

OnCell G3150A-LTE User's Manual

Edition 1.3, January 2019

www.moxa.com/product



© 2019 Moxa Inc. All rights reserved.

OnCell G3150A-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	1-3
LED Indicators	1-4
Beeper	1-5
Reset Button	1-5
2. Getting Started	2-1
First-time Installation and Configuration	2-2
Step 1: Install a SIM Card	2-2
Step 2: Turn On the OnCell G3150A-LTE	2-2
Step 3: Connect the OnCell G3150A-LTE to a Computer	2-2
Step 4: Configure an IP Address for the Computer	2-2
Step 5: Access the Web Console	2-3
Step 6: Establish a Cellular Connection	2-4
Step 7: Verify the Cellular Connection	2-4
3. Web Console Configuration	3-1
Accessing the Web Console	3-2
Configuration Menu Overview	3-4
Overview	3-6
General Setup	3-7
System Information Settings	3-7
Interface On/Off	3-8
Network Settings	3-8
System Time	3-9
Device Operation Mode	3-10
Cellular Settings	3-11
Cellular WAN Settings	3-11
GuaranLink	3-13
Auto IP Report Settings	3-16
GPS Settings	3-17
OnCell Central Manager Setting	3-18
Advanced Settings	3-18
DHCP Server	3-19
DDNS	3-20
Packet Filters	3-20
Port Forwarding Function	3-22
SNMP Agent	3-23
VPN	3-25
IPSec	3-25
OpenVPN	3-34
Serial Port Settings	3-42
Operation Mode	3-43
Logs and Notification	3-69
System Log	3-69
Syslog	3-70
E-Mail Notifications	3-71
Relay	3-73
Trap	3-73
SMS	3-74
Status	3-75
Serial	3-75
VPN	3-77
DNS Status	3-79
SIM Status	3-79
GPS Status	3-80
DHCP Client List (For AP Mode Only)	3-80
System Log	3-81
Relay Status	3-81
DI, Power, and System Status	3-81
Maintenance	3-84
Console Settings	3-84
Ping Command	3-85
Firmware Upgrade	3-85
Configuration Import & Export	3-86
Load Factory Default	3-87

Account Settings	3-87
Change Password	3-88
Miscellaneous Settings	3-89
Manual SMS.....	3-89
Remote SMS Control.....	3-90
Saving Configuration.....	3-91
Restart.....	3-92
Logout.....	3-92
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 G3150A-LTE industrial cellular gateway is an ideal wireless solution for remote monitoring applications. The wide-temperature support and power and antenna isolation design makes the OnCell G3150A-LTE 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 G3150A-LTE is a reliable, secure, LTE gateway with state-of-the-art global LTE coverage. This 4G cellular gateway provides a reliable connection to your Ethernet network for cellular applications.

To enhance industrial reliability, the OnCell G3150A-LTE features isolated power inputs, which together with high-level EMS and wide-temperature support give the OnCell G3150A-LTE the highest level of device stability for any rugged environment. In addition to dual-SIM GuaranLink support and dual power inputs, the OnCell G3150A-LTE supports network redundancy to ensure uninterrupted connectivity.

The OnCell G3150A-LTE also comes with a 3-in-1 serial port for serial communication over LTE cellular networks to enable data exchange with serial/Ethernet devices.

Package Checklist

Moxa's OnCell G3150A-LTE is shipped with the following items:

- OnCell G3150A-LTE
- 2 2G/3G/4G antennas, 2 dBi omni-directional with SMA male connectors
- DIN-rail kit
- Quick installation guide (printed)
- Warranty card

If any of these items is missing or damaged, please contact your customer service representative for assistance.

NOTE The above items come with the standard OnCell G3150A-LTE model, but the package contents may vary for customized versions.

Product Features

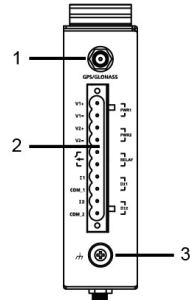
- Multiple LTE band support:
 - EU Model: B1/B3/B7/B8/B20
 - US Model: B2/B4/B5/B13/B17/B25
- Universal cellular bands support for GSM/GPRS/HSPA
- Dual cellular operator backup with dual-SIM GuaranLink for reliable cellular connectivity
- VPN secure connection capability with IPsec, GRE, and OpenVPN protocols
- Industrial-grade design:
 - Dual power input for power redundancy
 - Power isolation for 500-V power source insulation protection
 - -30 to 70°C wide operating temperature (wide temperature support only applies to certain SKUs)
 - Rugged hardware design well-suited for hazardous locations (ATEX Zone 2/IECEX)

Product Specifications

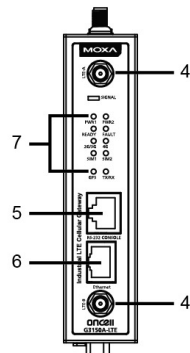
NOTE The latest specifications for Moxa's products can be found at <https://www.moxa.com>.

Functional Design

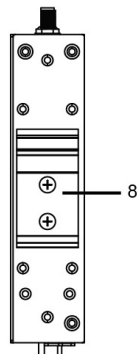
Top Panel View



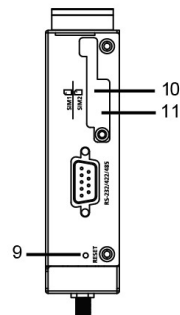
Front Panel View



Rear Panel View



Bottom Panel View



1. GPS antenna connector (female SMA)
2. Terminal block (top-down → PWR1 and PWR2, 1 digital relay and 2 digital inputs)
3. Grounding screw (M5)
4. 2x2 MIMO antenna ports for LTE (female SMA)
5. RS-232 serial console (RJ45)
6. 10/100 Base T(X) Ethernet port (RJ45)
7. LED display
8. DIN-rail mounting kit
9. Reset button
10. Dual SIM—SIM1
11. Dual SIM—SIM2

LED Indicators

The LEDs on the front panel of the OnCell G3150A-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. Additional information is available at *Chapter 3, Basic Settings* section.

Type	Color	State	Meaning																
Signal (1 LED)	Green	Blinking	The number of times this LED blinks indicates the cellular signal level when the OnCell G3150A-LTE is connected to a cellular network with an IP address. Blink interval: 200 ms Silent interval: 2 seconds																
			<table border="1"> <thead> <tr> <th>Number of Blinks</th> <th>Cellular RSSI</th> <th>RSSI Range (dBm)</th> <th></th> </tr> </thead> <tbody> <tr> <td>1</td> <td>$0 < \text{SNR} \leq 12$</td> <td>$113 < \text{RSSI} \leq -89$</td> <td>Marginal-Ok</td> </tr> <tr> <td>2</td> <td>$12 < \text{SNR} \leq 21$</td> <td>$-89 < \text{RSSI} \leq -73$</td> <td>Ok - Good</td> </tr> <tr> <td>3</td> <td>$22 < \text{SNR} \leq 31$</td> <td>$-73 < \text{RSSI} \leq -51$</td> <td>Excellent</td> </tr> </tbody> </table>	Number of Blinks	Cellular RSSI	RSSI Range (dBm)		1	$0 < \text{SNR} \leq 12$	$113 < \text{RSSI} \leq -89$	Marginal-Ok	2	$12 < \text{SNR} \leq 21$	$-89 < \text{RSSI} \leq -73$	Ok - Good	3	$22 < \text{SNR} \leq 31$	$-73 < \text{RSSI} \leq -51$	Excellent
			Number of Blinks	Cellular RSSI	RSSI Range (dBm)														
			1	$0 < \text{SNR} \leq 12$	$113 < \text{RSSI} \leq -89$	Marginal-Ok													
			2	$12 < \text{SNR} \leq 21$	$-89 < \text{RSSI} \leq -73$	Ok - Good													
3	$22 < \text{SNR} \leq 31$	$-73 < \text{RSSI} \leq -51$	Excellent																
NOTE: The Cellular RSSI value is based on the OnCell device signal strength returned by the AT+ CSQ AT command . You can also refer to the equivalent signal RSSI Range in dBm.																			
PWR1/ PWR2	Green	On	DC power source active																
		Off	Power is off																
Ready	Green	On	Steady on: System startup is complete and the system is in operation.																
		Blinking	Blinking slowly at 1-second intervals: The OnCell device has been located by the Wireless Search Utility.																
		Off	Power is off, or device is booting up.																
Fault	Red	On	Steady on: Device is booting up, or IP address conflict. Blinking slowly at 1-second intervals: Cannot get an IP address from the DHCP server																
		Off	Power is off, or no error condition exists.																
2G/3G	Amber	Blinking	GSM/GPRS/EDGE is connected. Blink interval: 500 ms																
		On	UMTS/HSPA is connected.																
		Off	GSM/GPRS/EDGE/UMTS/HSPA is disconnected.																
4G	Amber	On	LTE is connected																
		Off	LTE is disconnected.																
SIM1	Amber	On/Off	SIM 1 is active or inactive																
		Blinking	SIM 1 is not inserted or PIN code is incorrect																
SIM2	Amber	On/Off	SIM 2 is active or inactive																
		Blinking	SIM 2 is not inserted or PIN code is incorrect																
GPS	Green	On	GPS signal has been located																
		Blinking	Locating a GPS signal or less than four satellites located.																
		Off	No GPS signal has been located																
TX Rx	Amber	On	The serial port is transmitting data																
		Off	No data is being transmitted or received through the serial port																

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 G3150A-LTE. You can reboot the OnCell G3150A-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 **READY** LED starts blinking green. Release the button to reset the OnCell G3150A-LTE.



ATTENTION

- The OnCell G3150A-LTE is NOT a portable mobile device and should be located at least 20 cm away from the human body.
- The OnCell G3150A-LTE is NOT designed for the general public. A well-trained technician should be enlisted to ensure safe deployment of OnCell G3150A-LTE units, and to establish a wireless network.

Getting Started

This chapter explains how to install Moxa's OnCell G3150A-LTE for the first time, and quickly set up your wireless network and test whether the connection is running well. The *Configuration Menu Overview* in Chapter 3 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: Install a SIM Card
- Step 2: Turn On the OnCell G3150A-LTE
- Step 3: Connect the OnCell G3150A-LTE to a Computer
- Step 4: Configure an IP Address for the Computer
- Step 5: Access the Web Console
- Step 6: Establish a Cellular Connection
- Step 7: Verify the Cellular Connection

First—time Installation and Configuration

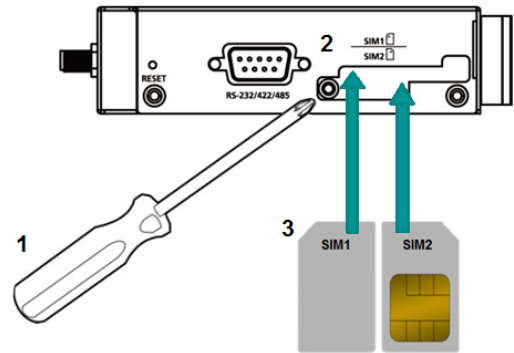
Before installing the OnCell G3150A-LTE, make sure that all items in the package checklist are in the box. In addition, you will need access to a notebook computer or PC equipped with an Ethernet port. The OnCell G3150A-LTE has a default IP address that you must use when connecting to the device for the first time.

Step 1: Install a SIM Card

Insert one or two 2G/3G/4G SIM cards into the SIM slots located on the bottom of the OnCell G3150A-LTE.

The SIM card slots are inside the OnCell G3150A-LTE's housing. To install a SIM card in one of the slots, do the following:

1. Turn off the OnCell G3150A-LTE.
2. Remove the screw on the SIM card slot cover.
3. Install a SIM card into the SIM card slot.
 - a. For SIM 1, orient the card such that the gold contacts are facing down and the cut-off edge is to the left.
 - b. For SIM 2, orient the card such that the gold contacts are facing up and the cut-off edge is to the right.
4. Put back the screw on the SIM card slot cover and secure the cover by tightening the screw.



Step 2: Turn On the OnCell G3150A-LTE

Turn on the OnCell G3150A-LTE by connecting the power terminal block to a DC power source.

Step 3: Connect the OnCell G3150A-LTE to a Computer

Since the OnCell G3150A-LTE supports MDI/MDI-X autosensing, you can use either a straight-through cable or crossover cable to connect the OnCell G3150A-LTE to a computer. When a connection is established, the LED indicator on the OnCell G3150A-LTE's LAN port lights up.

Step 4: Configure an IP Address for the Computer

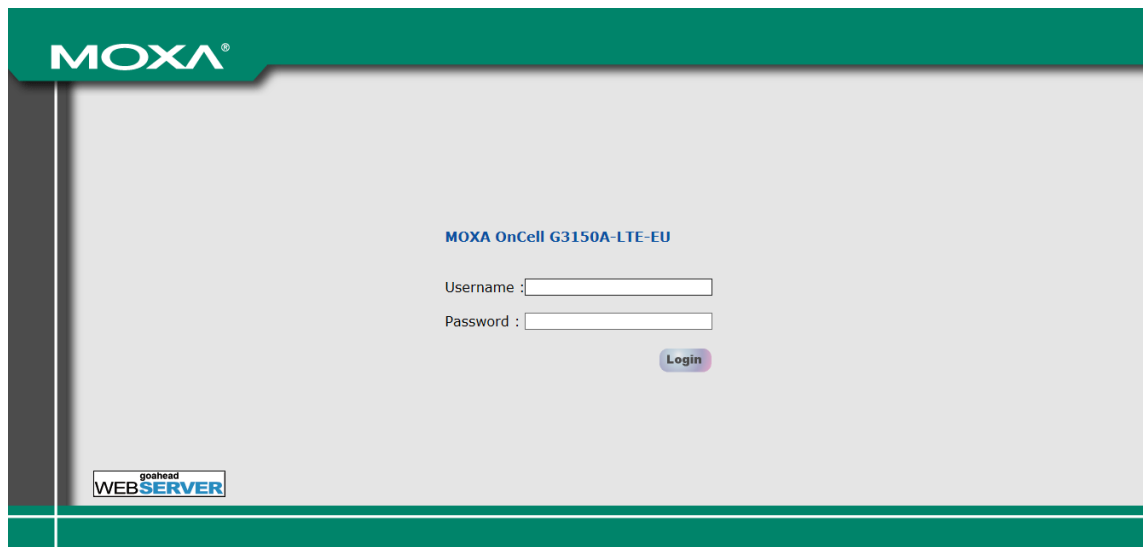
You must set an IP address for the computer so that it is on the same subnet as the OnCell G3150A-LTE. Since the OnCell G3150A-LTE's default IP address is **192.168.127.254** and the subnet mask is **255.255.255.0**, you should set the IP address of the computer to **192.168.127.xxx**.

NOTE In the OnCell G3150A-LTE, you can select **Maintenance > Load Factory Default** and click **Submit** to reset the OnCell G3150A-LTE to the factory default settings, which will reset the IP address to **192.168.127.254**.

Step 5: Access the Web Console

To access the OnCell G3150A-LTE web console:

1. Open a web browser and enter `http://192.168.127.254` in the address field.



NOTE Default user name and password:

User Name: **admin**

Password: **moxa**

Overview (Warn: Change the default password to ensure a higher level of security)

This screen displays current active settings

System Information

Model name	OnCell G3150A-LTE-EU
Device name	OnCell G3150A-LTE_0000

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

NOTE After you click **Apply** to apply the password change, the new password will be effective immediately and the web page will be refreshed. This is indicated by the text, **(Updated)** that appears next to the page header:

Change Password (Updated)

Step 6: Establish a Cellular Connection

After installing the 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 the cellular WAN settings and establish a cellular connection:

1. Log in to the web console.
2. Go to **Cellular Settings > Cellular WAN Settings** and enter the SIM card PIN and APN values.
3. Restart the OnCell G3150A-LTE.

The OnCell G3150A-LTE automatically establishes a cellular connection to the service provider after it restarts.

Step 7: Verify 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 an LED on the SIM card slot is blinking, it could mean that no SIM card is installed in the SIM slot or the SIM card PIN 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 G3150A-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** page in the web console.

Log in to the web console to display the **Overview** page. Check the Cellular RSSI, Cellular WAN IP address, and Cellular Mode fields to identify any connection problems.

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

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

3. Test the cellular network access on your computer.

Users with public SIM cards (instead of SIM cards with MDVPN service enabled) can test the connection to the Internet on your computer (assuming that your computer is connected to an Ethernet port on the OnCell G3150A-LTE).

An example of the configuration settings on the computer is given below:

- 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: 192.168.127.254 (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 process 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, *Advanced Settings, DHCP Server*.

Web Console Configuration

This chapter describes the web console that you can use to configure your OnCell G3150A-LTE and set up a wireless network. The following topics are covered in this chapter:

- ❑ **Accessing the Web Console**
 - Configuration Menu Overview
- ❑ **Overview**
- ❑ **General Setup**
 - System Information Settings
 - Interface On/Off
 - Network Settings
 - System Time
 - Device Operation Mode
- ❑ **Cellular Settings**
 - Cellular WAN Settings
 - GuaranLink
 - Auto IP Report Settings
 - GPS Settings
 - OnCell Central Manager Setting
- ❑ **Advanced Settings**
 - DHCP Server
 - DDNS
 - Packet Filters
 - Port Forwarding Function
 - SNMP Agent
- ❑ **VPN**
 - IPSec
 - OpenVPN
- ❑ **Serial Port Settings**
 - Operation Mode
- ❑ **Logs and Notification**
 - System Log
 - Syslog
 - E-Mail Notifications
 - Relay
 - Trap
 - SMS
- ❑ **Status**
 - Serial
 - VPN
 - DNS Status
 - SIM Status
 - GPS Status
 - DHCP Client List (For AP Mode Only)
 - System Log
 - Relay Status
 - DI, Power, and System Status
- ❑ **Maintenance**
 - Console Settings
 - Ping Command
 - Firmware Upgrade
 - Configuration Import & Export
 - Load Factory Default
 - Account Settings
 - Change Password
 - Miscellaneous Settings
 - Manual SMS
 - Remote SMS Control
- ❑ **Saving Configuration**
- ❑ **Restart**
- ❑ **Logout**

Accessing the Web Console

Moxa OnCell G3150A-LTE's web interface provides a convenient way to modify the configuration settings and access the built-in monitoring and network administration functions. The recommended web browser is Microsoft® Internet Explorer 7.0 and above with JVM (Java Virtual Machine) installed.

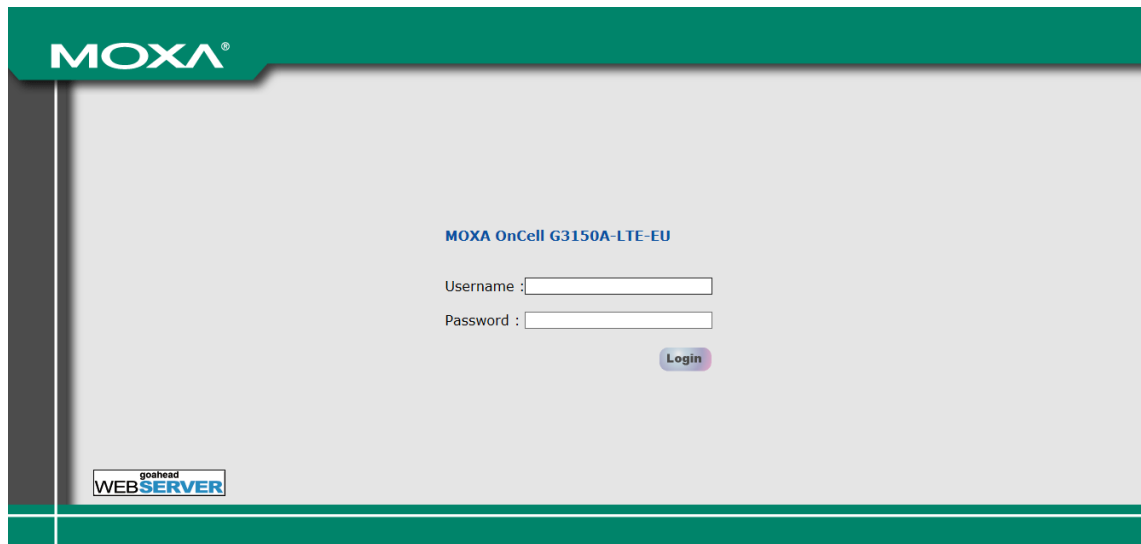
NOTE To use the OnCell G3150A-LTE's management and monitoring functions from a PC host connected to the same LAN as the OnCell G3150A-LTE, you must make sure that the PC host and the OnCell G3150A-LTE are on the same logical subnet.

The default IP address of an OnCell G3150A-LTE is **192.168.127.254**.

To access the OnCell G3150A-LTE's web-based console management interface, do the following

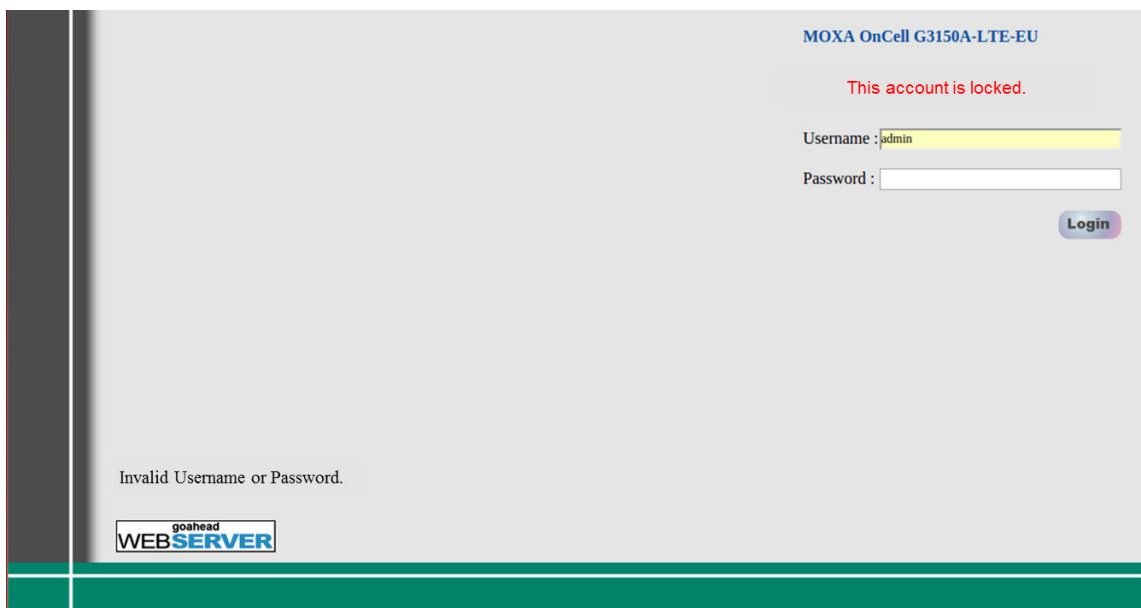
1. Open your web browser and type the OnCell G3150A-LTE's IP address in the address field; then, press **Enter**.
2. In the login page, enter the **Username** and **Password** (the default username is "admin" and password is "moxa") and click **Login**.

It may take a few seconds for the web page to load on your computer.



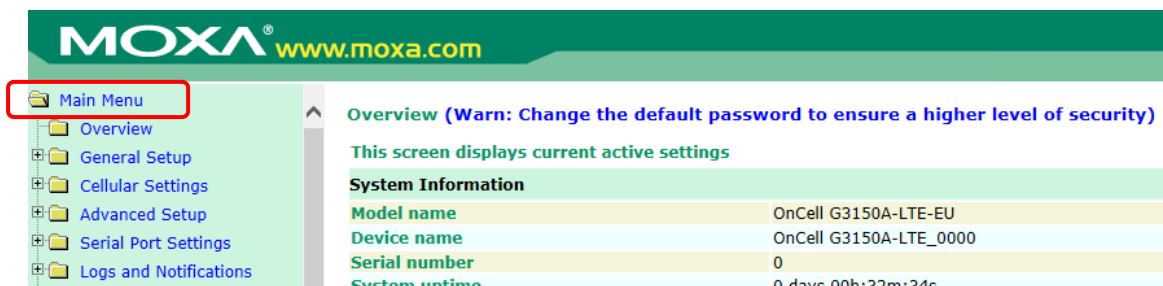
NOTE The model name of your OnCell G3150A-LTE is shown on the title bar of the web page. You can use this information to identify multiple OnCell G3150A-LTE units. The model name is shown as OnCell G3150A-LTE-XX, where XX is the country code. The country code indicates the OnCell G3150A-LTE version and the bandwidth that it uses. The figures shown in this document use an OnCell G3150A-LTE-US. The model name that is displayed for your OnCell G3150A-LTE may be different from the one shown in this manual.

If an incorrect username or password is entered, a warning message is displayed. The system will lock the user account based on the settings configured in **Maintenance->Account Settings**. The default retry count is 5 times and the default lockout time is 600 seconds. Once an account is locked, the user will have to wait out the duration of the lockout period before retrying.



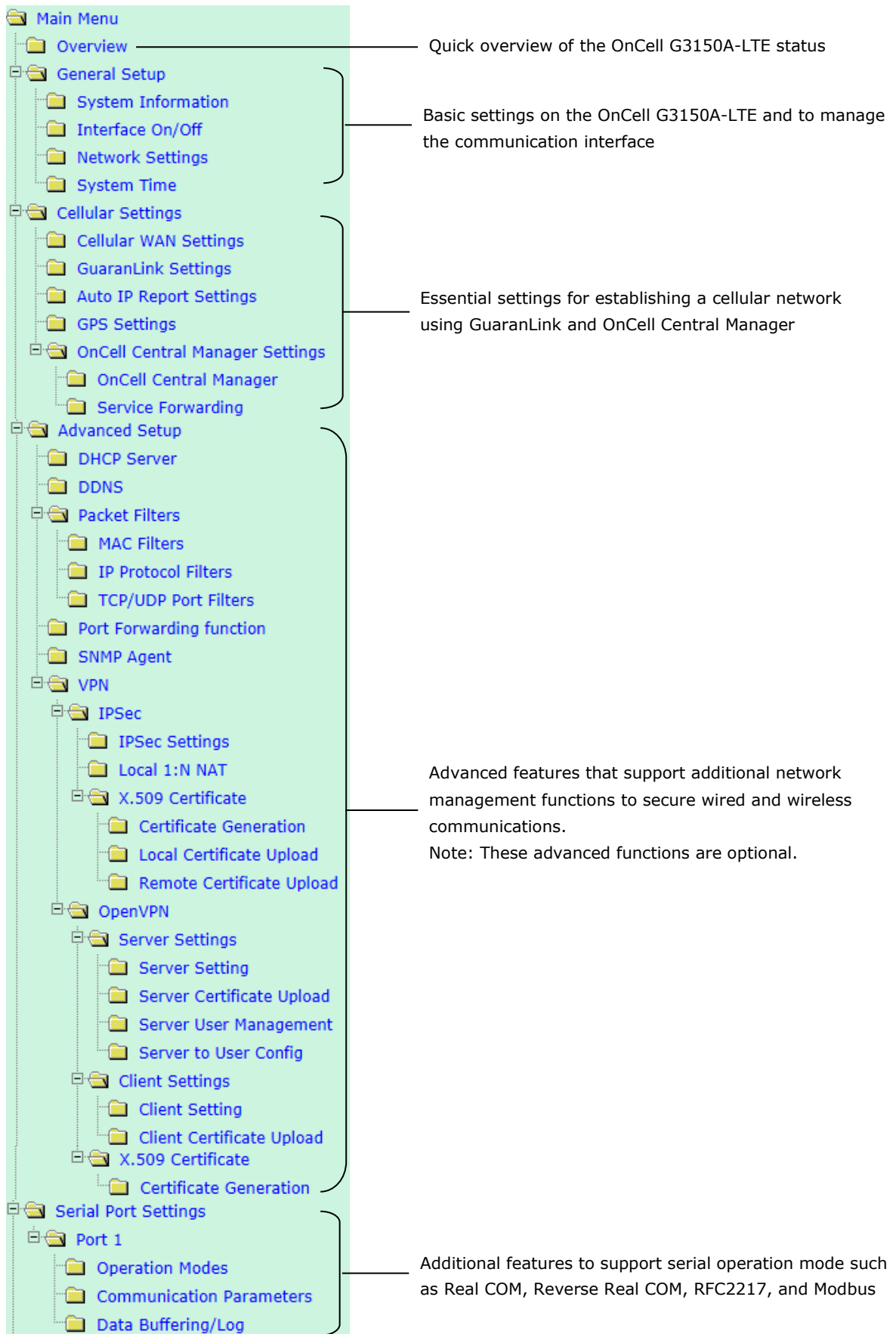
For additional details, see *Account Settings* under *Maintenance*.

