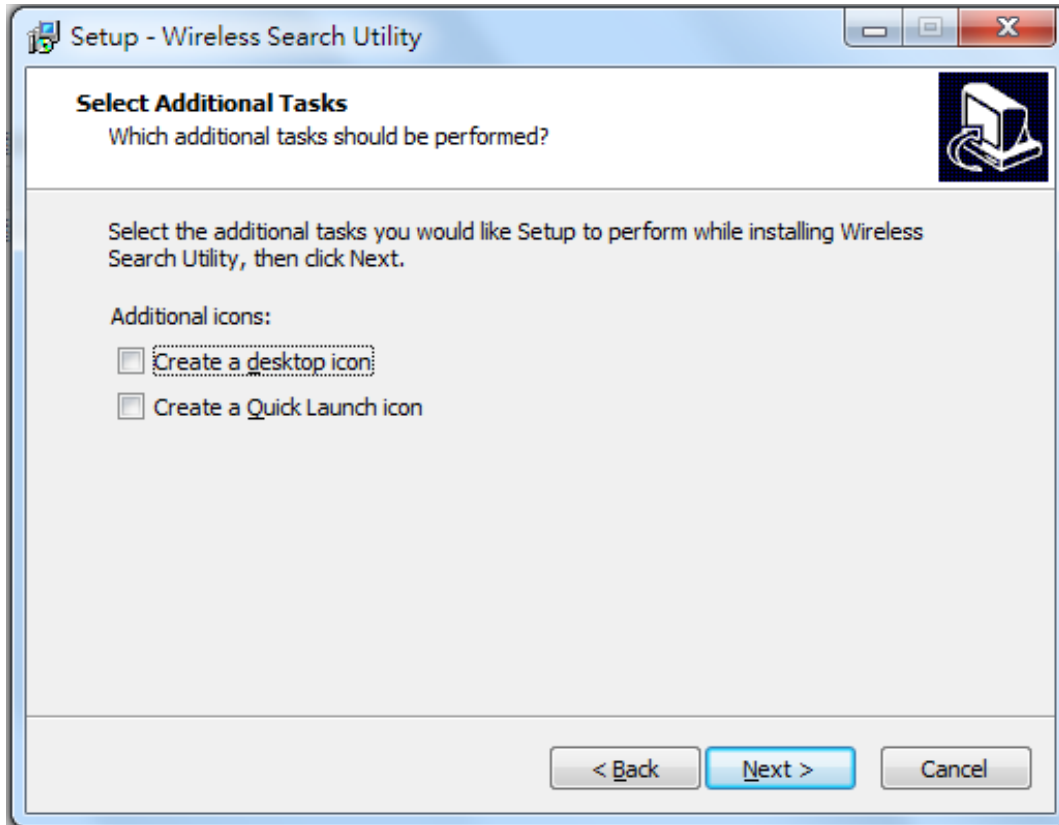
2. Click **Next** to install program files to the default directory, or click **Browse** to select an alternate location.



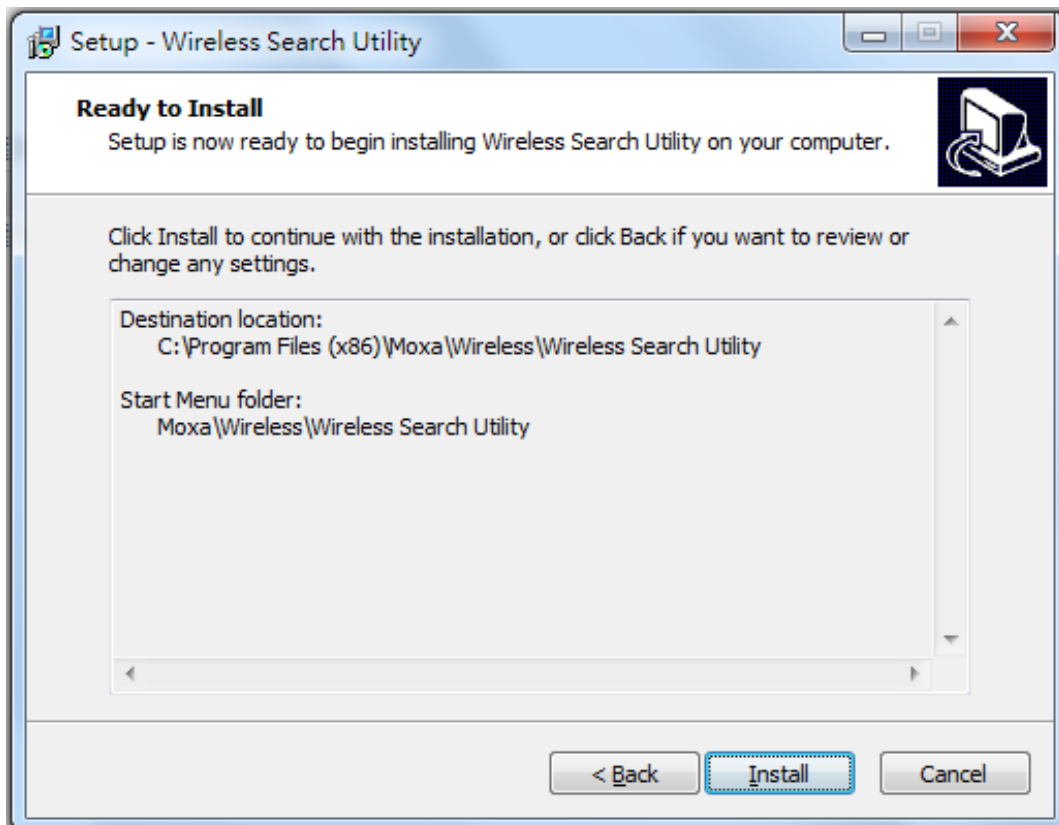
3. Click **Next** to create the program's shortcut files to the default directory, or click **Browse** to select an alternate location.



