CloudGate
Technical documentation

Copy taken from CloudGate Universe on: 14/05/2014
# Table of contents

## User Guide

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introducing the CloudGate</td>
<td>2</td>
</tr>
<tr>
<td>Base Unit Hardware</td>
<td>4</td>
</tr>
<tr>
<td>Expansion Cards</td>
<td>6</td>
</tr>
<tr>
<td>CloudGate Universe</td>
<td>9</td>
</tr>
<tr>
<td>Custom Developer Images</td>
<td>10</td>
</tr>
<tr>
<td>Network Interfaces</td>
<td>11</td>
</tr>
<tr>
<td>Installing the CloudGate</td>
<td>13</td>
</tr>
<tr>
<td>Attaching the Antennas</td>
<td>16</td>
</tr>
<tr>
<td>Installing the SIM</td>
<td>17</td>
</tr>
<tr>
<td>Activating the CloudGate</td>
<td>18</td>
</tr>
<tr>
<td>Powering On the CloudGate</td>
<td>22</td>
</tr>
<tr>
<td>Selecting a Wireless Provider</td>
<td>23</td>
</tr>
<tr>
<td>Installing Expansion Cards</td>
<td>26</td>
</tr>
<tr>
<td>Mounting the CloudGate</td>
<td>28</td>
</tr>
<tr>
<td>Configuring the Base Unit</td>
<td>30</td>
</tr>
<tr>
<td>Logging On to the Base Unit</td>
<td>32</td>
</tr>
<tr>
<td>Home Tab</td>
<td>33</td>
</tr>
<tr>
<td>Interfaces Tab</td>
<td>36</td>
</tr>
<tr>
<td>Ethernet Tab</td>
<td>37</td>
</tr>
<tr>
<td>3G Connection Tab</td>
<td>41</td>
</tr>
<tr>
<td>Ethernet Switch</td>
<td>49</td>
</tr>
<tr>
<td>WLAN Access Point Tab</td>
<td>52</td>
</tr>
<tr>
<td>WLAN Client</td>
<td>53</td>
</tr>
<tr>
<td>Firewall Tab</td>
<td>54</td>
</tr>
<tr>
<td>Connection Persistence</td>
<td>61</td>
</tr>
<tr>
<td>Provisioning Tab</td>
<td>64</td>
</tr>
<tr>
<td>System Tab</td>
<td>66</td>
</tr>
<tr>
<td>Configuring the VPN</td>
<td>73</td>
</tr>
<tr>
<td>Configuring Expansion Cards</td>
<td>77</td>
</tr>
<tr>
<td>Configuring the WLAN Card</td>
<td>78</td>
</tr>
<tr>
<td>WLAN Access Point Tab</td>
<td>79</td>
</tr>
<tr>
<td>WLAN Client Tab</td>
<td>83</td>
</tr>
</tbody>
</table>

## Hardware Guide

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mechanical Drawings</td>
<td>88</td>
</tr>
<tr>
<td>IP-65 requirement</td>
<td>90</td>
</tr>
<tr>
<td>Front and Back Panels</td>
<td>92</td>
</tr>
<tr>
<td>LED Descriptions</td>
<td>95</td>
</tr>
<tr>
<td>Main Board Specifications</td>
<td>98</td>
</tr>
<tr>
<td>Expansion Card Specifications</td>
<td>100</td>
</tr>
<tr>
<td>WLAN Card Specifications</td>
<td>101</td>
</tr>
<tr>
<td>Low Cost Serial Card Specifications</td>
<td>103</td>
</tr>
<tr>
<td>Industrial Serial Card Specifications</td>
<td>105</td>
</tr>
<tr>
<td>Basic Ethernet Switch Specifications</td>
<td>108</td>
</tr>
<tr>
<td>PoE Ethernet Switch Specifications</td>
<td>110</td>
</tr>
<tr>
<td>Developer Card Specifications</td>
<td>113</td>
</tr>
<tr>
<td>HDK Card</td>
<td>114</td>
</tr>
<tr>
<td>Telematics Card</td>
<td>115</td>
</tr>
<tr>
<td>RF Specifications</td>
<td>126</td>
</tr>
<tr>
<td>Antenna Recommendations</td>
<td>130</td>
</tr>
<tr>
<td>Ethernet Specifications</td>
<td>132</td>
</tr>
<tr>
<td>Environmental Specifications</td>
<td>135</td>
</tr>
<tr>
<td>Power Requirements</td>
<td>136</td>
</tr>
<tr>
<td>Internal Power Circuits</td>
<td>138</td>
</tr>
<tr>
<td>SIM Card Requirements</td>
<td>140</td>
</tr>
</tbody>
</table>
Welcome!

The CloudGate User Guide explains how to install and activate your CloudGate base unit, install custom expansion cards, and configure your device for use.

This guide is designed for:

- Distributors
- System integrators
- Field engineers

CloudGate hardware specifications and technical information are available in the Hardware Guide. Information about deploying CloudGate firmware, configuration and software updates is available in the Provisioning Server Guide.

Option also licences the CloudGate design to third party hardware and software developers who want to create custom expansion cards and software images for specific needs. For information on the developer program, contact Option Customer Support.
Introducing the CloudGate

The CloudGate M2M Gateway from Option provides LAN to WWAN routing and GPS functionality in a simple, cost-effective base unit. The CloudGate can be configured locally or remotely from a PC, tablet, or smartphone, and is certified on all major U.S. cellular operators (CDMA/EvDO and WCDMA/HSPA+).

With two expansion card slots for additional radio and wired interfaces, customizable software and configuration images, and a cloud-based provisioning system, the CloudGate is a flexible, intelligent platform for wireless M2M connectivity.

Base Unit Design

The CloudGate base unit design features LAN-to-WWAN and GPS interfaces and advanced error detection and repair watchdogs. When a component or software process loses connectivity, the device automatically resets or repowers itself. You can also schedule the device to reset at specific intervals to ensure daily, error-free operation.

Finally, CloudGates can be monitored and provisioned remotely, which vastly reduces the technician time on site, and enables firmware updates and new software features to be deployed quickly and efficiently.

Expansion Slots

To expand the capabilities of the base unit, you can add up to two expansion cards and deploy customized software, or developer images. Option offers several expansion cards with WLAN and Serial interfaces and a hardware development kit for system integrators to develop their own cards. Likewise, a software development kit is available to partners who need custom software for a site-specific application.

For more information on the CloudGate developer program, contact Option Customer Support.

Feature Overview

Reliability and Security

- Software and hardware watchdogs continually monitor for loss of connectivity and will repair the problem if detected
Software and configuration images are protected with digital signatures
Secure, redundant firmware and configuration images ensure the unit can revert to previous working settings if a problem is detected
Management functions are protected by certificate or password and applied over encrypted links

**Flexibilty**

- Two hardware expansion slots allow for additional radio and/or wired interfaces
- Expansion cards are designed with board-edge connectors for easy installation and replacement in the field
- Hardware and software development kits are available to partners for developing custom expansion cards and software images

**Provisioning**

- The CloudGate Universe allows for efficient deployment of firmware, configuration file and developer image updates to multiple CloudGates at once

**More Resources**

- [Introduction Video](#)
- [CloudGate Datasheet (US)](#)
- [CloudGate Datasheet (WCDMA)](#)
- [CloudGate Datasheet (Japan)](#)
- [CloudGate Portfolio](#)
- [CloudGate Accessories](#)
- [CloudGate Universe](#)
- [CloudGate for developers](#)
Base Unit Hardware

The mechanical housing for each base unit is identical. The **bottom front and bottom back panels** can be customized to accommodate different expansion cards and interfaces. Internally, the **main board** is also identical and is designed around a WWAN module\(^1\) and Ethernet interface.

The base unit incorporates two hardware expansion slots for additional radio and wired interfaces. Option offers a range of expansion cards but also licenses the expansion card format and connector details so that third parties can design their own **expansion cards** to fit specific needs.

The CloudGate base unit consists of:

- Light weight aluminum housing with DIN rail and wall mounting options
- Customizable bottom front and bottom back panels
- Two SMA-type **antenna interfaces**: WWAN Main and WWAN Div/GPS\(^1\)
- WLAN, GPS, System, and WWAN LEDs showing system status and signal strength\(^1\)
- 10/100 MB/s RJ-45 **Ethernet interface**
- 9-33 VDC power in with Micro-Fit\(^{TM}\), dual row, 4-circuit connector
- Two hardware expansion slots for additional radio or wired interfaces
- Internal main board with WWAN module, Ethernet interface and GPS\(^1\)
  - Freescale i.MX280 450MHz Processor
  - 64 MB Ram
  - 128 MB Flash
  - GTM68X WWAN module\(^1\)

**Base Unit Versions**

Three versions of the base unit exist:

- CG0192
Contains the GTM689 which can handle CDMA/EVDO and WCDMA technology.
Used in the U.S. and Canada and has the correct certification and approvals for these countries.

- **CG0112**
  - Contains the GTM681 which can handle only WCDMA technology.
  - Used in Europe and has the correct certification and approvals for these countries.

- **CG0102**
  - Does not contain a WWAN module.
  - Can be used in Europe, US and Canada

---

**Note 1:**
The CG0102 is a CloudGate without a WWAN module. The front plate will have no RF connectors and it will have no GPS functionality.

---

**Related Topics**
- Expansion Cards
- Mounting the CloudGate
- Mechanical Drawings
- Front and Back Panels
Expansion Cards

Option offers a several expansion cards. For custom solutions, Option also licenses a hardware development kit. Third parties can design their own expansion cards to fit specific needs.

The expansion cards offered by Option include:

- WLAN expansion card (CG2101)
- Low cost serial card (CG1101)
- Industrial serial card (CG1102)
- PoE Ethernet switch (CG1103)
- Basic Ethernet switch (CG1104)
- Developer card (CG1105)

WLAN Expansion Card - CG2101

- Provides 802.11abgn
- Simultaneous Access Point and Station mode for providing service or connection as a wireless LAN
- Failover to WLAN client for WAN connectivity
- Dual SSID

Low Cost Serial Card - CG1101
- Provides a single RS-232, 921.6Kbaud maximum speed.

**Industrial Serial Card - CG1102**

- One RS-232 port with 921.6 Kbaud maximum speed.
- 2 KV isolated RS-485 serial port, 921.6 kbaud, full duplex or half duplex; 2 wire or 4 wire with switchable termination.

**Basic Ethernet Switch - CG1104**

- 4-port 10/100Base-T
- µSD card

**PoE Ethernet Switch - CG1103**
• Power over Ethernet board. (requires special power supply)
• 4-port 10/100Base-T with 2 ports class 4 or 4 ports up to class 3 PoE
• µSD card

Developers Expansion Card - CG1105

• Extended format with headers on all interfaces to attach to development equipment
• Pre-wired RS-232 port, GPIO connected temperature sensor, a relay and SD card slot.

Related Topics

Installing Expansion Cards
Configuring Expansion Cards
CloudGate Universe

The CloudGate Universe is the configuration and deployment mechanism for the CloudGate. From the factory, CloudGate base units have no customization.

On power-up, the CloudGate connects to the CloudGate Universe over the wired Ethernet port and automatically downloads the appropriate update. If the Ethernet interface is unavailable, then the CloudGate uses the WWAN interface to download the updates.

Tip: You can set the CloudGate Universe enable or disable the automatic downloads.

The CloudGate downloads the following files from the CloudGate Universe:

- CloudGate firmware: device firmware provided by Option.
- CloudGate developer image: customized software that provides additional functionality to the CloudGate or controls third-party expansion cards.
- CloudGate config file: configuration settings that can be applied to one or more CloudGates
- CloudGate GOBI firmware image: software that updates changes to wireless operator firmware

Related Topics

CloudGate Universe Guide

3G Connection Tab
Custom Developer Images

To extend the base unit functionality provided by the CloudGate firmware, you can install developer software images onto an overlay file system and adapt the CloudGate to specific needs. Developer images can be created for custom applications and middleware, and to control third-party expansion cards.

Option licenses a software development kit which allows third parties to design developer images. For information on the CloudGate developer program, contact Option Customer Support.

Related Topics

CloudGate Universe
Network Interfaces

For connecting to the Internet, the CloudGate base unit comes with an Ethernet interface and a WWAN\(^1\) (3G) interface. An optional WLAN interface is available only when the WLAN expansion card is installed.

While the WWAN\(^1\) network interface is always a direct connection to the Internet, or WAN, the Ethernet interface and optional WLAN interface can act as either a WAN or a local Area Network (LAN). The LAN interface allows local devices to connect to the Internet through the CloudGate.

The network interfaces available on the CloudGate are:

- Ethernet interface: can be a WAN or LAN connection depending on the behavior of the **WAN/LAN switchover feature** at start-up or can be set manually.
- WWAN\(^1\) interface: always a WAN connection because it connects directly to the internet.
- WLAN interface: optional WLAN expansion card can be configured as either a WLAN client, which will act as a WAN interface, or as a WLAN access point, which will act as a LAN interface.

**Choosing a WAN or LAN Interface**

The CloudGate can have only one WAN connection at a time. However the CloudGate can be connected to several different LAN networks simultaneously.

In choosing the network interface, you can specify:

- Manual: the network interface is selected through the on device web interface on the Home page.
- Automatic: a priority list defines which network interface to use to connect to the WAN/internet. The network interface at the top of the list will try to connect to the WAN/internet first. If this succeeds then the CloudGate continues to use this network interface to connect to the WAN/internet. If the connection to the internet fails, the CloudGate tries the second interface in the priority list and so on. The priority list is defined in the on device web interface on the Home page.

**Warning:** In firmware versions 1.12.0 and older, the ability to choose between automatic mode and manual mode and to set a connection priority list are not available. These firmware versions always try to connect to the internet over the Ethernet interface first. When this interface is not able to connect to the internet, the CloudGate will try to connect to the internet via the WWAN interface.

**Note:** The CG0102 has no WWAN module!
Related Topics

Configuring the Base Unit
Ethernet Tab
3G Connection Tab
WAN/LAN switchover feature
Installing the CloudGate

To install the CloudGate base unit out of the box, review the installation requirements and then follow the installation steps listed below. For information about customizing the base unit, learn about installing expansion cards and provisioning the device with a custom developer image.

Installation Requirements

- CloudGate base unit
- Power supply between 9V and 33V DC with the correct Micro-Fit™ connector. See Power Requirements.
- Two WWAN antennas. See Antenna Recommendations.
- Ethernet cable
- Web browser on a laptop or smartphone.
- A service plan from a wireless service provider.¹
  - One of the next US wireless service providers:
    - Sprint
    - Verizon Wireless
    - AT&T (requires SIM)
    - T-Mobile (requires SIM)
  - For non US wireless service providers, any WCDMA based network will work.¹
Browser Requirements

For the Provisioning Server:

- Chrome 27.0 (.1453.110 m)
- Firefox 21.0
- Internet Explorer 9(.0.8112.16421)
- Internet Explorer 10 (.0.9200.16540)

For the CloudGate one-device web interface:

- Internet Explorer 9
- Safari 5.1
- Firefox (Windows 21.0, Mac 12.0)
- Chrome (Windows 27.0.1453.110, Mac 26.0.1410.65)
- Opera (Windows 12.02, Mac 12.10)

Installation Overview

Before installing your CloudGate device, read the safety guidelines carefully. Not following these guidelines can cause harm to the CloudGate, yourself or other persons.

To install the CloudGate base unit:

1. Attach the antennas.
2. Install the SIM, if your wireless operator is using a SIM card, or make sure that a service plan is associated with your device (for Sprint and Verizon).
3. Register the CloudGate on the Provisioning Server.
4. Power on the CloudGate.
5. Connect the CloudGate to a laptop and log in to the on-device web interface.
6. Select a wireless operator in the 3G Connection tab.