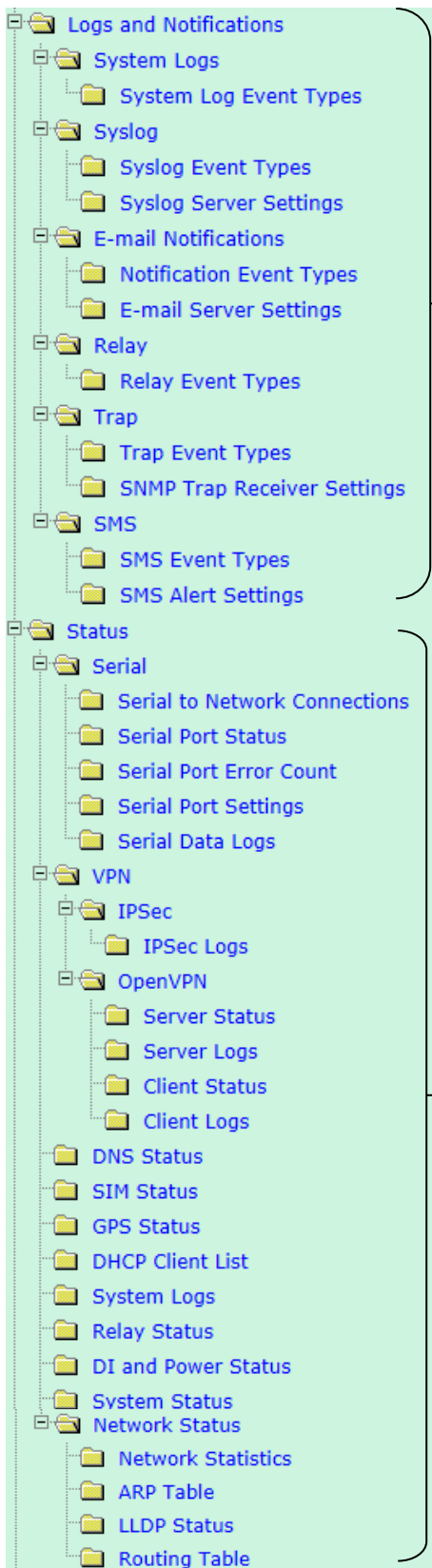
- Use the navigation panel on the left to access the configuration pages.



In the following sections we will describe each OnCell G3150A-LTE management function in detail, starting with an overview of the links in the navigation panel.

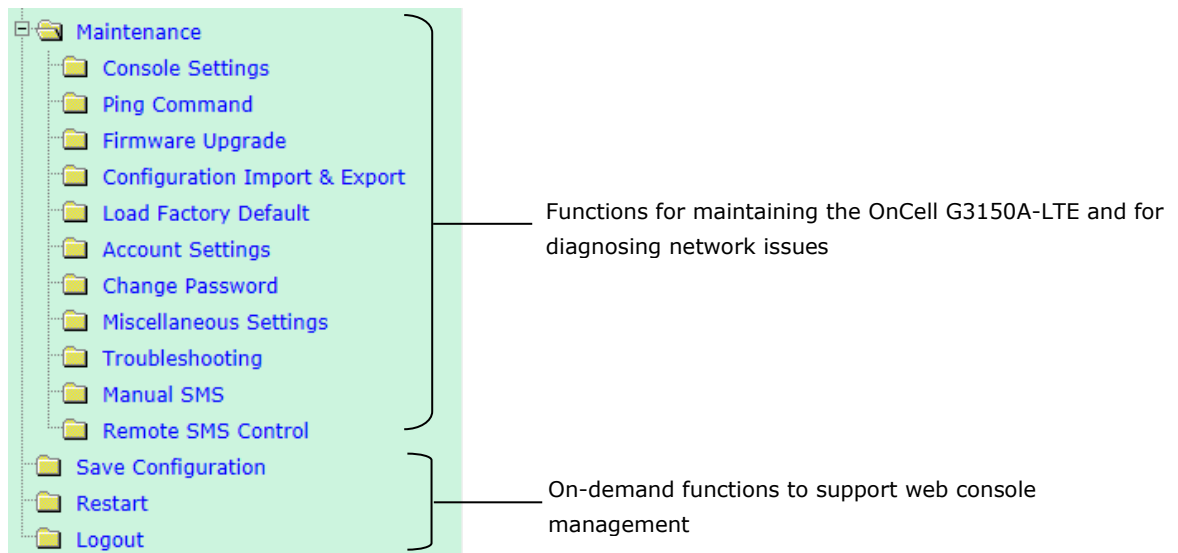
Configuration Menu Overview





Application-oriented device management functions to set up events, traps, and responses via relay warning, email, and SNMP notification.
Note: These functions are all optional.

Current status information for monitoring wired/wireless network performance, advanced services, and device management functions



Overview

The **Overview** page provides a summary of the OnCell G3150A-LTE’s current status. The information is categorized into **System Information**, **Device Information**, and **Cellular Information**.

Overview (Warn: Change the default password to ensure a higher level of security)

This screen displays current active settings

System Information	
Model name	OnCell G3150A-LTE-EU
Device name	OnCell G3150A-LTE_0000
Serial number	0
System uptime	0 days 01h:06m:09s
Firmware version	1.0 Build 16101119
Device Information	
Device MAC address	00:90:E8:00:00:00
IP address	192.168.127.254
Subnet mask	255.255.255.0
Cellular Information	
Cellular mode	No service
Cellular band	No service
Cellular channel	0
Cellular data bearer	No service
Cellular RSSI	0
Cellular WAN IP address	0.0.0.0
IMEI	356853050512823
IMSI	N/A

General Setup

The General Setup group includes the most commonly used settings required by administrators to maintain and control the OnCell G3150A-LTE.

System Information 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 G3150A-LTE units connected to your network.

System Information

Device name	<input type="text" value="OnCell G3150A-LTE_0000"/>
Device location	<input type="text"/>
Device description	<input type="text"/>
Device contact information	<input type="text"/>
Login Message	<input type="text"/>
Login authentication failure message	<input type="text" value="Invalid username or password"/>

Field	Description	Default setting
Device name	Enter a descriptive name (up to 31 characters). You can also include information that specifies the role or application of the OnCell G3150A-LTE unit.	OnCell G3150A-LTE_ <i>serial no</i>]
Device location	Specify the location (up to 31 characters) of the OnCell G3150A-LTE	N/A (Not applicable)
Device description	Enter a description (up to 31 characters) for the OnCell G3150A-LTE	N/A
Device contact information	Enter the contact information (up to 31 characters) of the person responsible for maintaining this OnCell G3150A-LTE	N/A
Login Message	Enter the message (up to 31 characters) to display to the user who logs in into this OnCell G3150A-LTE.	Blank
Login authentication failure message	Enter the message (up to 31 characters) that is displayed to the user when the login authentication fails.	Invalid username or password

Interface On/Off

Interface On/Off

LAN

Enable Disable

Cellular WAN

Enable Disable

Submit

Field	Description	Default setting
LAN	Provides the capability to enable/disable the LAN interface	Enable
Cellular WAN	Provides the capability to enable/disable the cellular WAN interface.	Enable



ATTENTION

Disabling the cellular WAN interface will disconnect access to remote cellular devices connected through the cellular WAN.

Network Settings

You can use the **Network Settings** page to configure TCP/IP settings for the OnCell G3150A-LTE.

Network Settings

IP address

192.168.127.254

Subnet mask

255.255.255.0

Primary DNS server

Secondary DNS server

Field	Description	Default setting
IP address	Enter the unique IP address of the OnCell G3150A-LTE	192.168.127.254
Subnet mask	Enter the subnet mask to specify the type of network to which the OnCell G3150A-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 for a website, you can access the website by entering its URL instead of the IP address.	N/A

System Time

You can synchronize the system time on the OnCell G3150A-LTE based on an NTP (Network Time Protocol) server or user-specified date and time information. The OnCell G3150A-LTE includes the system time in system logs.

NOTE The OnCell G3150A-LTE includes a built-in real time clock (RTC). We strongly recommend that you update the **Current local time** for the OnCell G3150A-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.

System Time

	<div style="display: flex; justify-content: space-around; border-bottom: 1px solid #ccc;"> Date (YYYY/MM/DD) Time (HH:MM:SS) </div>
Current local time	<div style="display: flex; justify-content: space-around; border-bottom: 1px solid #ccc;"> 1999 / 11 / 30 23 : 54 : 17 </div> <div style="text-align: center; margin-top: 5px;"> <input type="button" value="Set Time"/> </div>
Time protocol	SNTP
Time zone	<input type="text" value="(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London"/>
Daylight saving time	<input type="checkbox"/> Enable
Time server 1	<input type="text" value="time.nist.gov"/>
Time server 2	<input type="text"/>
Time sync interval	<input style="width: 50px;" type="text" value="600"/> (600~9999 seconds)
<input type="button" value="Submit"/>	

Field	Description	Default setting
Current local time	The fields indicate the current system time on the OnCell G3150A-LTE. Enter the date and time in the format <i>yyyy/mm/dd hh:mm:ss</i> 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.	N/A
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 .	N/A
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. 	N/A
Time server 1/2	Enter the IP address or the domain name of the primary or secondary NTP server.	time.nist.gov
Time sync interval	Specify how many seconds (600 to 9999) the OnCell G3150A-LTE must wait before requesting updates from the NTP server.	600

Device Operation Mode

The OnCell G3150A-LTE can be configured as an IP gateway for IP data communication (LAN or serial data). It can also be configured to send and receive SMS via AT commands using the serial modem mode.

Device Operation Mode

Device Operation Mode

Operation mode

IP gateway mode ▼

Submit

Field	Description	Default
Operation mode	<p>Set the OnCell device to one of the following operation modes</p> <p><i>IP gateway mode:</i> The OnCell is configured as an IP gateway capable of IP data communication.</p> <p><i>Serial modem mode:</i> The OnCell is configured as a pure serial modem capable of SMS-via-AT-commands communication.</p> <p>The AT commands supported in the serial modem mode are:</p> <ul style="list-style-type: none"> ATE (Local echo) <ul style="list-style-type: none"> • ATE0: No echo • ATE1: Echo AT+CSQ (Request signal) ATI (Query modem identification) <ul style="list-style-type: none"> • Manufacturer • Model Name • Revision • IMEI AT+CREG (Network registration) AT+COPS (PLMN selection) AT &F (Set current parameters to manufacturer's defaults) AT+CMGD (Delete message) AT+CMGF (Message format) <ul style="list-style-type: none"> • AT+CMGF=0 (PDU Mode) • AT+CMGF=1 (Text Mode) AT+CMGL (List Message) AT+CMGR (Read Message) AT+CMGS (Send Message) AT+CSMP (Set text mode parameters) AT+CSCS (Select message service) 	IP gateway mode

Cellular Settings

This section describes the pages that you can use to configure cellular connection settings on the OnCell G3150A-LTE:

- **Cellular WAN Settings**—Configure these settings to establish a cellular connection.
- **GuaranLink Settings**—Use this page to configure Moxa’s proprietary 4-tier link protection that ensures 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 G3150A-LTE to automatically send its WAN IP address to a specified host.
- **GPS Settings**—Configure these settings to enable the built-in GPS sensor to locate your OnCell G3150A-LTE.
- **OnCell Central Manager Settings**—For details on OnCell Central Manager settings, refer to the *OnCell Central Manager User’s Manual* available at www.moxa.com.

Cellular WAN Settings

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

The OnCell G3150A-LTE provides you with a scheduling function for managing your cellular connection. Depending on your application, you can use the scheduling function to specify when the radio should be turned on/off, when to disconnect the data transmission, or go into SMS-only mode and enable data transmission only during emergencies.

If you install two SIM cards in the OnCell G3150A-LTE, you can select the Dual SIM mode and enable the GuaranLink feature to enable the OnCell G3150A-LTE to regularly check the connection quality and perform an automatic switchover in case the cellular connection is down. This setting ensures operation redundancy.

Cellular WAN Settings

Field	Description	Default setting
Cellular connection fully functional time interval(s)	Always on —The radio is always on Scheduled —The OnCell G3150A-LTE is fully functional during the scheduled periods. At all other times, it will function based on the following configuration parameters.	Always on
Radio Power Off	If this option is selected, the radio power is turned off at all the other times except the time periods specified in the scheduling table above.	

Field	Description	Default setting
SIM 1 authentication type/	Select Auto if you want the OnCell device to automatically select either PAP or CHAP authentication method when setting up a data session.	Auto
SIM 2 authentication type	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. 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.	

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 G3150A-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: GuaranLink resets the cellular module without rebooting the device to force negotiation between the OnCell G3150A-LTE and the base station.
- Dual SIM cards: When the preferred SIM card fails to establish a connection, GuaranLink resets the cellular module without rebooting the device and establishes a cellular connection using the second SIM card account.
- If SIM 1 is chosen but SIM card is installed only in SIM 2 slot, no action will be performed. Please ensure that a SIM card is installed in the SIM card slot that you have selected for operation.
- If one of the SIM cards is absent or not readable, GuaranLink will automatically force a cellular connection using the other SIM card account. The system log will record this event. If the second SIM card is also absent or cannot be read, GuaranLink will not try again.
- If the cellular connection cannot be recovered by resetting the cellular module up to 30 times, the OnCell device will automatically reboot.

GuaranLink Settings

In the navigation panel, click **Cellular 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)

DNS/Ping remote host 1

DNS/Ping remote host 2

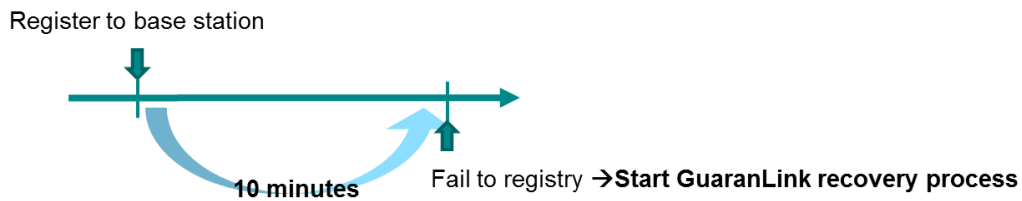
Warning: "DNS/Ping remote host" are only for "Cellular connection alive check"/"Packet-level connection check".

GuaranLink Check Settings

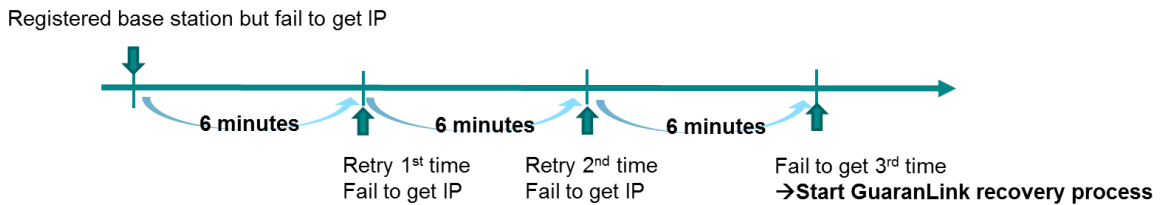
ISP initial connection check

Enable Disable

ISP Initial Connection Check (Default)



Data Session Retry (Default)



The following table describes the fields:

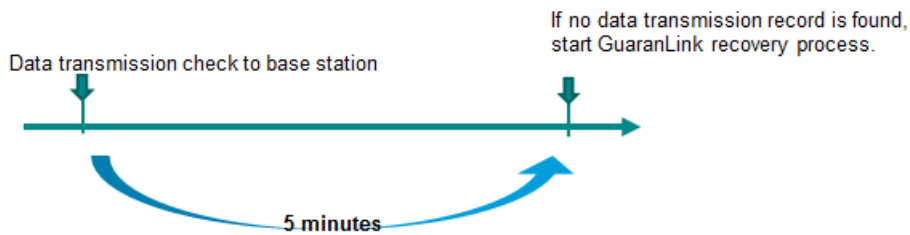
Field	Description	Default setting
GuaranLink	Select Enable to activate the GuaranLink feature. For operation redundancy, enable GuaranLink with Dual SIM mode so that the OnCell G3150A-LTE regularly checks the connection quality and performs an automatic switchover in case a cellular connection is down. Select Disable to deactivate the GuaranLink feature.	Disable
Register to network timeout	This field is used by the ISP initial connection check. Enter the time period (10–600 minutes) that the OnCell G3150A-LTE must wait before terminating the connection to an ISP and starting the GuaranLink recovery process.	10
Data session retry count	Enter the number of times (1 to 5; default is 3) the OnCell G3150A-LTE is to request an IP address from the ISP. If the OnCell G3150A-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 a DNS lookup test. To ensure accurate checks, we suggest entering the host domain name here.	N/A
ISP initial connection check	Select Enable to set the OnCell G3150A-LTE to complete the registration process to a base station before the timeout specified in the Register to network timeout field. If the OnCell G3150A-LTE fails to register to the base station within the timeout period, it starts the GuaranLink recovery process. Select Disable to allow the OnCell G3150A-LTE to wait until base station registration is successful.	Disable

Enable Disable
Cellular connection alive check interval (1 - 600 mins)
Cellular connection alive check retry count (1 - 5)

Enable Disable
Packet-level connection check action
Packet-level connection check interval (1 - 600 mins)
Packet-level connection check retry count (1 - 5)

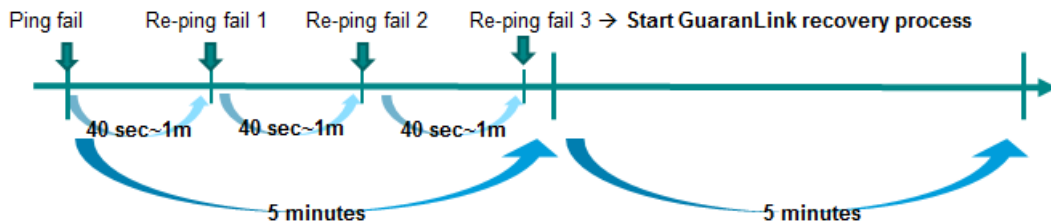
Enable Disable
Transmission connection check alive check interval (1 - 600 mins)

Transmission Connection Check (Default)



Cellular Connection Alive Check (Default)

Packet-Level Connection Check (Default)



Field	Description	Default setting
Cellular connection alive check	Depending on your ISP, cellular connection is terminated if there is no active data transmission for a certain period of time. Select Enable to set the OnCell G3150A-LTE to keep the cellular connection alive by performing a DNS lookup or remote host Ping <i>if no data is transmitted</i> 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 G3150A-LTE starts the GuaranLink recovery process.	Disable
Cellular connection alive check interval	Enter the time (between 1 to 600 minutes) the OnCell G3150A-LTE is to wait before performing a connection check.	5
Cellular connection alive check retry count	Enter the number of times the OnCell G3150A-LTE is to try the connection check in a 15-second time interval. If the connection check fails, the OnCell G3150A-LTE starts the GuaranLink recovery process.	3

Field	Description	Default setting
Packet-level connection check	Select Enable to check whether the cellular network is accessible using DNS lookup and remote host ping, <i>regardless of any existing data transmission</i> . If the connection check fails after the number of retries specified in the Packet-level connection check retry count field, the OnCell G3150A-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 G3150A-LTE is to wait before performing a connection check.	5
Packet-level connection check retry count	Enter the number the OnCell G3150A-LTE is to try the connection check before re-establishing the connection.	3
Transmission connection check	If a remote system regularly monitors connection to the OnCell G3150A-LTE, select Enable to set the OnCell G3150A-LTE to receive polling information from the remote system at regular intervals. If no polling information is received within the timeout period, the OnCell G3150A-LTE starts the GuaranLink recovery process.	Disable
Transmission connection alive check interval	Enter the time (between 1 to 600 minutes) the OnCell G3150A-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 G3150A-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 G3150A-LTE is to send the WAN IP address information.	N/A
Report to UDP port	Enter the listing port number on the remote host.	63100
Report period	Enter the number of minutes the OnCell G3150A-LTE is to wait before sending WAN IP address information.	99

Auto IP Report Format

The OnCell packet follows the "Type Length Value" format.

Type	Length	Value
1 byte	1 byte	Length bytes

The following table shows the 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

Example:

ID Value	Length	Note
05	04	C0,a8,81,71
09	04	30,12,19,89
0a	04	C0,a8,81,71
----	----	----

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 Client

Enable Enable ▾

Configuration

Report Protocol TCP ▾

Report to host

Report to port (1 - 65535)

Report period 30 (1 - 65535 secs)

Report Format

Report Format Nmea ▾

Report ID

Setting	Description	Factory Default
GPS	Enable or disable the GPS function.	Disable
GPS Client	Enable GPS client mode as TCP or UDP client	Disable
Report Protocol	Select TCP (client only) or UDP protocol to configure the GPS data report behavior.	TCP
Report to host	Enter an IP or hostname for the GPS data report server's TCP or UDP port.	-
Report to port	Enter a port number for server's TCP or UDP port	-
Report period	Use this option to specify how often the GPS data is automatically reported.	30 sec
Report Format	Select a GPS data report format. NMEA—GPS data report is sent in the standard NEMA format. General—GPS data report is sent in the latitude and longitude format.	NMEA
Report ID	Enter the ID that is to be used in the GPS data report header. The Report ID and MAC ID will be included in the NMEA or General format reports.	-

GPS Server

Enable

Configuration

Server port

Report period (1 - 65535 secs)

Report Format

Report Format

Report ID

Setting	Description	Factory Default
GPS Server	Enables GPS server mode on the server site.	Disable
Server Port	Enter a port number that the clients can use as an access port.	8919
Report period	Use this option to specify how often the GPS data is automatically reported from the server.	30 seconds
Report Format	Select a GPS data report format: NMEA —GPS data report is sent in the standard NEMA format. General —GPS data report is sent in the latitude and longitude format.	NMEA
Report ID	Enter the ID that is to be used in the GPS data report header. NMEA or General format will add ID and MAC format.	

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 G3150A-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. And, 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 G3150A-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 G3150A-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 (1~10 days)

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"/>
6	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
7	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
8	<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 G3150A-LTE as a DHCP server. Select Disable to set the OnCell G3150A-LTE as a DHCP client.	Disable
Default gateway	Enter the IP address of the default gateway that connects to an outside network.	N/A
Subnet mask	Enter the subnet mask to specify the type of network for the DHCP clients.	N/A
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.	N/A
Start IP address	Enter the starting IP address in the IP address pool.	N/A
Maximum number of users	Enter the number (between 1 and 999) of IP address to assign to DHCP clients.	N/A
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.	10

Field	Description	Default setting
Static DHCP Mapping	Local IP address and the MAC address of the connected devices (up to 16 devices) that obtain their IP address through DHCP.	N/A

DDNS

If a DHCP server assigns an IP address to the OnCell G3150A-LTE, you can configure dynamic DNS (DDNS) setting on the OnCell G3150A-LTE to allow remote servers to access the OnCell G3150A-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

DDNS function Enable ▾
Service provider no-ip.org ▾
Host name
Username admin
Password ••••

The following table provides the field descriptions:

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

Packet Filters

The OnCell G3150A-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 G3150A-LTE’s MAC filter is a policy-based filter that can allow or filter out IP-based packets with specified MAC addresses. The OnCell G3150A-LTE provides 32 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

MAC filters function Disable ▾
Policy Drop ▾

No.	<input type="checkbox"/> Active	Name	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"/>
6	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
7	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
8	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

Field	Description	Default setting
MAC filters function	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 G3150A-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 G3150A-LTE provides 32 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 192.168.1.255. Remember to check the **Active** check box for each entity to activate the setting.

IP Protocol Filters

IP protocol filters function

Disable

Policy

Drop

No.	<input type="checkbox"/> Active	Protocol	Source IP	Source Netmask	Destination IP	Destination Netmask
1	<input type="checkbox"/>	All				
2	<input type="checkbox"/>	All				
3	<input type="checkbox"/>	All				
4	<input type="checkbox"/>	All				
5	<input type="checkbox"/>	All				
6	<input type="checkbox"/>	All				
7	<input type="checkbox"/>	All				
8	<input type="checkbox"/>	All				

Field	Description	Default setting
IP protocol filters function	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 G3150A-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 G3150A-LTE provides 32 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

TCP/UDP port filters function

Disable ▾

Policy

Drop ▾

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"/>
4	<input type="checkbox"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	TCP ▾	<input type="text"/>
5	<input type="checkbox"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	TCP ▾	<input type="text"/>
6	<input type="checkbox"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	TCP ▾	<input type="text"/>
7	<input type="checkbox"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	TCP ▾	<input type="text"/>
8	<input type="checkbox"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	TCP ▾	<input type="text"/>

Field	Description	Default setting
TCP/UDP port filters function	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**

OnCell device itself is NOT included within this policy.

For device interface access and security settings, go to **Maintenance** -> **Console settings**.

Port Forwarding Function

You can configure port forwarding settings on the OnCell G3150A-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 G3150A-LTE filters out unrecognized packets to protect your LAN network when computers connected to the OnCell G3150A-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 G3150A-LTE to redirect traffic to a specific port on a LAN computer.

To access the **Port Forwarding** settings, select **Advanced Setup > Port Forwarding function**. The OnCell G3150A-LTE supports a total of 32 port-forwarding rules.

Port Forwarding function

Port forwarding

Disable ▾

No.	<input type="checkbox"/> Active	Protocol	WAN Port	LAN IP	LAN Port
1	<input type="checkbox"/>	TCP ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="checkbox"/>	TCP ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="checkbox"/>	TCP ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="checkbox"/>	TCP ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="checkbox"/>	TCP ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="checkbox"/>	TCP ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="checkbox"/>	TCP ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="checkbox"/>	TCP ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>

The following table includes the field descriptions:

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

SNMP Agent

The OnCell G3150A-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 G3150A-LTE's MIB is available for download from Moxa's official website and supports reading the attributes via SNMP (only the SNMP GET method is supported.)