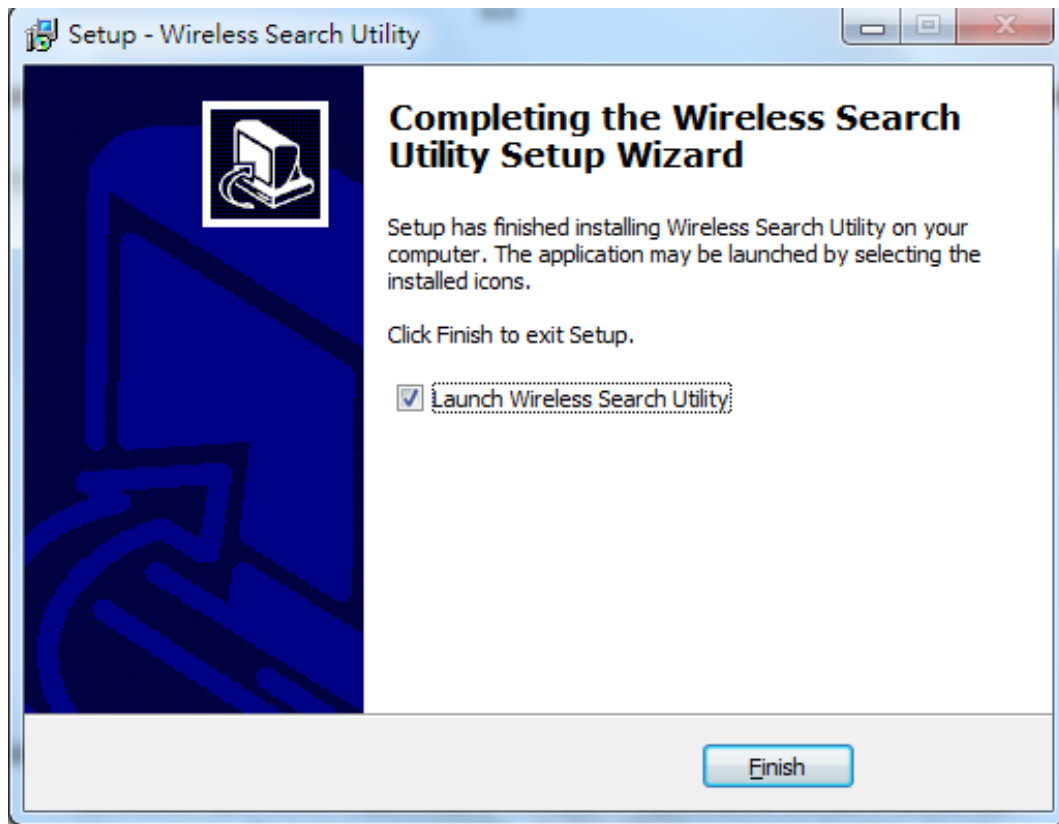
- 4. Click **Next** to select additional tasks.



- 5. Click **Next** to proceed with the installation. The installer then displays a summary of the installation options.



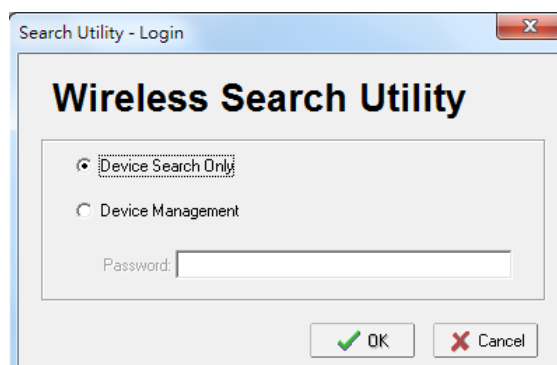
6. Click **Install** to begin the installation. The setup window will report the progress of the installation. To change the installation settings, click **Back** and navigate to the previous screen.
7. Click **Finish** to complete the installation of the Wireless Search Utility.