- For operators using a SIM card, the network settings will populate automatically for most SIM cards. Check the settings of the APN, Username and Password. Update them if appropriate. Click Save changes. Learn more about 3G network settings.
- For CDMA based operators (for Sprint or Verizon, no SIM card is required), click Start programming to start the activation sequence. Learn more about CDMA network settings.

Note
The CG0102 has no WWAN module!
Attaching the Antennas

The CloudGate base unit has two SMA-female antenna connectors on the front panel.

Before attaching the antennas, make sure they meet these RF specifications. Also refer to these antenna recommendations for a list of specific models.

For example, the following base unit is installed with two hinged, SMA antennas from Taoglas (Taoglas TG.09.0113 - DigiKey)

Related Topics

Front and Back Panels

RF Specifications
Installing the SIM

For some UMTS and 3G operators, such as AT&T, T-Mobile and European operators, you must install a SIM card associated with the service plan.

TIP For other wireless operators, such as Sprint or Verizon Wireless, makes sure a service plan is associated with the device before continuing the installation.

To install the SIM:

1. Using a T6 Torx screwdriver, remove the four screws from the top plate on the back panel, and then remove the plate.
2. Insert the SIM into the SIM slot.
3. Re-assemble the top cover plate and screws.

Related Topics

Selecting a Wireless Operator

SIM Card Requirements
Activating the CloudGate

When you activate the CloudGate, you add the device to the CloudGate Universe. The CloudGate Universe allows you to configure one or more devices with the same firmware, configuration, and developer images.

Using a Smartphone

To activate the CloudGate using a smartphone:

1. Install a QR scanner application on your smartphone.
2. Scan the QR code located on the bottom the device.
3. When your phone displays the Sign In page and the serial number of the device, sign in with your username and password, or click Don't have an account yet? and follow the instructions.
4. On the Activate device page, select the User group (your personal user group is the same as your username), and the type of activation.

5. Click **Activate**.

**Using a Laptop**

To activate a CloudGate using a laptop:
1. On a laptop, open an internet browser and go to the CloudGate Universe URL: http://cloudgate.option.com.
2. If you don’t have a user name and password, click click Don’t have an account yet? and follow the instructions.
3. Sign in and complete the Activate Device page. Select or enter a User group, (your personal user group is the same as your username), the type of activation, the serial number, and activation code.

![Activate device](image)

4. Click Activate.

---

**Related Topics**

Creating an Account on the CloudGate Universe
Activating the CloudGate Using the CloudGate Universe
Powering On the CloudGate

To power on the CloudGate:

1. Plug the power supply into the power connector on the back of the unit and into power source. Ensure the power supply meets these power requirements.
2. Observe the LEDs on the front panel. The CloudGate attempts to connect automatically with the CloudGate Universe and download the appropriate firmware, developer image, and configuration file. When the power-on sequence is complete, the System and WAN LEDs on the front panel turn green.

Related Topics

LED Descriptions
Selecting a Wireless Provider

For the minimum, out-of-the-box installation of the CloudGate base unit, you have to connect the device to a laptop and use the on-device web interface to select the appropriate wireless provider firmware.

**IMPORTANT:** When using the CloudGate WCDMA (CG0112) base unit (this is the version without CDMA technology), you don’t have to select the wireless operator and you can immediately go to step 7 on this page.

To connect the CloudGate to a laptop and select a wireless provider:

1. Connect an Ethernet cable to the Ethernet port on the CloudGate front panel and a network port on a laptop or computer.
2. In a web browser, go to the URL: 192.168.1.1.
3. In the login screen, enter the default username admin and password admin.
4. Click the 3G Connection tab in the top menu bar.
5. Scroll down to the image Configuration field and the wireless operator firmware options.
6. Select the appropriate wireless provider and click Save changes.

TIP: When using an AT&T SIM card, select AT&T. For all other operators using SIM cards, select UMTS generic.

1. Proceed with the wireless provider selection.

- For Verizon Wireless and Spint service

  Make sure the service plan is already associated with the unit (MEID). Scroll down to the CDMA section and click Start programming to complete the activation.

- For all SIM card based operators

  The network settings populate automatically for most SIM cards. Scroll down to the Network Settings section and check the APN, Username, and Password fields. Update if necessary and click Save changes. If the service plan requires a PIN code, scroll down to the PIN Settings section, enable and enter the PIN code, and click Save changes.
Related Topics

Configuring the Base Unit

3G Connection Tab
Installing Expansion Cards

CloudGate expansion cards are easy to install either during staging by a distributor or system integrator, or in the field by a technician.

Expansion cards are designed to fit in one of two expansion slots accessed from the unit’s front or back panels. In general, cards with antenna interfaces, such as the WLAN card, are installed in the back slot to avoid interference with the 3G antennas on the front of the base unit.

**TIP:** Another way to determine the appropriate slot, is to look at the card connector. Cards with the small connector are installed in the rear slot. Cards with the large connector are installed in the front slot.

To install an expansion card:

1. Make sure the unit is powered off.
2. Using a T6 Torx screwdriver, remove the three screws from the bottom plate on the front or back panel, and remove the plate.
3. With the expansion card in your hand, make sure the English labelling for any external interfaces, such WLAN Antenna or Serial Port, are facing up. In this orientation, the card connector is also right facing.
4. Slide the card into slot, using the side channels or grooves on the device to guide the card into place. Make sure the screw holes line up.
5. Push gently until the card is flush with the housing.
6. Secure the card with the screws.

The following table lists the expansion cards available from Option and the slot.
Removing Expansion Cards

Removing an expansion card requires different steps depending on the type of card. Contact Option Customer Support for assistance.

Related Topics

Configuring Expansion Cards
Mounting the CloudGate

The CloudGate can be mounted on a wall or DIN rail.

**IMPORTANT:** All mounting hardware is installer provided.

Mounting on a wall

The CloudGate can be mounted on a wall with six screws. The mounting holes in the base of the CloudGate have a diameter of 4.3 mm. Option recommends using screws with a minimum width of 4 mm and a minimum length of 30 mm (M4x30mm).

**TIP:** When choosing the mounting orientation of the unit, consider the direction of the cables and antennas. Make sure cables are routed with sufficient ease to all connectors, and that the antennas are unobstructed for easy positioning. The front panel LEDs should also be visible.

To wall mount the CloudGate:

1. Mark the six holes with a pencil on the wall.
2. Drill (if necessary) the holes in the mounting surface. Do not drill into the CloudGate housing. [Click here for a drawing of the mounting holes.](#)
3. Mount the CloudGate with six M4x30mm screws

Mounting on a DIN rail

To mount the CloudGate on a DIN rail, use two DIN rail adapters. Option recommends adaptors from the following companies:

- Phoenix Contact
• DSB Marketing
• Hammond
Configuring the Base Unit

When the CloudGate is connected to a laptop through an Ethernet cable, you can configure the device locally using the on-device web interface. The web interface allows you to configure one device at a time.

TIP: To provision a number of CloudGates at once, use the web interface to create a configuration file and use the CloudGate Universe to download the file to multiple devices.

Learn how to log on to the on-device web interface

The web interface displays a number of tabs based on the expansion cards installed. For the CloudGate base unit with no expansion cards, the following default tabs are available: Home, Ethernet, 3G Connection, Firewall, Connection Persistence, Provisioning, and System.

<table>
<thead>
<tr>
<th>Click this tab</th>
<th>To do these tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home</td>
<td>Verifying the Internet Connection</td>
</tr>
<tr>
<td></td>
<td>Checking the Firmware Version</td>
</tr>
<tr>
<td>Ethernet</td>
<td>Disabling the WAN/LAN Switchover Feature</td>
</tr>
<tr>
<td></td>
<td>Managing IP Configuration Settings</td>
</tr>
<tr>
<td>3G Connection¹</td>
<td>Configuring the WWAN Interface</td>
</tr>
<tr>
<td></td>
<td>Choosing a Wireless Operator</td>
</tr>
<tr>
<td></td>
<td>Setting Up SIM Parameters</td>
</tr>
<tr>
<td></td>
<td>Setting Up WWAN Connection Parameters</td>
</tr>
<tr>
<td></td>
<td>Choosing PIN Code Settings</td>
</tr>
<tr>
<td></td>
<td>Setting up Verizon Wireless or Sprint wireless operators</td>
</tr>
<tr>
<td>Firewall</td>
<td>Setting Default Firewall settings</td>
</tr>
<tr>
<td></td>
<td>Setting Up the DMZ</td>
</tr>
<tr>
<td></td>
<td>Setting Up Inbound Port Forwarding</td>
</tr>
<tr>
<td></td>
<td>Setting Up Outbound Port Filtering</td>
</tr>
<tr>
<td></td>
<td>Setting Up Outbound Trusted IPs</td>
</tr>
<tr>
<td>Connection Persistence</td>
<td>Configuring the Connection Watchdog</td>
</tr>
<tr>
<td></td>
<td>Configuring the Automatic Timed Reset</td>
</tr>
<tr>
<td>Provisioning</td>
<td>Setting up Automatic updates</td>
</tr>
<tr>
<td>Click this tab</td>
<td>To do these tasks</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| **System**    | Setting up the Time Zone  
|               | Setting up Remote Access to the CloudGate  
|               | Setting up a Dynamic DNS Service  
|               | Changing the Username and Password  
|               | Creating Log Files  
|               | Download a configuration file  
|               | Manually Resetting the CloudGate |

**Note1:**
The CG0102 will not show a “3G connection” tab as it has no WWAN module.
Logging On to the Base Unit

To log on to the on-device web interface:

1. In a web browser, go to the URL: 192.168.1.1.

2. Enter the user name and password, and then click Login.
   - Use the default username admin and password admin. You can change the default username and password later if necessary.
Home Tab

The Home tab displays the CloudGate connection status, the connection settings, the different available LAN interfaces and the firmware and software versions installed.

Connection status.
Displays the type of Internet connection and reports if the unit is connected or not connected.

Connection settings

Internet connection enabled:
• This parameter enables (yes) or disables (No) the WAN interface.

Connections strategy:
• This parameter defines which interface should be chosen to connect to the internet (WAN interface) in case multiple solutions are possible. Two possible solutions are available: Manual and priority based.

  Manual
• In manual mode, the interface with a blue background will be the one and only interface to the internet (WAN interface).
• In order to change the interface press on the “use this” button behind the interface you would like to be the WAN interface.
**Priority based**

- In priority based mode the CloudGate will first try to make a WAN connection with the interface on the top row of the table.
- When the first interface is unable to make a connection to the internet the second interface will be taken.
- When the second interface fails the next line will be taken.
- In order to change the priorities, press on the arrows behind the interface you would like to change.

### Important:
The CloudGate decides that he's not connected anymore when:
- For the ethernet connection the cable is removed.
- For the 3G connection when a disconnect message of the network is received.
- For the WLAN connection when out of range.

This functionality can be extended when used together with the connection persistence feature.

**LAN interfaces**

- This is a list of the available LAN interfaces and there IP address.
VPN Tunnels
This is a list of the active VPN tunnels.

System information

Device serial number
- This shows the serial number of the CloudGate

Firmware version
- This is the version of the Option firmware. Every CloudGate needs an Option firmware!

Image version
- This is the version of the developers image. This image is only required in case you need features which are not part of the Option firmware.

Configuration version
- This is the version of the configuration file.
- A configuration file is not mandatory, it's a way to provision CloudGate settings to multiple units.
Interfaces Tab

The interfaces menu groups the settings of all connection technologies

- Ethernet
- 3G Connection
- WLAN Client
- WLAN Access point
The **Ethernet** tab configures the behavior of the Ethernet port on startup and manages IP network settings.

**Enabled**
- Enables (Yes) the ethernet interface on the main board of the CloudGate or disables (No) the ethernet interface.
Mode

- This will define the state of the Ethernet interface. In case the WAN/LAN Switchover feature is disabled.
- In case the WAN/LAN switchover feature is enabled, the state of the ethernet interface will be as in the following table:

<table>
<thead>
<tr>
<th>Result of WAN/LAN switchover feature</th>
<th>State of &quot;Mode&quot;</th>
<th>End result</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN</td>
<td>LAN</td>
<td>WAN</td>
</tr>
<tr>
<td>WAN</td>
<td>WAN</td>
<td>WAN</td>
</tr>
<tr>
<td>LAN</td>
<td>LAN</td>
<td>LAN</td>
</tr>
<tr>
<td>LAN</td>
<td>WAN</td>
<td>WAN</td>
</tr>
</tbody>
</table>

WAN/LAN Switchover

- The WAN/LAN switchover feature defines the state of the Ethernet port after the CloudGate is powered on. By default, WAN/LAN Switchover is enabled. Learn more about the WAN/LAN switchover feature.
- If set to Yes, the Cloudgate tries to connect to the internet through the ethernet connection, such as an ADSL or cable modem. If a connection is unavailable, the port switches to LAN mode and acts as a LAN interface.
- Set to No to power on the Ethernet port as defined in the "mode" parameter.
### IP address

- Sets the IP address of the CloudGate. By default the IP address is 192.168.1.1 you can change this to any value you want.

### Netmask

- Sets the netmask of the CloudGate. By default the netmask is set to 255.255.255.0 you can change this to any value you want.

### Enable DHCP server

- Enables the DHCP server. By default the DHCP server is enabled. (When the ethernet port is in LAN state). In case you want to use static IP addresses in your network you can disable the DHCP server.

### DHCP range

- Sets the DHCP range for the DHCP server.

### DNS 1 and DNS 2

When the CloudGate is in **LAN mode** the DNS fields will be empty by default. As a result the CloudGate itself will act as a DNS server. All the connected ethernet devices will receive an DNS address which is equal to the CloudGates IP address (by default 192.168.1.1) When the DNS server inside the Cloudgate can’t resolve the DNS request it will forward the request to the DNS server of the WAN connection.

When the CloudGate is in **WAN mode** the DNS address will be defined by the DHCP server of the internet provider. When the DNS fields are changed to another value than the other IP address will be used for the DNS server.

### Reserved leases

- Lists the DHCP leases which are assigned to a certain MAC address.
- Click **Add** to assign another lease and link a MAC address to an IP address.

### Active leases

- Lists the active DHCP leases of the devices connected to the CloudGate.
- Click **Reserve** to add the lease to the Reserve leases list.
### Reserved leases

<table>
<thead>
<tr>
<th>Hostname</th>
<th>MAC</th>
<th>Lease time</th>
<th>IP</th>
<th>Active</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option-Canada</td>
<td>00:15:b7:6d:f1:67</td>
<td>1d</td>
<td>192.168.1.237</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

### Active leases

<table>
<thead>
<tr>
<th>Hostname</th>
<th>MAC</th>
<th>IP</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option-Canada</td>
<td>00:15:b7:6d:11:67</td>
<td>192.168.1.237</td>
<td>Reserve</td>
</tr>
</tbody>
</table>

**Related Topics**

[WAN/LAN Switchover Feature](#)
3G Connection Tab

The 3G Connection tab configures the CloudGate WWAN interface, as well as 3G and CDMA network settings.

Click the left sidebar to jump to the following sections:

- Connection Status
- General
- Network Settings
- PIN Settings
- CDMA

Connection Status

The Connection status section provides information about the wireless network.
**Operator Name**
- Displays the name of the wireless operator the CloudGate is connected to.

**Signal Strength**
- Displays the received signal strength.

**ECIO**
- Displays the energy per chip over the interference. This is a typical way to indicate the quality of 3G networks.

**Technology**
- Displays the technology used by the wireless operator.
Voice number

- Displays the voice number linked to the SIM card for 3G wireless operators.

---

**General**

The General section configures the WWAN interface on the CloudGate.

![General configuration screen](image)

*Note: when using an AT&T SIM card select "AT&T", for all other wireless operators using SIM cards select "UMTS generic".*
**Enabled**

- Enables and disables the WWAN (3G) interface,
- Set to **Yes** (default) to enable the WWAN interface. If there is no Internet connection available on the Ethernet interface, the device automatically connects to the network using the WWAN interface on startup.
- Set to **No** to disable the the WWAN interface. The only network connection possible is through the Ethernet interface.