SNMP security modes and security levels supported by the OnCell G3150A-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.
	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

SNMP agent	Disable ▾
Remote management	Disable ▾
Read community	public
Write community	private
SNMP agent version	V1, V2c ▾
Admin authentication type	No Auth ▾
Authentication username	admin ▾
Admin encryption method	Disable ▾
Private key	

Private MIB information

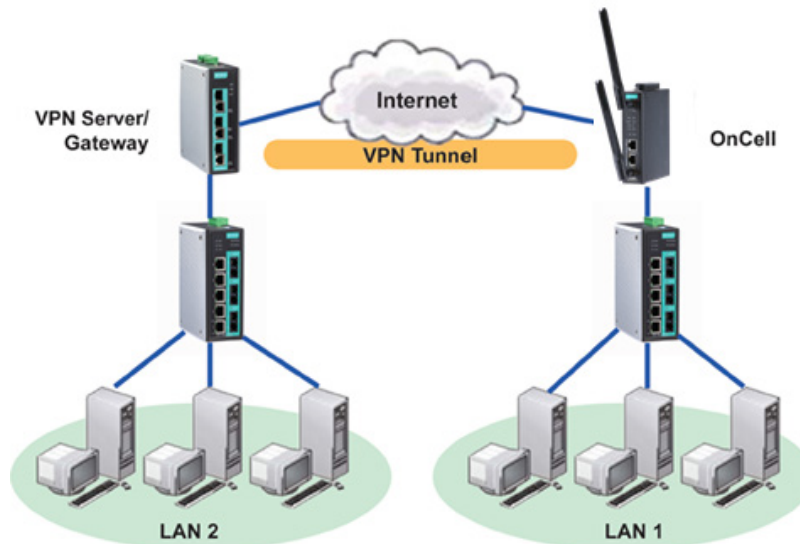
Device object ID enterprise.8691.15.32

Field	Description	Default Setting
SNMP agent	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 G3150A-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
Authentication username	The username to use for SNMP authentication	admin
Admin encryption method	Select Disable for no data encryption Select DES to use DES-based data encryption Select AES to use AES-based data encryption	Disable
Private key	Enter the key (up to 63 characters) for data encryption	N/A
Private MIB information Device object ID	The object ID (OID) is the enterprise value for the OnCell G3150A-LTE. This value is not configurable.	N/A

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. The OnCell G3150A-LTE can act as a VPN client or VPN server. Once the connection is established, cellular devices can communicate with other network devices on the same private network.

The following figure shows an example of a network topology:

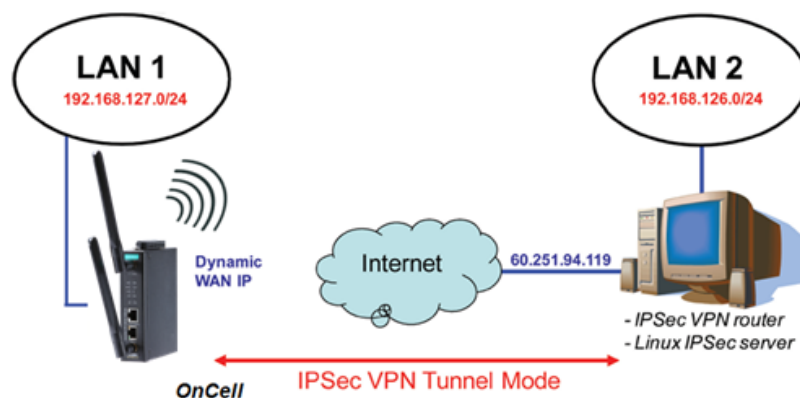


IPSec

Overview—OnCell G3150A-LTE IPSec Feature

The IPSec feature on the OnCell G3150A-LTE:

- Provides Layer-3 (IP-layer) security in a network with gateway-to-gateway topology as illustrated in the following figure
- Initiates a VPN connection from the OnCell G3150A-LTE to a VPN Server
- Operates in Tunnel mode with **IPSec VPN tunnel** with:
 - Manual Key/ESP, IKE/PSK encryption
 - DES/3DES/AES128 encryption
 - MD5/SHA1 authentication
- Provides IPSec NAT traversal and PFS (perfect forwarding secrecy)
- Provides IPSec over GRE protocol



IPSec Settings

You can enable or disable the IPSec and NAT traversal functions and configure up to five VPN tunnels by selecting **Advanced Settings > VPN > IPSec Settings**.

IPSec Settings

IPSec Disable ▾
 NAT traversal Disable ▾

Status	Name	Remote Endpoint	Local Subnet	Remote Subnet	Action
Disabled					<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Disable					<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Disable					<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Disable					<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Disable					<input type="button" value="Edit"/> <input type="button" value="Delete"/>

The following table provides the field descriptions.

Field	Description	Factory Default
IPSec	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 Settings

IPSec enable Disable ▾

Connection name (Must begin with an alphabet)

Connection type Site to Site ▾

Startup mode Start in Initial ▾

Remote VPN gateway

Local network

Local netmask

Local ID

Remote network

Remote netmask

Remote ID

NAT type None ▾

GRE enable Disable ▾

None ▾

None

Local 1:1 NAT

Local 1:N NAT

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 G3150A-LTE to initiate a connection with the remote VPN gateway. Select Wait for Connecting to set the OnCell G3150A-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.	N/A
Local network	Enter the IP of the local network.	N/A
Local netmask	Enter the netmask of the local network.	N/A
Local ID	Enter an ID (IP/FQDN/User_FQDN) to identify and authenticate the local VPN gateway.	N/A
Remote network	Enter the IP of the remote network.	N/A
Remote netmask	Enter the netmask of the remote network.	N/A
Remote ID	Enter an ID (IP/FQDN/User_FQDN) to identify and authenticate the remote VPN endpoint.	N/A
NAT type	Select this check box to activate 1:1 or 1:N network address translation (NAT) Local 1:1 NAT—Virtual IP addresses are used for communication via the VPN tunnel. These addresses are linked to the real IP addresses for the network that has been connected. The subnet mask remains unchanged. Local 1:N NAT—The device has one IP address, which can be used to access the device externally. For incoming data packets, the device can convert the specified sender WAN port to internal IP address. For example, this function can be used to enable PLCs from different sites to have the same IP address.	None
GRE enable	Enables generic routing encapsulation (GRE) in IPSec tunneling.	Disable

Key Exchange (Phase1)

Operation mode
Authentication mode
Encryption algorithm
Hash algorithm
DH group
Negotiation times (0:forever)
IKE life time min.
Rekey expire time min.
Rekey fuzz percentage %

Data Exchange (Phase2)

Perfect forward secrecy
SA life time min.
Encryption algorithm
Hash algorithm

Dead Peer Detection

DPD action
DPD delay seconds
DPD timeout seconds

Field	Description	Factory Default
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 respective sections in this guide.	Pre-shared key
Encryption algorithm	Select the DES, 3DES or AES128 algorithm for the VPN ISAKMP phase 1 encryption mode.	3DES
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 times	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

Field	Description	Factory Default
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%

Field	Description	Factory Default
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.	3DES
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 G3150A-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. • Restart by Peer: Re-establish the VPN tunnel on Wait for connecting mode. 	Disable
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.

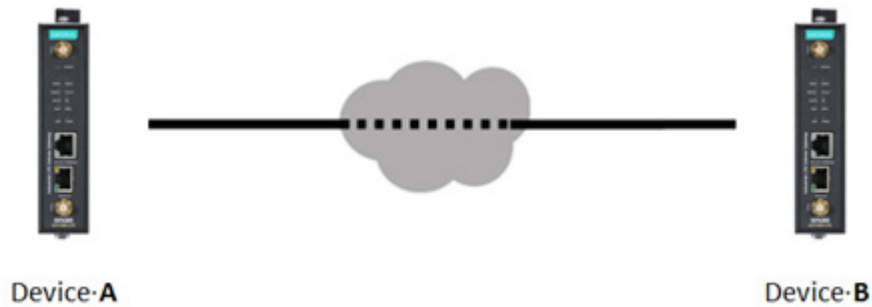
Make sure that you configure the same key on the OnCell G3150A-LTE and the remote VPN gateway.

Configuring RSA Signature Settings

To configure RSA signature settings, complete the following steps:

1. In the Tunnel Settings screen, select RSA Signature from the Authentication mode drop-down list.
2. Generate or import a local private key. Perform one of the following actions:
 - Click **Generate Local Private Key**. The OnCell G3150A-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 G3150A-LTE successfully imports the selected key, the system displays the key information in the **Local private key** field.
3. Generate or import a remote private key. Perform one of the following actions:
 - Click **Generate Remote Public Key**. The OnCell G3150A-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 G3150A-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 remote certificate (*local_CA_A.pem*).

Local 1:N NAT

OnCell G3150A-LTE can support up to 32 TCP/UDP connections for 1:N network address translation (NAT).

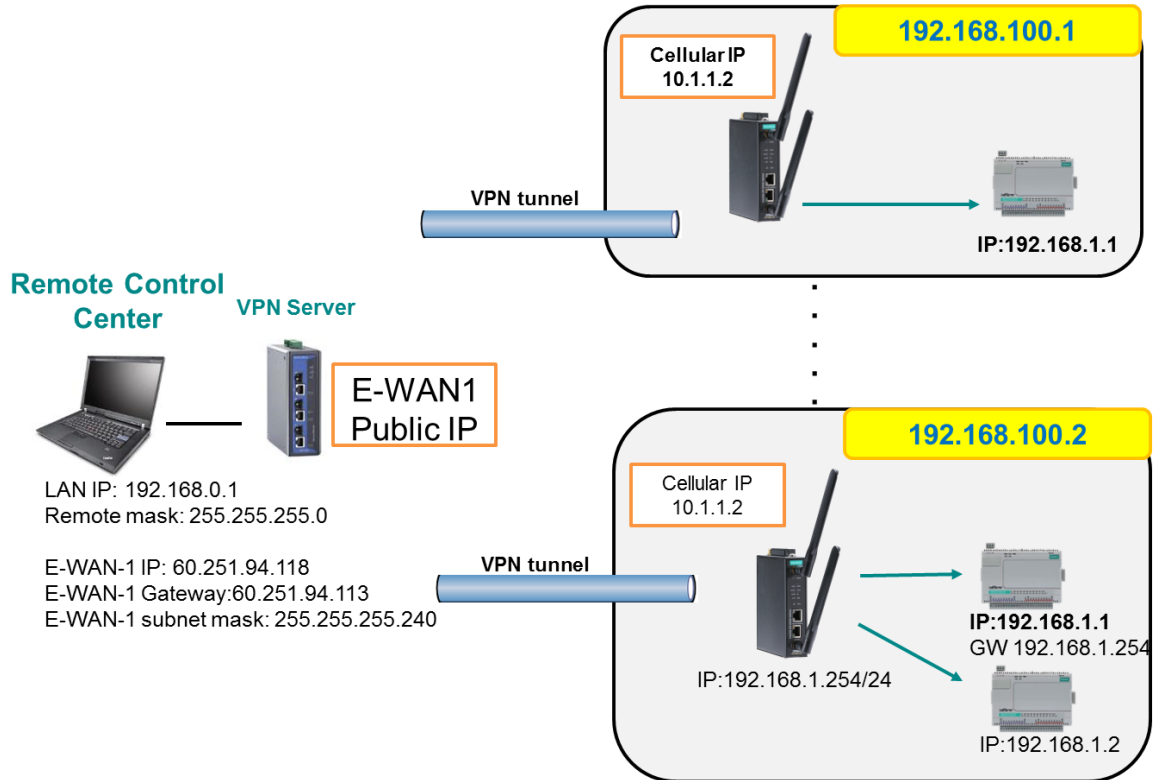
Local 1:N NAT

No	<input type="checkbox"/> Activate	Protocol	WAN Port	LAN IP	LAN Port
1	<input type="checkbox"/>	TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="checkbox"/>	TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="checkbox"/>	TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="checkbox"/>	TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="checkbox"/>	TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="checkbox"/>	TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>

Field	Description	Default setting
Activate	Select this check box to activate the 1:N NAT	Always on
Protocol	Select the protocol to use in the NAT policy.	TCP
WAN Port	Enter the WAN port number to redirect to specific LAN IP. Make sure that the port number specified is not already used by OP modes.	N/A
LAN IP	Enter the IP address of a LAN device to receive the redirected traffic.	N/A
LAN Port	Enter the port number on a LAN device to which to redirect traffic.	N/A

1:N Concept

PC:192.168.0.1-----[VPN]---Internet---[Public-IP-VPN---192.168.100.1---NAT]-----192.168.1.1=>PLC(1)
 ----Internet---[Public-IP-VPN---192.168.100.2---NAT]-----192.168.1.1=>PLC(2)



X.509 Certificate

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 G3150A-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 validity (days)

Certificate password (4 to 63 characters)

Country name (2 letter code)

State or province name (full name)

Locality (E.g., City)

Organization (E.g., Company)

Organizational unit (E.g., Section)

Name (E.g., server FQDN or your name)

Email address

Name	Subject	Action
Root CA		<input type="button" value="Delete"/>
Trusted CA1		<input type="button" value="Choose File"/> No file chosen <input type="button" value="Import"/> <input type="button" value="Delete"/>
Trusted CA2		<input type="button" value="Choose File"/> No file chosen <input type="button" value="Import"/> <input type="button" value="Delete"/>

Local Certificate Setting

Certificate days

Certificate password (4 to 63 characters)

Organizational unit name (eg, section)

Certificate name

Email address

Name	Certificate Days	Certificate Password	Organizational Unit Name	Certificate Name	Email Address	Action
Local certificate 1						<input type="button" value="Certificate Export"/> <input type="button" value="PKCS#12 Export"/> <input type="button" value="Delete"/>
Local certificate 2						<input type="button" value="Certificate Export"/> <input type="button" value="PKCS#12 Export"/> <input type="button" value="Delete"/>
Local certificate 3						<input type="button" value="Certificate Export"/> <input type="button" value="PKCS#12 Export"/> <input type="button" value="Delete"/>
Local certificate 4						<input type="button" value="Certificate Export"/> <input type="button" value="PKCS#12 Export"/> <input type="button" value="Delete"/>
Local certificate 5						<input type="button" value="Certificate Export"/> <input type="button" value="PKCS#12 Export"/> <input type="button" value="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.
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 can import on to a remote VPN gateway.
4. Click **PKCS#12 Export** to export the private key file for local certificates on the OnCell G3150A-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 G3150A-LTE.

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

Local Certificate Upload

PKCS#12 upload No file chosen

Password

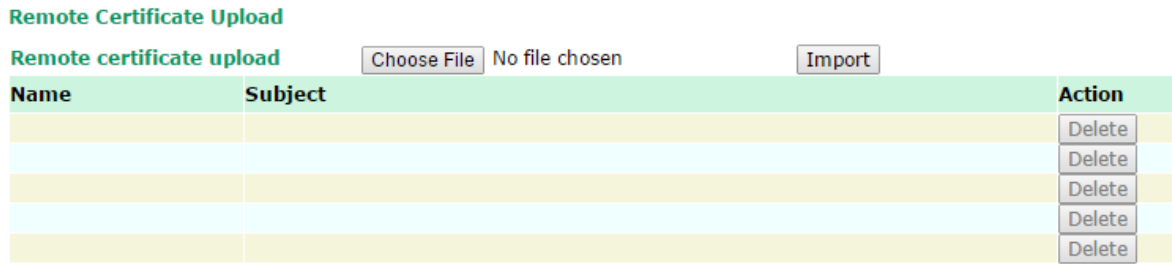
Name	Password	Subject	Action
			<input type="button" value="Delete"/>
			<input type="button" value="Delete"/>
			<input type="button" value="Delete"/>
			<input type="button" value="Delete"/>
			<input type="button" value="Delete"/>

1. Click **Advanced Settings > VPN > X.509 Certificate > Local Certificate Upload**.
2. In the **PKCS#12 upload** field, click **Choose File** to select a local certificate file
3. In the **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.



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**.

OpenVPN

Overview—OnCell G3150A-LTE OpenVPN Feature

The OnCell G3150A-LTE OpenVPN:

- Provides SSL/TLS (layer-4) security in a network with gateway-to-gateway topology. It can create either a layer-3 based IP tunnel (TUN), or a layer-2 based Ethernet (TAP) that can carry any type of Ethernet traffic.
- Supports both server and client mode communication through TCP/UDP to transfer encrypt data
- Provides server mode to push the network behind the OnCell G3150A-LTE to the server site so as to make end-to-end connection possible (Figure 1)
- Acts as an OpenVPN server to force gateway routing and redirect all external connections only through the VPN server’s gateway. (Figure2)
- Enables the OnCell G3150A-LTE to act as an OpenVPN server to allow duplicate OpenVPN clients access under the same account name. This also allows OpenVPN clients to communicate with each site. (Figure 3)

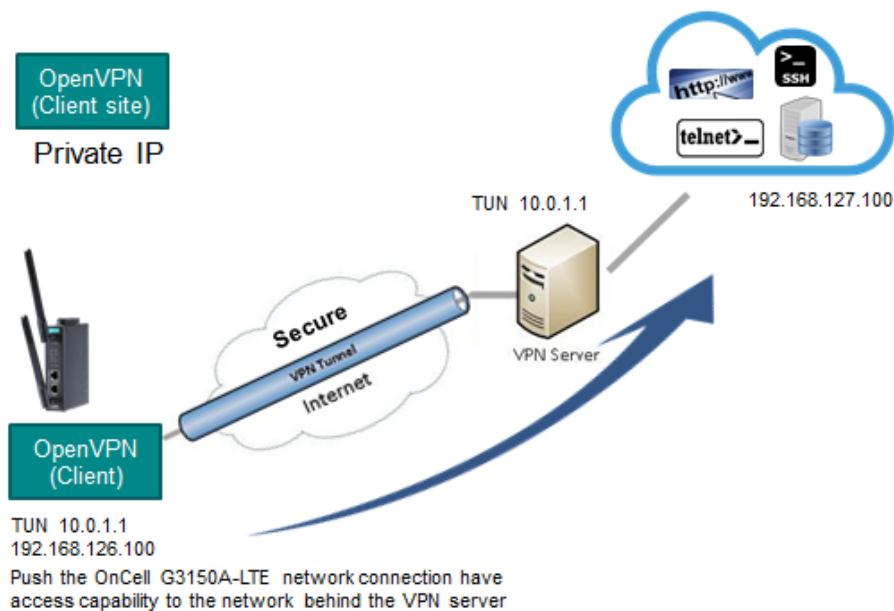


Figure 1: Push Network

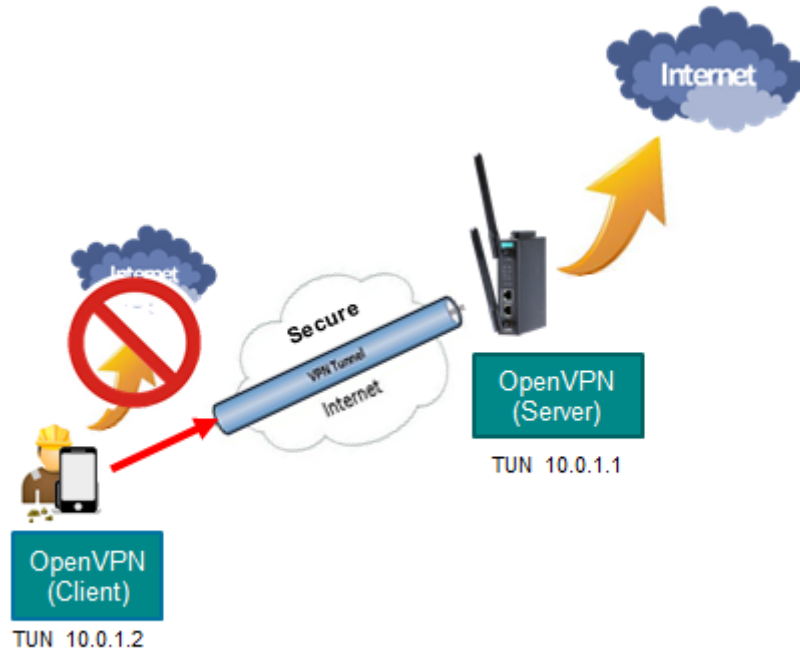


Figure 2: Redirect to Default Gateway

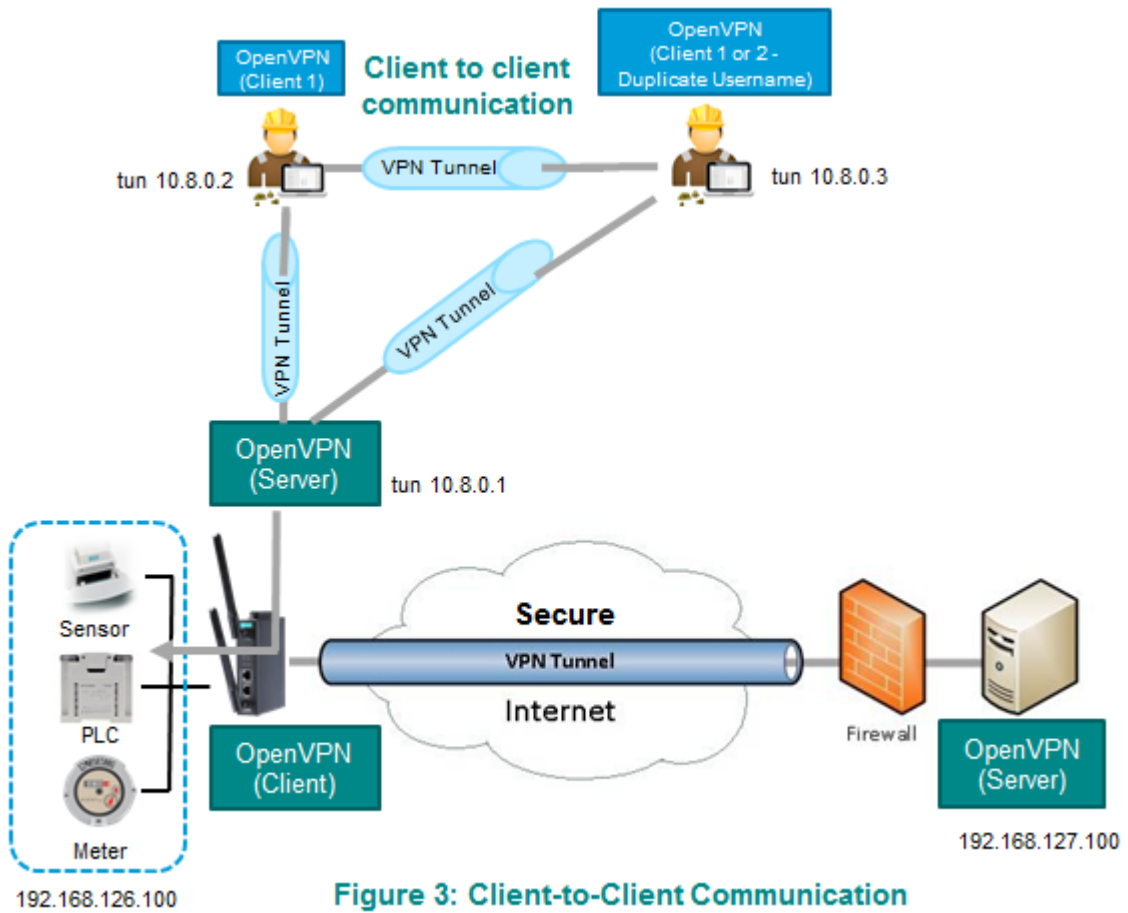
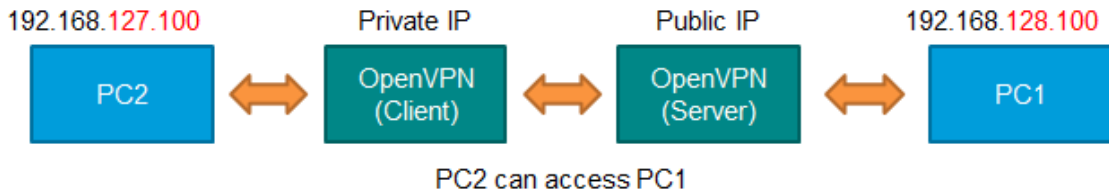


Figure 3: Client-to-Client Communication

OpenVPN—Router Mode

Use this OpenVPN mode to connect two sites that are under different subnets (in Layer 3) and encrypt the TCP/UDP package data transmission. Router mode cannot process broadcast or multicast frames.



OpenVPN—Bridge Mode

Use this OpenVPN mode to have two sites under the same subnet (in Layer 2) and encrypt IP packages during data transmission.



Server Settings

Server Setting—TUN (Router Mode)

Server Setting	
OpenVPN	Enable ▾
Interface type	TUN (Router) ▾
Network IP	10.8.0.0
Netmask	255.255.255.0
Push network IP	192.168.127.0
Push netmask	255.255.255.0
Protocol	UDP ▾
Port number	1194
Encryption algorithm	BlowFish CBC ▾
Hash algorithm	SHA1 ▾
LZO compression	Enable ▾
User authentication	Password ▾
Keepalive	Enable ▾
Redirect to default gateway	Disable ▾
Client-to-client communication	Disable ▾
Allow duplicate user name	Disable ▾

Setting	Description	Factory Default
OpenVPN	Select Enable to activate the VPN tunnel.	Disable
Interface Type	Select OpenVPN tunnel connection by router mode or bridge mode	TUN (Router)
Network IP	This is the virtual network used for private communications between server and client hosts. The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to the connecting clients.	10.8.0.0
Netmask	Enter the subnet netmask of virtual network.	255.255.255.0
Push network IP	This is the network that will be accessible from the remote endpoint. You may leave this blank if you don't want to add a route to the local network through this tunnel on the remote machine. This is generally set to your LAN network.	192.168.127.0
Push netmask	Enter the netmask of the network behind the VPN server.	255.255.255.0
Protocol	Select the protocol to be used for VPN.	UDP
Port number	Enter the port number for TCP / UDP connection	1194
Encryption algorithm	Select authentication mode for key exchange. The configuration fields vary depending on the authentication mode you select.	BlowFish CBC
Hash algorithm	Select the MD5 or SHA-1 VPN key exchange phase 1 hash mode.	SHA1
LZO compression	Compress tunnel packets using the LZO algorithm	Enable
User authentication	Only password authentication is supported in server mode	N/A
Keepalive	Select Enable to check if the client connection is alive.	Disable
Redirect to default gateway	Select Enable to force all clients generated traffic to pass through the tunnel	Disable
Client-to-client communication	Select Enable to allow communication between clients connected to the server. If this function is disabled, the OnCell will only be able to communicate with the server (see Figure 3: Client-to-Client Communication above.)	Disable
Allow duplicate user name	Select Enable to allow multiple concurrent connections from clients using the same common name. Note: This setting is not recommended but may be needed in some scenarios.	Disable

Server Setting—TAP (Bridge Mode)

Server Setting

OpenVPN	Disable ▾
Interface type	TAP (Bridge) ▾
DHCP Proxy	Enable ▾
External Gateway IP	192.168.127.254
External Gateway Netmask	255.255.255.0
IP Pool Start	192.168.127.1
IP Pool End	192.168.127.253
Protocol	UDP ▾
Port number	1194
Encryption algorithm	BlowFish CBC ▾
Hash algorithm	SHA1 ▾
LZO compression	Enable ▾
User authentication	Password ▾
Keepalive	Enable ▾
Client-to-client communication	Disable ▾
Allow duplicate user name	Disable ▾

Setting	Description	Factory Default
DHCP Proxy	Select Disable to activate the DHCP function.	Disable
External Gateway IP	Enter the remote site VPN server gateway IP address.	192.168.127.254
External Gateway Netmask	Enter the remote site VPN server subnet netmask.	255.255.255.0
IP Pool Start	This is the network that will access to remote VPN server and the IP range that can be assigned (clients number) in this local network. The IP address entered here will be the start IP for the local network (client).	192.168.127.1
IP Pool End	The IP address entered here will be the end point of the IP address for the local network (client).	192.168.127.253

NOTE The Bridge mode is the recommended mode for multicast and broadcast requirements.

Server Certificate Upload

Client Certificate Upload

Name	Subject	Action
Root CA		<input type="button" value="Choose File"/> No file chosen <input type="button" value="Import"/> <input type="button" value="Delete"/>

PKCS#12 upload

No file chosen

Password

....

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

Setting	Description
Root CA	Browse your local drive and choose the certificate generated by X.509 then click import to import the certificate.
PKCS#12 Upload	Browse your local drive and choose the certificate with password which generated by X.509 then click import to import the certificate.
Password	Enter the password that you fill in X.509 password column.
Server CA	The column shows the information of certification password and subject that imported.

Server User Management

Enables management and export of user configurations.