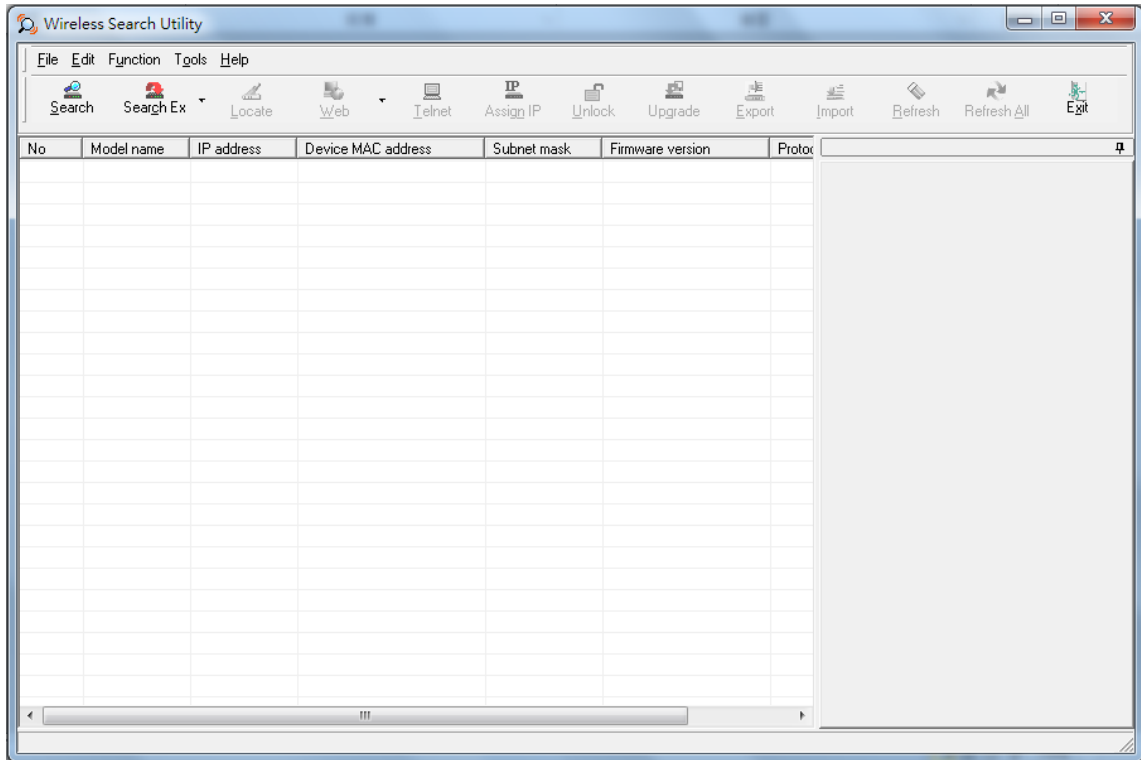
Configuring the Wireless Search Utility

The Broadcast Search function is used to locate all OnCell G3470A-LTE APs that are connected to the same LAN as your computer. After locating an OnCell G3470A-LTE, you will be able to change its IP address. Since the Broadcast Search function searches by TCP packet and not IP address.

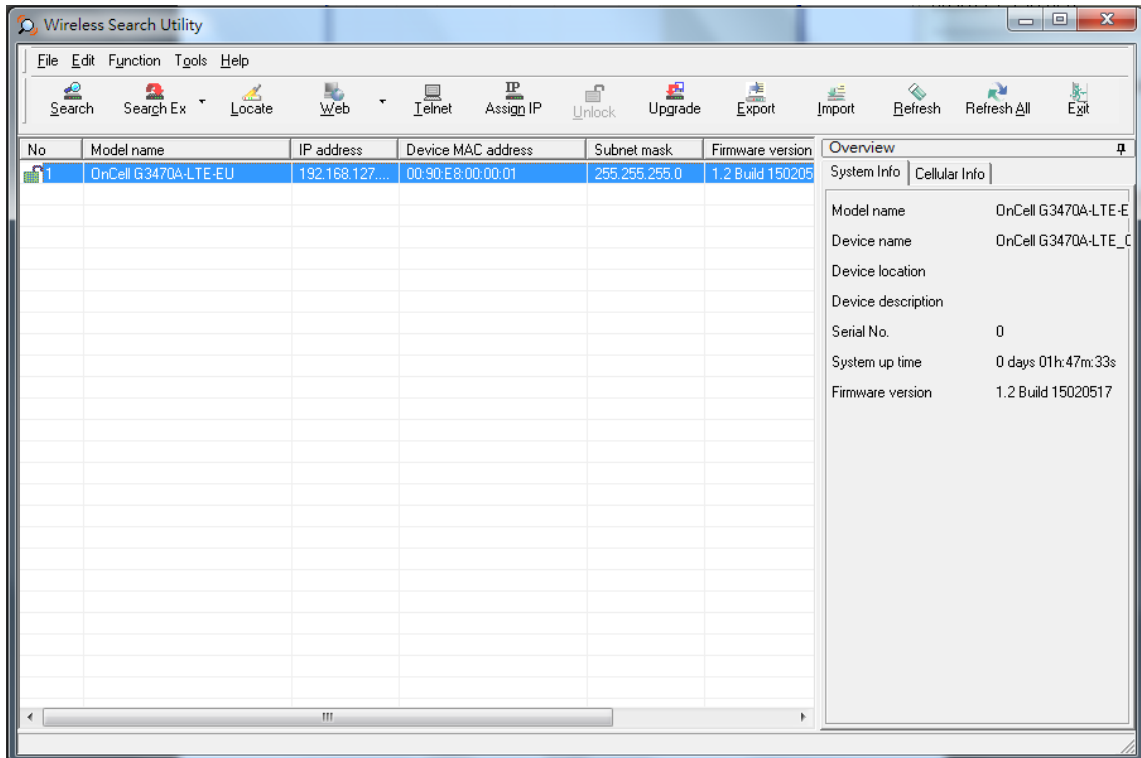
1. Start the **Wireless Search Utility** program.
If this is the first time you start the program, you are prompted to set the password (must be longer than four characters).
2. In the Wireless Search Utility screen, choose one of the following options and click OK.
 - **Device search only**–Search for OnCell G3470A-LTE units and to view each OnCell G3470A-LTE's configuration.
 - **Device management**–Assign IP addresses, upgrade firmware, and locate devices.