**Only upon traffic**

- By default, the device is always connected to the network and can send and receive data in both directions: Internet to CloudGate, and CloudGate to Internet. To protect the device from unauthorized access and ensure you only pay for the data you want to send, you can configure the device to connect only when it has data to transmit.
- Set to **Yes** to connect the device to the WWAN when it has data to send and disconnect it immediately after. Note that when the device is disconnected, it is also unable to receive data. Option recommends enabling this feature only if you are interested in one way, CloudGate-to-Internet data flow.
- Set to **No** (default) to disable sending data only upon traffic.

**IMPORTANT:** Remote login to the CloudGate does not work when Only upon traffic is enabled.

**Connect while on roaming**

- Manages international roaming settings for a device installed in a vehicle.
- If set to **Yes**, international roaming is enabled.
- If set to **No**, international roaming is disabled. Option recommends disabling this feature to prevent high roaming costs.

**IMPORTANT:** National roaming is always allowed on the CloudGate. The Connect while on roaming feature only has an impact on international roaming behaviour.

**WWAN Div Antenna present**

- Enables antenna diversity.
- The base unit supports two antenna interfaces: WWAN with Diversity/GPS and WWAN Main. Using both antennas ensures better reception in low coverage areas and increased throughput.
- If set to **Yes**, antenna diversity is enabled and both physical antennas must be installed.
- If set to **No**, make sure only one antenna is connected to WWAN Main on the front panel.

**IMPORTANT:** Installing one antenna with diversity enabled (set to **Yes**), results in poor or unstable performance. Make sure that diversity is disabled when there is only one antenna installed.

**Passthrough Mode**

Option CloudGate - Last updated on 14/05/2014
By default, Passthrough Mode is disabled (set to No).
If set to Yes, the connected laptop receives an IP address from the wireless operator through the CloudGate.

**IMPORTANT:** When passthrough is active, data sent to port 80 will always redirect to the WebGui of the CloudGate!

### Image configuration

- Selects the wireless operator firmware the device will use on the network.

**IMPORTANT:** When using the CloudGate WCDMA (CG0112) base unit (this is the version without CDMA technology), you don't have to select the wireless operator. The device uses the UMTS Generic setting.

If Verizon Wireless or Sprint is selected, the web interface jumps to the CDMA section. Click **Start Programming** to provision the unit for CDMA.

If UMTS Generic is selected for T-Mobile or any operator not listed, you may be required to enter a PIN code. In the PIN code section, enter the appropriate settings and click **Save changes** to provision the unit for UMTS 3G.

If AT&T is selected, you may be required to enter a PIN code. In the Pin Code section, enter the settings and click **Save changes** to provision the unit for AT&T 3G.

### Connection Hunting

Connection hunting is a feature developed by Option that allows the CloudGate to actively search for another network in case the primary network is not available.

**IMPORTANT:** The connection hunting feature is only available on CloudGate WCDMA + CDMA (CG0192)

When enabled a new section of the menu will appear allowing the user to select which other networks the CloudGate should try to connect to in case the primary connection cannot be established.

The fallback time field allows to select the time the CloudGate needs to try to connect to each of the alternative networks before trying the next network.
Network Settings

If AT&T or UMTS Generic is the chosen wireless operator firmware, you can configure a number of 3G network settings.

**APN**

- Sets the APN value automatically based on the SIM card installed.

**IMPORTANT:** When the APN which is set automatically, is not the correct one, you can change it manually. When the APN is manually changed, the CloudGate will remember this and will use this APN every time it detects this individual SIM card. When a different SIM card is inserted the CloudGate will again choose the APN automatically.

**Authentication method**

- Selects the authentication method:
  - **Automatic:** (default). Uses PAP authentication for connecting to the network, followed by CHAP authentication.
  - **PAP:** Uses PAP authentication protocol for connecting to the network.
  - **CHAP:** Uses CHAP authentication protocol for connecting to the network.
  - **NONE:** No authentication protocol used.

**Username**

- Defines a user name if required by the wireless network subscription.
Password

- Defines a password if required by the wireless network subscription.

Network selection method

- Sets the network selection method when roaming:
  - **Automatic**: Registers the device to the network corresponding to the SIM card installed. When roaming, the device connects to the roaming partner designated by the wireless operator.
  - **Manual**: Scans for networks and then lets you select a network different from your home network.

PIN Settings

When you select **AT&T** or **UMTS Generic** as the wireless operator, you may have to enter a PIN code.

Enable PIN

- Enables the PIN code and displays a field for entering the value.

Save PIN

- Automatically saves the PIN code.
If Verizon Wireless or Sprint is the chosen wireless operator, click **Start programming** to provision the CloudGate.
Ethernet Switch

When the Ethernet expansion board is inserted into the CloudGate a new item "Ethernet Switch" will be listed in the interfaces tab.

- only LAN functionality is available on the Ethernet Switch outputs, no WAN functionality.

3 fields are available in this tab:

- General
- IP Config
- Data Counters

**General**

In the general section of the ethernet switch these settings can be selected:

- Enabled: Yes / No
- **The MTU packet size**: Value range 68 to 1500
IP Config

The IP configuration field allows to set:

- **IP address**: This is the IP address on which the cloudgate will be reachable from the ethernet switches network.

  Default the CloudGate uses subnet 4 on the Ethernet switch card. Subnet 1 is reserved for the main Ethernet interface, Subnet 2 & 3 for the WLAN SSID1 & SSID2 interfaces.

- **Net mask**: Allows to configure a specific netmask, default 255.255.255.0
- **Enable DHCP Server**: When enabled the DHCP service of the cloudgate will be available to all devices connected through the ethernet switch, when enabled the address range can be selected.
- **DNS 1 & 2**: these fields allow specification of custom primary and secundary DNS servers using thier IP address.

The reserved and active leases table allow to manage the devices able to connect too ports of the Ethernet Switch card. To add a device manually to the list click the "add" button. Host name, Mac & IP address are required. A specific lease time can be selected.
### Data counters

Data counters will trace the incoming & outgoing traffic of the Ethernet switch's outputs since last start.

<table>
<thead>
<tr>
<th>Data Counters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data received: 0 bytes</td>
</tr>
<tr>
<td>Packets received: 0</td>
</tr>
<tr>
<td>Data transmitted: 0 bytes</td>
</tr>
<tr>
<td>Packets transmitted: 0</td>
</tr>
</tbody>
</table>
WLAN Access Point

If the WLAN Card is inserted into the CloudGate it has the ability to be configured as a WLAN access point with a single or double SSID. This page allows to configure the generic accesspoint settings and the individual SSID settings.

Please click here for more information
WLAN Client

When the WLAN card is inserted in the CloudGate the WLAN Client tab allows to set up the CloudGate as a WLAN Client connecting to a pre existing WLAN Network

For more information please click here
Firewall Tab

The Firewall tab controls how data passes from one type of interface to another. There are three different sources or destinations for CloudGate data:

- A WAN interface, which is a connection to the Internet
- A LAN connection, which is a connection to a laptop or other computer on the same network interface
- The CloudGate itself, called the Local network

**TIP:** When the device is powered on, the Ethernet interface behaves as a WAN or LAN depending on the mode configured through the WAN/LAN Switchover feature.

Click the left sidebar to jump to the following sections:

- Default Policies
- DMZ
- Inbound Port Forwarding
- Outbound Port Forwarding
- Outbound Trusted IPs
- Static Routing

### Default Policies

The Default Policies section sets the basic firewall rules.

<table>
<thead>
<tr>
<th>Default policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN -&gt; WAN</td>
</tr>
<tr>
<td>LAN -&gt; LAN</td>
</tr>
<tr>
<td>LAN -&gt; Local</td>
</tr>
<tr>
<td>WAN -&gt; Local</td>
</tr>
</tbody>
</table>

**Default Policies**

- Sets the default firewall rules to accept or reject data flow between the following interfaces:
  - LAN to WAN
  - LAN to LAN
LAN to LOCAL
WAN to LOCAL

- Sets the action for each rule:
  - Accepted: the data is allowed to pass from one interface type to the other interface type.
  - Rejected: the data is not allowed to pass from one interface type to the other interface type; the CloudGate drops the data packets and sends a reject message to the source of the packets.
  - Dropped: the data is not allowed to pass from one interface type to the other interface type; the CloudGate drops these data packets without sending a reject message.

Note: The WAN to LOCAL traffic is by default "Dropped". This makes sure that no traffic coming from the internet can enter the CloudGate.

DMZ

The DMZ section configures the demilitarized zone.

This feature forward all incoming data to a specific IP address.

**DMZ**

<table>
<thead>
<tr>
<th>Enabled</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN Interface</td>
<td>ALL</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>Required&lt;br&gt;ex: 192.168.1.1</td>
<td></td>
</tr>
</tbody>
</table>

**Enabled**

- Enables the DMZ.

**WAN Interface**

- Selects the WAN interface the data will be coming from for forwarding.

**IP Address**

- Sets the IP address for forwarding all data coming from a WAN interface.
Inbound Port Forwarding

The Inbound Port Forwarding section forwards data from a WAN interface to a designated IP address and port.

Inbound Port Forwarding

Lists the inbound forwarding rules, up to a maximum of 40.

These rules allow you to forward data from a WAN interface to the IP address set in the destination field.

The port forwarding rules have a higher priority than the DMZ rule!

Click Add to create a forwarding rule. Enter the port information and target IP address in the dialog box and click Save.
Outbound Port Filtering

The Outbound Port Filtering section defines the data allowed to pass from the Local or LAN interface to the WAN interface.
• Lists the outbound port filtering rules, up to a maximum of 20.
• By default, all data can be sent to a WAN interface. When an outbound port filtering rule is added, the data sent over the chosen port will be allowed, rejected or dropped.
• Click **Add** to create a filtering rule. Enter the port range and select whether to **Allow**, **Reject** or **Drop** the data sent over the chosen port and click **Save**.

Outbound Trusted IPs

The Oubound Trusted IPs section defines IP addresses that can be contacted when LAN-to-WAN traffic is not allowed.

• When the LAN to WAN traffic is rejected or dropped based on the default firewall policies, no data can be transmitted from the LAN to the WAN network.
• The outbound trusted IP list defines the IP addresses that can be contacted even when LAN-to-WAN traffic is not allowed.
Enter an IP address and click **Add**.

**Static Routing**

Static routing allows you to define a specific gateway for an IP address.

- **Interface**: Specify on which interface you would like to have the static routing.
- **Target**: Specify the destination IP address.
- **Netmask**: Specify the netmask of the destination IP address.
- **Gateway**: Specify the gateway which has to be used to send packets to the target IP address.

![Edit static routing](image)

**Inbound Rules WAN -> LAN/LOCAL**

Next is a list of the PORT FORWARDING rules by priority from high to low:

1. HTTPS (port determined in the >SYSTEM tab
2. Port forwarding rules
3. DMZ

Priority example: If you enable HTTPS and DMZ, you can still use the HTTPS because those port forwarding's are processed before the DMZ redirect.
Outbound Rules LAN -> WAN

Outbound rules in order of priority:

1. Port filter rules. (Only used when trusted IP is disabled)
2. Trusted IP rules (if enabled forces general LAN -> WAN rules to Reject/Drop)
3. General LAN -> WAN rule (in case of trusted IP always Reject or Drop)
Connection Persistence

The **Connection Persistence** tab configures the watchdogs that monitor CloudGate operation and performance.

The following actions can be configured to make sure the CloudGate works properly.

- **Connection watchdog**: This watchdog tests if the active WAN interface is able to connect to the internet. If not it will trigger the next WAN interface in the priority list. When it detects that the 3G interface is not able to contact the internet it will trigger the next WAN interface in the priority list and it will reset or reconnect the WWAN module. [You can find here a flow chart of the feature.]
- **Timed Reset**: resets the CloudGate after a period of time.

### Connection Watchdog

The **Connection Watchdog** page allows you to configure the connection watchdog settings.

#### Enabled
- Set to **Yes** to enable the connection watchdog and monitor the active WAN interface for data received.
- If no data is received after a certain period of time (= checking interval), the connection watchdog

![Connection Watchdog Configuration](image-url)
will:
- Try to lookup the URL/IP addresses
- If activated, try to ping the URL/IP addresses.
- If both actions fail then the next WAN interface in the priority list will be activated. When the failing WAN interface is the 3G interface than the WWAN module will be reset or try to re-establish a connection.

Addresses to Check

- Specifies the IP addresses or URL’s to send a DNS request or PING to if the connection watchdog is enabled
- A maximum of 5 IP addresses or URL’s can be specified.

**IMPORTANT:** The URL’s in the table must be the URL name, not the used protocol.

For example:
- www.google.com will be accepted.
- http://www.google.com will not work

Use PING in addition to DNS

- Sends a PING and DNS request to the specified URL/IP addresses

Checking interval

- If no data is received during a time equal to the "checking interval" the connection persistance will start the URL/IP lookup feature.

Watchdog action

- Resets the WWAN module or tries to re-establish the connection to the wireless network. Resetting the WWAN module can take about 2 minutes, reconnecting to the wireless network will take about 20 seconds.

**Timed Reset**

The Timed Reset section sets up the device to reset on a daily, weekly or monthly basis.
Enabled

- Set to **Yes** to enable the **Timed Reset** watchdog. The CloudGate will reset at the specified time interval.

Frequency

- Set to **Daily** and select the time of the day at which you want to perform the reset.
- Set to **Weekly** and select the days of the week you want to perform the reset, and the time of day. Selected days are green.
- Set to **Monthly** and enter the day of the month and the time of the day.
Provisioning Tab

The Provisioning tab configures how and when the CloudGate checks for updates from the CloudGate Universe.

By default, the CloudGate base unit connects to the CloudGate Universe each time the device is powered on, and checks for an updated image. The device downloads and installs the update over the WAN interface.

Check for Updates

- Checks the CloudGate Universe for firmware, developer image, and configuration file updates
- Click the **Check for Updates** button to check for updates even if **Enable automatic provisioning** is disabled.

Upload Option Provisioning File
Select file

- Updates the unit with an image from a hard drive.
- Click **Browse** to select the file and then click **Upload**.

**Settings**

Enable Automatic Provisioning

- Controls automatic updates from the CloudGate Universe.
- Set to **Yes** to automatically check for updates. This happens:
  - Each time the unit is powered on.
  - Depending on the "check in frequency" parameter on the CloudGate Universe.
- Set to **No** to disable automatic provisioning.
System Tab

The System tab configures remote access settings, log file parameters, and manual reset settings.

Click the left side bar to jump to the following sections:

- Timezone
- Remote Access
- Dynamic DNS
- Username and Password
- Logging
- Config Export
- System Reboot and Factory Reset

Timezone

- Sets the timezone used by the unit for the Timed Reset watchdog.

Remote Access through HTTPS

The Remote Access section configures a port on the CloudGate for remote access. With remote access, you can log into the one-device web interface from a remote PC or laptop.
To set up remote login:

1. Click the **3G connection** tab and make a note of the IP address of the WAN connection displayed in IP Configuration.
2. Click the **System** tab.
3. Set the **Remote access through HTTPS** field to **Yes**.
4. Enter the port number for which remote login is allowed.
5. Click **Save changes**.

To log in to the CloudGate remotely:

1. On a remote laptop, go to the URL: `https://IPaddress:portnumber`.
2. Enter the user name and password.

**Dynamic DNS**
Dynamic DNS

Enabled

- Set to **Yes** to enable Dynamic DNS.

Service Provider

- Selects the dynamic DNS service provider.

Host name

- Defines the host name for the DNS service provider account.

User name

- Defines the user name you have set up with the DNS service provider.

Password

- Defines the password you have set up with the DNS service provider.