Server User Management

Status	Username	Remote Network IP	Remote Netmask	Action
Disable				<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Disable				<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Disable				<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Disable				<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Disable				<input type="button" value="Edit"/> <input type="button" value="Delete"/>

User Management Settings

User Active

User name

Password

Confirm password

Remote Network

Remote Netmask

Setting	Description	Factory Default
Edit	Click Edit to open the User Management Settings window.	-
User Active	Select Enable to activate User accessibility	Disable
User Name	Enter User Name.	admin
Password	Enter the password.	moxa

Client Settings

Client Setting

Status	Interface Type	Remote Server	Protocol	Encryption Cipher	LZO Compression	Authentication Mode	Action
Disabled	TUN		UDP	BlowFish CBC	ENABLE	Password	<input type="button" value="Edit"/>

Client Setting

Client enable
Interface type
Remote server IP
Protocol
Port number
Encryption algorithm
Hash algorithm
LZO compression
User authentication
User name
Password

Setting	Description	Factory Default
Client enable	Select Enable to activate OpenVPN Client	Disable
Interface type	Select OpenVPN tunnel connection by router mode or bridge mode	TUN(Router)
Remote server IP	This is the virtual network used for private communications between this server and client hosts. The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to the connecting clients. The remote site must assign a server IP, public IP, or carrier private network that is accessible to the clients.	10.8.0.0
Protocol	Select the protocol to be used for VPN.	UDP
Port number	Enter the remote server port number for TCP / UDP connection	1194
Encryption algorithm	Select authentication mode for key exchange. The configuration fields vary depending on the authentication mode you select.	BlowFish CBC
Hash algorithm	Select the MD5 or SHA-1 VPN key exchange phase 1 hash mode.	SHA1
LZO compression	Compress tunnel packets using the LZO algorithm	Enable
User authentication	Select password or certification to protect the authentication choose either one	password
User name	Enter the user name for the client that you set on the server.	N/A
Password	Enter the client password that you set on the server (up to 15 characters.)	N/A

Client Certificate Upload

Client Certificate Upload

Name	Subject	Action
Root CA		<input type="button" value="Choose File"/> No file chosen <input type="button" value="Import"/> <input type="button" value="Delete"/>

PKCS#12 upload

No file chosen

Password

....

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

Setting	Description	Factory Default
Root CA	Browse your local drive or import a certificate code.	
PKCS#12 Upload	Browse your local drive or import a certificate code.	
Password	Default password "moxa"	moxa
Client CA	The column shows the client certification password and subject imported.	

NOTE Before using the OpenVPN function, run an NTP check on the device to ensure that it is synchronized with the local time for proper authentication to take place.

X.509 Certificate

X.509 is a digital certificate method commonly used for OpenVPN authentication. You can generate a self-signed root CA or local certificate on the OnCell G3150A-LTE and import or export the certificate on a remote VPN gateway.

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

Certificate Generation

Root Certificate Generation

Certificate validity: 365 (days)

Country name (2 letter code):

State or province name (full name):

Locality (E.g., City):

Organization (E.g., Company):

Organizational unit (E.g., Section):

Name (E.g., server FQDN or your name): OnCell-G3150A-LTE

Email address:

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

Certificate Generation

Server:

Certificate validity: (days)

Certificate password (4 to 63 characters):

Organizational unit (E.g., Section):

Email address:

Name	Subject	Action
Server CA		<input type="button" value="Delete"/> <input type="button" value="PKCS#12 Export"/>
Client CA		<input type="button" value="Delete"/> <input type="button" value="PKCS#12 Export"/>

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.

Setting	Description
Certificate validity	Enter the number of days the certificate is valid for.
Country name(2 letter code)	Enter the country.
State or province name(full name)	Enter the state or the province.
Locality (E.g., city)	Enter the city.
Organization(E.g., company)	Enter the name of the organization.
Organizational unit(E.g., section)	Enter the unit or section in the organization.
Name(E.g., server, FQDN or your name)	Enter a name (such as a server name or your name).
Email address	Enter an email address.

2. Click Generate Root CA.

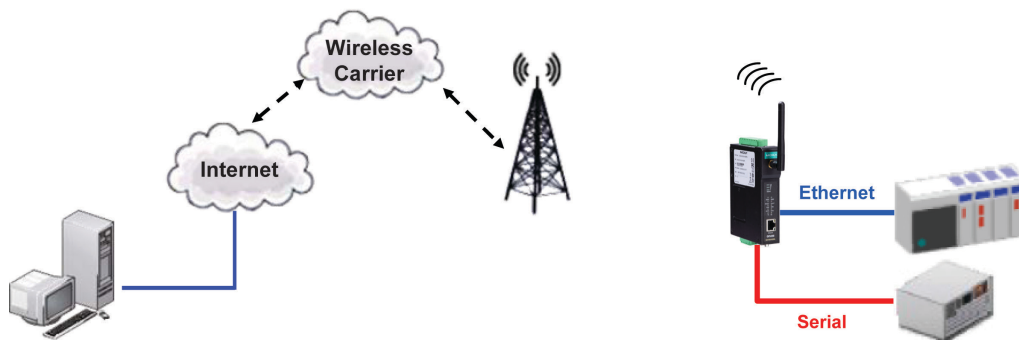
After you have generated the root CA certificate, generate a local certificate and export the key files. In the Certificate Generation screen, enter information in the fields under Local Certificate Settings.

Setting	Description
Certificate Generation	Generate a certificate for Server or Client
Certificate validity	Enter the number of days the certificate is valid for.
Certificate Password (4 to 63 characters)	Enter a password to create a password-protected certificate.
Organizational unit (E.g., Section)	Enter the unit or section in the organization.
Email address	Enter an email address.

Serial Port Settings

In this section, we describe the various operation modes of the OnCell G3150A-LTE. The OnCell G3150A-LTE modes are grouped by type of application, such as Device Control. The options include an operation mode that relies on a driver installed on the host computer, and operation modes that rely on TCP/IP socket programming concepts.

The OnCell G3150A-LTE can enable cellular network-in a serial device. OnCell G3150A-LTE device is assigned an IP address by the Internet service provider (ISP). In addition, the OnCell G3150A-LTE can enable cellular connectivity in Ethernet devices on the local Ethernet. See the *OnCell Central Manager user's manual* for details.



The OnCell G3150A-LTE enables traditional serial (RS-232/422/485) devices for transmitting data over the cellular network. The IP gateway is a computer equipped with a CPU and TCP/IP protocols that can bi-directionally translate data between the serial and IP formats. With the OnCell G3150A-LTE, your computer will be able to access, manage, and configure remote facilities and equipment over the cellular network from anywhere in the world.

Traditional SCADA and data collection systems rely on serial ports to collect data from various kinds of instruments. Since the OnCell G3150A-LTE network-enables instruments equipped with an RS-232, RS-422, or RS-485 communication port, your SCADA and data collection system will be able to access all instruments connected to a standard TCP/IP network, regardless of whether the devices are used locally or at a remote site.

The OnCell G3150A-LTE is an external IP-based network device that allows you to expand a serial port for a host computer on demand. As long as your host computer supports the TCP/IP protocol, you will not be limited by the host computer’s bus limitation (such as ISA or PCI), nor will you be limited if you do not have drivers for various operating systems.

In addition to providing socket access, the OnCell G3150A-LTE also comes with a Real COM driver and a Reverse Real COM driver that transmits all serial signals intact. This enables you to preserve your existing COM-based software without needing to invest in additional software.

Three different socket modes are available: TCP Server, TCP Client, and UDP. The main difference between the TCP and UDP protocols is that TCP guarantees delivery of data by requiring the recipient to send an acknowledgement to the sender. UDP does not require this type of verification, making it possible to offer faster delivery. UDP also allows you to unicast data to one IP, or multicast the data to a group of IP addresses.

Operation Mode

Serial Port Settings

Port Setting Basics

To configure the operation mode and settings for a port, expand **Serial Port Settings** in the navigation panel, and then expand the port that you would like to configure. Individual port settings are grouped into three categories in the navigation panel: Operation Modes, Communication Parameters, and Data Buffering/Log.

Port 1

Application Device Control ▾

Mode RealCOM ▾

TCP alive check time RealCOM

Max connection RFC2217

Reverse RealCOM

Disabled Mode

Operation Modes

Port 1

Application Disable ▾

When the **Application** is set to **Disable**, the relevant port will be disabled.

Device Control Applications

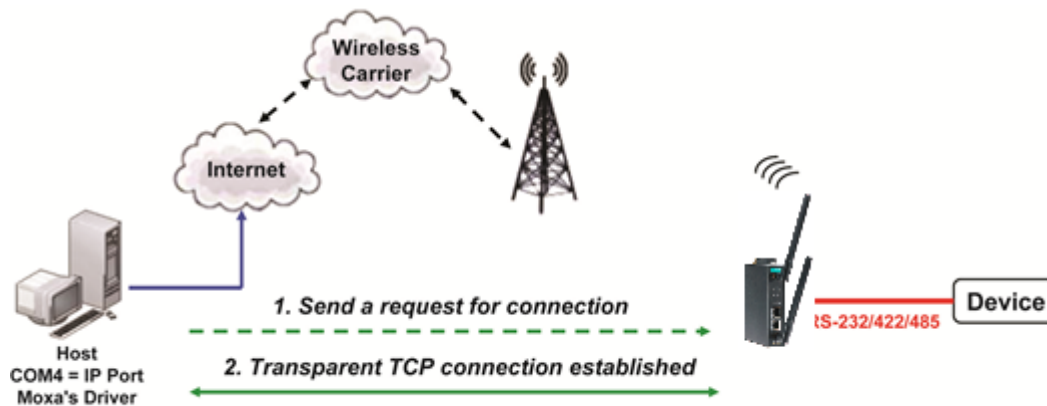
The OnCell G3150A-LTE offers the following modes for device control applications: Real COM, Reverse Real COM, and RFC2217 modes.

Real COM Mode

NOTE You can download the Moxa Drivers for operation modes from www.moxa.com.
File Name: NPort/OnCell Windows Driver Manager

In Real COM mode, the bundled drivers are able to establish a transparent connection between a host and a serial device by mapping the serial port on the OnCell G3150A-LTE to a local COM port on the host computer. Real COM mode supports up to 2 simultaneous connections that enable 2 hosts to simultaneously collect data from the same serial device.

One of the major conveniences of using Real COM mode is that it allows you to use software that was written for pure serial communication applications. The OnCell COM driver intercepts data sent to the host's COM port, packs it into a TCP/IP packet, and then redirects it through the host's Ethernet card to the Internet. At the other end of the connection, the OnCell G3150A-LTE accepts the IP frame from the cellular network, unpacks the TCP/IP packet, and then transparently sends the data through the serial port to the attached serial device.



Port 1



Application Device Control ▾
Mode RealCOM ▾
TCP alive check time 7 (0 - 99 min)
Max connection 1 ▾
Ignore jammed IP Enable Disable
Allow driver control Enable Disable
Connection goes down RTS always low always High
DTR always low always High

Data Packing

Packing length 0 (0 - 1024)
Delimiter 1 00 (Hex) Enable
Delimiter 2 00 (Hex) Enable
Delimiter process Do Nothing ▾ (Processed only when Packing length is 0)
Force transmit 0 (0 - 65535 ms)

Submit

Setting	Description	Factory Default
TCP alive check time	This field specifies how long the OnCell G3150A-LTE will wait for a response to "keep alive" packets before closing the TCP connection. The OnCell G3150A-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 G3150A-LTE will force the existing TCP connection to close. For socket and device control modes, the OnCell G3150A-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 and will not send any "keep alive" packets.	7 min
Max connection	This field is used if you need to receive data from different hosts simultaneously. When set to 1, only one specific host can access this port of the OnCell G3150A-LTE, and the OnCell COM driver on that host will have full control over the port. When set to 2, the specified number of hosts' OnCell COM driver may open this port at the same time. When multiple hosts on the OnCell COM driver open the port at the same time, the COM driver only provides a pure data tunnel --no control ability unless "Allow Driver Control" is enabled. The serial port parameters will use firmware settings instead of depending on your application program (AP). Application software that is based on the COM driver will receive a driver response of "success" when the software uses any of the Win32 API functions. The firmware will only send data back to the driver on the host. Data will be sent first-in-first-out when data comes into the OnCell G3150A-LTE from the Cellular or Ethernet interface.	1

Setting	Description	Factory Default
 <p>ATTENTION When Max connection is greater than 1, the OnCell G3150A-LTE will use a multi connection application (i.e., 2 hosts are allowed access to the port at the same time). When using a multi connection application, the OnCell G3150A-LTE will use the serial communication parameters as defined here in the web console, and all hosts connected to the port must use identical serial settings. If one of the hosts opens the COM port with different serial settings, data will not be transmitted properly.</p>		
<p>Ignore jammed IP</p>	<p>This option determines how the port will proceed if multiple hosts are connected and one or more host(s) stops responding when the port is transmitting data. If you select Disable, the port will wait until the data has been transmitted successfully to all hosts before transmitting the next group of data. If you select Enable, the port will ignore the host that stopped responding and continue data transmission to the other hosts.</p>	<p>Disable</p>
<p>Allow driver control</p>	<p>This option determines how the port will proceed if driver control commands are received from multiple hosts that are connected to the port. If Disable is selected, driver control commands will be ignored. If Enable is selected, control commands will be accepted, with the most recent command received taking precedence.</p>	<p>Disable</p>
<p>Connection goes down</p>	<p>You can configure what happens to the RTS and DTR signals when the Cellular or Ethernet connection goes down. For some applications, serial devices need to know the Cellular or Ethernet link status through RTS or DTR signals sent through the serial port. Use "always low" if you want the RTS and DTR signal to change their state to low when the Cellular or Ethernet connection gets disconnected. Use "always high" if you do not want the cellular or Ethernet connection status to affect the RTS or DTR signals.</p>	<p>Always High</p>
<p>Packing length</p>	<p>The Packing length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. At the default of 0 for packet length, no maximum amount is specified and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.</p>	<p>0</p>
<p>Delimiter 1 Delimiter 2</p>	<p>When Delimiter 1 is enabled, the serial port will queue the data in the buffer and send the data to the Cellular or Ethernet port when a specific character, entered in hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to control when data should be sent.</p>	<p>00</p>
 <p>ATTENTION In order to enable a delimiter, packet length must be set to 0. Delimiter 2 should only be enabled in conjunction with Delimiter 1 and never on its own; otherwise there may be data errors. Even when a delimiter is enabled, the OnCell G3150A-LTE will still pack and send the data when the amount of data exceeds 1 KB.</p>		

Setting	Description	Factory Default
Delimiter process	<p>The Delimiter process field determines how the data is handled when a delimiter is received. Delimiter 1 must be enabled for this field to have effect. If Delimiters 1 and 2 are both enabled, both characters must be received for the delimiter process to take place.</p> <ul style="list-style-type: none"> • Do Nothing: Data in the buffer will be transmitted when the delimiter is received. • Delimiter + 1: Data in the buffer will be transmitted after 1 additional byte is received following the delimiter. • Delimiter + 2: Data in the buffer will be transmitted after 2 additional bytes are received following the delimiter. • Strip Delimiter: Data in the buffer is first stripped of the delimiter before being transmitted. 	Do Nothing
Force transmit	<p>This parameter defines how large a gap in serial communication the OnCell G3150A-LTE will allow before packing the serial data in its internal buffer for network transmission.</p> <p>As data is received through the serial port, it is stored by the OnCell G3150A-LTE in the internal buffer. The OnCell G3150A-LTE transmits the data stored in the buffer via TCP/IP when the internal buffer is full or as specified by the force-transmit time.</p> <p>When this field is set to 0, the force transmit time is disabled and transmission is determined solely by the data in the internal buffer. When the force transmit time is set to a value from 1 to 65535, the TCP/IP protocol software will pack the serial data received for transmission after the gap in serial communication exceeds the specified force transmit time.</p> <p>The optimal force-transmit time setting depends on your application. However, it must be set to a value that is more than one-character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is $(10 \text{ (bits)} / 1200 \text{ (bits/s)}) \times 1000 \text{ (ms/s)} = 8.3 \text{ ms}$. Therefore, you should set the force transmit time to be greater than 8.3 ms, so in this case, it must be greater than or equal to 10 ms.</p> <p>If it is necessary to send a series of characters in the same packet, the serial device will need to send that series of characters within the specified force transmit time, and the total length of data must be less than or equal to the OnCell G3150A-LTE's internal buffer size (1 KB per port).</p>	0 ms

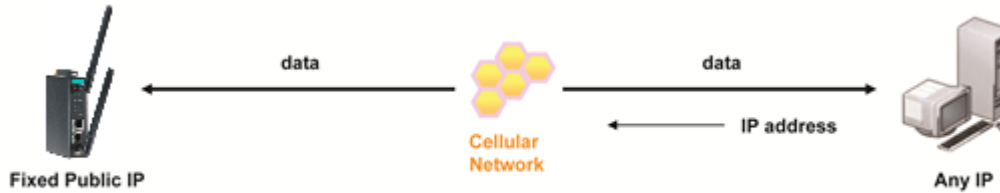
Types of Real COM Connection

This section illustrates the types of Real COM connections you can use, depending on the service you obtain from your local cellular service provider.

Fixed Public IP for OnCell

If your cellular service provider offers a fixed public IP address after you connect to the cellular network, you can access the OnCell G3150A-LTE via a host PC using either a private IP or public IP.

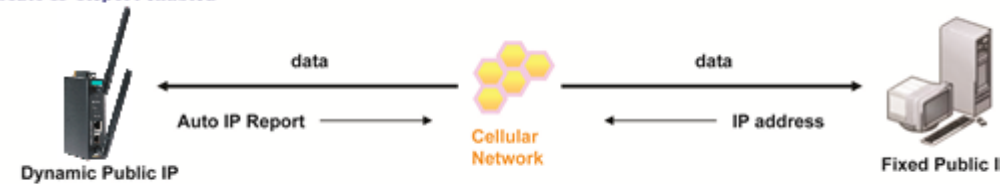
Real COM mode



Utilize Auto IP report

If your cellular service provider offers a dynamic public IP address after you connect to the cellular network, you can access the OnCell G3150A-LTE via a host PC using a fixed public IP. Since the IP address of the OnCell G3150A-LTE is changed each time it is connected to the cellular network, the host IP can be notified of the change by an Auto IP Report message sent from the OnCell G3150A-LTE. Please refer to *Auto IP Report Settings* to see the format of the Auto IP Report Protocol.

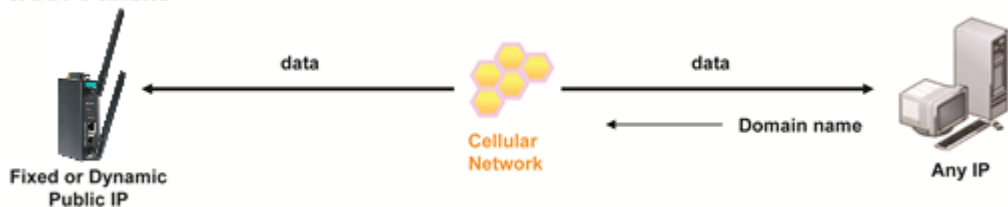
Real COM mode & Auto IP Report enabled



Domain name with DDNS

If your cellular service provider offers a public IP address after you connect to the cellular network, you can also access the OnCell G3150A-LTE using the domain name. To do this, you will need to register with a DDNS service provider and then enable the DDNS function in the OnCell G3150A-LTE. Please refer to Appendix B for more information.

Real COM mode & DDNS enabled



RFC 2217 Mode

RFC-2217 mode is similar to Real COM mode in that a driver is used to establish a transparent connection between a host computer and a serial device by mapping the serial port on the OnCell G3150A-LTE to a local COM port on the host computer. RFC2217 defines general COM port control options based on the Telnet protocol. Third party drivers supporting RFC-2217 are widely available on the Internet and can be used to implement virtual COM mapping to your OnCell G3150A-LTE's serial port.


Port 1

Application
Mode
TCP alive check time (0 - 99 min)
TCP port

Data Packing

Packing length (0 - 1024)
Delimiter 1 (Hex) Enable
Delimiter 2 (Hex) Enable
Delimiter process (Processed only when Packing length is 0)
Force transmit (0 - 65535 ms)

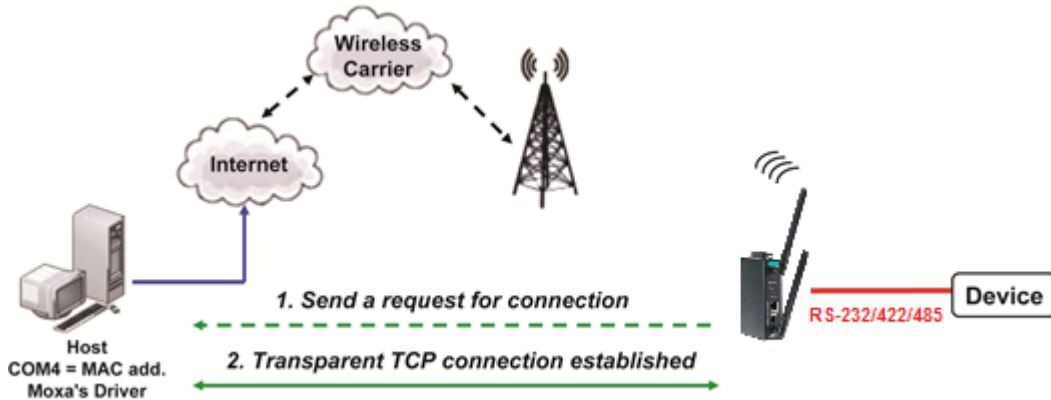
Setting	Description	Factory Default
TCP alive check time	This field specifies how long the OnCell G3150A-LTE will wait for a response to "keep alive" packets before closing the TCP connection. The OnCell G3150A-LTE checks connection status by sending periodic "keep alive" packets. If the remote host does not respond to the packet within the time specified in this field, the OnCell G3150A-LTE will force the existing TCP connection to close. For socket and device control modes, the OnCell G3150A-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 and will not send any "keep alive" packets.	7 min
TCP port	This is the TCP port number assignment for the serial port on the OnCell G3150A-LTE. It is the port number that the serial port uses to listen to connections, and that other devices must use to contact the serial port. To avoid conflicts with well-known TCP ports, the default is set to 4001.	4001
Packing length	The Packing length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. At the default of 0 for packet length, no maximum amount is specified and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.	0
Delimiter 1 Delimiter 2	When Delimiter 1 is enabled, the serial port will queue the data in the buffer and send the data to the Cellular or Ethernet port when a specific character, entered in hex format, is	00

Setting	Description	Factory Default
	received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to control when data should be sent.	
 ATTENTION In order to enable a delimiter, the packet length must be set to 0. Delimiter 2 should only be enabled in conjunction with Delimiter 1 and never on its own to avoid data errors. Even when a delimiter is enabled, the OnCell G3150A-LTE will still pack and send the data when the amount of data exceeds 1 KB.		
Delimiter process	<p>The Delimiter process field determines how the data is handled when a delimiter is received. Delimiter 1 must be enabled for this field to have effect. If Delimiters 1 and 2 are both enabled, both characters must be received for the delimiter process to take place.</p> <ul style="list-style-type: none"> • Do Nothing: Data in the buffer will be transmitted when the delimiter is received. • Delimiter + 1: Data in the buffer will be transmitted after 1 additional byte is received following the delimiter. • Delimiter + 2: Data in the buffer will be transmitted after 2 additional bytes are received following the delimiter. • Strip Delimiter: Data in the buffer is first stripped of the delimiter before being transmitted. 	Do Nothing
Force transmit	<p>This parameter defines how large a gap in serial communication the OnCell G3150A-LTE will allow before packing the serial data in its internal buffer for network transmission.</p> <p>As data is received through the serial port, it is stored by the OnCell G3150A-LTE in the internal buffer. The OnCell G3150A-LTE transmits the data stored in the buffer via TCP/IP when the internal buffer is full or as specified by the force-transmit time.</p> <p>When this field is set to 0, the force transmit time is disabled and transmission is determined solely by the data in the internal buffer. When the force transmit time is set to a value from 1 to 65535, the TCP/IP protocol software will pack the serial data received for transmission after the gap in serial communication exceeds the specified force transmit time. The optimal force-transmit time setting depends on your application. However, it must be set to a value that is more than one-character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is (10 (bits) / 1200 (bits/s)) × 1000 (ms/s) = 8.3 ms. Therefore, you should set the force transmit time to be greater than 8.3 ms, so in this case, it must be greater than or equal to 10 ms.</p> <p>If it is necessary to send a series of characters in the same packet, the serial device will need to send that series of characters within the specified force transmit time, and the total length of data must be less than or equal to the OnCell G3150A-LTE's internal buffer size (1 KB per port).</p>	0 ms

Reverse Real COM Mode

NOTE You can download the Moxa Drivers for operation modes from www.moxa.com.
File Name: NPort/OnCell Windows Driver Manager

Reverse Real COM mode uses a mechanism similar to port mapping to enable your remote device that is using a private IP address to remain accessible to external hosts. When this mode is enabled, the Moxa driver that comes with the device establishes a transparent connection from the device to the remote host by mapping the device's serial port to a local COM port on the remote host. Reverse Real COM mode supports up to 2 simultaneous connections that enable serial devices to send data to 2 hosts simultaneously.