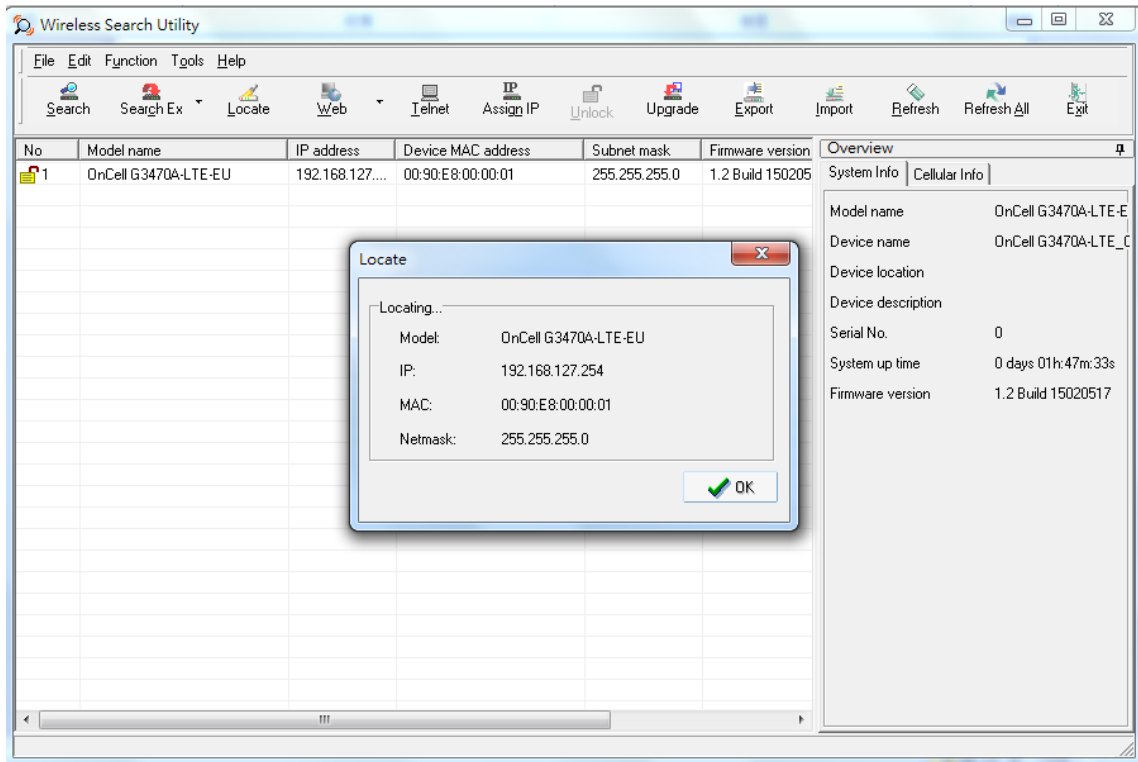
3. Click **Search**.



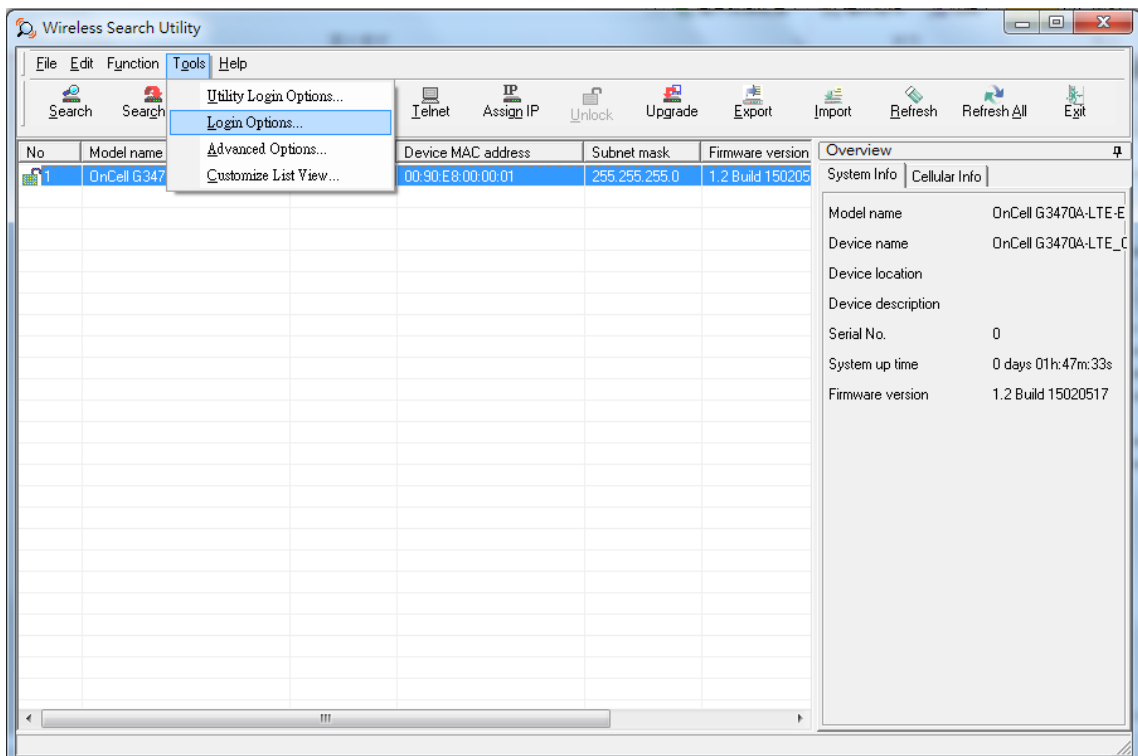
4. The "Searching" window indicates the progress of the search. When the search is complete, all devices that were located will be displayed in the Wireless Search Utility window.



- Click **Locate** to cause the selected device to beep.