Use HTTPS

- Allows you to use HTTPS for the service.
- Set to **Yes** to enable HTTPS login.

**Status**

- Displays status information.
- Click **Update** to refresh the status.

**Username and Password**

**Username**

- Sets a new username for logging on to the on-device web interface.

**Password**

- Resets the password.

**Logging**

Option customer support may request logfiles to diagnose a problem.
To create a logfile:

1. Click **Yes** to enable logging.
2. Set additional logging parameters according to Option Customer Support recommendations.
3. Click **Save changes**.
4. Reproduce the CloudGate problem.
5. Download the log file by clicking **Download log file**.

### Enable logging
- If set to **Yes**, the unit logs all CloudGate activity.

### Maximum log file size
- Sets the maximum log file size. Option recommends 256 kB.

### Select log levels
- Sets the log levels. In order of severity the levels are: Info, Warning, Error, Debug

### Download log file
- Downloads the file to a hard drive or USB stick.

### Clear log file
• Removes the log file from the unit's memory.

**Config Export**

![Config Export](image)

**Download config**

• Click to save the device configuration to a file on a laptop. The configuration file can then be uploaded to the Provisioning Server and used for provisioning multiple devices.

**System Reboot and Factory Reset**

Two different manual resets are possible on the CloudGate: system reboot and factory reset.

💡 **TIP:**

Automatic resets of the WWAN interface are managed by the [connection watchdog](https://example.com) feature. Automatic resets of the CloudGate are managed by the [timed reset](https://example.com) feature.

**System reboot**

![System reboot](image)

**Factory reset**

![Factory reset](image)

**System reboot**

To reboot the CloudGate:
1. Click **System reboot**.
2. In the confirmation dialog box, click **Reboot** to confirm.

Note: This is the same as pressing the hardware reset button on the back of the CloudGate for one second.

**Factory Reset**

To reset the CloudGate to the factory default settings and overwrite all custom configuration changes:

1. Click **Factory Reset** to restart the device with the original firmware version from the factory.
2. Click **Factory reset** to confirm.

💡 TIP: This is the same as pressing the hardware reset button on the back of the CloudGate for more than five seconds.

**Hardware Reset Button**

The hardware reset button is located on the unit back panel. Using a pen or small screwdriver, press and hold:

- Hold for one second to perform a normal reset.
- Hold for five seconds or more to perform a factory reset.
Configuring the VPN

The VPN tab allows adding and configuring IPSec tunnels. By default the CloudGate has no IPSec tunnels preconfigured.

A tunnel can easily be added by clicking the “+ add IPsec Tunnel” button, a window will prompt for the user to enter a name for the new tunnel.

When the tunnel is successfully added a new field in the VPN tab will appear for each tunnel that is added.

Tunnels can be removed in the bottom right corner of the field of each tunnel using the “delete tunnel” button.

Configuring a Tunnel

3 elements can be configured for each tunnel.
• Identity
• IKE Settings
• IPsec Settings

All fields must be configured for the tunnel to become active

Identity

The identity section provides the ability to configure:

![Identity Configuration Form]

- The basic authentication method: currently only PSK is available,
- a pre shared key,
- the interface on which the tunnel should be used. Here the user can select if the tunnel can only be used on a specific connection type or all connection types
- Remote Host:
Remote & Local identity: These are optional fields that can be used in case the other tunnel endpoint has configured a local identity. This field may contain an IP or a FQDN (fully qualified domain name).

Local and Remote subnet. These are optional fields that can be used to define the subnet on your local and remote setup.

**IKE Settings**

The Internet Key Exchange is a protocol used to set-up the security associations in the IP sec protocol suit.

![IKE Settings](image)

- IKE Version: V1,V2
- Negotiation Mode (only for IKE V1): Main & Aggressive
- IKE Encryption: 3DES, AES128, AES 256
- IKE Authentication: MD5, SHA1, SHA256
- IKE Key Group: DH1, DH2, DH5, DH14
- IKE SA Lifetime: must be a value between 60 - 86400


**IPsec Settings**

These fields are used to configure the IPsec tunnel's encryption details.

![IPsec Settings](image)
- IPsec Encryption: 3DES, AES128, AES 256
- IPsec Authentication: MD5, SHA1, SHA256
- IPsec Key Group: DH1, DH2, DH5, DH14
- IPsec SA Lifetime: must be a value between 60 - 86400
Configuring Expansion Cards

If the CloudGate is installed with an Option expansion card, the device automatically detects and identifies the card and displays the appropriate configuration tab in the menu bar.

The additional configuration tabs are:

- **WLAN Access Point**: configures the access point of the WLAN expansion card

<table>
<thead>
<tr>
<th>Click this tab</th>
<th>To do these tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN Access Point</td>
<td>Enable the WLAN access point</td>
</tr>
<tr>
<td></td>
<td>Configure the SSID of the WLAN access point</td>
</tr>
<tr>
<td></td>
<td>Configure WLAN card IP address information</td>
</tr>
<tr>
<td>WLAN Client</td>
<td>Enable the WLAN client</td>
</tr>
<tr>
<td></td>
<td>Connect the device to a WLAN network</td>
</tr>
<tr>
<td></td>
<td>Disconnect the device from a WLAN network</td>
</tr>
</tbody>
</table>
Configuring the WLAN Card

The WLAN expansion card from Option acts as both a WLAN access point and WLAN client. The WLAN access point allows the CloudGate to connect other wireless devices to a wired or 3G network. The WLAN client allows the CloudGate to send and receive data over a WLAN network.

To use the WLAN expansion card, first, install the expansion card, and then configure the card by clicking the following tabs in the menu:

- WLAN Access Point
- WLAN Client
WLAN Access Point Tab

The WLAN Access Point tab lets you to manage the broadcast settings of the wireless access point. You can see this tab only when the CloudGate is installed with the WLAN expansion card.

General

**Enabled**

- Enables the WLAN access point

**WLAN Mode**

- Selects a 2.4Ghz or 5GHz access point.

**Channel**

- Selects the WLAN channel on which the access point has to work.

---

Information: The WLAN channel can only be selected when the WLAN client is disabled. In case the WLAN client is active, the access point will use the channel used by the WLAN client!

**Enable second SSID**

- Activates a second SSID.
SSID 1

**General**

- **Network name (SSID)**
  - Allows you to change the SSID.

- **Broadcast SSID**
  - If set to **Yes**, the SSID will be broadcasted.

- **Encryption**
  - Allows you to choose the type of encryption.

- **Password**
  - Sets the password.

**IP Config**
### IP Config

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>192.168.2.1</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Enable DHCP server</td>
<td>Yes</td>
</tr>
<tr>
<td>DHCP range</td>
<td>100 to 250</td>
</tr>
<tr>
<td>DNS 1</td>
<td></td>
</tr>
<tr>
<td>DNS 2</td>
<td></td>
</tr>
</tbody>
</table>

### Reserved leases

<table>
<thead>
<tr>
<th>Hostname</th>
<th>MAC</th>
<th>Lease time</th>
<th>IP</th>
<th>Active</th>
<th>Actions</th>
</tr>
</thead>
</table>

### Active leases

| Hostname | MAC  | IP   | Actions |

**IP address**

- Sets the IP address of the WLAN access point.

**Netmask**

- Sets the netmask of the WLAN access point.

**Enable DHCP server**

- Enables the DHCP server.

**DHCP range**
• Sets the DHCP range for the DHCP server.

**DNS 1 and DNS 2**

When the CloudGate is in **LAN mode** the DNS fields will be empty by default. As a result the CloudGate itself will act as a DNS server. All the connected ethernet devices will receive an DNS address which is equal to the CloudGates IP address (by default 192.168.1.1) When the DNS server inside the Cloudgate can't resolve the DNS request it will forward the request to the DNS server of the WAN connection.

When the CloudGate is in **WAN mode** the DNS address will be defined by the DHCP server of the internet provider. When the DNS fields are changed to another value than the other IP address will be used for the DNS server.

**Reserved leases**

• Lists the DHCP leases which are assigned to a MAC address.
• Click **Add** to assign another lease and link a MAC address to an IP address.

**Active leases**

• Lists the active DHCP leases of the devices connected to the Wi-Fi access point.
• Click **Reserve** to add the lease to the Reserve leases list.

---

**SSID2**

The SSID2 tab allows you to set or change some parameters for the second SSID. These parameters are identical as the parameters for the first SSID.
WLAN Client Tab

The WLAN Client tab allows the device to send and receive data over a WLAN network. The tab is available only when the CloudGate is installed with a WLAN expansion card.

Using this tab you can:

- Enable the WLAN client
- Connect to a WLAN network
- Manually Connect to a WLAN network
- Disconnect from a WLAN network
Enabled

- Click Yes to enable the WLAN client, and then click Save changes.

---

**IP Config**

**IP Mode**

- Click Dynamic to use IP addresses provided by the DHCP server
- Click Static to use a fixed IP address. Enter the IP address, netmask and DNS information.

**IP Config**

- Displays the IP, netmask and gateway addresses of the connected WLAN network.

---

**Available & Known networks**

- Lists the WLAN networks within range and displays the signal quality, SSID, status, and encryption method of each.
- Click the Refresh icon 🔄 to refresh the network list.

---

**Connecting to a WLAN Network**

To connect to a WLAN network:

1. Click the network name.

![m2msolutions](image)

2. Enter the network password and click Connect.
3. Note the status change to connected in the Available & Known Networks list.

Creating a Manual Connection to a WLAN Network

If the WLAN network you want to use is not in the list of known networks, you can create a manual connection.

1. Click **Manual connection**.

2. Enter the network SSID, select an encryption type and enter the network password.

3. Click **Save**.
Disconnecting from a WLAN Network

1. Click the Wi-Fi network to disconnect.

2. Click **Forget network**.
Welcome!

The CloudGate Hardware Guide provides the detailed technical information and hardware specifications for the CloudGate base unit.

This guide is designed for:

- Third-party developers
- Distributors
- System integrators
- Field engineers

Details about installing and configuring the CloudGate are available in the User Guide. Information about deploying CloudGate firmware, configuration and software updates is available in the Provisioning Server Guide.

Option also licences the CloudGate design to third party hardware and software developers who want to create custom expansion cards and software images for specific needs. For information on the developer program, contact Option Customer Support.
Mechanical Drawings

3D file of the CloudGate.

3D file of the front plate.

Below you can find the dimensions of the CloudGate.
IP-65 requirement

Below you can find the parts for the encasing which are needed to fulfill the requirements for IP-65.

All these parts can be ordered by TAKACHI:

- 1x box BCAK 203013G or BCPK 203013S,
- 1x plate BMP 2030P,
- 1 x screws (20pcs) MT4-8T,
- 1x bracket (2x4 pcs) BLF-2G(PC-GF) or CK-26P (metal SS)
- 3x cable gland MG-12S (3 inputs)
**Encasing M2M box**

<table>
<thead>
<tr>
<th>Box</th>
<th>BCAK 203013G (ABS+Key)UL94HB 200x300x131,5</th>
<th>BCPK 203013S (PC + Key)UL94VO 200x300x131,5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Plate</strong></td>
<td>BMP 2030P (ABS) WxDxt 166,5x266x4</td>
<td></td>
</tr>
<tr>
<td><strong>screws</strong></td>
<td>MT4-8T 20PCS M4 tapping</td>
<td></td>
</tr>
<tr>
<td><strong>Bracket</strong></td>
<td>BLF-2G (PC-GF) 4 Mounting brackets 4 screws M5x12</td>
<td>CK-26P (metal SS) 4 Mounting brackets 4 screws M5x10</td>
</tr>
<tr>
<td><strong>Cable gland</strong></td>
<td>MG-12S Ø12 cable range Ø3-6,5mm</td>
<td></td>
</tr>
</tbody>
</table>
Front and Back Panels

The front and back of the CloudGate case consists of a top panel and a bottom panel secured with Torx T6 screws.

The top panels are designed by Option and cannot be changed. The bottom panels can be customized based on the requirements of the expansion card.

Front Panel

Connectors

<table>
<thead>
<tr>
<th></th>
<th>WWAN Diversity antenna connector</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SMA-female</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Ethernet port</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>10/100 Mbps RJ-45</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>WWAN Main antenna connector</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>SMA-female</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Torx T6 screws</th>
</tr>
</thead>
</table>
**LEDs**

**LED Descriptions**

**Bottom Front Panel**

The bottom front panel covers the front expansion slot and is removed when installing a Primary Expansion Card.

Option provides a custom panel for the following expansion cards:

- Low Cost Serial Card
- Industrial Serial Card
- Basic Ethernet Switch
- PoE Ethernet Switch
- Telematics Card

**Back Panel**

![Back Panel Image]

**Connectors**
<table>
<thead>
<tr>
<th>1</th>
<th>Power connector</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• 9-33 VDC</td>
</tr>
<tr>
<td></td>
<td>• Micro-Fit 3.0, dual row, 4 circuits</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2</th>
<th>Reset button</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Press and hold for less than five seconds to reset the unit to the last working settings.</td>
</tr>
<tr>
<td></td>
<td>• Press and hold for five seconds or more to reset the unit to factory settings</td>
</tr>
</tbody>
</table>

**Bottom Back Panel**

The bottom back panel covers the opening for the back expansion slot and is removed when installing a Secondary Expansion Card.

Option provides a custom panel for the following expansion cards:

- Wi-Fi Card
LED Descriptions
<table>
<thead>
<tr>
<th><strong>LED</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>
| **WLAN State**                  | Indicates the connection status of the WLAN interface  
**Off:** not installed  
**Orange:** WLAN board = OK, client not connected and AP not enabled  
**Orange blinking:** AP disabled and Client connected / data traffic  
**Red:** board error/ (Any that causes AP or Client not to work)  
**Green:** AP enabled  
**Green flashing:** AP enabled and Client connected/data traffic                                                                                                                                                                                                                       |
| **WLAN Client Signal Strength** | Indicates the signal strength of the WLAN **CLIENT** interface when connected to a WLAN access point  
**Off:** The WLAN **CLIENT** is off or not connected  
**Orange:** The WLAN Client is receiving a moderate signal strength  
**Red:** The WLAN Client is receiving bad signal strength  
**Green:** The WLAN client is receiving good signal strength  
**Green flashing:** n/a                                                                                                                                                                                                                                                                  |
| **GPS/Aux State**               | Indicates the GPS operation  
**Off:** off  
**Orange:** on, no fix  
**Red:** error  
**Green:** on, has fix  
**Green flashing:** n/a                                                                                                                                                                                                                                                                 |
| **GPS/Aux signal strength**     | Indicates the signal strength of the GPS  
**Off:** no signal  
**Orange:** moderate GPS signal  
**Red:** bad GPS signal  
**Green:** good GPS signal  
**Green flashing:** n/a                                                                                                                                                                                                                                                                 |
| **System State**                | Indicates successful power on and device readiness  
**Off:** no power  
**Orange:** booting  
**Red:** error  
**Green:** on  
**Green flashing:** n/a                                                                                                                                                                                                                                                                 |
| **WWAN State**                  | Indicates WWAN or 3G interface availability and use  
**Off:** no power or not connected  
**Orange:** on, not connected  
**Red:** WWAN error  
**Green:** on, connected  
**Green flashing:** data traffic                                                                                                                                                                                                                                                                 |
| **WWAN Signal Strength**        | Indicates WWAN or 3G interface signal strength  
**Off:** no power or not connected  
**Red:** bad signal strength (< -104dbm)  
**Orange:** moderate signal strength (>= -104dbm & < -94dbm)  
**Green:** good signal strength (>= -94dbm)                                                                                                                                                                                                                                                                 |
Main Board Specifications

The CloudGate is designed with one main board and two additional expansion boards.

Main Board

The main board is identical for each base unit and is designed around a micro-controller which controls a WWAN module\(^1\) and the Ethernet interface.