Port 1


Application	Device Control	
Mode	Reverse RealCOM	
TCP alive check time	7 (0 - 99 min)	
Ignore jammed IP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Allow driver control	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Destination address 1	<input type="text"/>	TCP port: 60950 Cmd port: 60966
Destination address 2	<input type="text"/>	TCP port: 60950 Cmd port: 60966
Designated local TCP port 1	<input type="text" value="0"/>	
Designated local cmd port 1	<input type="text" value="0"/>	
Designated local TCP port 2	<input type="text" value="0"/>	
Designated local cmd port 2	<input type="text" value="0"/>	
Connection goes down	RTS <input type="radio"/> always low <input checked="" type="radio"/> always High DTR <input type="radio"/> always low <input checked="" type="radio"/> always High	

Data Packing

Packing length	<input type="text" value="0"/> (0 - 1024)
Delimiter 1	<input type="text" value="00"/> (Hex) <input type="checkbox"/> Enable
Delimiter 2	<input type="text" value="00"/> (Hex) <input type="checkbox"/> Enable
Delimiter process	Do Nothing (Processed only when Packing length is 0)
Force transmit	<input type="text" value="0"/> (0 - 65535 ms)

Submit

Setting	Description	Factory Default
TCP alive check time	This field specifies how long the OnCell G3150A-LTE will wait for a response to "keep alive" packets before closing the TCP connection. The OnCell G3150A-LTE checks 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 G3150A-LTE will force the existing TCP connection to close. For socket and device control modes, the OnCell G3150A-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 and will not send any "keep alive" packets.	7 min
Ignore jammed IP	This option determines how the port will proceed, if multiple hosts are connected and one or more of the hosts stop responding as the port is transmitting data. If you select Disable, the port will wait until the data has been transmitted successfully to all hosts before transmitting the next group of data. If you select Enable, the port will ignore the host that stopped responding and continue data transmission to the other hosts.	Disable
Allow driver control	This option determines how the port will proceed if driver control commands are received from multiple hosts that are connected to the port. If Disable is selected, driver control commands will be ignored. If Enable is selected, control commands will be accepted, with the most recent command received taking precedence.	Disable
Destination address 1 through 2	Specifying an IP address allows the OnCell G3150A-LTE to connect actively to the remote host. At least one destination must be provided.	None
TCP port	This is the TCP port number assignment for the remote host/server. It is the port number that the OnCell G3150A-LTE's serial port uses to establish connections with a remote host/server. To avoid conflicts with well-known TCP ports, the default is set to 60950.	60950
Command port	The Command port is the COM port for listening to SSDK commands from the host. In order to prevent a COM port conflict with other applications, the user can set the Command port to another port if needed.	60966
 ATTENTION Up to 2 connections can be established between OnCell G3150A-LTE hosts. Port 60950 might be blocked by a firewall. You should make sure the port is NOT blocked before you start using it.		
 ATTENTION The destination IP address parameter can be the IP address, domain name, or the name defined in the host table.		
Designated local port 1 through 2	Use these fields to specify the designated local ports. (Example: 7010 through 7320)	0

Setting	Description	Factory Default
Connection goes down	You can configure what happens to the RTS and DTR signals when the Cellular or Ethernet connection goes down. For some applications, serial devices need to know the Cellular or Ethernet link status through RTS or DTR signals sent through the serial port. Use "always low" if you want the RTS and DTR signal to change their state to low when the Cellular or Ethernet connection gets disconnected. Use "always high" if you do not want the cellular or Ethernet connection status to affect the RTS or DTR signals.	Always high
Packet length	The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. At the default of 0 for packet length, no maximum amount is specified and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.	0
Delimiter 1 Delimiter 2	When Delimiter 1 is enabled, the serial port will queue the data in the buffer and send the data to the Cellular or Ethernet port when a specific character, entered in hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to control when data should be sent.	00
 ATTENTION In order to enable a delimiter, packet length must be set to 0. Delimiter 2 should only be enabled in conjunction with Delimiter 1 and never on its own to avoid data errors. Even when a delimiter is enabled, the OnCell G3150A-LTE will still pack and send the data when the amount of data exceeds 1 KB.		
Delimiter process	<p>The Delimiter process field determines how the data is handled when a delimiter is received. Delimiter 1 must be enabled for this field to have effect. If Delimiters 1 and 2 are both enabled, both characters must be received for the delimiter process to take place.</p> <ul style="list-style-type: none"> • Do Nothing: Data in the buffer will be transmitted when the delimiter is received. • Delimiter + 1: Data in the buffer will be transmitted after 1 additional byte is received following the delimiter. • Delimiter + 2: Data in the buffer will be transmitted after 2 additional bytes are received following the delimiter. • Strip Delimiter: Data in the buffer is first stripped of the delimiter before being transmitted. 	Do Nothing
Force transmit	<p>This parameter defines how large a gap in serial communication the OnCell G3150A-LTE will allow before packing the serial data in its internal buffer for network transmission.</p> <p>As data is received through the serial port, it is stored by the OnCell G3150A-LTE in the internal buffer. The OnCell G3150A-LTE transmits the data stored in the buffer via TCP/IP when the internal buffer is full or as specified by the force-transmit time.</p> <p>When this field is set to 0, the force transmit time is disabled and transmission is determined solely by the data in the</p>	0 ms

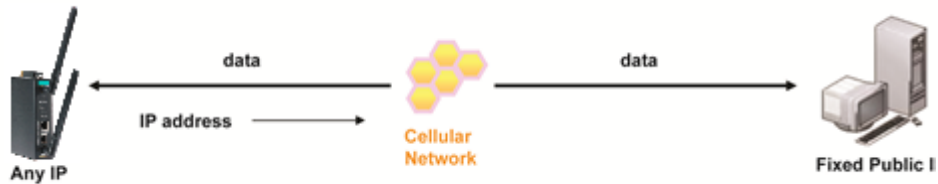
Setting	Description	Factory Default
	<p>internal buffer. When the force transmit time is set to a value from 1 to 65535, the TCP/IP protocol software will pack the serial data received for transmission after the gap in serial communication exceeds the specified force transmit time. The optimal force-transmit time setting depends on your application. However, it must be set to a value that is more than one-character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is (10 (bits) / 1200 (bits/s)) × 1000 (ms/s) = 8.3 ms. Therefore, you should set the force transmit time to be greater than 8.3 ms, so in this case, it must be greater than or equal to 10 ms.</p> <p>If it is necessary to send a series of characters in the same packet, the serial device will need to send that series of characters within the specified force transmit time, and the total length of data must be less than or equal to the OnCell G3150A-LTE’s internal buffer size (1 KB per port).</p>	

Types of Reverse Real COM Connection

Reverse Real COM to PC’s IP address

Most cellular service providers only provide customers with a dynamic private IP address, which means that the OnCell G3150A-LTE will only obtain an IP address once it is connected to the cellular network. Reverse Real COM is a great feature that allows a PC host to access an OnCell G3150A-LTE configured with private IP address.

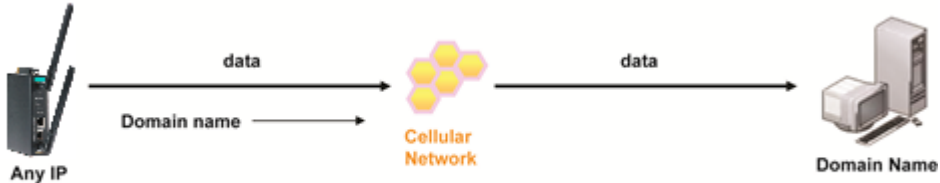
Reverse Real COM mode



Reverse Real COM to PC’s domain name

With Reverse Real COM mode, you can connect to a PC host using the PC’s IP address. You can also connect to your PC host with the PC’s domain name, if you have one. Please refer to Appendix B for more information.

Reverse Real COM mode



Socket Applications

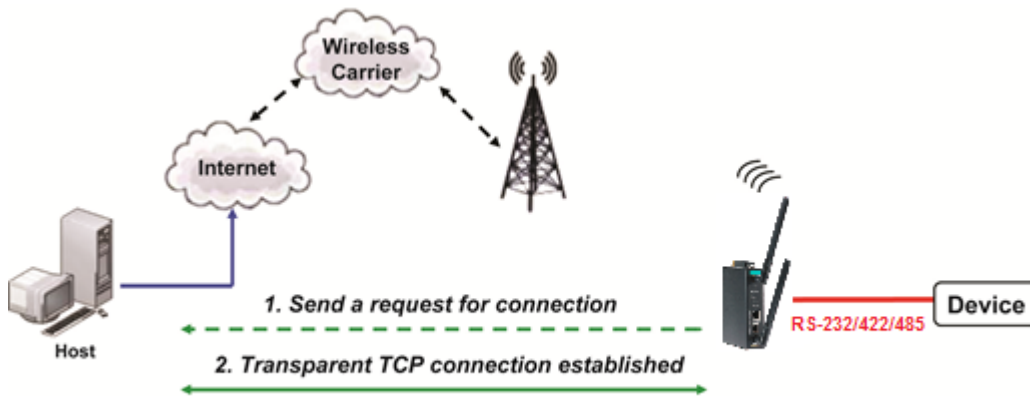
The OnCell G3150A-LTE offers the following modes for socket applications: TCP Server, TCP Client, and UDP.

TCP Server Modes

In TCP Server mode, the serial port on the OnCell G3150A-LTE is assigned a port number. The host computer initiates contact with the OnCell G3150A-LTE, establishes the connection, and receives data from the serial device. This operation mode also supports up to 2 simultaneous connections, enabling multiple hosts to collect data from the same serial device at the same time.

As illustrated in the figure, data transmission proceeds as follows: The host requests a connection from the OnCell G3150A-LTE, which is configured for TCP Server mode. Once the connection is established, data can be transmitted in both directions between the host and the OnCell G3150A-LTE.

TCP Server mode includes optional data encryption using SSL





Port 1


Application	Socket
Mode	TCP Server
TCP alive check time	7 (0 - 99 min)
Max connection	1
Ignore jammed IP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Allow driver control	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Inactivity time	0 (0 - 65535 ms)
TCP port	4001
Cmd port	966
Connection goes down	RTS <input type="radio"/> always low <input checked="" type="radio"/> always High DTR <input type="radio"/> always low <input checked="" type="radio"/> always High

Data Packing

Packing length	0 (0 - 1024)
Delimiter 1	00 (Hex) <input type="checkbox"/> Enable
Delimiter 2	00 (Hex) <input type="checkbox"/> Enable
Delimiter process	Do Nothing (Processed only when Packing length is 0)
Force transmit	0 (0 - 65535 ms)

Submit

Setting	Description	Factory Default
TCP alive check time	This field specifies how long the OnCell G3150A-LTE will wait for a response to "keep alive" packets before closing the TCP connection. The OnCell G3150A-LTE checks 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 G3150A-LTE will force the existing TCP connection to close. For socket and device control modes, the OnCell G3150A-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 and will not send any "keep alive" packets.	7 min
 ATTENTION You should make sure the inactivity time value used here is less than the inactivity time value on the GSM/GPRS configuration page. The GSM/GPRS connection must be maintained in order to achieve the inactivity time behavior of the TCP connection.		
Inactivity time	This field specifies how long the OnCell G3150A-LTE will wait for incoming and outgoing data through the serial port before closing the TCP connection. The TCP connection is closed if there is no incoming or outgoing data through the serial port for the specified Inactivity time . If this field is set to 0 , the TCP connection is kept active until a connection close request is received.	0ms
 ATTENTION If used, the Inactivity time setting should be greater than the Force transmit time. To prevent the unintended loss of data due to the session being disconnected, it is highly recommended that this value is set large enough so that the intended data transfer is completed.		
Max connection	This field is used if you need to receive data from different hosts simultaneously. When set to 1, only a single host may open the TCP connection to the serial port. When set to 2, the specified number of hosts may open this port at the same time. When multiple hosts establish a TCP connection to the serial port at the same time, the OnCell G3150A-LTE will duplicate the serial data and transmit it to all the hosts. Cellular or Ethernet data is sent on a first-in first-out basis to the serial port when data comes into the OnCell G3150A-LTE from the Cellular or Ethernet interface.	1
Ignore jammed IP	This option determines how the port will proceed if multiple hosts are connected and one or more of the hosts stop responding as the port is transmitting data. If you select Disable , the port will wait until the data has been transmitted successfully to all hosts before transmitting the next group of data. If you select Enable , the port will ignore the host that stopped responding and continue data transmission to the other hosts.	Disable
Allow driver control	This option determines how the port will proceed if driver control commands are received from multiple hosts that are connected to the port. If Disable is selected, driver control commands will be ignored. If Enable is selected, control commands will be accepted, with the most recent command received taking precedence.	Disable
TCP port	This is the TCP port number assignment for the serial port on the OnCell G3150A-LTE. It is the port number that the serial port uses to listen to connections, and that other devices must use to contact the serial port. To avoid conflicts with well-known TCP ports, the default is set to 4001.	4001
Command port	The Command port is the TCP port for listening to SSDK commands from the host. In order to prevent a TCP port conflict with other applications, the user can set the Command port to another port if needed.	966

Setting	Description	Factory Default
Packet length	The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. At the default of 0 for packet length, no maximum amount is specified and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.	0
Delimiter 1 Delimiter 2	When Delimiter 1 is enabled, the serial port will queue the data in the buffer and send the data to the Cellular or Ethernet port when a specific character, entered in hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to control when data should be sent.	00
 ATTENTION In order to enable a delimiter, packet length must be set to 0. Delimiter 2 should only be enabled in conjunction with Delimiter 1 and never on its own; otherwise there may be data errors. Even when a delimiter is enabled, the OnCell G3150A-LTE will still pack and send the data when the amount of data exceeds 1 KB.		
Delimiter process	The Delimiter process field determines how the data is handled when a delimiter is received. Delimiter 1 must be enabled for this field to have effect. If Delimiters 1 and 2 are both enabled, both characters must be received for the delimiter process to take place. <ul style="list-style-type: none"> • Do Nothing: Data in the buffer will be transmitted when the delimiter is received. • Delimiter + 1: Data in the buffer will be transmitted after 1 additional byte is received following the delimiter. • Delimiter + 2: Data in the buffer will be transmitted after 2 additional bytes are received following the delimiter. • Strip Delimiter: Data in the buffer is first stripped of the delimiter before being transmitted. 	Do Nothing
Force transmit	This parameter defines how large a gap in serial communication the OnCell G3150A-LTE will allow before packing the serial data in its internal buffer for network transmission. As data is received through the serial port, it is stored by the OnCell G3150A-LTE in the internal buffer. The OnCell G3150A-LTE transmits the data stored in the buffer via TCP/IP when the internal buffer is full or as specified by the force-transmit time. When this field is set to 0, the force transmit time is disabled and transmission is determined solely by the data in the internal buffer. When the force transmit time is set to a value from 1 to 65535, the TCP/IP protocol software will pack the serial data received for transmission after the gap in serial communication exceeds the specified force transmit time. The optimal force-transmit time setting depends on your application. However, it must be set to a value that is more than one-character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is (10 (bits) / 1200 (bits/s)) × 1000 (ms/s) = 8.3 ms . Therefore, you should set the force transmit time to be greater than 8.3 ms, so in this case, it must be greater than or equal to 10 ms. If it is necessary to send a series of characters in the same packet, the serial device will need to send that series of characters within the specified force transmit time, and the total length of data must be less than or equal to the	0 ms

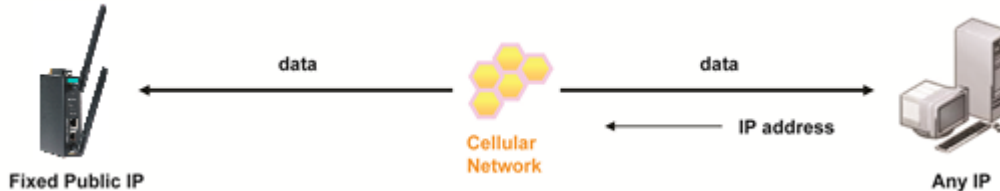
Setting	Description	Factory Default
	OnCell G3150A-LTE's internal buffer size (1 KB per port).	

Types of TCP Server Connection

Fixed Public IP for the OnCell

If your cellular service provider offers a fixed public IP address after you connect to the cellular network, you can access the OnCell G3150A-LTE from a host PC using either a private IP or public IP.

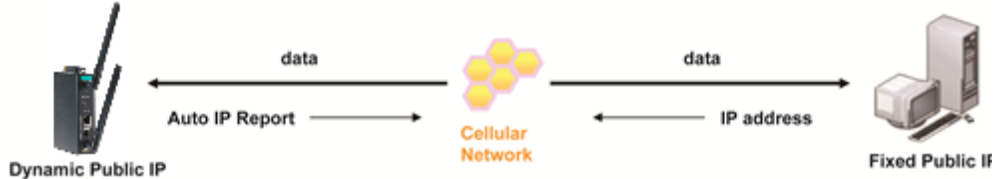
TCP Server mode



Using Auto IP report

If your cellular service provider offers a dynamic public IP address after you connect to the cellular network, you can access the OnCell G3150A-LTE from a host PC using a fixed public IP. Since the IP address of the OnCell G3150A-LTE is changed every time it is connected to the cellular network, the host IP can be aware of the change by the Auto IP Report message sent from the OnCell G3150A-LTE. Please refer to *Auto IP report settings* for the format of the Auto IP Report Protocol.

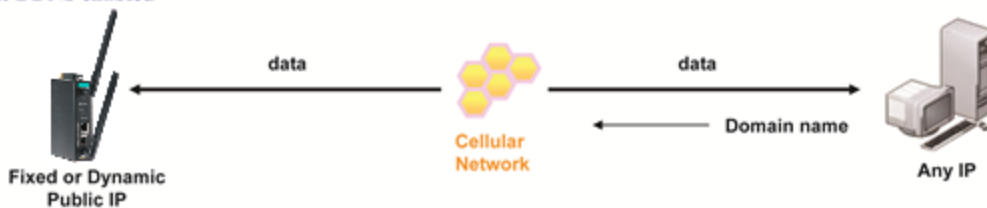
TCP Server mode & Auto IP Report enabled



Domain name with DDNS

If your cellular service provider offers a public IP address after you connect to the cellular network, you can also use the domain name to access the OnCell G3150A-LTE. You would need to register with a DDNS service provider and then enable the DDNS function in the OnCell G3150A-LTE. Please refer to Appendix B for more information.

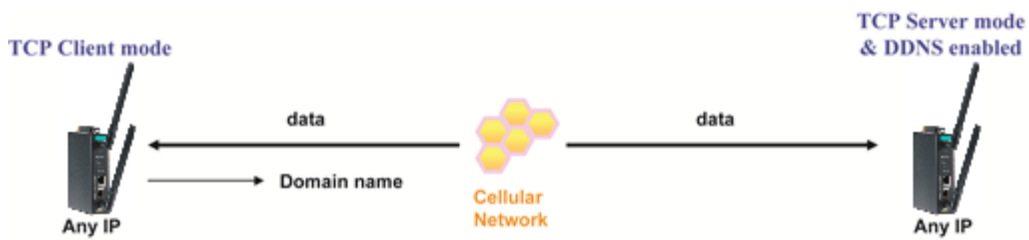
TCP Server mode & DDNS enabled



Connecting TCP client and TCP server within the same cellular service provider

In order to connect properly, the IP addresses of the two OnCell devices must belong to the same subnetwork. To ensure that this is the case, use the same cellular service provider to connect the devices to the network. In

In addition, you will need to request that the cellular service provider provide you with two private IP addresses (e.g., 192.168.1.1 and 192.168.1.2).



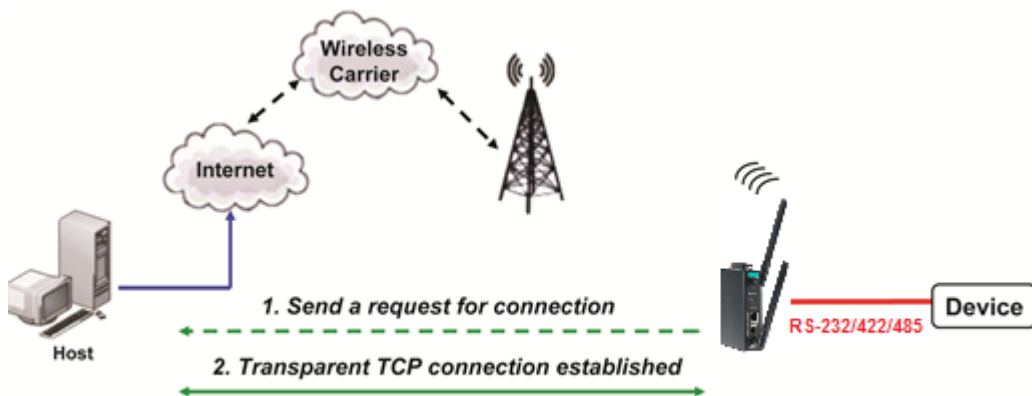
TCP Client Modes

In TCP Client mode, the OnCell G3150A-LTE can actively establish a TCP connection to a pre-defined host computer when serial data arrives. After the data has been transferred, the OnCell G3150A-LTE can automatically disconnect from the host computer by using the Inactivity time settings.

As illustrated in the figure below, data transmission proceeds as follows:

1. The OnCell G3150A-LTE, configured for TCP Client mode, requests a connection to the host.
2. Once the connection is established, data can be transmitted in both directions between the host and the OnCell G3150A-LTE.

TCP Client mode includes optional data encryption using SSL.



Port 1

Application

Mode

TCP alive check time (0 - 99 min)

Inactivity time (0 - 65535 ms)

Ignore jammed IP Enable Disable

Allow driver control Enable Disable

Destination address 1 Port

Destination address 2 Port

Destination address 3 Port

Destination address 4 Port

Designated local port 1

Designated local port 2

Designated local port 3

Designated local port 4

Connection control

Data Packing


Packing length (0 - 1024)





Delimiter 1 (Hex) Enable


Delimiter 2 (Hex) Enable

Delimiter process (Processed only when Packing length is 0)

Force transmit (0 - 65535 ms)

Setting	Description	Factory Default
TCP alive check time	This field specifies how long the OnCell G3150A-LTE will wait for a response to "keep alive" packets before closing the TCP connection. The OnCell G3150A-LTE checks 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 G3150A-LTE will force the existing TCP connection to close. For socket and device control modes, the OnCell G3150A-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 and will not send any "keep alive" packets.	7 min
 ATTENTION You should make sure the inactivity time value used here is less than the inactivity time value on the GSM/GPRS configuration page. The GSM/GPRS connection must be maintained in order to achieve the inactivity time behavior of the TCP connection		
Inactivity time	This field specifies how long the OnCell G3150A-LTE will wait for incoming and outgoing data through the serial port before closing the TCP connection. The TCP connection is closed if there is no incoming or outgoing data through the serial port for the specified Inactivity time . If this field is set to 0 , the TCP connection is kept active until a connection close request is received.	0ms

Setting	Description	Factory Default
 <p>ATTENTION If used, the Inactivity time setting should be greater than the Force transmit time. To prevent the unintended loss of data due to the session being disconnected, it is highly recommended that this value is set large enough so that the intended data transfer is completed.</p>		
 <p>ATTENTION Inactivity time is ONLY active when Connection Control (see below) is set to Any character/Inactivity time.</p>		
<p>Ignore jammed IP</p>	<p>This option determines how the port will proceed if multiple hosts are connected and one or more of the hosts stop responding as the port is transmitting data. If you select Disable, the port will wait until the data has been transmitted successfully to all hosts before transmitting the next group of data. If you select Enable, the port will ignore the host that stopped responding and continue data transmission to the other hosts.</p>	<p>Disable</p>
<p>Destination address 1 through 4</p>	<p>Specifying an IP address allows the OnCell G3150A-LTE to connect actively to the remote host. At least one destination must be provided.</p>	<p>None</p>
<p>TCP port</p>	<p>This is the TCP port number assignment for the serial port on the OnCell G3150A-LTE. It is the port number that the serial port uses to listen to connections, and that other devices must use to contact the serial port. To avoid conflicts with well-known TCP ports, the default is set to 4001.</p>	<p>4001</p>
<p>Command port</p>	<p>The Command port is the TCP port for listening to SSDK commands from the host. In order to prevent a TCP port conflict with other applications, the user can set the Command port to another port if needed.</p>	<p>966</p>
 <p>ATTENTION Up to 4 connections can be established between the OnCell G3150A-LTE and hosts. The connection speed or throughput may be low if any one of the four connections is slow, since the one slow connection will slow down the other 3 connections.</p>		
 <p>ATTENTION The Destination IP address parameter can be the IP address, domain name, or the name defined in the host table. For some applications, the user may need to send the data actively to the remote destination domain name.</p>		
<p>Designated local port 1 through 4</p>	<p>Use these fields to specify designated local ports or leave blank and designated by system.</p>	<p>0</p>
<p>Connection control</p>	<p>This setting determines the parameters under which a TCP connection is established or disconnected. The different options are given in the following table. In general, both the Connect condition and Disconnect conditions are given.</p>	<p>Startup/ None)</p>

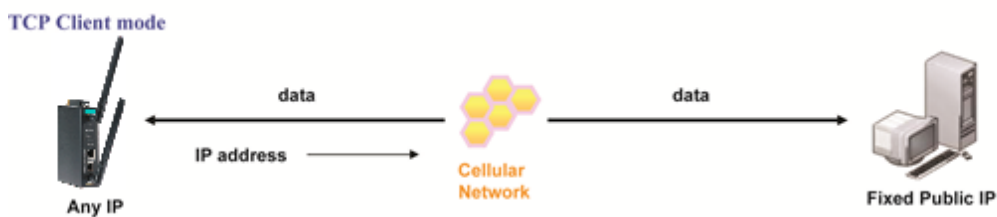
Setting	Description	Factory Default
Option	Description	
Startup/None (default)	A TCP connection will be established on startup, and will remain active indefinitely.	
Any Character/None	TCP connection will be established when any character is received from the serial interface, and will remain active indefinitely.	
Any Character/ Inactivity Time	A TCP connection will be established when any character is received from the serial interface, and will be disconnected when Inactivity time is reached.	
DSR On/DSR Off	A TCP connection will be established when a DSR signal of OnCell is "On", and will remain active indefinitely.	
DSR On/None	A TCP connection will be established when a DSR "On" signal is received, and will remain active indefinitely.	
DCD On/DCD Off	A TCP connection will be established when a DCD signal of OnCell is "On", and will remain active indefinitely.	
DCD On/None	A TCP connection will be established when a DCD "On" signal is received, and will remain active indefinitely.	
Packing length	The Packing length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. At the default of 0 for packet length, no maximum amount is specified and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.	0
Delimiter 1 Delimiter 2	When Delimiter 1 is enabled, the serial port will queue the data in the buffer and send the data to the Cellular or Ethernet port when a specific character, entered in hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to control when data should be sent.	00
 ATTENTION In order to enable a delimiter, packet length must be set to 0. Delimiter 2 should only be enabled in conjunction with Delimiter 1 and never on its own; otherwise there may be data errors. Even when a delimiter is enabled, the OnCell G3150A-LTE will still pack and send the data when the amount of data exceeds 1 KB.		
Delimiter process	The Delimiter process field determines how the data is handled when a delimiter is received. Delimiter 1 must be enabled for this field to have effect. If Delimiters 1 and 2 are both enabled, both characters must be received for the delimiter process to take place.	Do Nothing

Setting	Description	Factory Default
	<ul style="list-style-type: none"> • Do Nothing: Data in the buffer will be transmitted when the delimiter is received. • Delimiter + 1: Data in the buffer will be transmitted after 1 additional byte is received following the delimiter. • Delimiter + 2: Data in the buffer will be transmitted after 2 additional bytes are received following the delimiter. • Strip Delimiter: Data in the buffer is first stripped of the delimiter before being transmitted. 	
Force transmit	<p>This parameter defines how large a gap in serial communication the OnCell G3150A-LTE will allow before packing the serial data in its internal buffer for network transmission.</p> <p>As data is received through the serial port, it is stored by the OnCell G3150A-LTE in the internal buffer. The OnCell G3150A-LTE transmits the data stored in the buffer via TCP/IP when the internal buffer is full or as specified by the force-transmit time.</p> <p>When this field is set to 0, the force transmit time is disabled and transmission is determined solely by the data in the internal buffer. When the force transmit time is set to a value from 1 to 65535, the TCP/IP protocol software will pack the serial data received for transmission after the gap in serial communication exceeds the specified force transmit time.</p> <p>The optimal force-transmit time setting depends on your application. However, it must be set to a value that is more than one-character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is (10 (bits) / 1200 (bits/s)) × 1000 (ms/s) = 8.3 ms. Therefore, you should set the force transmit time to be greater than 8.3 ms, so in this case, it must be greater than or equal to 10 ms.</p> <p>If it is necessary to send a series of characters in the same packet, the serial device will need to send that series of characters within the specified force transmit time, and the total length of data must be less than or equal to the OnCell G3150A-LTE’s internal buffer size (1 KB per port).</p>	0 ms

Types of TCP Client Connection

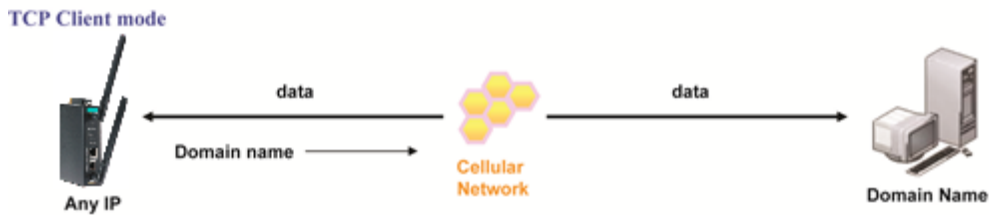
TCP Client to PC’s IP address

The OnCell G3150A-LTE will only be able to connect to a host PC if the PC is using a public IP address.



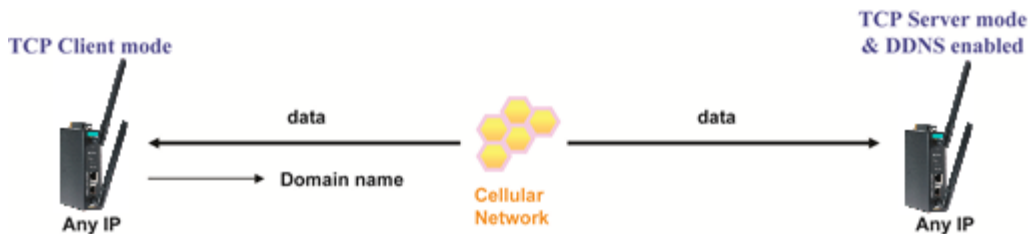
TCP Client to PC's domain name

To connect to a host PC, the host PC must be configured with public IP address. If it is using a dynamic public IP, then the OnCell G3150A-LTE can connect to it using the host's domain name. Please refer to Appendix B for more information.