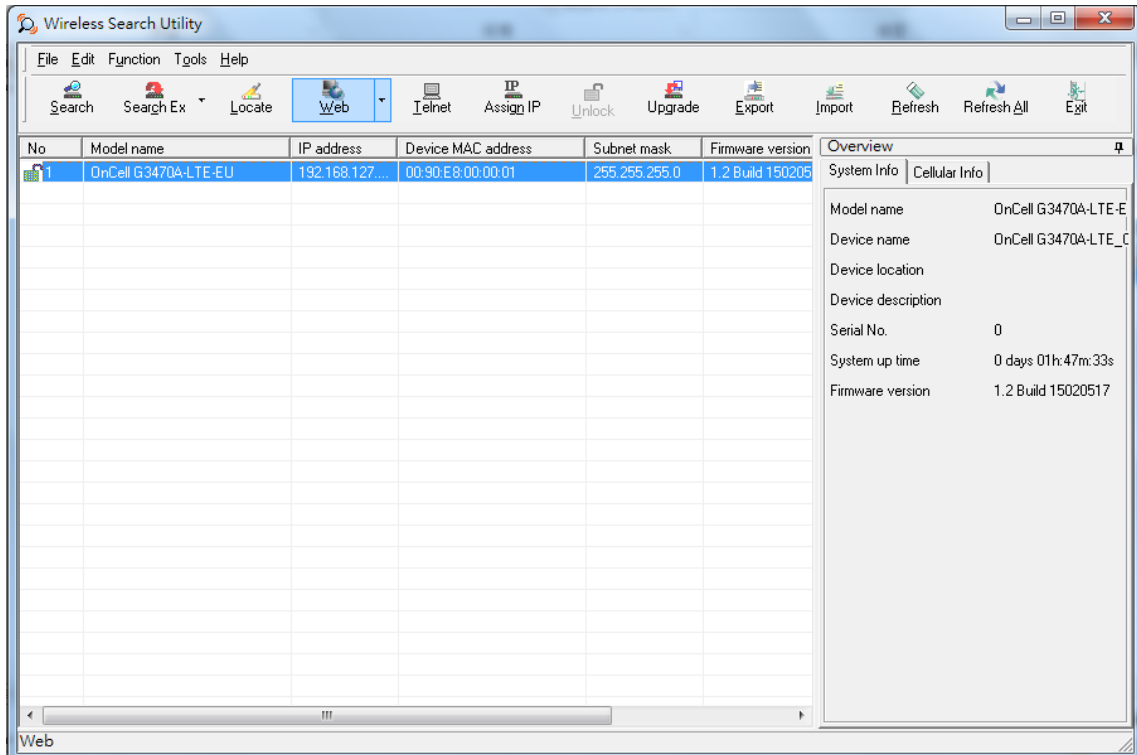


- Make sure that your device is **unlocked** before using the search utility's icons setting. The device will unlock automatically if the password is set to the default. Otherwise you must enter the new password manually.
- Go to **Tools > Device login Options** to manage and unlock additional AWKs.

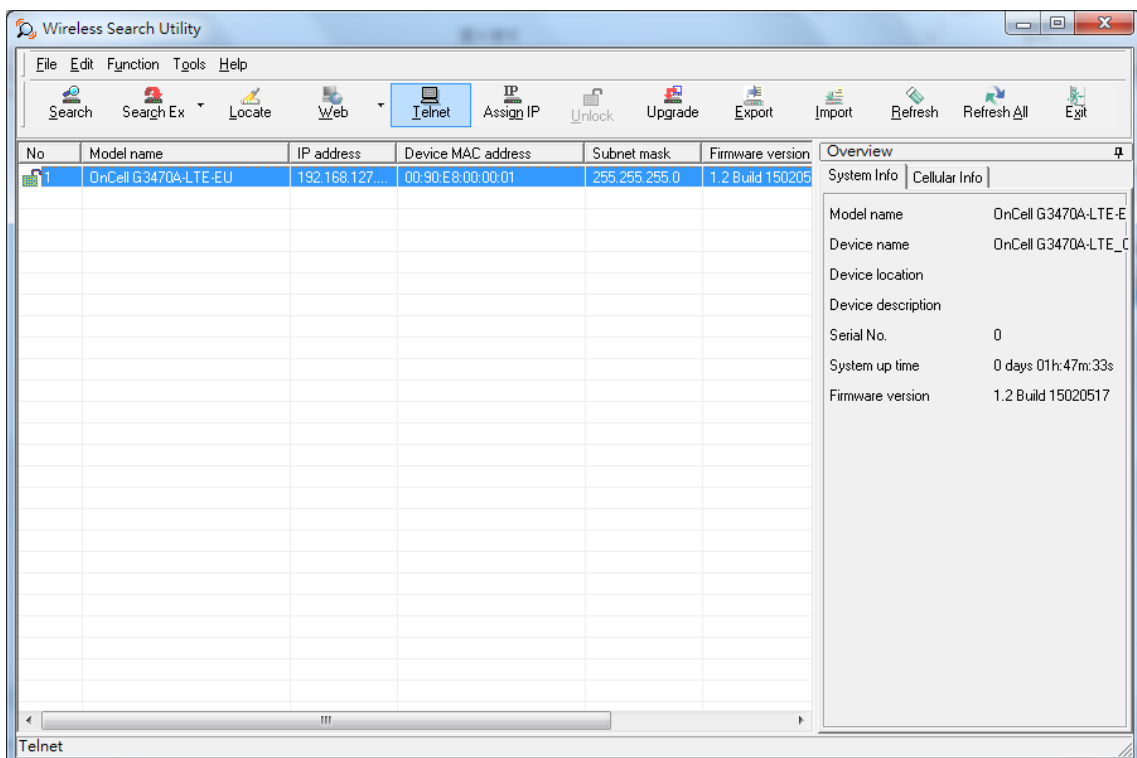


- Use the scroll down list to select the MAC addresses of the devices that you want to manage, and then click **Add**. Key in the password for the device and then click **OK** to save. If you return to the search page and search for the device again, you will find that the device will unlock automatically.