Main Board Block Diagram (PDF)

Power Input

- V_PWR: min 9V DC, max 33V DC

Internal Power Supply

- Power input: V_PWR, min 9V DC, max 33V DC
- Stable 3.4V power rail
- Reverse polarity protection
- Over-voltage protection up to 60V
- Current limiter at 1.2A
- One-time fuse of 2A

Main Board Processor

- Freescale i.MX280 @ 450MHz
  - 64 MB RAM
  - 128 MB Flash memory
  - GTM68X WWAN module\(^1\)
  - Ethernet interface
  - Two expansion board connectors

Primary Expansion Board

The primary expansion board has the following interfaces:

- Power supply: V_PWR, 3V4, 3V3
- 24 Mhz clock signal
- Master reset signal
- High speed USB interface
- High speed OTG USB interface
- SDIO interface
- GPIO signals
- Serial interface

---

**Secondary Expansion Board**

The secondary expansion board has the following interfaces:

- Power supply: V_PWR, 3V4, 3V3
- 24 Mhz clock signal
- Master reset signal
- High speed USB interface
- SDIO interface
- GPIO signals

⚠️ **Note1:**
The CG0102 has no WWAN module!
Expansion Card Specifications

WLAN Card
Low Cost Serial Card
Industrial Serial Card
Basic Ethernet Switch
PoE Ethernet Switch
Developer Card
Telematics Card
HDK Card
WLAN Card Specifications

Specifications:

- According to 802.11 abgn spec
- Simultaneous access point and Client mode
- Dual SSID
- Up to 10 simultaneous users
- Supported encryption: WPA-PSK, WPA2-PSK, mixed WPA/WPA2-PSK

RF Specifications:

- The antenna connector on the front panel of the WLAN expansion card is a RP-female connector.
  - Click here for more RF specifications.
  - Click here for antenna recommendations.

⚠ Note: 5GHz WLAN operation
In order to reduce the potential for harmful interference to co-channel mobile satellite systems, the operation in the 5150-5250MHz band (channels 36 to 48) is restricted to indoor usage only. Outdoor usage in these channels is allowed in the US.

⚠ Note: group re-keying
The WLAN client of the CloudGate connected to a WLAN access point configured with WPA and group re-keying disabled is currently not supported.

⚠ RF EXPOSURE WARNING
A minimum distance of 20cm must be maintained between the user's body and the device antenna.
Industry Canada radiation exposure statement

This equipment complies with Industry Canada's RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p) is not more than necessary for successful communication.

This radio transmitter, IC 2734A-CG2101, has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

- 2.4GHz band: 3dBi (50Ω)
- 5GHz band: 3dBi (50Ω)
Low Cost Serial Card Specifications

Specifications:

- Female DB9 connector
- One serial port RS-232, 921.6 Kbaud maximum speed

Note: The serial card is DCE device!
Connect the CloudGate with a DTE device (laptop)

In order to connect the CloudGate to a laptop or any other DTE device you should use a regular straight cable.

![Diagram showing connections between CloudGate (DCE) and Laptop (DTE) ports](image)

Connect the CloudGate with another DCE device (modem, PLC,...)

In order to connect the CloudGate to another DCE device you should use a cross cable. (= null modem cable)

![Diagram showing connections between CloudGate (DCE) and DCE ports](image)
Industrial Serial Card Specifications

Specifications:

RS232

- One RS-232 serial port, 921.6 Kbaud maximum speed
- The RS232 interface on the industrial serial card is identical to the one on the low cost serial card. Please have a look at this [low cost serial card](#) for more info on the RS232 interface.

RS485

- One 22 KV isolated RS-485 serial port, 921.6 Kbaud maximum speed
- Connector: Examples of the connector you should use are:
  - Phoenix (MC 1,5/5ST-3.81)
  - Würth (691361300005)
- Termination switch: With this switch you can choose to terminate the RS485 network with a 120 Ohm resistor
- Wire selection: This switch allows you to use a 4 wire network or a 2 wire network

You can use the CloudGate in a 2 wire network as shown below:
You can use the CloudGate in a 4 wire network as shown below:

Note:
By default the TX and RX of the RS485 connection are disabled. So you have to enable them before you can start using the RS485 port. (You can enable this by using the DE and RE signals). For a 2 wire interface (=half duplex) you should of course only enable one direction at the same time.

Below an example of how to do this in your code. (The example shows how to activate both DE and RE)

```c
#include <stdio.h>
#include <string.h>
#include <fcntl.h>
#include <unistd.h>
#include <unistd.h>
```
```c
#include <sys/ioctl.h>
#include <errno.h>
/**************************************************************************
* Manifest Constants
**************************************************************************/
#ifndef TIOCM_OUT1
#define TIOCM_OUT1 0x2000
#define TIOCM_OUT2 0x4000
#endif
#define TIOCM_RE TIOCM_OUT1
#define TIOCM_DE TIOCM_OUT2
/**************************************************************************/  
int main (void)  
{  
  int fd = open("/dev/ttySP4", O_RDWR || O_NONBLOCK);  
  if (fd < 0) { printf("failed to pen device\n"); return 0; }  
  int status, err;  
  /* switch on RS485 TRANSMIT buffer and RECEIVE buffer */  
  ioctl(fd, TIOCMGET, &status);  
  status |= (TIOCM_DE | TIOCM_RE);  
  if ((err = ioctl(fd, TIOCMSET, &status)))  
  {  
    printf("ioctl error 0x%x, errno 0x%x, status %x", err, errno, status);  
  }  
  close(fd);  
  return 0;  
}
```
Basic Ethernet Switch Specifications

This section describes the Ethernet interface on the Basic Ethernet expansion board.

Specifications

- RJ-45 receptacle tab on top
- 4-port 10/100 Base-T
- One uSD card connector available
- Auto-MDIX

Pinout

Yellow LED:
- Active when operating speed is 100Mbps
- Inactive when operating speed is 10 Mbps or when not connected

Green LED:
- Active when valid links is detected
- Blinks when activity is detected
- Inactive when not connected
IMPORTANT: The auto-MDIX feature is always activated on the CloudGate. This feature automatically detects the required cable connection type (straight or crossed), and configures the connection appropriately, removing the need for crossover cables. In order for auto-MDIX to work correctly, auto-negotiation (auto speed and auto duplex) must be enabled on both sides of the link. Note that auto negotiation is always active on the CloudGate.

<table>
<thead>
<tr>
<th>Pin #</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pin 1</td>
<td>TX/RX+</td>
</tr>
<tr>
<td>Pin 2</td>
<td>TX/RX-</td>
</tr>
<tr>
<td>Pin 3</td>
<td>RX/TX+</td>
</tr>
<tr>
<td>Pin 4</td>
<td>Not used</td>
</tr>
<tr>
<td>Pin 5</td>
<td>Not used</td>
</tr>
<tr>
<td>Pin 6</td>
<td>RX/TX-</td>
</tr>
<tr>
<td>Pin 7</td>
<td>Not used</td>
</tr>
<tr>
<td>Pin 8</td>
<td>Not used</td>
</tr>
</tbody>
</table>
PoE Ethernet Switch Specifications

This section describes the Ethernet interface on the Ethernet PoE expansion board.

Specifications

- RJ-45 receptacle tab on top
- 4-port 10/100 Base-T
- Can function as a 2 ports Class 4 PoE or a 4-port Class 3 PoE
- Auto-MDIX

Pinout

Yellow LED:
- PoE indicator

Green LED:
- Active when valid links is detected
- Blinks when activity is detected
- Inactive when not connected
Option CloudGate - Last updated on 14/05/2014

IMPORTANT: The auto-MDIX feature is always activated on the CloudGate. This feature automatically detects the required cable connection type (straight or crossed), and configures the connection appropriately, removing the need for crossover cables. In order for auto-MDIX to work correctly, auto-negotiation (auto speed and auto duplex) must be enabled on both sides of the link. Note that auto negotiation is always active on the CloudGate.

Power Supply

- Connector: Examples of the connector you should use are:
  - Phoenix (MC 1,5/2ST-3,81)
  - Würth (691361300002)
- Operating voltage: 50 - 57Vdc, typical 56Vdc
- Power consumption: The mainboard of the Cloudgate consumes about 10W, the ethernet board can consume up to 60W (4x15w or 2 x 30W. So the total power should not exceed 70W.
- The POE ethernet board has an internal one time fuse of 2A
- The power plug is delivered together with the PoE Ethernet Switch expansion card. The plug is visible within the red circle in the picture below. This plug allows you to connect an external power supply to the socket on the PoE expansion card.

IMPORTANT: the polarity of the external power supply is indicated on the metal front plate of the expansion card.
**SAFETY WARNING**
When the PoE expansion board is inserted in the CloudGate, the CloudGate must be powered from the PoE power supply. The main power input on the back of the CloudGate will be disabled!

**SAFETY WARNING**
The PoE power supply operates on DC power provided via a DC power supply or AC power adapters. Only use power supplies rated at 56Vdc and make sure the product is installed near a power outlet that is easily accessible. This product is regarded a class III equipment where protection against electric shock is provided by means of power supplied from a SELV (Safety Extra Low Voltage) circuit and does not generate hazardous voltages within itself.

**SAFETY WARNING**
When using the PoE board at a power level lower or equal to 30W the temperature range in which you can use this board is equal to the temperature range of the CloudGate itself (-30°C to +70°C). However when the PoE board operates at a power level between 30W and 60W the temperature range is limited to -30°C to +45°C. When using an AC adapter make sure that the ambient temperature doesn’t exceed the specified temperature limits of the AC adapter.
Developer Card Specifications

The Developer card has the next functions available.

- One RS232 interface (8 pin)
- One SD card interface
- Two USB interfaces (one normal, one OTG)
- One temperature sensor
- One relay
- One analog input signal
- I2C bus
- Optocoupler
HDK Card

The HDK card allows hardware developers to make a prototype of their own board. The board contains a USB port and a large breadboard area for prototyping.

Important: When you plan to develop your own expansion card, you have to sign a License Agreement first. This will allow us to make you a Hardware Developer and will give you access to the Hardware Developer Kit, containing all the necessary hardware documentation in order to get started.
Please ask your Option contact person for a copy of the Licence Agreement.
Telematics Card

The telematics card can be delivered with or without plug on board:

- Telematics base board
- Telematics base board + I/O plug on board
- Telematics base board + CAN I/O plug on board

Telematics Board Block Diagram (PDF)

Telematics Base Board (CG1106)

On board features

- Cortex 32 bit MCU for I/O processing
- 3-axis 12 bit digital accelerometer
- 2 SIM sockets for SIM backup or roaming SIM functionality
- USB1: USB OTG interface
- USB2: USB type A interface
- DTE interface (UART0)
Front connectors

- USB OTG micro-AB-type connector, labeled as “USB1” on the front plate
- USB type A connector, labeled as “USB2” on the front plate
- DTE interface, labeled as “SERIAL 1 (RS232)” on the front plate

DTE interface

This interface is available on a male DB9 connector. The pinout is given in the table below:

<table>
<thead>
<tr>
<th>Pin number</th>
<th>Signal</th>
<th>Jumper position dependent signal (*)</th>
<th>Jumper position dependent signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RS232_DCD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>RS232_RXD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>RS232_TXD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>RS232_DTR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>GND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>RS232_DSR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>RS232_RTS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>RS232_CTS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>RS232_RI / V_PWR</td>
<td>RS232_RI if jumper in position 2-3</td>
<td>V_PWR if jumper in position 1-2</td>
</tr>
</tbody>
</table>

V_PWR is the input voltage of the Cloudgate, i.e. from 9 to 33 VDC. If there is no jumper present, then pin 9 of the DB9 connector is N.C. The factory default jumper connects pin 9 with the Ring Indicator (RS232_RI) input of the serial interface. The picture below shows the jumper in RI position.

There is also a corresponding marking on the PCB.
Telematics I/O Plug On Board (CG3101)

This board can be plugged onto the Telematics Base Board. The picture below shows the base board with the I/O expander plugged onto it.

Features

The I/O plug on board provides following features:

- 5 digital inputs (-150V to +150V)
- 2 analog inputs (0V to 3.3V, 12-bits resolution)
- 6 digital outputs (push-pull 0V to 3.3V OR open collector 0V to 30V/250mA)
- AUX serial port (UART4)
- 1-wire bi-directional interface

Note: The AUX serial port UART4 can be used with or without HW flow control:
In case it is used without HW flow control it takes 1 digital input and 1 digital output.
In case it is used with HW flow control it takes 2 digital inputs and 2 digital outputs

Electrical specifications

Digital inputs (DI1, DI2, DI3, DI4, DI5)

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Parameter</th>
<th>Conditions</th>
<th>Min</th>
<th>Max</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>VN</td>
<td>Input voltage</td>
<td>absolute maximum</td>
<td>-150</td>
<td>150</td>
<td>V</td>
</tr>
<tr>
<td>VI</td>
<td>Low level input voltage</td>
<td>-</td>
<td>1.04</td>
<td>V</td>
<td></td>
</tr>
<tr>
<td>VH</td>
<td>High level input voltage</td>
<td>1.90</td>
<td>-</td>
<td>V</td>
<td></td>
</tr>
<tr>
<td>ILKG</td>
<td>Input leakage current</td>
<td>0.0-3.3V</td>
<td>-</td>
<td>+0.1</td>
<td>mA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+/-150V</td>
<td>-</td>
<td>+1.5</td>
<td>mA</td>
</tr>
</tbody>
</table>

Analog inputs (AI1, AI2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Conditions</th>
<th>Min</th>
<th>Max</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input range</td>
<td>0.0-3.3</td>
<td>0.0</td>
<td>3.3</td>
<td>V</td>
</tr>
<tr>
<td>Input impedance</td>
<td>-</td>
<td>-</td>
<td>52</td>
<td>kΩ</td>
</tr>
<tr>
<td>Resolution</td>
<td>12-bit</td>
<td>0.8</td>
<td>-</td>
<td>mV</td>
</tr>
<tr>
<td>DNL error</td>
<td>+/-1</td>
<td>-</td>
<td>LSB</td>
<td></td>
</tr>
<tr>
<td>INL error</td>
<td>+/-1.5</td>
<td>-</td>
<td>LSB</td>
<td></td>
</tr>
</tbody>
</table>

Digital outputs (DO1, DO2, DO3, DO4, DO6, DO7)

<table>
<thead>
<tr>
<th>Mode</th>
<th>Symbol</th>
<th>Parameter</th>
<th>Conditions</th>
<th>Min</th>
<th>Max</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>push-pull</td>
<td>V_N</td>
<td>Low level output voltage</td>
<td>open circuit</td>
<td>0.0</td>
<td>-</td>
<td>V</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$I_D &lt; 8mA$</td>
<td>-</td>
<td>0.2</td>
<td>V</td>
</tr>
<tr>
<td></td>
<td>V_H</td>
<td>High level output voltage</td>
<td>open circuit</td>
<td>-</td>
<td>3.3</td>
<td>V</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$I_D &lt; 8mA$</td>
<td>1.9</td>
<td>-</td>
<td>V</td>
</tr>
<tr>
<td>open collector</td>
<td>I_SINK</td>
<td>Output sink current</td>
<td>-</td>
<td>250</td>
<td>-</td>
<td>mA</td>
</tr>
<tr>
<td></td>
<td>V_EXT</td>
<td>Open collector external pull-up voltage</td>
<td>open circuit</td>
<td>0.0</td>
<td>30.0</td>
<td>V</td>
</tr>
<tr>
<td></td>
<td>V_SINK</td>
<td>Low output voltage at max sink current</td>
<td>@ 250mA</td>
<td>-</td>
<td>0.2</td>
<td>V</td>
</tr>
</tbody>
</table>

- The digital outputs can be used in push-pull mode or as open collector. The selection is made by FW, based on certain eeprom parameter settings.
- In push-pull mode a DO can source up to 20mA in the “high” state. But the sum of the output currents
of all pins will be limited to 80mA max.