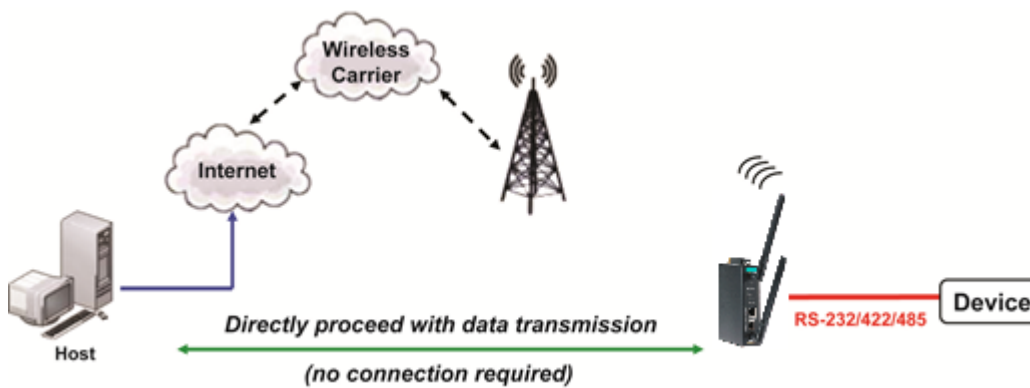
Connecting TCP client and TCP server within the same cellular service provider

In order to connect properly, the IP addresses of the two OnCell devices must belong to the same subnetwork. To ensure that this is the case, use the same cellular service provider to connect the devices to the network. In addition, you will need to request that the cellular service provider provide you with two private IP addresses (e.g., 192.168.1.1 and 192.168.1.2).



UDP Mode

Compared to TCP communication, UDP is faster and more efficient. In UDP mode, you can unicast to one host or multicast to multiple hosts and the serial device can receive data from one or multiple host computers. These traits make UDP mode especially well-suited for message display applications.





Port 1

Application
Mode
Destination IP address 1 Begin End Port
Destination IP address 2 Begin End Port
Destination IP address 3 Begin End Port
Destination IP address 4 Begin End Port
Local listen port

Data Packing

Packing length (0 - 1024)
Delimiter 1 (Hex) Enable
Delimiter 2 (Hex) Enable
Delimiter process (Processed only when Packing length is 0)
Force transmit (0 - 65535 ms)

Setting	Description	Factory Default
Destination address 1 through 4	In UDP mode, you may specify up to 4 ranges of IP addresses for the serial port to connect to. At least one destination range must be provided.	None
 ATTENTION The maximum selectable IP address range is 64 addresses. However, when using multicast, you may enter IP addresses of the form xxx.xxx.xxx.255 in the Begin field. For example, enter 192.168.127.255 to allow the OnCell G3150A-LTE to broadcast UDP packets to all hosts with IP addresses between 192.168.127.1 and 192.168.127.254.		
Local listen port	This is the UDP port that the OnCell G3150A-LTE listens to and that other devices must use to contact the OnCell G3150A-LTE. To avoid conflicts with well-known UDP ports, the default is set to 4001.	4001
Packing length	The Packing length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. At the default of 0 for packet length, no maximum amount is specified and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.	0
Delimiter 1 Delimiter 2	When Delimiter 1 is enabled, the serial port will queue the data in the buffer and send the data to the Cellular or Ethernet port when a specific character, entered in hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to control when data should be sent.	00

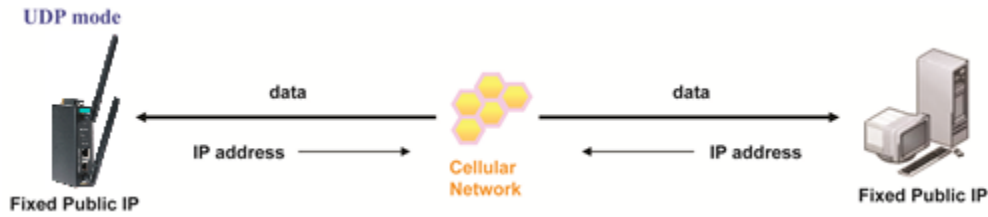

ATTENTION In order to enable a delimiter, packet length must be set to 0. **Delimiter 2** should only be enabled in conjunction with **Delimiter 1** and never on its own; otherwise there may be data errors. Even when a delimiter is enabled, the OnCell G3150A-LTE will still pack and send the data when the amount of data exceeds 1 KB.

Setting	Description	Factory Default
Delimiter process	<p>The Delimiter process field determines how the data is handled when a delimiter is received. Delimiter 1 must be enabled for this field to have effect. If Delimiters 1 and 2 are both enabled, both characters must be received for the delimiter process to take place.</p> <ul style="list-style-type: none"> • Do Nothing: Data in the buffer will be transmitted when the delimiter is received. • Delimiter + 1: Data in the buffer will be transmitted after 1 additional byte is received following the delimiter. • Delimiter + 2: Data in the buffer will be transmitted after 2 additional bytes are received following the delimiter. • Strip Delimiter: Data in the buffer is first stripped of the delimiter before being transmitted. 	Do Nothing
Force transmit	<p>This parameter defines how large a gap in serial communication the OnCell G3150A-LTE will allow before packing the serial data in its internal buffer for network transmission.</p> <p>As data is received through the serial port, it is stored by the OnCell G3150A-LTE in the internal buffer. The OnCell G3150A-LTE transmits the data stored in the buffer via TCP/IP when the internal buffer is full or as specified by the force-transmit time.</p> <p>When this field is set to 0, the force transmit time is disabled and transmission is determined solely by the data in the internal buffer. When the force transmit time is set to a value from 1 to 65535, the TCP/IP protocol software will pack the serial data received for transmission after the gap in serial communication exceeds the specified force transmit time.</p> <p>The optimal force-transmit time setting depends on your application. However, it must be set to a value that is more than one-character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is $(10 \text{ (bits)} / 1200 \text{ (bits/s)}) \times 1000 \text{ (ms/s)} = 8.3 \text{ ms}$. Therefore, you should set the force transmit time to be greater than 8.3 ms, so in this case, it must be greater than or equal to 10 ms.</p> <p>If it is necessary to send a series of characters in the same packet, the serial device will need to send that series of characters within the specified force transmit time, and the total length of data must be less than or equal to the OnCell G3150A-LTE's internal buffer size (1 KB per port).</p>	0 ms

Types of UDP Connection

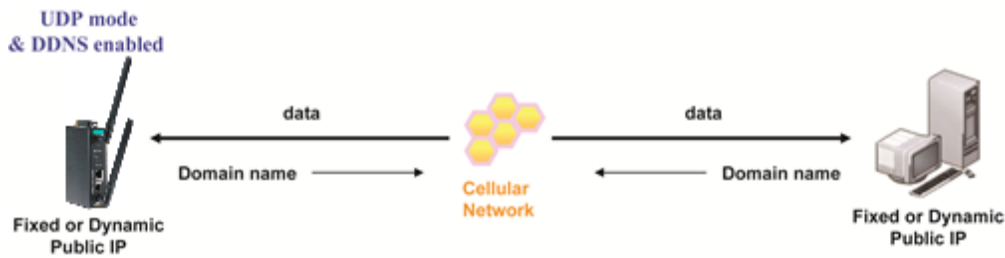
Fixed Public IPs for both OnCell and Host PC

If your cellular service provider offers a fixed public IP address after you connect to the cellular network, you can access the OnCell G3150A-LTE from a host PC that has a fixed public IP.



Domain name with DDNS

If your cellular service provider assigns a public IP address after you connect to the cellular network, you can also access the OnCell G3150A-LTE using the domain name. If your service provider assigns a public IP address (either fixed or dynamic) to your cellular device and your control center is the side that initiates the connection, you can enable the DDNS function and UDP mode to allow other devices on the Internet to connect to your device using its domain name. This will ensure that your device will remain reachable even when its public IP address is updated. Note that you will need to register your device with a DDNS server. Please refer to Appendix B for more information.



Communication Parameters

Communication Parameters

Port

Port alias

Setting	Description	Factory Default
Port alias	This optional field allows you to assign an alias to a port for easier identification.	None

Serial Parameters

Baud rate

Data bits

Stop bits

Parity

Flow control

FIFO Enable Disable

Interface

**ATTENTION**

The serial parameters for the each serial port on the OnCell G3150A-LTE should match the parameters used by the connected serial device. You may need to refer to your serial device's user's manual to determine the appropriate serial communication parameters.

Setting	Description	Factory Default
Baudrate	This field configures the port's baudrate. Select one of the standard baudrates from the dropdown box, or select Other and then type the desired baudrate in the input box.	115200
ATTENTION The serial parameters for the each serial port on the OnCell G3150A-LTE should match the parameters used by the connected serial device. You may need to refer to your serial device's user's manual to determine the appropriate serial communication parameters.		
Data bits	The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. At the default of 0 for packet length, no maximum amount is specified and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.	8
Stop bits	When Delimiter 1 is enabled, the serial port will queue the data in the buffer and send the data to the Cellular or Ethernet port when a specific character, entered in hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to control when data should be sent.	1
Parity	This field configures the parity parameter.	None
Flow control	This field configures the flow control type.	RTS/CTS
FIFO	This field enables or disables the 128-byte FIFO buffer. The OnCell G3150A-LTE provides FIFO buffers for each serial port, for both the Tx and Rx signals. Note, however, that you should disable the port's FIFO setting if the attached serial device does not have a FIFO buffer of its own. This is because a serial device that does not have its own buffer may not be able to keep up with data sent from the OnCell's FIFO buffer.	Disable
Interface	You may configure the serial interface to RS-232, RS-422, RS-485 2-wire, or RS-485 4-wire.	RS-232

Data Buffering/Log

The OnCell G3150A-LTE supports port buffering to prevent the loss of serial data when the Cellular or Ethernet connection is down. Port buffering can be used in Real COM, Reverse Real COM, RFC2217, TCP Server, TCP Client modes. For other modes, the port buffering settings will have no effect. The maximum buffer up to 256K, the data over 256K will overwrite previous data buffering.

Port 1

Port buffering (256K)

Enable Disable

Serial data logging (256K)

Enable Disable

Setting	Description	Factory Default
Port buffering	You may enable port buffering by setting this field to Enable .	Disable
Serial data logging	If this field is set to Yes, the OnCell G3150A-LTE will store data logs on the system RAM for all serial ports. Note that this data is not saved when the OnCell G3150A-LTE is powered off.	Disable

Logs and Notification

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 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 G3150A-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 logging** check box to enable the selected event types. All default values are enabled (checked). The log for system events can be seen in **Logs and Notifications > System Log**.

System Log Event Types

Event Type	<input type="checkbox"/> Enable Logging
System-related events	<input checked="" type="checkbox"/> Active
Network-related events	<input checked="" type="checkbox"/> Active
Configuration-related events	<input checked="" type="checkbox"/> Active
Power events	<input checked="" type="checkbox"/> Active
DI events	<input checked="" type="checkbox"/> Active
VPN events	<input checked="" type="checkbox"/> Active

The following table describes the types of system logs:

System-related events	Event is triggered when...
System restart (warm start)	The OnCell G3150A-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 G3150A-LTE.
Console authentication failure	An incorrect password is entered.
Firmware upgraded	The OnCell G3150A-LTE's firmware is updated.
Power events	Event is triggered when...
Power 1/2 transition (On -> Off)	The OnCell G3150A-LTE is powered down in PWR1/2.
Power 1/2 transition (Off -> On)	The OnCell G3150A-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 Type	<input type="checkbox"/> Enable Logging
System-related events	<input checked="" type="checkbox"/> Active
Network-related events	<input checked="" type="checkbox"/> Active
Configuration-related events	<input checked="" type="checkbox"/> Active
Power events	<input checked="" type="checkbox"/> Active
DI events	<input checked="" type="checkbox"/> Active
VPN events	<input checked="" type="checkbox"/> Active

Syslog Server Settings

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

Syslog Server Settings

Syslog server 1	<input type="text"/>
Syslog port	<input type="text" value="514"/>
Syslog server 2	<input type="text"/>
Syslog port	<input type="text" value="514"/>
Syslog server 3	<input type="text"/>
Syslog port	<input type="text" value="514"/>

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

E-Mail Notifications

Notification Event Types

Select the **Active** checkbox to enable an event item. By default, all values are deactivated (unchecked). For information on the event types, refer to the System Log Event Types section.

Notification Event Types

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

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)	<input type="text"/>
User name	admin
Password	••••
From e-mail address	<input type="text"/>
To e-mail address 1	<input type="text"/>
To e-mail address 2	<input type="text"/>
To e-mail address 3	<input type="text"/>
To e-mail address 4	<input type="text"/>



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 G3150A-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.	Admin

Password

Setting	Description	Factory Default
Password	This field is for your mail server's password, if required.	moxa

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 Type	<input type="checkbox"/> Enable Notification
Power 1 transition (On-->Off)	<input type="checkbox"/> Active
Power 2 transition (On-->Off)	<input type="checkbox"/> Active
DI 1 transition (On-->Off)	<input type="checkbox"/> Active
DI 1 transition (Off-->On)	<input type="checkbox"/> Active
DI 2 transition (On-->Off)	<input type="checkbox"/> Active
DI 2 transition (Off-->On)	<input type="checkbox"/> Active
LAN link on	<input type="checkbox"/> Active
LAN link off	<input type="checkbox"/> Active

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

Select Active to enable the event types.

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

Trap Event Types

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

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

SMS Alert Settings

You can set the OnCell G3150A-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

Field	Description	Factory Default
To phone number 1/2/3/4	Enter the phone numbers to which the OnCell G3150A-LTE sends SMS notifications.	

Status

Serial

Serial to Network Connections

Go to **Serial to Network Connections** under **Serial Status** to view the operation mode and status of each connection for each serial port. All monitor functions will refresh automatically every 15 seconds.

The Real COM mode, Reverse Real COM mode and TCP server mode support up to 2 devices connection, TCP Client mode support up to 4 devices connection.

Serial to Network Connections

Auto refresh

Port	OP Mode	Connections
1	Device Control/RealCOM	[192.168.127.55]

Serial Port Status

Go to **Serial Port Status** under **Serial Status** to view the current status of each serial port. **Serial Port Status Buffering** monitors port buffering usage (bytes) of the serial port. Go to **Serial Port Settings > Port 1 > Data Buffering/Log** to enable Port buffering function.

A green dot indicates active, and a gray dot indicates inactive

Serial Port Status

Auto refresh

Port	TxCnt	RxCnt	TxTotalCnt	RxTotalCnt	DSR	DTR	RTS	CTS	DCD	Buffering
1	64	68	64	68						0

Serial Port Error Count

Go to **Serial Port Error Count** under **Serial Status** to view the error count for each serial port.

Serial Port Error Count

Auto refresh

Port	ErrCnt			
	Frame	Parity	Overrun	Break
1	7	10	0	119

	Description
Frame	Errors due to wrong Baudrate, Parity (even/odd), and Stop bit settings.
Parity	Errors in parity setting (parity on / off) between both sites.
Overrun	The number of times the operation-mode application overload in order to handle the data transmission.
Break	The transmission breaks originating from serial devices connected behind the OnCell G3150A-LTE

Serial Port Settings

Go to **Serial Port Settings** under **Serial Status** to view a summary of the settings for each serial port.

Serial Port Settings

Auto refresh

Port	Baud Rate	Data Bits	Stop Bits	Parity	Flow Control		FIFO	Interface
					RTS/CTS	XON/XOFF		
1	115200	8	1	None	On	Off	Disable	RS-232

Serial Data Log

Data logs for the serial port can be viewed in ASCII or HEX format. After selecting the serial port and format, you may click **Select all** to select the entire log if you wish to copy and paste the contents into a text file. R - Receiver / T - Transmission to the serial device.

Serial Data Logs

Select port Port1

[\[ASCII\]](#)[\[HEX\]](#)

```

2016/12/5 22:38:12[R:9] Moxa-Test
2016/12/5 22:38:14[R:9] Moxa-Test
2016/12/5 22:38:16[R:9] Moxa-Test
2016/12/5 22:38:18[R:9] Moxa-Test
2016/12/5 22:38:20[R:9] Moxa-Test
2016/12/5 22:38:22[R:9] Moxa-Test
2016/12/5 22:38:24[R:9] Moxa-Test
2016/12/5 22:38:26[R:9] Moxa-Test
2016/12/5 22:38:28[R:9] Moxa-Test
2016/12/5 22:38:30[R:9] Moxa-Test
2016/12/5 22:38:32[R:9] Moxa-Test
2016/12/5 22:38:34[R:9] Moxa-Test
2016/12/5 22:38:37[R:9] Moxa-Test
2016/12/5 22:38:39[R:9] Moxa-Test
2016/12/5 22:38:41[R:9] Moxa-Test
2016/12/5 22:38:43[R:9] Moxa-Test
2016/12/5 22:38:45[R:9] Moxa-Test
2016/12/5 22:38:47[R:9] Moxa-Test
2016/12/5 22:38:49[R:9] Moxa-Test
2016/12/5 22:38:51[R:9] Moxa-Test
    
```

VPN

VPN System Log Description

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 G3150A-LTE.

System Log Entry	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.
[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.

IPSec Logs

The IPSec triggered events are recorded in IPSec Logs. 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.

```
"santiago2"[1] 49.216.148.168 #12: NAT-Traversal: Result using draft-ietf-ipsec-nat-t-ike (MacOS X): peer is NATed
"santiago2"[1] 49.216.148.168 #12: transition from state STATE_MAIN_R1 to state STATE_MAIN_R2
"santiago2"[1] 49.216.148.168 #12: STATE_MAIN_R2: sent MR2, expecting MI3
"santiago2"[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
"santiago2"[1] 49.216.148.168 #12: transition from state STATE_MAIN_R2 to state STATE_MAIN_R3
"santiago2"[1] 49.216.148.168 #12: new NAT mapping for #12, was 49.216.148.168:57473, now 49.216.148.168:57474
"santiago2"[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}
"santiago2"[1] 49.216.148.168 #12: the peer proposed: 192.168.128.0/24:0/0 -> 192.168.127.0/24:0/0
"santiago2"[1] 49.216.148.168 #12: find_client_connection starting with santiago2
"santiago2"[1] 49.216.148.168 #12: looking for 192.168.128.0/24:0/0 -> 192.168.127.0/24:0/0
"santiago2"[1] 49.216.148.168 #12: concrete checking against sr#0 192.168.128.0/24 ->
```

Export Log Clear Log Refresh

OpenVPN Status and Logs

The OpenVPN triggered events at Server and Clients are recorded in each Status and Logs.

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.

Server Status

```
OpenVPN CLIENT LISTUpdated,Thu Dec 29 09:50:26 2016Common Name,Real Address,Bytes Received,Bytes Sent,Connected Sinceadmin,101.14.19.200:41344,1068,2534,Thu Dec 29 09:50:12 2016ROUTING TABLEVirtual Address,Common Name,Real Address,Last Ref192.168.10.6,admin,101.14.19.200:41344,Thu Dec 29 09:50:14 2016192.168.128.0/24,admin,101.14.19.200:41344,Thu Dec 29 09:50:14 2016GLOBAL STATSMax bcst/mcast queue length,0END
```

Export Status Log Refresh

Server Logs

```
Thu Dec 29 09:48:15 2016 OpenVPN 2.3.10 mips-be-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [MH [IPv6] built on Dec 23 2016Thu Dec 29 09:48:15 2016 library versions: OpenSSL 1.0.0d 8 Feb 2011 LZO 2.09Thu Dec 29 09:48:15 2016 NOTE: the current --script-security setting may allow this configuration to call user-defined scriptsThu Dec 29 09:48:16 2016 WARNING: POTENTIALLY DANGEROUS OPTION --client-cert-not-required may accept clients which do not present a certificateThu Dec 29 09:48:16 2016 WARNING: file '/configData/ovpn/ovpnsvr/private/srvKey.pem' is group or others accessibleThu Dec 29 09:48:16 2016 TUN/TAP device tun0 openedThu Dec 29 09:48:16 2016 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0Thu Dec 29 09:48:16 2016 /sbin/ifconfig tun0 192.168.10.1 pointopoint 192.168.10.2 mtu 1500Thu Dec 29 09:48:16 2016 UDPv4 link local (bound): [undef]Thu Dec 29 09:48:16 2016 UDPv4 link remote: [undef]Thu Dec 29 09:48:16 2016 Initialization Sequence CompletedThu Dec 29 09:50:14 2016 101.14.19.200:41344 [admin] Peer Connection Initiated with [AF_INET]101.14.19.200:41344Thu Dec 29 09:50:14 2016 admin/101.14.19.200:41344 MULTI_sva: pool returned IPv4=192.168.10.6, IPv6=(Not enabled)Thu Dec 29 09:50:16 2016 admin/101.14.19.200:41344 send_push_reply(): safe_cap=94(
```

Export Log Clear Log Refresh

Client Status

```
OpenVPN STATISTICSUpdated,Thu Dec 29 09:52:49 2016TUN/TAP read bytes,0TUN/TAP write bytes,0TCP/UDP read bytes,3170TCP/UDP write bytes,1810Auth read bytes,192pre-compress bytes,0post-compress bytes,0pre-decompress bytes,0post-decompress bytes,0END
```

Export Status Log Refresh

Client Logs

```
Thu Dec 29 09:50:09 2016 OpenVPN 2.3.10 mips-be-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [MH] [IPv6] built on Dec 23 2016Thu Dec 29 09:50:09 2016 library versions: OpenSSL 1.0.0d 8 Feb 2011, LZO 2.09Thu Dec 29 09:50:09 2016 WARNING: file '/var/ovpn/ovpncli/ovpnclient1.secret' is group or others accessibleThu Dec 29 09:50:09 2016 NOTE: the current --script-security setting may allow this configuration to call user-defined scriptsThu Dec 29 09:50:09 2016 Socket Buffers: R=[114688->114688] S=[114688->114688]Thu Dec 29 09:50:09 2016 UDPv4 link local: [undef]Thu Dec 29 09:50:09 2016 UDPv4 link remote: [AF_INET]42.68.153.20:11943Thu Dec 29 09:50:12 2016 TLS: Initial packet from [AF_INET]42.68.153.20:11943, sid=1ff6915e 7fedf748Thu Dec 29 09:50:12 2016 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent thisThu Dec 29 09:50:13 2016 VERIFY OK: depth=1, C=TW, ST=Taiwan, L=Taipei, O=MOXA, OU=IW, emailAddress=info@moxa.com, CN=OnCell-G3150A-LTEThu Dec 29 09:50:13 2016 VERIFY OK: nsCertType=SERVERThu Dec 29 09:50:13 2016 VERIFY OK: depth=0, C=TW, ST=Taiwan, O=MOXA, OU=IW, CN=OnCell-G3150A-LTE, emailAddress=info@moxa.comThu Dec 29 09:50:13 2016 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit keyThu Dec 29 09:50:13 2016 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authenticationThu Dec 29
```

Export Log Clear Log Refresh

- NOTE**
- *Status:* You can view OpenVPN connection status such as OpenVPN is connected, disconnected and initiating connection and information on the client’s access to the server in the server logs.
 - *Logs:* The Logs show more detailed information than the Status and provide engineers with information for review and trouble shooting. Additional information includes negotiation process, key exchange, and error recordings.

DNS Status

The **DNS Status** screen displays the DNS server to which the OnCell G3150A-LTE is connected and the DNS server information.

Go to DNS Status for DNS server settings information designated at General Setup > Network Settings.

It shows OnCell G3150A-LTE’s DNS assigned by DNS server and Server 3/4 is stand for Primary DNS and Secondary DNS information at General Setup > Network Settings

DNS Status

Auto Update

	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 G3150A-LTE.

SIM Status

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

GPS Status

The **GPS Status** screen displays various GPS related information including Time, Latitude, Longitude, Connected satellites, and Altitude.

GPS Status

Auto Update

Name	Data	Description
Time	05:54:33	UTC of Position
Latitude	24.986216 N	2459.103765 N (Latitude, N or S)
Longitude	121.553787 E	12133.136177 E (Longitude, E or W)
Number of Satellites in use	04	Satellites are in view
Altitude	203.1 M	Antenna altitude above/below mean sea level (geoid) Meters (Antenna height unit)

DHCP Client List (For AP Mode Only)

The DHCP Client List shows all the clients that require and have successfully received IP assignments. You can click the **Refresh** button to refresh the list.

DHCP Client List

MAC	IP
1. 00:13:ce:e1:ee:ef	192.168.127.2

Select all Refresh

You can press **Select all** button to select all content in the list for further editing.

MAC	IP
1. 00:13:ce:e1:ee:ef	192.168.127.2

- Cut
- Copy
- Paste
- Select All
- Print

Select all Refresh

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, Power, and System Status

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

DI and Power Status

Auto refresh

Input Status	On / Off
Power 1 status	Off
Power 2 status	On
DI 1 status	Off
DI 2 status	Off

System Status

The System Status screen displays the OnCell G3150A-LTE internal memory capacity status and CPU loading information.

System Status

Memory Info		
Total	(kB)	126472
Used	(kB)	32828
Free	(kB)	93644
CPU Info		
Usage	(%)	0.04

Refresh

Network Status

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

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
UDP	REchoRply	0			SEchoRply	0
	Received	5			Sent	969
TCP	ErrHeader	0	ErrPorts	964		
	Received	85			Sent	84
TCP	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)

ARP Table

The ARP table is for maintenance people to ping the destination device and get the destination MAC address so as to clarify the connection issue.

ARP Table

IP Address	Mac Address
192.168.127.3	6C:C2:17:7D:6D:DA

Refresh

LLDP

The LLDP displays the information of the device that connected to OnCell G3150A-LTE.

LLDP Status

Interface	Neighbor Information				
	System Name	ID	IP	Port	Port Description

Refresh

Field	Description	Default setting
Interface	The device physical internet interface, such as Wi-Fi, Cellular and Ethernet port.	Interface
System Name	A user-defined device system name.	System Name
ID	A user-defined device ID.	ID
IP	The device IP address	IP

Ping Command

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 G3150A-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 G3150A-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 G3150A-LTE will reboot itself.

When upgrading your firmware, the OnCell G3150A-LTE's other functions will not be accessible.

Firmware Upgrade

Select firmware file No file chosen



ATTENTION

Please make sure the power source is stable when you upgrade your firmware. An unexpected power disruption may damage your OnCell G3150A-LTE.

Configuration Import & Export

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

- Configuration settings on the OnCell G3150A-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. The password is up to 31 characters.

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 using a general SNMP tool and use to remotely control or configure the OnCell G3150A-LTE.

Configuration Import & Export

Configuration File Encryption Setting (Excluding ABC-01)

Encryption of import/export configuration

Enable Disable

Password

Apply

Configuration Import

Select configuration file

Choose File No file chosen

Import Configuration

Configuration Export

Export Configuration

ABC-01 Configuration Import

Import Configuration

ABC-01 Configuration Export

Export Configuration

SNMP MIB file Export

Export MIB

To download the configuration to the OnCell G3150A-LTE, complete the following steps:

1. Turn off the OnCell G3150A-LTE.
2. Connect ABC-01 to the OnCell G3150A-LTE's RS-232 console.
3. Turn on the OnCell G3150A-LTE.
4. The OnCell G3150A-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 G3150A-LTE emits three short beeps before continuing the boot up process.
5. After the boot up process is complete, the OnCell G3150A-LTE emits two beeps, and the **Ready** LED turns solid green.

Load Factory Default

Use this function to reset the OnCell G3150A-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 G3150A-LTE.