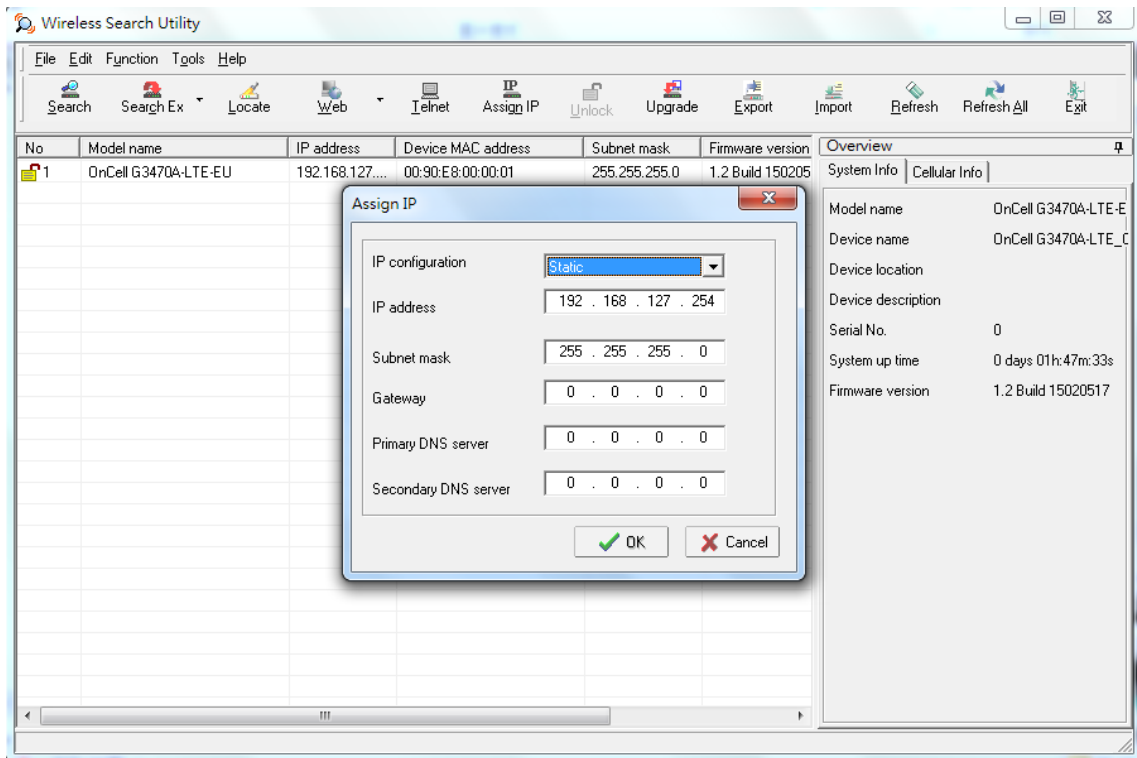
To modify the configuration of the highlighted device, click the **Web** icon to open the web console. This will take you to the web console, where you can make all configuration changes. Refer to Chapter 3, "Using the Web Console," for information on how to use the web console.



Click **Telnet** if you would like to use telnet to configure your devices.



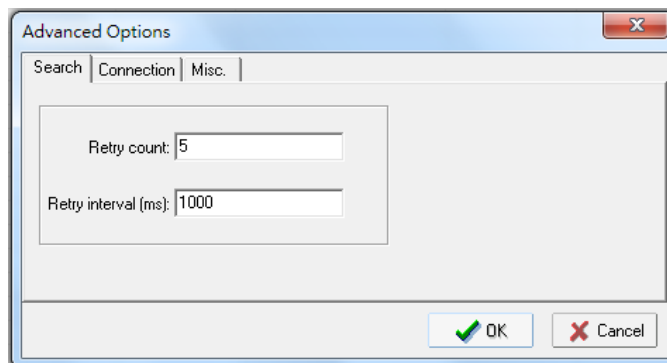
Click **Assign IP** to change the IP setting.



The three advanced options—**Search**, **Connection**, and **Miscellaneous**—are explained below:

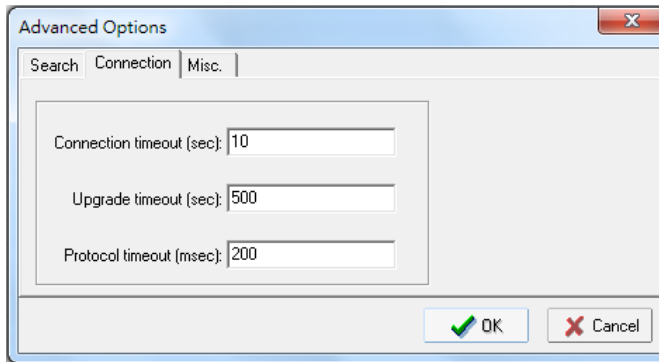
Search

- **Retry count (default=5):** Indicates how many times the search will be retried automatically.
- **Retry interval (ms):** The time to wait between retries.