**I/O connector**

The external I/O’s are available on a Molex Micro-Fit 3.0™ connector, labeled as “GPIO” on the front plate.

The following table gives the front view and the pin numbering of the I/O connector.

<table>
<thead>
<tr>
<th>Pin number</th>
<th>Signal</th>
<th>Jumper position dependent signal(*)</th>
<th>Jumper position dependent signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>D3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>D14 / R1232 RX</td>
<td>D14 if jumper J3 is in position 13-14</td>
<td>RS232 RX if jumper J3 is in position 15-16</td>
</tr>
<tr>
<td>4</td>
<td>A1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>GND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>DO1 / R1232 RTS</td>
<td>DO1 if jumper J2 is in position 9-10</td>
<td>RS232 RTS if jumper J2 is in position 11-12</td>
</tr>
<tr>
<td>7</td>
<td>DO3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>1-WIRE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>GND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>D11 / -</td>
<td>D11 if jumper J5 is in position 21-22</td>
<td>N.C. if jumper J5 is in position 23-24</td>
</tr>
<tr>
<td>11</td>
<td>D15 / RS232 CTS</td>
<td>D15 if jumper J4 is in position 17-18</td>
<td>RS232 CTS if jumper J4 is in position 19-20</td>
</tr>
<tr>
<td>12</td>
<td>D/5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>A/2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>GND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>DO2 / RS232 TX</td>
<td>DO2 if jumper J1 is in position 5-6</td>
<td>RS232 TX if jumper J1 is in position 7-8</td>
</tr>
<tr>
<td>16</td>
<td>DO4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>DO6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>DO7</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(*) factory default jumper settings

The counter connector is a Molex Micro-Fit 3.0™ Receptacle Housing, Dual Row, 18 circuits. Part number of the receptacle housing: 43025-1800. Part number of the crimp terminals: 43030-0001. Datasheet and product specification can be found attached:

-Micro-Fit 3.0™ specifications
-Datasheet receptacle
-Datasheet crimp terminals

Information about the crimp tools can be found on the Molex website.
I/O jumper configuration

The jumpers allow to make a selection of certain signals on the external I/O connector.

The I/O expander card is delivered with 5 jumpers. The factory default positions are indicated in the picture (and also in green in the table below):

The table below gives the jumper settings.

<table>
<thead>
<tr>
<th>Pin 15</th>
<th>Pin 6</th>
<th>Pin 3</th>
<th>Pin 11</th>
<th>Pin 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>5</td>
<td>9</td>
<td>11</td>
<td>13</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>7</td>
<td>11</td>
<td>13</td>
</tr>
</tbody>
</table>

The factory settings are shown in green:

- Green = jumper present
- White = no jumper present

Important notes:

- Jumpers always need to be placed in “vertical position”
- Do not put any jumper on position 1-2
- Do not put any jumper on position 3-4
- The signals on pin 15, 6, 3 and 11 can be configured. The corresponding jumper has to be either on
the left hand side or in the right hand side position. Never put a jumper on both positions at the same

time.

In order to achieve a proper functioning of the I/Os, the FW settings need to correspond with the

settings of the jumpers.
- For pin 10 the jumper always needs to be present on pin 21-22. If it is in position 23-24 then pin 10 of

the I/O connector is not connected


Telematics CAN I/O Plug On Board (CG3102)

This board can be plugged onto the Telematics Base Board.

The picture below shows the base board with the CAN I/O expander plugged onto it.

![Telematics CAN I/O Plug On Board (CG3102)](image)

**Features**

The CAN I/O plug on board provides following features:

- 5 digital inputs (-150V to +150V)
- 2 analog inputs (0V to 3.3V, 12-bits resolution)
- 4 digital outputs (push-pull 0V to 3.3V OR open collector 0V to 30V/250mA)
- AUX serial port (UART4)
- 1-wire bi-directional interface
- CAN bus interface

Note: The AUX serial port UART4 can be used with or without HW flow control:

- In case it is used without HW flow control it takes 1 digital input and 1 digital output.
In case it is used with HW flow control it takes 2 digital inputs and 2 digital outputs.

## Electrical specifications

### Digital inputs (DI1, DI2, DI3, DI4, DI5)

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Parameter</th>
<th>Conditions</th>
<th>Min</th>
<th>Max</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>$V_N$</td>
<td>Input voltage</td>
<td>absolute maximum</td>
<td>-150</td>
<td>150</td>
<td>V</td>
</tr>
<tr>
<td>$V_{IL}$</td>
<td>Low level input voltage</td>
<td></td>
<td></td>
<td>1,04</td>
<td>V</td>
</tr>
<tr>
<td>$V_{IH}$</td>
<td>High level input voltage</td>
<td></td>
<td>1,90</td>
<td></td>
<td>V</td>
</tr>
<tr>
<td>$I_{LKG}$</td>
<td>Input leakage current</td>
<td>0.0-3.3V</td>
<td>-</td>
<td>+0.1</td>
<td>mA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+/-150V</td>
<td>-</td>
<td>+1.5</td>
<td>mA</td>
</tr>
</tbody>
</table>

### Analog inputs (AI1, AI2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Conditions</th>
<th>Min</th>
<th>Max</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input range</td>
<td></td>
<td>0,0</td>
<td>3,3</td>
<td>V</td>
</tr>
<tr>
<td>Input impedance</td>
<td></td>
<td></td>
<td>52 kΩ</td>
<td></td>
</tr>
<tr>
<td>Resolution</td>
<td>12-bit</td>
<td>0,8</td>
<td></td>
<td>mV</td>
</tr>
<tr>
<td>DNL error</td>
<td>+/-1</td>
<td></td>
<td></td>
<td>LSB</td>
</tr>
<tr>
<td>INL error</td>
<td>+/-1.5</td>
<td></td>
<td></td>
<td>LSB</td>
</tr>
</tbody>
</table>

### Digital outputs (DO1, DO2, DO6, DO7)

<table>
<thead>
<tr>
<th>Mode</th>
<th>Symbol</th>
<th>Parameter</th>
<th>Conditions</th>
<th>Min</th>
<th>Max</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>push-pull</td>
<td>$V_{OL}$</td>
<td>Low level output voltage</td>
<td>open circuit</td>
<td>0,0</td>
<td>-</td>
<td>V</td>
</tr>
<tr>
<td></td>
<td>$I_D &lt; 8mA$</td>
<td></td>
<td></td>
<td></td>
<td>0,2</td>
<td>V</td>
</tr>
<tr>
<td></td>
<td>$V_{OH}$</td>
<td>High level output voltage</td>
<td>open circuit</td>
<td></td>
<td>3,3</td>
<td>V</td>
</tr>
<tr>
<td></td>
<td>$I_D &lt; 8mA$</td>
<td></td>
<td></td>
<td></td>
<td>1,9</td>
<td>V</td>
</tr>
<tr>
<td>open collector</td>
<td>$I_{SINK}$</td>
<td>Output sink current</td>
<td></td>
<td>-</td>
<td>250</td>
<td>mA</td>
</tr>
<tr>
<td></td>
<td>$V_{EXT}$</td>
<td>Open collector external pull-up voltage</td>
<td>open circuit</td>
<td>0,0</td>
<td>30,0</td>
<td>V</td>
</tr>
<tr>
<td></td>
<td>$V_{SINK}$</td>
<td>Low output voltage at max sink current</td>
<td>@ 250mA</td>
<td>-</td>
<td>0,2</td>
<td>V</td>
</tr>
</tbody>
</table>

- The digital outputs can be used in push-pull mode or as open collector. The selection is made by FW, based on certain eeprom parameter settings.
- In push-pull mode a DO can source up to 20mA in the “high” state. But the sum of the output currents of all pins will be limited to 80mA max.
**I/O connector**

The external I/O’s are available on a Molex Micro-Fit 3.0™ connector, labeled as “GPIO” on the front plate.

The following table gives the front view and the pin numbering of the I/O connector.

<table>
<thead>
<tr>
<th>Pin number</th>
<th>Signal</th>
<th>Jumper position dependent signal (*)</th>
<th>Jumper position dependent signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>DI2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>DI4 / RS232 RX</td>
<td>DI4 if jumper J3 is in position 13-14</td>
<td>RS232 RX if jumper J3 is in position 15-16</td>
</tr>
<tr>
<td>4</td>
<td>AI1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>GND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>DO1 / RS232 RTS</td>
<td>DO1 if jumper J2 is in position 9-10</td>
<td>RS232 RTS if jumper J2 is in position 11-12</td>
</tr>
<tr>
<td>7</td>
<td>CANH</td>
<td>CAN bus termination</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>1-WIRE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>GND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>DI1 / -</td>
<td>DI1 if jumper J5 is in position 21-22</td>
<td>N.C. if jumper J5 is in position 23-24</td>
</tr>
<tr>
<td>11</td>
<td>DI3 / RS232 CTS</td>
<td>DI3 if jumper J4 is in position 17-18</td>
<td>RS232 CTS if jumper J4 is in position 19-20</td>
</tr>
<tr>
<td>12</td>
<td>DI5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>AI2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>GND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>DO2 / RS232 TX</td>
<td>DO2 if jumper J1 is in position 5-8</td>
<td>RS232 TX if jumper J1 is in position 7-8</td>
</tr>
<tr>
<td>16</td>
<td>CANL</td>
<td>CAN bus termination</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>DO6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>DO7</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(*) factory default jumper settings

The counter connector is a Molex Micro-Fit 3.0™ Receptacle Housing, Dual Row, 18 circuits. Part number of the receptacle housing: 43025-1800. Part number of the crimp terminals: 43030-0001. Datasheet and product specification can be found attached:

[Micro-Fit 3.0™ specifications](#)

[Datasheet receptacle](#)

[Datasheet crimp terminals](#)

Information about the crimp tools can be found on the Molex website.
**CAN bus termination**

The termination of the CAN bus can be configured by jumper settings. If the jumper is present then the on-board termination is connected to the bus. By default the jumpers are present on the card. Depending on the topology of the CAN bus the user can disconnect the on-board termination circuitry by removing the jumpers.

**I/O jumper configuration**

The jumpers allow to make a selection of certain signals on the external I/O connector.

The CAN I/O expander card is delivered with 7 jumpers. The factory default positions are indicated in the picture (and also in green in the table below).

The table below gives the jumper settings.

<table>
<thead>
<tr>
<th>CANL</th>
<th>CANH</th>
<th>DO2</th>
<th>RS232 TX</th>
<th>DO1</th>
<th>RS232 RTS</th>
<th>Di4</th>
<th>RS232 RX</th>
<th>Di3</th>
<th>RS232 CTS</th>
<th>Di1</th>
<th>N.C.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
<td>12</td>
<td>14</td>
<td>16</td>
<td>18</td>
<td>20</td>
<td>22</td>
<td>24</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>9</td>
<td>11</td>
<td>13</td>
<td>15</td>
<td>17</td>
<td>19</td>
<td>21</td>
<td>23</td>
</tr>
</tbody>
</table>

Pin 16 | Pin 7 | Pin 15 | Pin 6 | Pin 3 | Pin 11 | Pin 10

The factory settings are shown in green:
• Green = jumper present
• White = no jumper present

Important notes:

• Jumpers always need to be placed in “vertical position”
• Jumpers on position 1-2 and 3-4 can be removed if needed, based on the actual topology of the CAN bus
• The signals on pin 15, 6, 3 and 11 can be configured. The corresponding jumper has to be either on the left hand side or in the right hand side position. Never put a jumper on both positions at the same time.
  In order to achieve a proper functioning of the I/Os, the FW settings need to correspond with the settings of the jumpers.
• For pin 10 the jumper always needs to be present on pin 21-22. If it is in position 23-24 then pin 10 of the I/O connector is not connected.
RF Specifications

**WWAN Interface**

**Supported Frequencies**
- GSM, GPRS, and Edge bands: 850/900/1800/1900
- WCDMA bands: I, II, IV, V, VIII
- CDMA bands: BC0,1

**Output Power**
- Power Class 4 (2W, 33dBm) for GSM, GPRS 850/900 MHz bands
- Power Class 1 (1W, 30dBm) for GSM, GPRS 1800/1900 MHz bands
- Power Class E2 (0.5W, 27dBm) for Edge 850/900MHz bands
- Power Class E2 (0.4W, 26dBm) for Edge 1800/1900 MHz bands
- Power Class 3 (0.25W, 24dBm) for UMTS 850/900/1900/2100 MHz bands

**Antenna Interfaces**

**Main WWAN Antenna**
The main antenna is labelled **WWAN Main** on the front panel. [Learn about antenna recommendations.](#)

**Connectors**
- The RF connector on the CloudGate is SMA female.
- The antenna itself or the connector to the antenna should be SMA male.
Frequency Range

- Allows all frequency bands which the integrator wants to use

Performance

- Radiation pattern: Omni-directional
- Efficiency over all used frequencies: > 50%
- Maximum VSWR: < 2.5:1 with 50 Ω reference impedance

Polarization

- Linear

⚠️ RF EXPOSURE WARNING

To comply with FCC and Industry Canada regulations limiting both maximum RF output and human exposure to RF radiation, maximum antenna gain must not exceed:

- Cellular (800MHz) band < 4 dBi
- PCS (1900MHz) band < 3.5 dBi
- AWS (1700MHz) band < 3.5 dBi

To comply with the CE regulations, maximum antenna gain must not exceed the antenna gain of the Taoglas TG.09.0113 antenna.

Diversity WWAN Antenna

The diversity antenna is labelled WWAN Div GPS on the front panel. Learn about antenna recommendations.

IMPORTANT The diversity antenna is by default disabled (from firmware version 1.9.0 onwards). Learn how to enable the diversity antenna.

Connectors

- Uses the same type of connector as the main WWAN antenna

Frequency range

- Receive diversity only works on WCDMA and CDMA bands
- Only WCDMA and CDMA bands have to be supported by the diversity antenna.
- The GPS frequency must also be supported if GPS functionality is desired on the CloudGate.

Efficiency

- Radiation pattern: Omni-directional
- Efficiency over all used frequencies: > 25%
- Maximum VSWR: < 2.5:1 with 50 Ω reference impedance
Polarization

- Linear

**Mutual coupling** (main antenna and diversity antenna)

- Isolation: > 8dB
- Envelope correlation coefficient: < 0.5

**GPS Antenna**

The CloudGate only supports passive GPS antennas. There is no power supply for active antennas on the RF connector. For accurate GPS operation make sure the GPS antenna has a clear view of the sky.

**Maximum VSWR**

- < 2.5:1 with 50ohms reference impedance

**Polarization**

- RHCP antenna or a vertical polarized antenna

**Frequency range**

- Frequency range for GPS: 1575.42MHz ± 1MHz

**Efficiency**

- Efficiency: > 50%.

---

**Note1:**

The CG0102 will not support: the main WWAN interface, the diversity WWAN interface nor the GPS interface, as it doe not contain the WWAN module.

---

**WLAN interface**

The WLAN antenna is labelled **WLAN Main** on the bottom back panel. Learn about antenna recommendations.

For the Wi-Fi expansion card the following parameters are required for the antenna:

**Connector**

- The RF connector on the Wi-Fi expansion card is an RP-SMA female connector
The RF connector on the Wi-Fi antenna should be an RP-SMA male connector.

**Frequency range**

- 2.4 Ghz
- 5 Ghz

The integrator should only choose the frequencies he would like to use.

**Performance**

- Radiation pattern: Omni-directional
- Efficiency over all used frequencies: > 50%
- Maximum VSWR: < 2.5:1 with 50 Ω reference impedance

**Polarization**

- Linear

---

⚠️ **RF EXPOSURE WARNING**

To comply with CE, FCC and IC regulations limiting both maximum RF output and human exposure to RF radiation, maximum antenna gain must not exceed 3 dBi.
Antenna Recommendations

A number of good antennas are available on the market for use with the CloudGate. Below is a list of antennas which can be used as a reference for each functionality.