Load Factory Default

Reset to Factory Default Values

Click "**System Reset**" to reset all system settings, including the console password, to factory default values.

The system will be restarted immediately after the reset to factory default values.

Account Settings

To ensure that devices located at remote sites are secure from hackers, we recommend setting up a high-strength password the first time you configure the device.

Password Policy

Minimum password length (4 - 16 characters)
Password strength check
Password validity (0 - 365 days, 0 is disable)
Password retry count (0 - 10, 0 is disable)
Lockout time (60 - 3600 seconds)

Account List

No.	Active	Account Name	User Level	HTTP/HTTPS	Telnet/SSH /Console	Moxa Services	Diagnostics	Action
1	<input checked="" type="checkbox"/>	admin	Admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
2	<input type="checkbox"/>		Admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
3	<input type="checkbox"/>		Admin User	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
4	<input type="checkbox"/>		Admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
5	<input type="checkbox"/>		Admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
6	<input type="checkbox"/>		Admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
7	<input type="checkbox"/>		Admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
8	<input type="checkbox"/>		Admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

* Only characters allowed in the Account Name are alphabets, numerals, at sign (@), period (.), and underscore(_).

Field	Description	Default setting
Minimum password length	By default, passwords can be between 4 and 16 characters. For improved security, we recommend changing the minimum password length to at least 8 characters the first time you configure the device.	4
Password strength check	Enable the password strength check option to ensure that users are required to select high-strength passwords. Note: See the Change Password section below for details.	Disable
Password validity	The number of days after which the password must be changed. Passwords should be updated regularly to protect against hackers.	90 days
Password retry count	The number of consecutive times a user can enter an incorrect password while logging in before the device's login function is locked.	5
Lockout time	The number of seconds the device's login function will be locked after n consecutive unsuccessful login attempts, where n = the password retry count.	600 seconds

Click **Edit** to create a new, or edit an existing, user account. The items shown below can be configured.

Account Settings

Active

User level

Account name (A-Z, a-z, 0-9, '@', '.', and '_')

New Password

Confirm Password

- Your password must follow the password policy.
- The minimum password length is 4 characters.

Accessible Access Portal

HTTP/HTTPS Enable Disable

Telnet/SSH/Console Enable Disable

Moxa Service Enable Disable

Diagnostic Enable Disable

Field	Description	Default Setting
Active	Select Enable to enable the user account.	Disable
User level	Administrator: Allows the user to access the Web UI, change the device's configuration, and use the device's import/export capability. User: Allows the user to access the Web UI, but the user will not be able to change the device's configuration or use the device's import/export capability.	Admin
Account name	The username of the account.	Admin
New Password	The password used to log in to the device.	moxa
Confirm Password	Retype the password. If the Confirm Password and New Password fields do not match, you will be asked to reenter the password.	N/A

Change Password

Use the **Change Password** function to change the 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.

Note: 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.

Change Password

Current password

New password

Confirm password

- Your password must follow the password policy.
- The minimum password length is 4 characters.

NOTE If the **Password-strength test** option is enabled, you will be prompted to use passwords that adhere to the following password policy:

- The password must contain at least one digit: 0, 1, 2, ..., 9.
- The password must contain both upper and lower case letters:
A, B, ..., Z, a, b, ..., z.
- The password must contain at least one of the following special characters:
~!@#\$%^&*_-_|;:.,<>[]{}
- The password must have more characters than the minimum password length (default = 4).

Miscellaneous Settings

Additional settings that help you manage your OnCell G3150A-LTE are available on this page.

Miscellaneous Settings

Reset button Always enable Disable factory reset function after 60 seconds.

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

- **Always enable**—Set the reset button to perform a factory restore on the OnCell G3150A-LTE. This is the default option.
- **Disable factory reset function after 60 seconds**—Deactivate the factory reset function of the reset button 60 seconds after the OnCell G3150A-LTE restarts.

Troubleshooting

Troubleshooting

Export current device information

Export

Diagnostics

Diagnostic script

Choose File No file chosen

Export diagnostic results

to a file to a TFTP server

TFTP sever IP

Diagnostic script name

N/A

Last start time

N/A

Last end time

N/A

Diagnostic status

Diagnostic result

N/A

Run Script

Stop Script

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 item number
- The time the message was sent
- The destination phone number
- Status of the message—Information on whether the SMS was successfully sent.

Manual SMS

Manual Sending SMS Settings

Phone number

SMS content (Max. 160 characters)
 Characters remaining: 160

Note: Special characters such as '^', '\', '|', '\n', '\r', '\t', '\{', and '\}' require two bytes.

Remote SMS Control

In cases where the OnCell G3150A-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 G3150A-LTE or restart the OnCell G3150A-LTE.

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

Remote SMS Control

Remote SMS control Disable ▾

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
Upgrade firmware remotely	<input type="checkbox"/>	<input type="checkbox"/>	@password@upgrade@URL
Change OCM IP address	<input type="checkbox"/>	<input type="checkbox"/>	@password@ip.change@IP
Start cellular connection	<input type="checkbox"/>	<input type="checkbox"/>	@password@cellular.start
Stop cellular connection	<input type="checkbox"/>	<input type="checkbox"/>	@password@cellular.stop
Start IPsec connection	<input type="checkbox"/>	<input type="checkbox"/>	@password@ipsec.start
Stop IPsec connection	<input type="checkbox"/>	<input type="checkbox"/>	@password@ipsec.stop
Start OpenVPN connection	<input type="checkbox"/>	<input type="checkbox"/>	@password@openvpn.start
Stop OpenVPN connection	<input type="checkbox"/>	<input type="checkbox"/>	@password@openvpn.stop

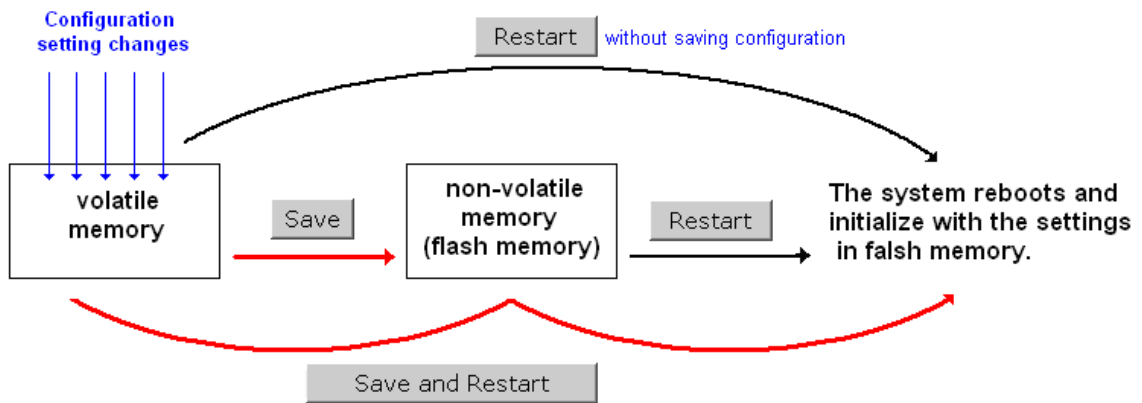
Field	Description	Default Setting
Remote SMS Control	Select Enable to activate the remote SMS control feature.	Disable
Password	Enter a password (4 to 16 characters).	N/A
Auth type	To restrict access to the OnCell G3150A-LTE, select the Caller ID authentication type.	None
Caller ID	If you use the caller ID authentication type, enter the caller ID number that can send SMS control messages to the OnCell G3150A-LTE.	N/A
Action	Select this check box to perform the SMS control action.	
Acknowledge	Select this check box to send a reply to the SMS sender after the operation is completed.	

For example, if you enter "12345" for the password and send an SMS message with the content "@12345@cell.report" to the OnCell G3150A-LTE, the OnCell G3150A-LTE sends an SMS message with the current status back to the sender.

Saving Configuration

The following figure shows how the OnCell G3150A-LTE stores the configuration changes into volatile and non-volatile memory. All data stored in volatile memory will be erased when the OnCell G3150A-LTE is shutdown or rebooted. Because the OnCell G3150A-LTE starts up and initializes with the settings stored in flash memory, all new changes must be saved to the flash memory before restarting the OnCell G3150A-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 changes will remain in the non-volatile memory until you save the configurations.

Save Configuration

You must save the changes and restart the system for configuration changes to take effect. Click **Save** to save configuration changes to the system memory.



Network Settings After Reboot

Network Info	
LAN IP address	192.168.126.254
LAN subnet mask	255.255.0.0

Restart

If you submitted configuration changes, you will see a blinking message 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 the changes, you will be given two options. Clicking the **Restart** button will reboot the OnCell G3150A-LTE directly, and all changes will be ignored. Clicking the **Save and Restart** button will apply all changes before rebooting the OnCell G3150A-LTE.

Restart

!!! Warning !!!

Click **Restart** to discard configuration changes and restart the system.

Click **Save and Restart** to save configuration changes and restart the system.

Scheduled Restart

Restart time 1 Enable : (HH:MM)

Restart time 2 Enable : (HH:MM)

Network Settings After Reboot

Network Info

LAN IP address	192.168.127.254
LAN subnet mask	255.255.255.0

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.

The configuration has been changed without saving to flash.
Do you want to restart the device anyway?

You will not be able to run any of OnCell G3150A-LTE's functions while the device is rebooting.

You can use the **Scheduled Restart** function to schedule automatic reboot of the OnCell device by specifying up to two restart times (HH:MM) per day. To set up a scheduled restart, click on the Enable box for the Restart time 1 or 2, enter the time and click **Submit**.

Logout

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

Logout

Click **Logout** to log out of the web console.

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

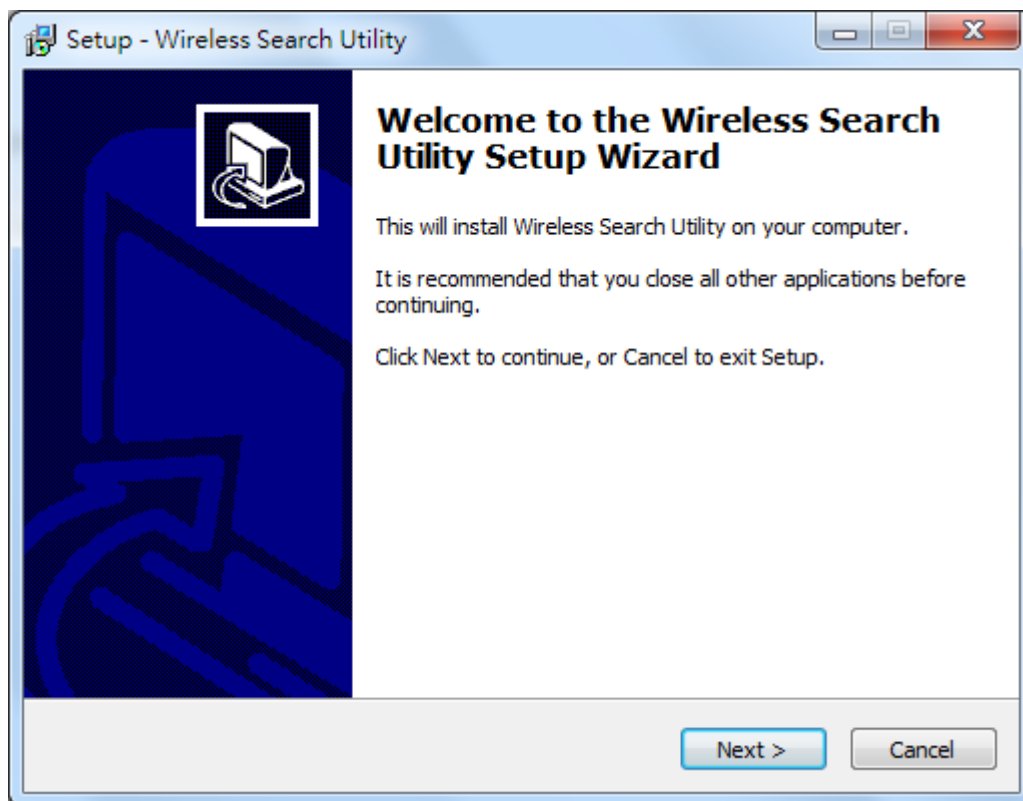
The Documentation & Software CD included with your OnCell G3150A-LTE is designed to make the installation and configuration procedure easy and straightforward. This auto-run CD includes the Wireless Search Utility (to broadcast search for all OnCell G3150A-LTE units accessible over the network), the OnCell G3150A-LTE User's Manual, and Quick Installation Guide.

Wireless Search Utility

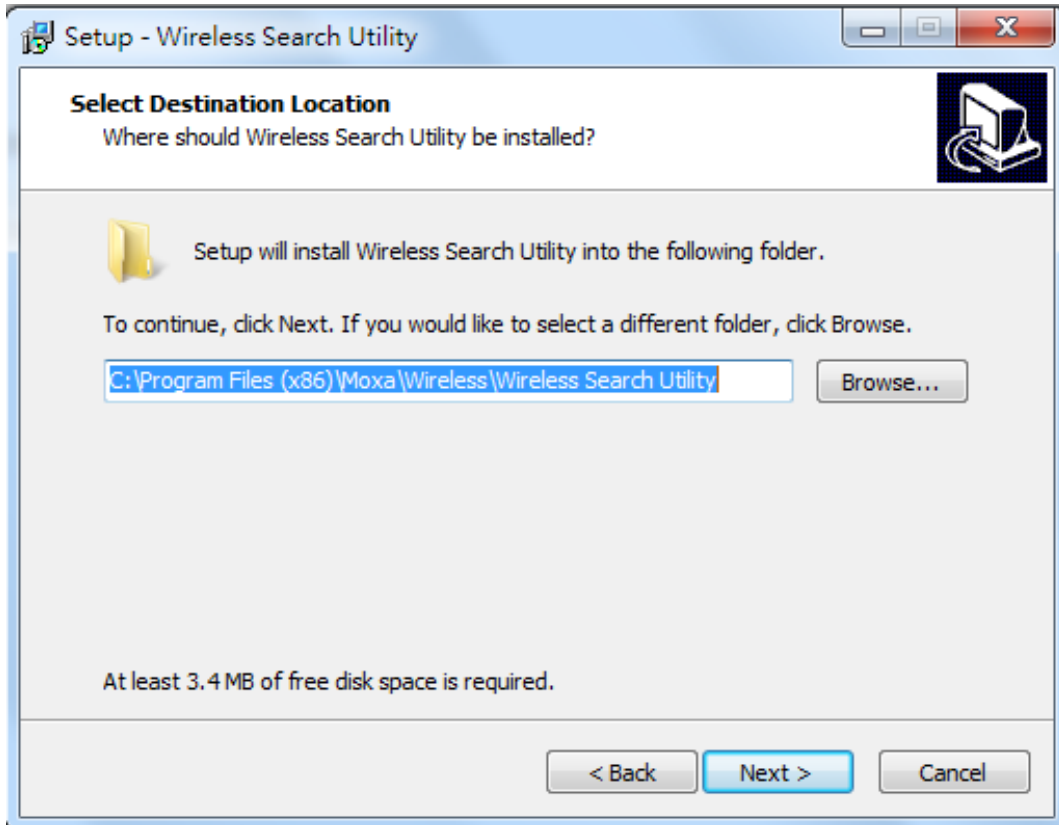
Installing the Wireless Search Utility

Download the executable for the Wireless Search Utility from the Moxa website and run it. In the installation screen, click **Yes** to proceed.

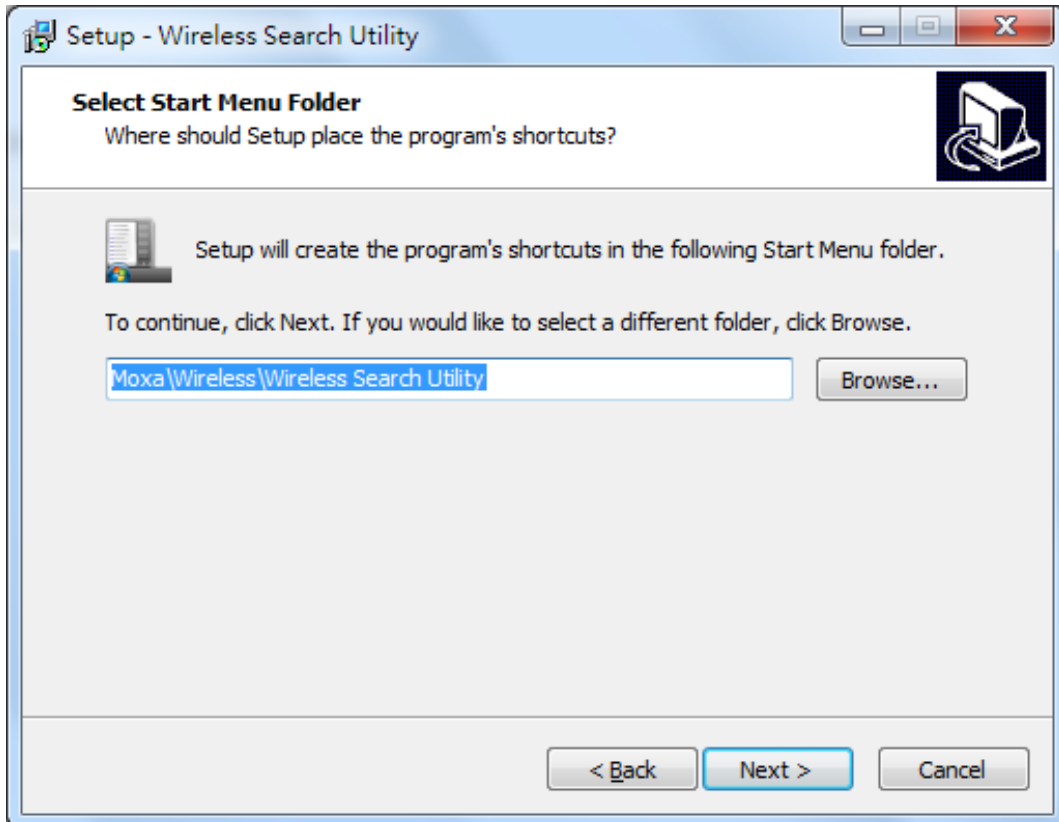
1. In the welcome screen, click **Next** to proceed with the installation.



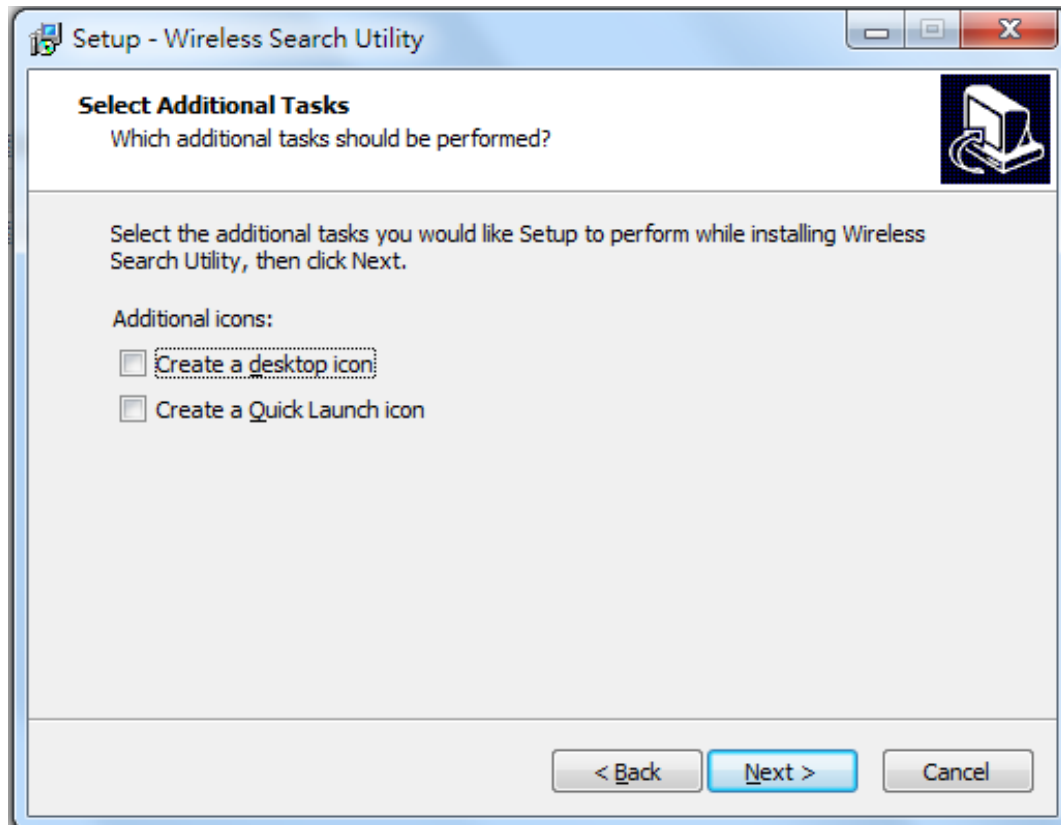
2. Click **Next** to install program files to the default directory, or click **Browse** to select an alternate location.



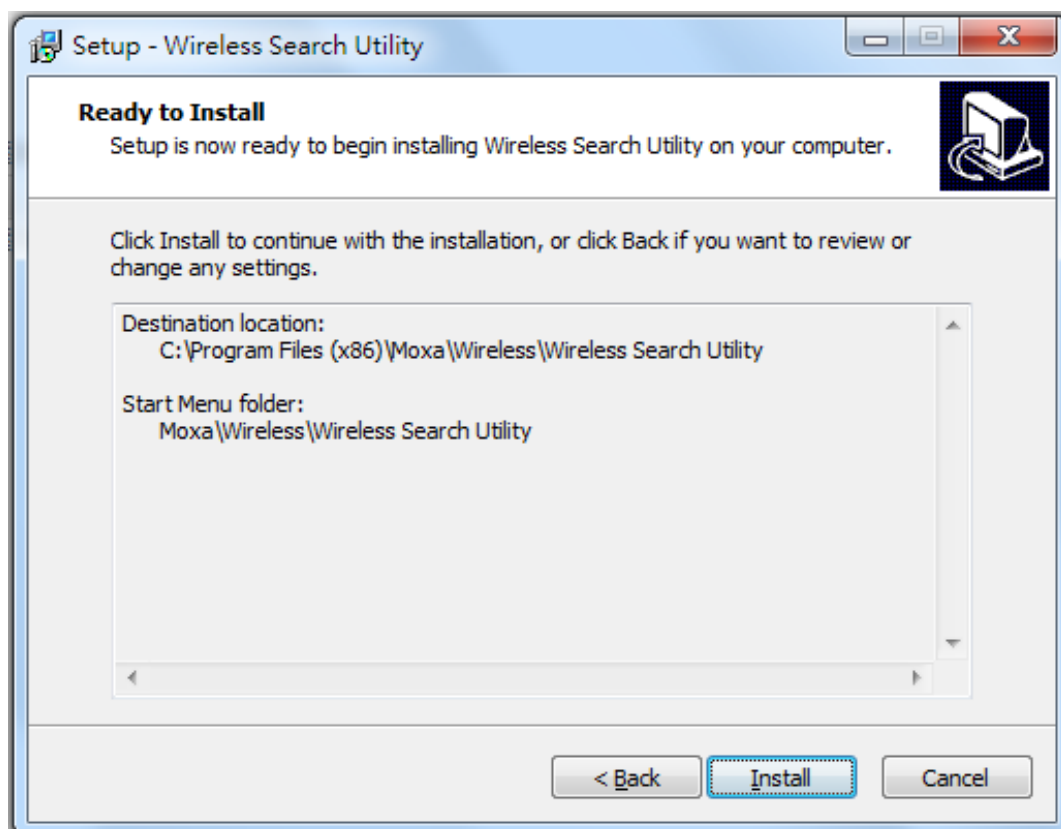
3. Click **Next** to create the program's shortcut files to the default directory, or click **Browse** to select an alternate location.



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

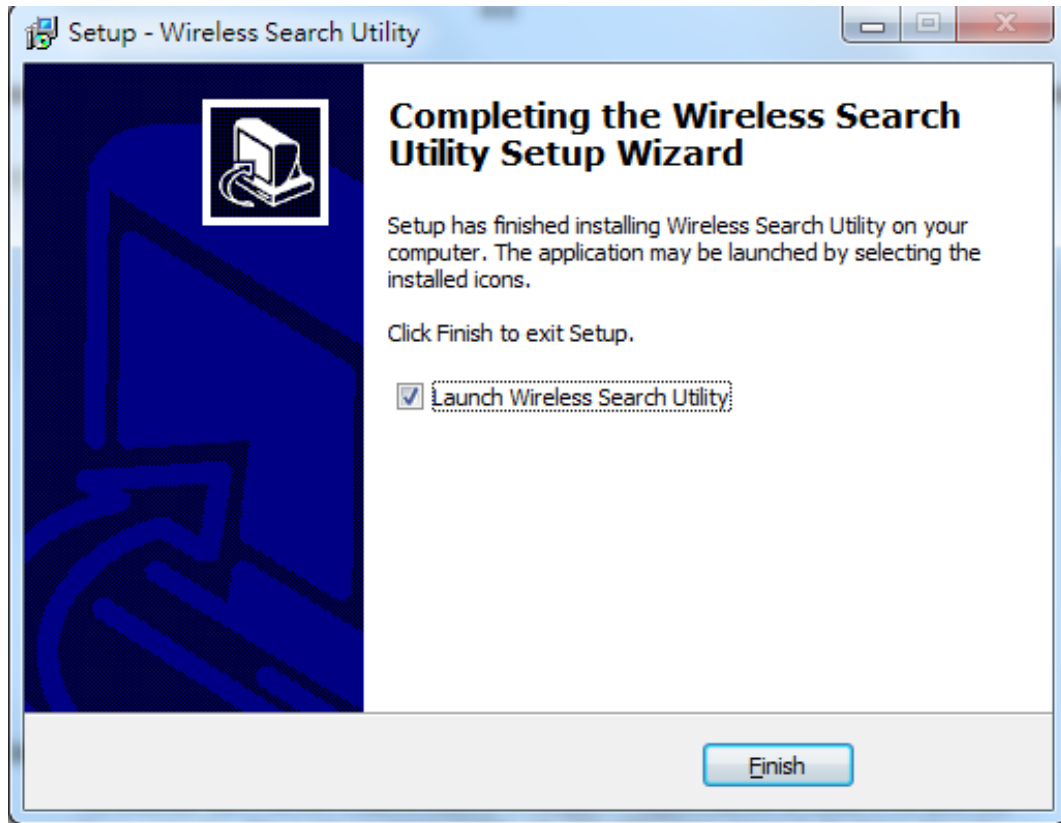


- Click **Next** to proceed with the installation. The installer then displays a summary of the installation options.



- 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.

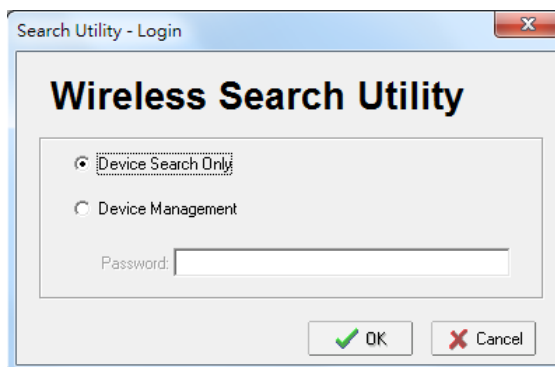
7. Click **Finish** to complete the installation of the Wireless Search Utility.