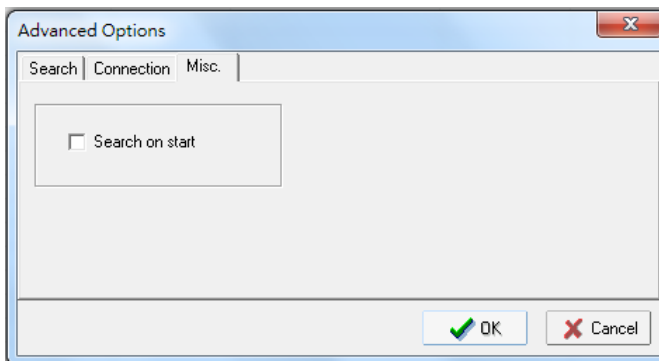
Connection

- **Connection timeout (secs):** Use this option to set the waiting time for the **Default Login**, **Locate**, **Assign IP**, **Upload Firmware**, and **Unlock** to complete.
- **Upgrade timeout (secs):** Use this option to set the waiting time for the connection to disconnect while the firmware is upgrading. Use this option to set the waiting time for the Firmware to write to flash.
- **Protocol timeout (msec):** Use this option to set the waiting time for package round trip while sending out comments . If no response within 200 msec will recognize connection failed.



Misc.

Search on start: Checkmark this box if you would like the search function to start searching for devices after you log in to the Wireless Search Utility.



A

Supporting Information

This chapter presents additional information about this product. You can also learn how to contact Moxa for technical support.

The following topics are covered in this appendix:

- ❑ **Firmware Recovery**
- ❑ **DoC (Declaration of Conformity)**
 - Federal Communication Commission Interference Statement
 - R&TTE Compliance Statement

Firmware Recovery

When the **Ready**, **FAULT**, **Signal Strength**, **4G**, **3G**, **2G**, and **GPS** LEDs turn on simultaneously and blink at one-second interval, it means the system booting has failed. It may result from some wrong operation or uncontrollable issues, such as an unexpected shutdown during firmware update. The OnCell G3470A-LTE is designed to help administrators recover such damage and resume system operation rapidly. You can refer to the following instructions to recover the firmware:

Connect to the OnCell G3470A-LTE's RS-232 console with 115200bps and N-8-1. You will see the following message shown on the terminal emulator every one second.



Take the following steps for the firmware recovery:

1. Change the IP address of the laptop to 192.168.127.1.
2. Set up a TFTP sever in your laptop.
3. Download OnCell G3470A-LTE's firmware from Moxa Website
4. Change firmware file name to g3470.rom
5. Connect to the OnCell G3470A-LTE's RJ45 Ethernet port

If setting is correct, you will see the following message shown on the terminal emulator, and the OnCell G3470A-LTE will reboot when the firmware recovery process has been finished.

Trying eth0

Using eth0 device

TFTP from server 192.168.127.1; our IP address is 192.168.127.254

Filename 'g3470.rom'.

Load address: 0x80060000

Loading:

```
*#####
#####
#####
```

DoC (Declaration of Conformity)

Federal Communication Commission Interference Statement

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

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

FCC Caution: To assure continued compliance, (example – use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This transmitter must not be co-located or operated in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

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

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.

FCC 15.407(e): Within the 5.15-5.25 GHz band, U-NII devices will be restricted to indoor operations to reduce any potential for harmful interference to co-channel MSS operations.

R&TTE Compliance Statement

Moxa declares that the apparatus OnCell G3470A-LTE complies with the essential requirements and other relevant provisions of Directive 1999/5/EC.

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France (with Frequency channel restrictions), Germany, Greece, Ireland, Italy, Luxembourg, Portugal, Spain, Sweden, The Netherlands, and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Norway and Switzerland.

EU Countries Not Intended for Use

None.

Potential Restrictive Use

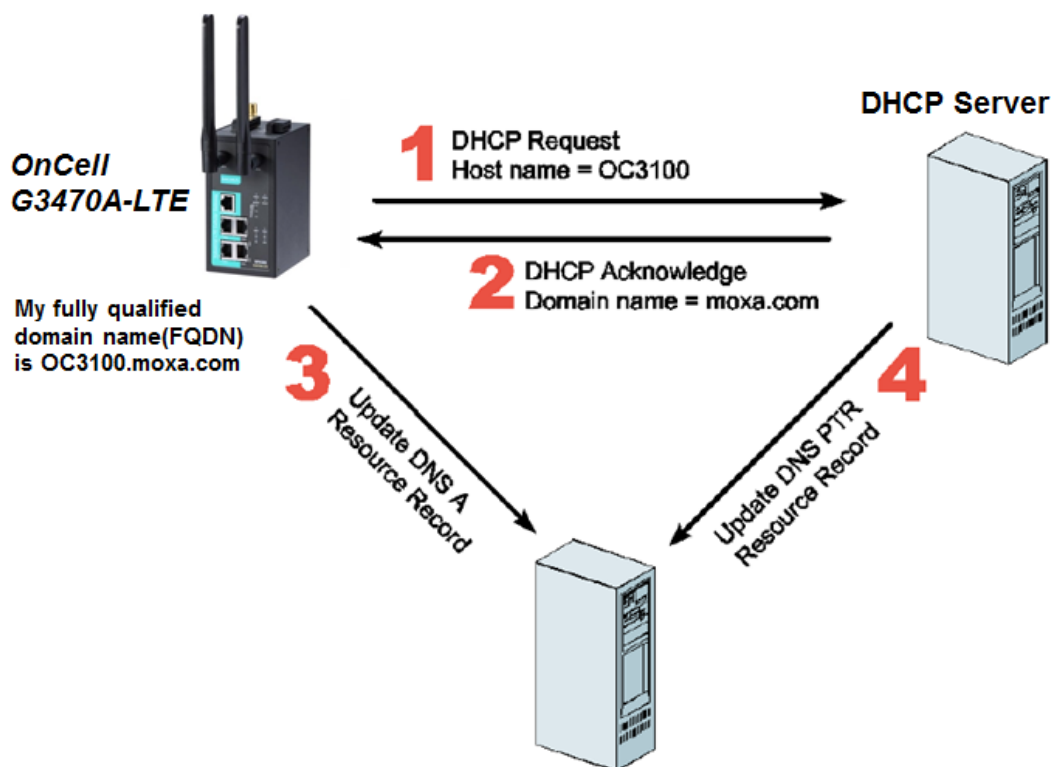
France: only channels 10, 11, 12, and 13.