All antennas listed below are made by [Taoglas](#) and are available via [DigiKey](#)

**Main WWAN Antenna**

Taoglas TG.09.0113

- Recommended as the standard Main and Diversity antennas
- Recommended for all bands except GPS

**Diversity and GPS Antenna**

There are two recommended options for the Diversity and GPS Antenna.

**Option A**

Taoglas TG.30.8113

- Recommended for all bands including GPS
• Can be used as main antenna but very large

Option B

Taoglas TG.10.0113

• Not recommended for the main antenna (marginal low band performance)
• Recommended for high band diversity antenna
• Acceptable as low band (700-800-850-900MHz) Diversity antenna
• Recommended for GPS antenna

WLAN Antenna

Taoglas GW.59.3153

• Recommended for both 2.4 Ghz and 5 Ghz bands

Related Topics

RF Specifications
3G Connection Tab
Ethernet Specifications

This section describes the Ethernet interface on the CloudGate main board.

**Ethernet Interface**

- RJ-45 receptacle tab on top
- 10/100 Mbps
- 100BASE-TX
- Auto-MDIX

**Pinout**

Yellow LED:

- Active when operating speed is 100Mbps
- Inactive when operating speed is 10 Mbps or when not connected

Green LED:

- Active when valid links are detected
- Blinks when activity is detected
- Inactive when not connected
WAN/LAN Switchover Feature

The WAN/LAN switchover feature defines the state of the Ethernet port at power-on. By default, this feature is enabled. Learn how to disable WAN/LAN Switchover.

Two modes are possible:

- WAN mode: the Ethernet interface act as a WAN interface
- LAN mode: the Ethernet interface acts as a LAN interface

Each time the unit is powered on:

- CloudGate sends a DHCP discover message over the Ethernet interface.
- When it receives a DHCP offer it proceeds with the DHCP protocol and the Ethernet interface remains in WAN state.
- When it does not receive a DHCP offer it resends the DHCP discover message five times. If no DHCP offer is received after five tries, the CloudGate starts running a DHCP server on the Ethernet interface and act as a LAN interface.

TIP: WAN/LAN detection only happens during power on. The ethernet connection remains in the
same state (WAN or LAN) until a power cycle or reset has happened.

**Related Topics**

[Ethernet Tab](#)
Environmental Specifications

- Operating temperature: -30°C to 70°C
- Storage temperature: -40°C to 85°C
- Humidity operational: 5% - 95% non condensing
Power Requirements

Base Unit Power Supply

- Input voltage must be between 9V - 33V DC
- Internal electronic fuse limits the input current to 1.2A

![Option recommends to use a wire between the CloudGate and the external power supply of 22 AWG!]

⚠️ SAFETY WARNING
This device operates on DC power provided via a DC power supply or AC power adapters. Only use power supplies in the range 9-33V DC and make sure the product is installed near a power outlet that is easily accessible. This product is regarded a class III equipment where protection against electric shock is provided by means of power supplied from a SELV (Safety Extra Low Voltage) circuit and does not generate hazardous voltages within itself.

⚠️ SAFETY WARNING
When using an AC adapter make sure that the ambient temperature doesn’t exceed the specified temperature limits of the AC adapter.

As a reference, the power supply available from Option has the following parameters:

- Output voltage 12V DC
- Max output current 1A

In case you would like to use an industrial power supply Option recommends the next:


It can be sourced through Farnel, Mouser, digikey, ...

Power Connector

The power connector is a Micro-Fit connector from Molex (MX-43025-0400)
Preventing Fuse Overload

⚠️ SAFETY WARNING

On old CloudGate models, a huge inrush current caused by capacitors inside the CloudGate may cause an internal fuse to break. When using an external power supply with an output voltage higher than 15V, Option recommends using a special cable which will reduce the amplitude of these charge currents. This cable can be obtained at your CloudGate distributor. If the fifth digit of the serial number of the CloudGate is a "C", the CloudGate is an older model and susceptible to this remark. If the fifth digit is not a C, the fuse of your CloudGate will not get broken due to these charge currents.
Internal Power Circuits

The voltage applied by the power adapter to the CloudGate is converted into different voltage levels by the main board. Two different power circuits make five different voltage rails.

Dedicated high current power circuit

- Provides two different voltage rails which both can deliver high current levels:
  - **V_PWR**: Is the voltage level of the power adapter limited to 1.2A. A little voltage drop lower than 1V will be caused by the protection circuit.
  - **3V4**: A 3.4V power rail made by a dedicated power circuit which is used on the main board but also accessible by the expansion boards.

Low power circuit generated by the micro controller

- Provides three voltage rails for very limited power:
  - **3V3**: A 3.3V power rail provided by the micro controller is used on the main board but also accessible to the expansion boards.
  - **1V8**: A 1.8V power rail provided by the micro controller and only used on the main board.
  - **1V2**: A 1.2V power rail provided by the micro controller and only used on the main board.

<table>
<thead>
<tr>
<th>Voltage Rail</th>
<th>Voltage</th>
<th>Usage</th>
<th>Max Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>V_PWR</td>
<td>Equals the applied voltage of the power adapter. Use for power-hungry devices</td>
<td>Current is limited to 1.2A</td>
<td></td>
</tr>
<tr>
<td>3V4</td>
<td>3.4V</td>
<td>Powers all standard digital components on the expansion cards</td>
<td>3A maximum of which the main board is already using 1.5A. Only 1.5A is left for both expansion cards. (The sum of both expansion cards should be lower than 1.5A)</td>
</tr>
<tr>
<td>3V3</td>
<td>3.3V</td>
<td>Powers low power components or level translators from I/O signals on expansion connectors towards other components used the expansion cards</td>
<td></td>
</tr>
<tr>
<td>1V8</td>
<td>1.8V</td>
<td>Internal use only</td>
<td>Internal use only</td>
</tr>
<tr>
<td>1V2</td>
<td>1.2V</td>
<td>Internal use only</td>
<td>Internal use only</td>
</tr>
</tbody>
</table>
Internal Power Circuits Block Diagram

Filter + Protection:
- Reverse polarity protection
- 2A One Time Fuse
- 1.2A Electronic Fuse
- OVP up to 60V

Buck Conv:
Vin = 8 ~ 33V
Vout = 3.4V
Iout = 3A max

PMU

i.MX280
SIM Card Requirements

The CloudGate has an integrated (U)SIM interface compatible with the ISO7816 IC card standard. The 3GPP standard defines three operational voltages for the supply voltage of the SIM card: 1.8V, 3V and 5V. The CloudGate supports two voltages: 1.8V and 3V. The 5V-only SIM cards are rarely used and are not supported by the CloudGate.

General requirements:

- Changing of SIM cards while in operating mode, or hot-swapping, is not supported.
- Detection of the SIM card removal can take up to 30 seconds.
- The CloudGate will not be able to communicate with the SIM card after re-insertion. As a result, the CloudGate needs to be reset after re-insertion of the SIM.

Learn how to install a SIM card.
Certification and Operator Approvals

For detailed info about the obtained regulatory certification and operator approvals, please select your CloudGate product:

- CloudGate 3G Americas
- CloudGate 3G EMEA
- CloudGate 3G JP/APAC
- CloudGate Ethernet

Safety warnings

⚠️ Please read the following guidelines carefully. Not following these guidelines can cause harm to the CloudGate, yourself or other persons.

⚠️ RF EXPOSURE WARNING
A minimum distance of 20cm must be maintained between the user’s body and the device antennas.

General recommendations for use

- do not open your product when powered.
- do not expose to liquid, moisture or humidity.
- do not drop, throw or try to bend your product.
- do not paint your product.
- do not touch the antenna unnecessarily.

Ambient temperatures

Do not operate your product at ambient temperatures beyond the range of -30 and +70 degrees Celsius (exception: PoE functionality is limited to 45°C when using more than 30W). When using an AC adapter make sure that the ambient temperature doesn’t exceed the specified temperature limits of the AC adapter.

In restricted areas, such as dedicated equipment rooms or electrical closets, where the temperature can exceed 65°C, the temperature of the surface might reach high values and therefore under these conditions the products need to be protected against accidental contact. We recommend that operators who plan to use this product at these high temperatures stick a warning sticker, in accordance with IEC 60417-5041 (DB:2002-10), on a visible part of the device, or attach a sticker with the following text:

⚠️ WARNING
Explosive atmosphere

Turn off your device in any area with a potentially explosive atmosphere. It is rare, but your device could generate sparks, which could cause an explosion or fire. Areas with a potentially explosive atmosphere are not always clearly marked. They include fueling areas (petrol filling stations), below deck on boats, fuel or chemical transfer or storage facilities and areas where the air contains chemicals or particles, such as grain, dust, or metal powders. Do not transport or store your product in the compartment of a vehicle which contains flammable gas, liquid or explosives.

Blasting areas – construction sites

Turn off your product when in a blasting area in order to avoid interfering with two-way radios used in blasting operations.

Do not use on aircraft

Using a wireless devices on aircraft can cause interference. Do not use it when the plane is on the ground without permission from the aircraft crew.

Driving

Do not operate your device while driving. Park the vehicle first.

Medical equipment

Do not use near medical equipment, especially life support equipment that might be susceptible to radio interference.

ESD notice

Electrostatic Discharge (ESD) is caused by a buildup of static electricity and can happen when making contact with a product. To limit the likelihood of Electrostatic Discharge, it is recommended to:

- avoid conditions that result in high static electricity (carpet, cool and dry air,...);
- avoid touching any connectors when handling the unit; only touch the casing if possible;
- ground yourself prior to handling by touching a large metal object.

In case the product encounters loss of performance after an Electrostatic Discharge, please reset the device in order to restore it to normal functionality.

Class A device

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures. The operation of the CloudGate is restricted for use in a commercial, industrial or business environment.
Manufacturer's disclaimer statement

The information in this document is subject to change without notice and does not represent a commitment on the part of the vendor. No warranty or representation, either expressed or implied, is made with respect to the quality, accuracy, or fitness for any particular purpose of this document. The manufacturer reserves the right to make changes to the content of this document and/or the products associated with it at any time without obligation to notify any person or organization of such changes. In no event will the manufacturer be liable for direct, indirect, special, incidental, or consequential damages arising out of the use or inability to use this product or documentation, even if advised of the possibility of such damages.

For questions regarding your product or declaration, contact:
Option | Gaston Geenslaan 14 | 3001 Leuven | Belgium | www.option.com

To identify this product we refer to the Part, Series, or Model number found on the product.
CloudGate 3G Americas

Model: CG0192

FCC

This device complies with the applicable FCC rule parts. The FCC approval is valid for the CloudGate 3G Americas and the following expansion cards:

- model: CG1101, the Low cost serial card;
- model: CG1102, the Industrial serial card;
- model: CG1103, the Ethernet switch with PoE;
- model: CG1104, the Ethernet switch;
- model: CG1106, the Telematics base board;
- model: CG2101, the WLAN expansion card;
- model: CG3101, the Telematics I/O expander;
- model: CG3102, the CAN I/O expander.

Industry Canada

This device complies with the applicable IC rules. The IC approval is valid for the CloudGate 3G Americas and the following expansion cards:

- model: CG1101, the Low cost serial card;
- model: CG1102, the Industrial serial card;
- model: CG1103, the Ethernet switch with PoE;
- model: CG1104, the Ethernet switch;
- model: CG1106, the Telematics base board;
- model: CG2101, the WLAN expansion card;
- model: CG3101, the Telematics I/O expander;
- model: CG3102, the CAN I/O expander.

IFETEL & NOM (MEXICO)

This device completed the IFETEL homologation and carries the IFETEL number RTIOPCG14-0272. The device also obtained NOM approval and carries the NOM NYCE mark.
PTCRB

The CloudGate 3G Americas is PTCRB certified. PTCRB certification is only needed for the basic configuration, not for the expansion cards.

Operator approvals

The CloudGate 3G Americas is approved by several network carriers in America.

United States:
- Aeris
- AT&T
- Sprint
- T-Mobile
- Verizon Wireless

Canada:
- Bell Mobility
- Telus

Mexico:
- Telcel

Regulatory information

This device complies with Part 15 of the FCC rules and with Industry Canada license-exempt RSS standards. 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.

Federal communications commission notice

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.
Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

**Exposure Information to Radio Frequency Energy**

Users concerned with the risk of Radio Frequency exposure may wish to limit the duration of their calls and to position the antenna as far away from the body as is practical.

**Modifications**

Any changes or modifications made to this device that are not expressly approved by Option could void the user’s authority to operate the equipment.
CloudGate 3G EMEA

Model: CG0112

CE

This device complies with the essential requirements of the R&TTE directive (1999/5/EC) issued by the Commission of the European Union.

The CloudGate 3G EMEA is certified together with the following expansion cards:

- model CG1101, the Low cost serial card;
- model CG1102, the Industrial serial card;
- model CG1103, the Ethernet switch with PoE;
- model CG1104, the Ethernet switch;
- model CG1106, the Telematics base board;
- model CG2101, the WLAN expansion card;
- model CG3101, the Telematics I/O expander;
- model CG3102, the CAN I/O expander.

The R&TTE declaration of conformity can be downloaded at the bottom of this page.

E-mark

The CloudGate 3G EMEA is complying with the Automotive EMC requirements according to regulation UN ECE-R10 revision 4 and EU Automotive EMC directive 2004/104/EC.

The CloudGate 3G EMEA is certified together with the following expansion card:

- model CG2101, the WLAN expansion card.

Waste from Electrical and Electronic Equipment (WEEE)
Attention: Your product is marked with this symbol. Electrical and electronic equipment should not be disposed of with general household waste. There is a separate collection system for these items.

Please contact your supplier for information on their disposal policy. You may be charged for the costs of take-back and recycling. In some countries, small products in small quantities may be disposed of at designated collection facilities. Please contact your local authority for details.

CE Declaration of Conformity (R&TTE)
CloudGate 3G JP/APAC

Model: CG0122

Japan

This device complies with the Japanese Radio Law and Telecommunications Business Law. The CloudGate 3G JP/APAC can be used with the following expansion cards:

- model: CG1101, the Low cost serial card;
- model: CG1102, the Industrial serial card;
- model: CG1103, the Ethernet switch with PoE;
- model: CG1104, the Ethernet switch;
- model: CG1106, the Telematics base board;
- model: CG2101, the WLAN expansion card;
- model: CG3101, the Telematics I/O expander.

3G Antennas

The CloudGate 3G JP/APAC can only be used in Japan with one of the antennas listed below.

Taoglass antennas:
- TG.09.0113
- TG.10.0113
- TG.30.8113

Pulse antennas:
- GPSCP00
- GPSCWCP00
- GPSDM700-2500FFS
- GPSDM700-5800SSS (minimum attenuation needed: 1.5dB)
- RO8061-21702NM
- RO8061-21702NF
- RO8063-21704NM (minimum attenuation needed: 1.5dB for FDD 1)
- RO8063-21704NF (minimum attenuation needed: 1.5dB for FDD 1)
- SLPT698-2170DMN (minimum attenuation needed: 2.7dB for FDD 1, 0.6dB for FDD 6, 0.3dB for FDD 8)
- SLPT698-2170NMOHF (minimum attenuation needed: 2dB for FDD 1, 0.7dB for FDD 6, 0.3dB for FDD 8)
- SPDA24700-2700
- W1920G0915
- W1920G3658
- WA700-2700SMA
NOTE
Some of the antennas listed are high gain antennas and can only be used when additional attenuation is applied. For these antennas the minimum attenuation needed is indicated per frequency band.

WLAN Antennas

The WLAN expansion card can only be used in Japan with one of the antennas listed below.