Configuring the Wireless Search Utility

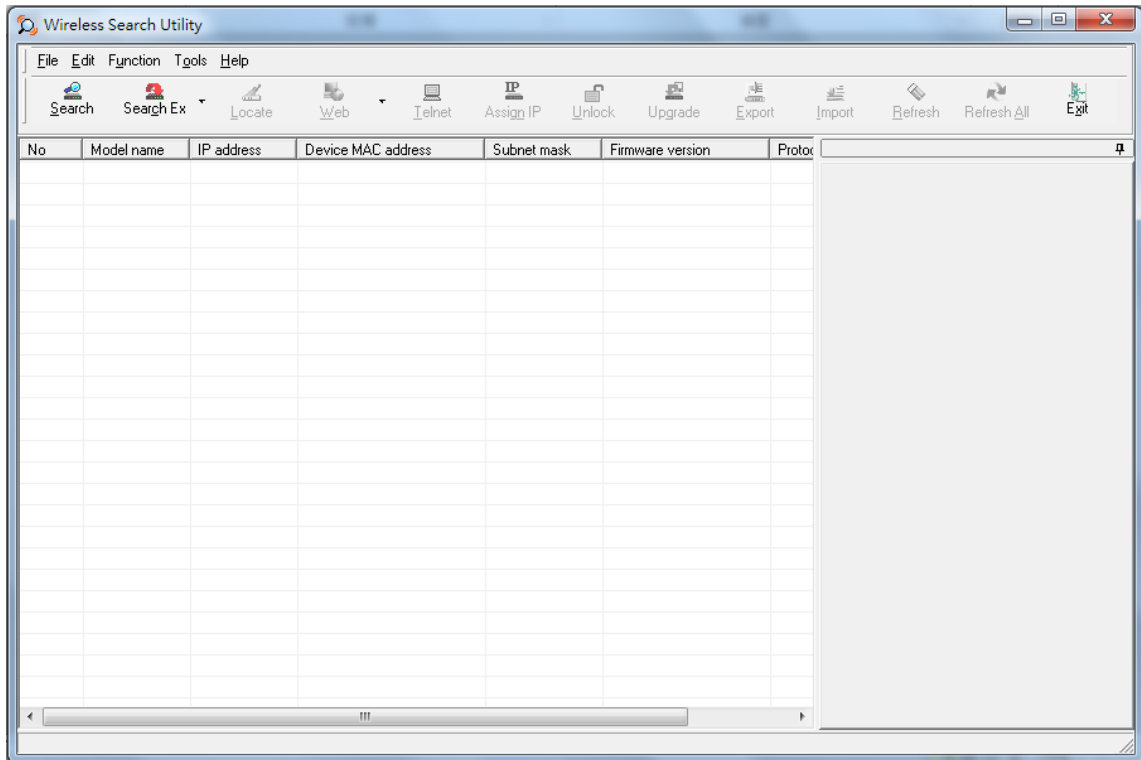
The Broadcast Search function is used to locate all OnCell G3150A-LTE APs that are connected to the same LAN as your computer. After locating an OnCell G3150A-LTE, you will be able to change its IP address since the Broadcast Search function searches by UDP packet and not IP address.

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 G3150A-LTE units and to view each OnCell G3150A-LTE's configuration.
 - **Device management**—Assign IP addresses, upgrade firmware, and locate devices.

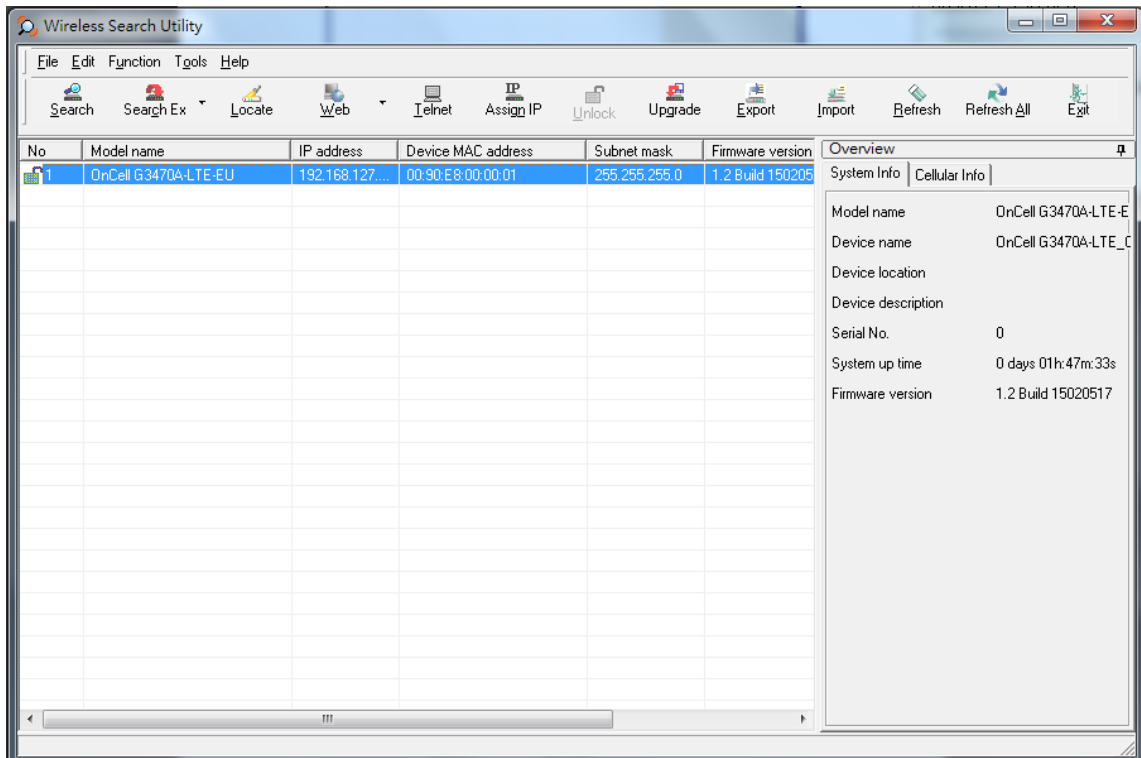


NOTE To apply device search and management, ensure your device at factory default setting or remove your SIM card. This is to avoid assigned IP different from default subnet and result in function failure.

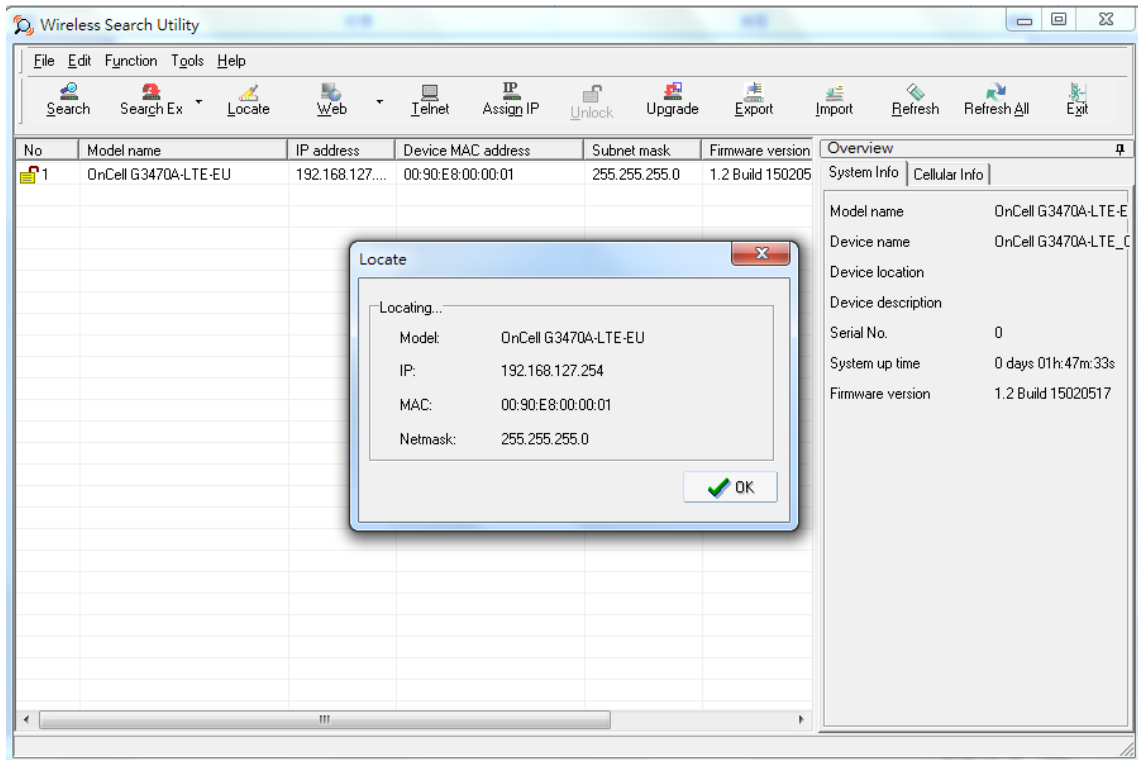
3. Click **Search**.



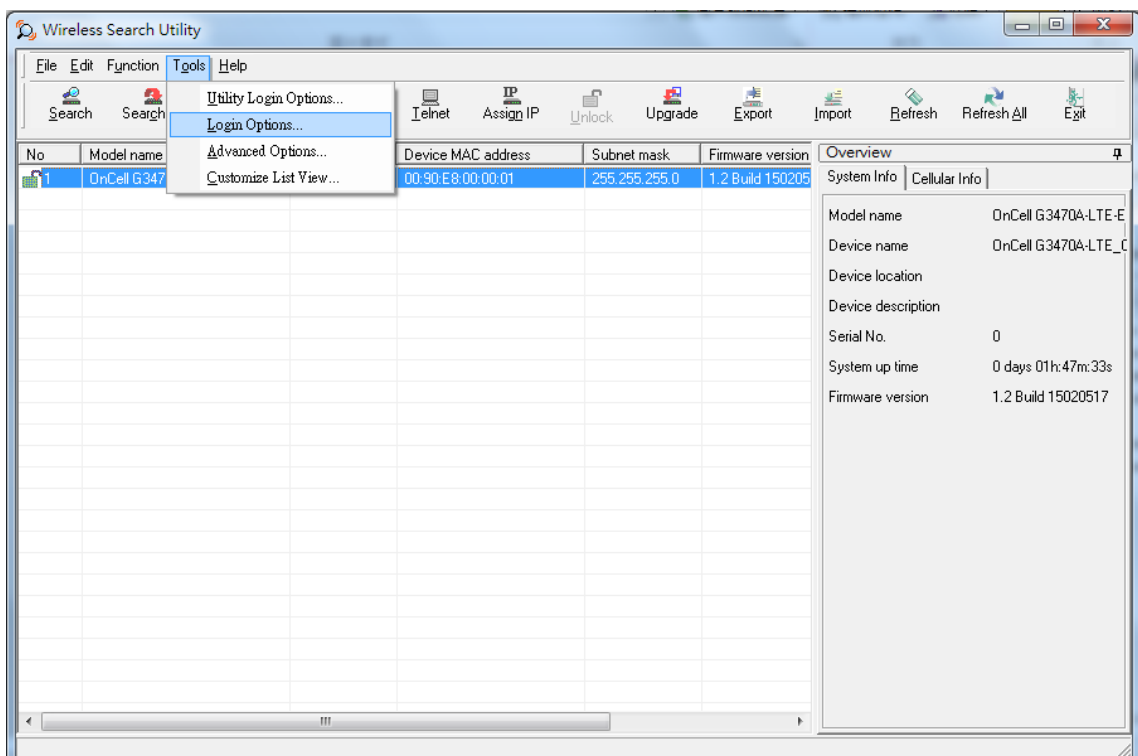
4. The "Searching" window indicates the progress of the search. When the search is complete, all devices that were located will be displayed in the Wireless Search Utility window.



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

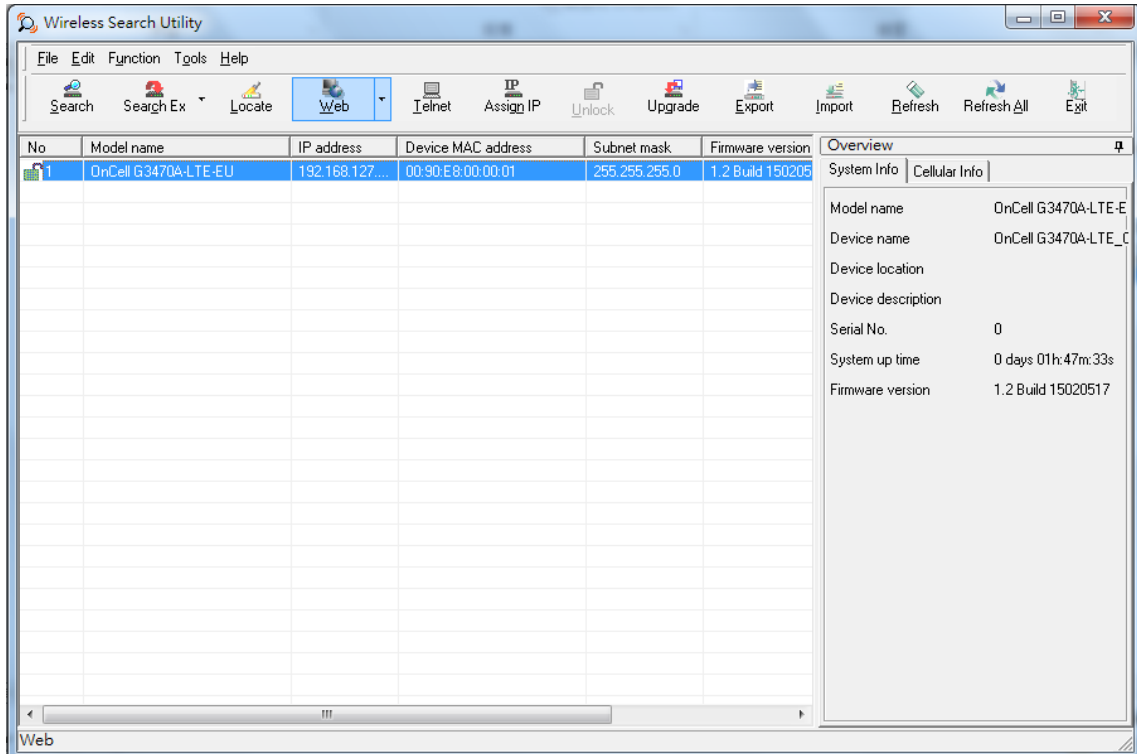


- Make sure that your device is **unlocked** before using the search utility's icons setting. The device will unlock automatically if the password is set to the default. Otherwise you must enter the new password manually.
- Go to **Tools > Device login Options** to manage and unlock additional AWKs.

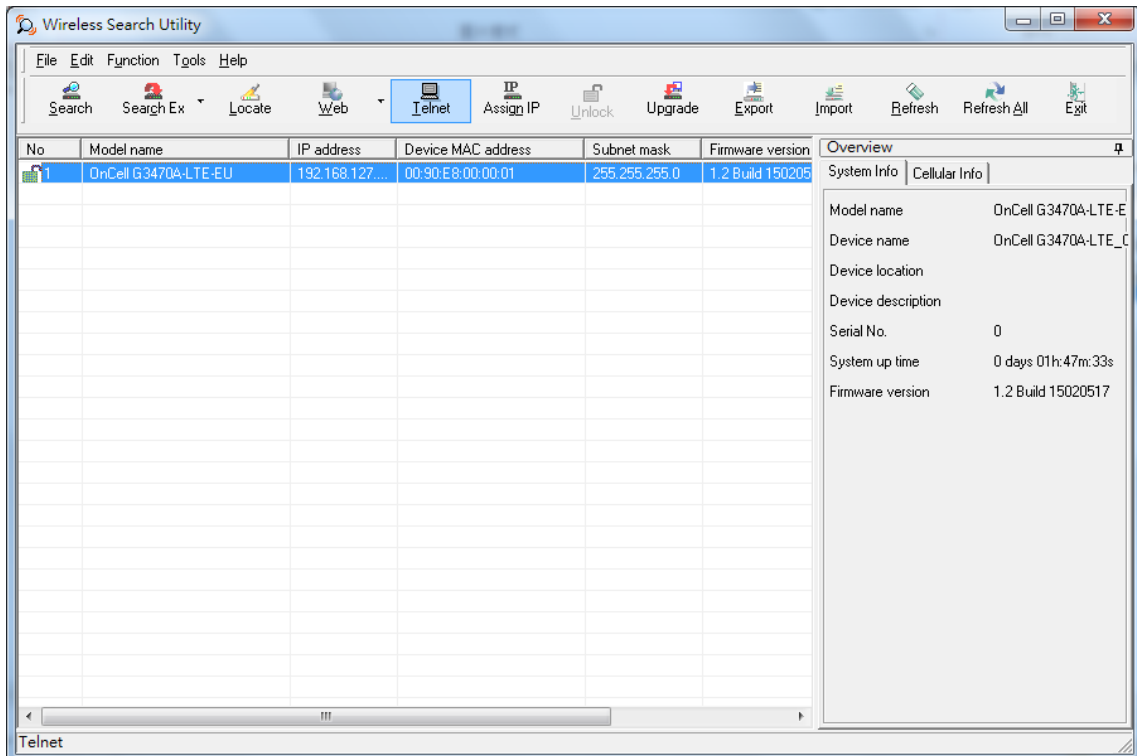


- Use the scroll down list to select the MAC addresses of the devices that you want to manage, and then click **Add**. Key in the password for the device and then click **OK** to save. If you return to the search page and search for the device again, you will find that the device will unlock automatically.

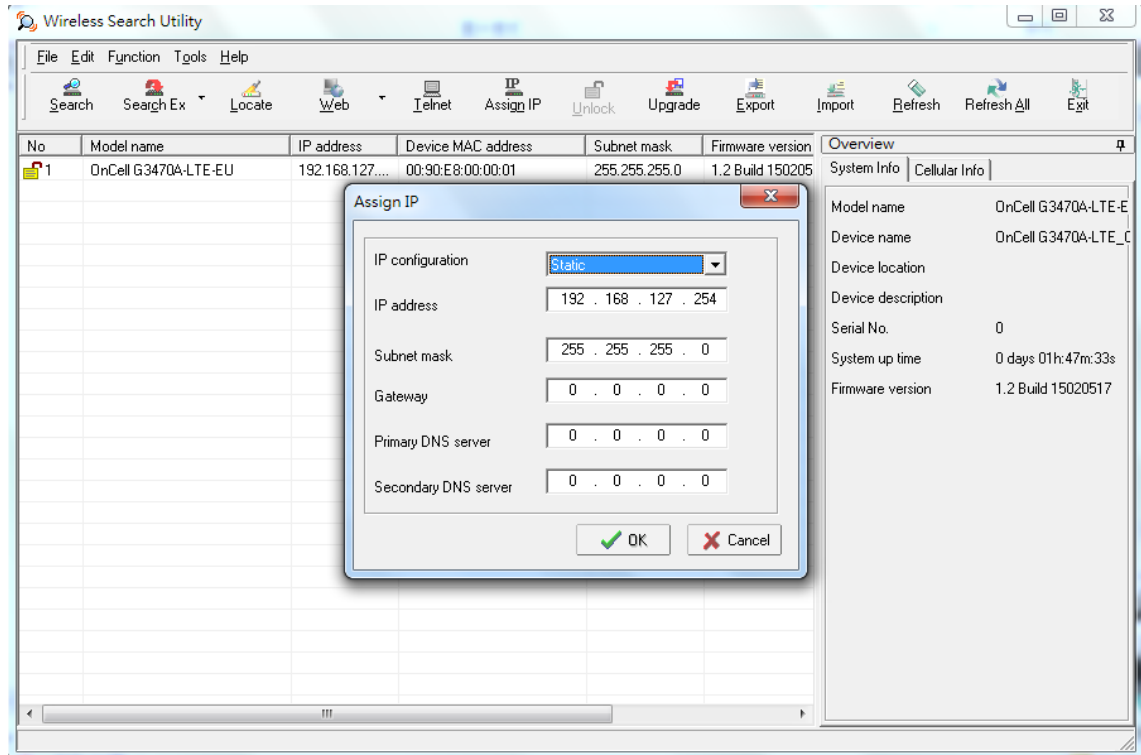
To modify the configuration of the highlighted device, click the **Web** icon to open the web console. This will take you to the web console, where you can make all configuration changes. Refer to Chapter 3, *Using the Web Console*, for information on how to use the web console.



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



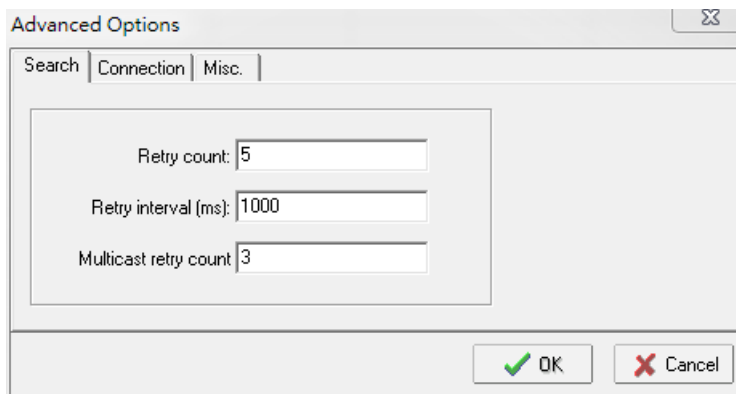
Click **Assign IP** to change the IP setting.



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

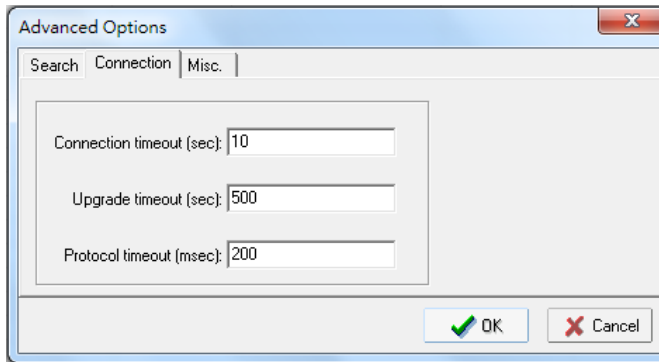
Search

- **Retry count (default=5):** Indicates how many times the search will be retried automatically.
- **Retry interval (ms):** The time to wait between retries.
- **Multicast retry count (default = 3):** Indicates how many times the search will be retried automatically by multicast mode.



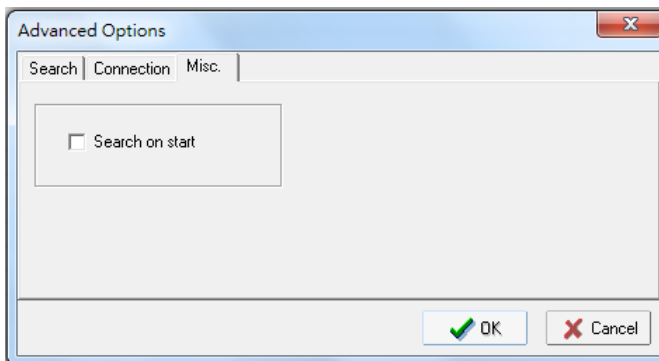
Connection

- **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 G3150A-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 G3150A-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 G3150A-LTE's firmware from Moxa Website
4. Change firmware file name to OnCell G3150A-LTE.rom
5. Connect to the OnCell G3150A-LTE's RJ45 Ethernet port

If setting is correct, you will see the following message shown on the terminal emulator, and the OnCell G3150A-LTE will reboot when the firmware recovery process has been finished.

Trying eth0

Using eth0 device

TFTP from server 192.168.127.1; our default IP address is 192.168.127.254

Filename 'OnCell G3150A-LTE.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 G3150A-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.

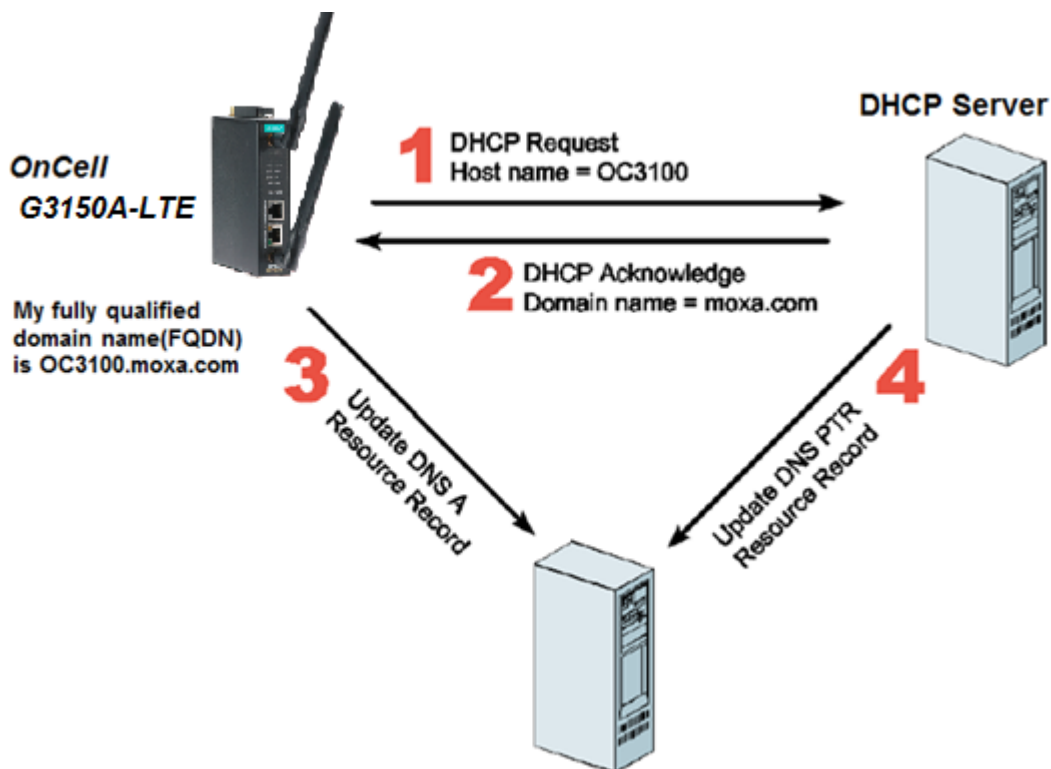
B

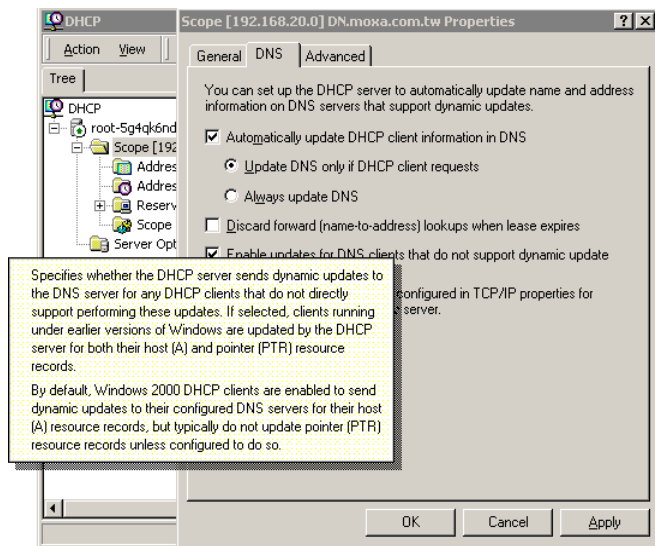
Dynamic Domain Name Server

This appendix explains how to use the OnCell G3150A-LTE with DDNS. When the OnCell G3150A-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 G3150A-LTE using its domain name instead of its IP address.

The following is a summary of the process:

1. The OnCell G3150A-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 G3150A-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 G3150A-LTE has authorization to update the DNS server, it will register its FQDN (Fully Qualified Domain Name) with the DNS server. The OnCell G3150A-LTE's FQDN will be in the format *server name.domain name* ("OC3100.moxa.com" in the illustration).
4. If the OnCell G3150A-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 G3150A-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)