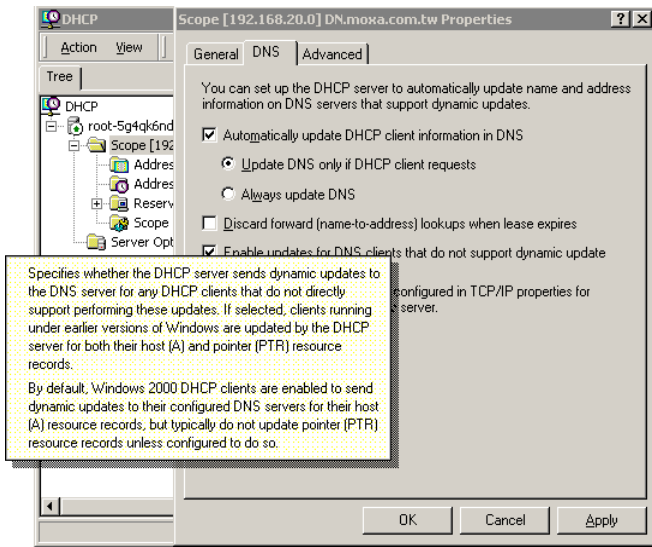
Dynamic Domain Name Server

This appendix explains how to use the OnCell G3470A-LTE with DDNS. When the OnCell G3470A-LTE receives its IP address from a DHCP (Dynamic Host Configuration Protocol) server, remote servers will be unable to access it using a fixed IP address. With DDNS (Dynamic Domain Name Server), a remote server can access the OnCell G3470A-LTE using its domain name instead of its IP address.

The following is a summary of the process:

1. The OnCell G3470A-LTE sends a request for an IP address to the DHCP server. At the same time, it notifies the DHCP server of its desired server name ("OC3100" in the illustration) according to the option 12 standard.
2. The DHCP server replies with the IP address that is assigned to the OnCell G3470A-LTE, along with the domain name ("moxa.com" in the illustration) and the IP addresses for the DNS server and gateway.
3. If the OnCell G3470A-LTE has authorization to update the DNS server, it will register its FQDN (Fully Qualified Domain Name) with the DNS server. The OnCell G3470A-LTE's FQDN will be in the format *server name.domain name* ("OC3100.moxa.com" in the illustration).
4. If the OnCell G3470A-LTE is not authorized to update the DNS server, the DHCP server can be used to update the DNS server. The DHCP server will register the DNS server with the PTR RR (the record of request for a domain name with IP address).





The above screenshot shows how DHCP can be set up to update the DNS.

Well-Known Port Numbers

In this appendix, we provide a list of port numbers that may cause network problems if you set the OnCell G3470A-LTE to one of these ports. Refer to RFC 1700 standards for a list of well-known port numbers or to the following introduction from the IANA:

The port numbers are divided into three ranges: the Well Known Ports, the Registered Ports, and the Dynamic and/or Private Ports.

The Well Known Ports range from 0 through 1023.

The Registered Ports range from 1024 through 49151.

The Dynamic and/or Private Ports range from 49152 through 65535.

The Well Known Ports are assigned by the IANA, and on most systems, can only be used by system processes or by programs executed by privileged users. The following table shows famous port numbers among the listed well-known port numbers. For more details, please visit the IANA website at <http://www.iana.org/assignments/port-numbers>.

TCP Socket	Application Service
0	Reserved
1	TCP Port Service Multiplexer
2	Management Utility
7	Echo
9	Discard
11	Active Users (sysstat)
13	Daytime
15	Netstat
20	FTP data port
21	FTP control port
23	Telnet
25	SMTP (Simple Mail Transfer Protocol)
37	Time (Time Server)
42	Host name server (names server)
43	Whois (nickname)
49	Login Host Protocol (login)
53	Domain Name Server (domain)
79	Finger protocol (finger)
80	World Wide Web (HTTP)
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol
213	IPX
160 to 223	Reserved for future use

UDP Socket	Application Service
0	Reserved
2	Management Utility
7	Echo
9	Discard
11	Active Users (sysstat)
13	Daytime
35	Any private printer server
39	Resource Location Protocol
42	Host name server (names server)
43	Whois (nickname)
49	Login Host Protocol (login)
53	Domain Name Server (domain)
69	Trivial Transfer Protocol (TFTP)
70	Gopher Protocol
79	Finger Protocol
80	World Wide Web (HTTP)
107	Remote Telnet Service
111	Sun Remote Procedure Call (Sunrpc)
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol (NTP)
161	SNMP (Simple Network Mail Protocol)
162	SNMP Traps
213	IPX (used for IP Tunneling)