Taoglass antennas:

- GW.59.3153

Pulse antennas:

- GPSDM700/2500FFS
- GPSDM700/5800GGT
- NMO4E4900B
- NMO5E2400B
- W1027
- W1030
- W1038
- W1043
- RO2408NF (minimum attenuation needed: 1.7dB for 2.4GHz)
- RO2408NM (minimum attenuation needed: 1.9dB for 2.4GHz)
- RO5210NF (minimum attenuation needed: 3.1dB for 5GHz)
- RO5210NM (minimum attenuation needed: 3.2dB for 5GHz)
- SB24003
- SLPT698/2170DMN
- SLPT698/2170NMOHF
- SLPT2400/5900DMN
- SLPT2400/5900NMOHF
- SLPT2400DMN
- SLPT2400NMOHF
- SLPT4900NMOHF
- SLPT4900DMN
- W1028B
- W5001
- W5010
- W5011

NOTE
Some of the antennas listed are high gain antennas and can only be used when additional attenuation is applied. For these antennas the minimum attenuation needed is indicated per frequency band.
WARNING
Operation in the 5GHz frequency band is restricted to indoor use only.
CloudGate Ethernet

Model: CG0102

**FCC**

This device complies with the applicable FCC rule parts. The FCC approval is valid for the CloudGate Ethernet and the following expansion cards:

- model CG1101, the Low cost serial card;
- model CG1102, the Industrial serial card;
- model CG1103, the Ethernet switch with PoE;
- model CG1104, the Ethernet switch;
- model CG1106, the Telematics base board;
- model CG2101, the WLAN expansion card;
- model CG3101, the Telematics I/O expander;
- model CG3102, the CAN I/O expander.

**Industry Canada**

This device complies with the applicable IC rules. The IC approval is valid for the CloudGate Ethernet and the following expansion cards:

- model CG1101, the Low cost serial card;
- model CG1102, the Industrial serial card;
- model CG1103, the Ethernet switch with PoE;
- model CG1104, the Ethernet switch;
- model CG1106, the Telematics base board;
- model CG2101, the WLAN expansion card;
- model CG3101, the Telematics I/O expander;
- model CG3102, the CAN I/O expander.

**CE**

This device complies with the essential requirements of the R&TTE directive (1999/5/EC) issued by the Commission of the European Union.

The CloudGate Ethernet is certified together with the following expansion card models:

- model CG1101, the Low cost serial card;
- model CG1102, the Industrial serial card;
- model CG1103, the Ethernet switch with PoE;
- model CG1104, the Ethernet switch;
- model CG1106, the Telematics base board;
- model CG2101, the WLAN expansion card;
- model CG3101, the Telematics I/O expander;
- model CG3102, the CAN I/O expander.

The R&TTE declaration of conformity can be downloaded at the bottom of this page.

**Waste Electrical and Electronic Equipment (WEEE)**

[Image]

Attention: Your product is marked with this symbol. Electrical and electronic equipment should not be disposed of with general household waste. There is a separate collection system for these items.

Please contact your supplier for information on their disposal policy. You may be charged for the costs of take-back and recycling. In some countries, small products in small quantities may be disposed of at designated collection facilities. Please contact your local authority for details.

---

**Regulatory information**

This device complies with Part 15 of the FCC rules and with Industry Canada license-exempt RSS standards. 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.

---

**Federal communications commission notice**

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.
Modifications

Any changes or modifications made to this device that are not expressly approved by Option could void the user's authority to operate the equipment.

CE Declaration of Conformity (R&TTE)
Certification of third-party expansion cards

Option offers third-party hardware developers the possibility to design their own expansion cards for the CloudGate. The CloudGate and the Option expansion cards are compliant with the necessary regulatory requirements, but third-party hardware developers should still make sure the final product remains compliant when inserting their expansion cards into the CloudGate. Before placing these tailor-made expansion cards in the market, it’s the hardware developer’s task to evaluate its expansion card for continued compliance. This page aims to give some initial guidance on the amount of certification that is needed.

The regulatory requirements for expansion cards are typically concerned with the correct use of the radio spectrum, EMC, safety and health regulations. They check if the product is working according to RF regulations and is safe for use; for example, no unwanted emissions, not too high power emissions, the effective use of RF spectrum, etc. Finally, also correct labeling and information to the end user is needed.

The amount of testing and certification work highly depends on the supported functionality. Digital devices containing no wireless transmitter can still transmit unwanted emissions (unintentional radiators) which can interfere with other devices. Devices containing a wireless transmitter should make sure their RF behavior is within specification and meets safe limits for people.

The most common regulatory approvals are described now.

**Federal Communications Commission (FCC)**

When selling/operating your own expansion card in the USA, it shall comply with the rules of the Federal Communications Commission. When the expansion card contains a wireless transmitter, more testing will be need than when the expansion card doesn’t have a wireless transmitter.

**Expansion card without wireless transmitter**

Even when a digital device contains no wireless transmitter, it can still emit RF noise and cause interference to other digital devices. To tackle this, the FCC has imposed rules for these “unintentional radiators”. The FCC requirements can be found in FCC Part 15, subpart B “unintentional radiators”. Depending on the type of Part 15B device, a different equipment authorization procedure is required. Most expansion cards will fall in the category “Class A digital devices, peripherals & external switching power supplies” and will be subject to the “Verification” method. This means testing the conducted and radiated emissions and keeping the test results on record, while no FCC logo or FCC ID is needed.

These FCC Part 15, subpart B tests can be executed in authorised test labs.

**Expansion card with wireless transmitters**

Expansion cards with wireless transmitters shall still comply with the requirements for the non-transmitting parts explained above. In addition one should check the requirements for the specific frequency of
the transmitter. Typically tests are required for RF output power, modulation characteristics, occupied bandwidth, frequency stability and radiated spurious emissions. In addition the expansion card will mostly be required to carry its own FCC ID. When the expansion card makes use of an already certified radio module, the test results might be fully or partially re-used and there’s no need for a new FCC ID.

The FCC differentiates between licensed and unlicensed transmitters.

- licensed transmitters: devices operating in a frequency that is licensed by the FCC (e.g. PCS 1900MHz or cellular 850MHz). The FCC strictly controls interference in these bands!
- unlicensed transmitters: devices operating in unlicensed frequency bands. Different technologies can be used in these frequency bands and interference restrictions are less severe (e.g. 2.4GHz WLAN, Bluetooth, Zigbee...).

Technical standards for licensed and unlicensed equipment are found in the various radio service rule parts. Depending on the specifications of your expansion card, testing is needed for the applicable rule part(s). Some common rule parts include:

- FCC Part 15C for Intentional Radiators (2.4GHz band);
- FCC Part 15E for UNII devices (5GHz band);
- FCC Part 24 Personal communications services (1900MHz band);
- ...

Please visit the FCC website for more detailed info on the equipment authorization procedures and the different FCC rule parts.

These FCC tests can be executed in authorised test labs.

**Industry Canada (IC)**

When you want to sell/use your expansion card in both Canada and USA, it is advised to do the IC and FCC testing together. Typically the same testing can be performed, resulting in reduced testing costs.

**Expansion card without wireless transmitter**

Digital devices without transmitter are typically categorized as "interference causing equipment". These devices shall comply with ICES-003 requirements for Digital Apparatus and are approved through the method of Self-Declaration of Compliance (SDoC). Similar as FCC Part 15B devices, compliance is checked for conducted and radiated emissions. When compliant with the limits, the product shall carry a compliance label stating “CAN ICES-3 (A)/NMB-3 (A)” for a typical Class A device.

These ICES-003 tests can be executed in authorised test labs.

**Expansion card with wireless transmitters**
Expansion cards with wireless transmitters shall still comply with the requirements for the non-transmitting parts explained above. In addition one should check the requirements for the specific frequency of the transmitter. Typically tests are required for RF output power, modulation characteristics, occupied bandwidth, frequency stability and spurious emissions. In addition the expansion card might be required to carry the IC ID.

When the expansion card makes use of an already certified radio module, the test results might be fully or partially re-used.

Similar as for FCC, Industry Canada differentiates between licensed and unlicensed ("license-exempt") transmitters. Depending on the specifications of your expansion card, testing is needed for the applicable standard(s). The technical standards for licensed and unlicensed equipment are found in the various Radio Standards Specifications:

- RSS-210 for License-exempt radio apparatus (2.4GHz, 5GHz,....);
- RSS-132 for cellular telephone systems (850MHz);
- RSS-133 for 2GHz personal communication services (1900MHz);
- ...

Please visit the Industry Canada website for more info on the radio equipment certification procedures and Industry Canada's standards page.

These IC tests can be executed in authorised test labs.

**CE**

Before selling/operating a device in the European Union it needs to be compliant with all the applicable directives and regulations. The most common are:

- R&TTE directive;
- Automotive EMC directive;
- RoHS directive;
- REACH regulation;

When developing a new expansion card one should make sure the full device is still compliant.

For the R&TTE directive, this means evaluating the product according to the applicable standards related to EMC emissions, EMC immunity (ESD, surge,....), radio spectrum, RF exposure and product safety. Some typical standards include:

- EN 301489 and/or EN 55022/55024 for EMC emissions and immunity (ESD,....);
- EN 60950-1 for ITE safety;
- EN 300 328 for 2.4GHz devices;
- EN 301 893 for 5GHz devices;
- EN 62311 for RF exposure;

When compliance is demonstrated a Declaration of Conformity shall be written to declare the product is compliant with the R&TTE directive (and some other CE directives). The use of a Notified Body is optional, but might be useful to check what amount of testing is needed. In that case the Notified
Body number shall be added behind the CE mark.

Please visit the European Commission website for more details on the different EU directives and regulations.

ℹ️ The info on this page is for information purpose only. Other certification might be needed and actual certification requirements might differ from the information on this page. It's the responsibility of the third-party hardware developer, to make sure the product complies with the applicable regulatory requirements.
CloudGate Universe Guide

Welcome!

The CloudGate Universe Guide explains how to deploy firmware, configuration and developer images to multiple devices.

This guide is designed for:

- Distributors
- System integrators
- Developers
- Field engineers

Information about installing and configuring the CloudGate is available in the User Guide. Details about CloudGate hardware specifications and technical information are available in the Hardware Guide.

Option also licences the CloudGate design to third party hardware and software developers who want to create custom expansion cards and software images for specific needs. For information on the developer program, contact Option Customer Support.
Introducing the CloudGate Universe

The CloudGate Universe Server is the configuration and deployment mechanism for the CloudGate. From the factory, CloudGate base units have no customization.

On power-up, the CloudGate connects to the CloudGate Universe over the wired Ethernet port and automatically downloads the appropriate update. If the Ethernet interface is unavailable, then the CloudGate uses the WWAN interface to download the updates.

The CloudGate can download the following files from the CloudGate Universe:

- CloudGate firmware: device firmware provided by Option.
- CloudGate developer image: customized software that provides additional functionality to the device or controls third-party expansion cards.
- CloudGate config file: configuration settings that can be applied to one or more CloudGates
- CloudGate GOBI firmware image: software that updates changes to wireless operator firmware
Creating an Account

To create an account:

1. In a web browser, enter the URL: http://cloudgate.option.com.
2. On the login page, click on the Sign up button.
3. Enter your user details on the Sign up page and click Create new account. Your account will be created and a confirmation email sent to you. Click the link in the email to activate your account.
Click **I want to activate my device** to activate your device at the same time as creating an account. This step is optional because you can always activate devices once you are logged in.

Click **I have received a group invitation code** if someone else has given you access to their devices by sending you a group invitation code. Enter the code and click **Sign up** to create an account.
Activating a CloudGate Using CloudGate Universe

You can activate a CloudGate three ways:

- When you create an account.
- On the CloudGate Universe once you are logged in.
- Using your smartphone.

Activating a Device While Creating an Account

To activate a CloudGate at the same time as creating an account:

1. In a web browser, enter the URL: http://cloudgate.option.com.
2. On the login page, click on the Sign up button.
3. Enter your user details in the Sign up page, and click I want to activate my device.
4. Enter the device serial number and activation code.
5. Click **Create new account** to activate your unit and create an account.
Activating a Device Once Logged On to the CloudGate Universe

To activate a CloudGate once you are logged in to the CloudGate Universe:

1. Make sure the Devices tab is selected, and click the **Activate device** button.

2. Complete the fields and then click **Activate**.
Logging on to CloudGate Universe

To log on to CloudGate Universe:

1. In a web browser, enter the URL: http://cloudgate.option.com.
2. Enter your username and password and click **Sign In**.

- Click **Forgot your password?** and follow the instructions to reset your password.
- Click **Don't have an account yet?** to create an account.
Editing Your User Profile

Once your create an account, you can change your user profile, including:

- Username
- Password
- Email address
- Company name
- Language settings

To edit your user profile:

1. Click the username in the menu and select Edit Profile.

2. Edit the fields as required.

3. If changing the email address or password, enter the current password.
4. Click **Save**.
Quick Tour

Here’s a quick tour of the main CloudGate Universe pages:

- **Provisioning page**
- **Content page**
- **Groups page**

## Provisioning Page

The Provisioning page lists each active device in your account and displays the following device properties:

- **Name**: defines the name of the device.
- **Description**: defines a description of the device as required.
- **Type**: displays the device type assigned by the system depending on the serial number.
- **Serial number**: displays the serial number given to the device during production.
- **Check in frequency**: defines when the device contacts the Provisioning server to check for updates.

## Content Page
The Content page lists the images available on the CloudGate Universe:

- **CloudGate Firmware**: required firmware developed by Option.
- **CloudGate Config**: configuration settings for one or more devices; can be a custom config or default Option config.
- **CloudGate Developer Image**: optional, customized software on top of the mandatory Option firmware created by third party developers or integrators for additional functionality, or for controlling third-party expansion cards; only available to members of the Option Developer Program.

> You can only see the "Cloudgate Developer Image" tab when you are a developer. Normal users will not see this tab!

- **CloudGate GOBI Firmware**: required firmware developed by Qualcomm that updates the wireless operator firmware.

> You can only change the "CloudGate Gobi Firmware" on a CloudGate - WCDMA+EVDO (=CG0192)
The Groups page organizes devices into user groups with firmware and software image presets—or "default releases". With a "default release" assigned to each user group, you can easily provision many devices with identical releases of firmware and software.

Group properties include:

- **Devices:** lists the devices in the group.
- **Content:** displays the firmware and software updates assigned to the group.
- **Users:** lists the user accounts attached to the group.
- **Admins:** lists the user accounts with permission to create groups and templates.
- **Default releases:** defines the set of firmware, configuration and developer images assigned to the group.
Upgrading Devices

The main function of the CloudGate Universe is to provide an easy-to-use mechanism for upgrading CloudGate devices before and after deployment in the field.

You can do the following tasks:

- **Sort and select devices** by group, serial number and other criteria so that you can quickly find the devices you need to update
- **Edit device name and description** if necessary
- **Set the check in, or update frequency**, which defines when a device checks the CloudGate Universe for available updates
- **Select specific images for automatic download** when the device connects with the CloudGate Universe
- **Disable updates** if you don't want automatic downloads to occur
- **Apply default releases** so that you provision groups of devices with similar settings in one step
- **Download images to a laptop** or hard drive if you need to update a device manually
Displaying and Sorting the Device List

The Provisioning page list is an inventory of all CloudGate base units for which the user has provisioning access (this includes devices activated by the current user and devices in groups the user belongs to).

TIP The currently logged in user is identified by the account name on the right side of the menu.

The Device list is displayed by clicking Provisioning in the menu. The list can be sorted a number of ways and devices selected through clicking or shift+clicking. The Details pane on the right contains tools for editing device properties, such as the assigned release of firmware, time of the next scheduled update, and the user group assigned to each device. To display device properties, select a device in the list, and then click the Device properties, Release slots, and User groups tabs.

Sorting the Device List

When there are too many devices to view on one screen, use the filters to display devices with similar characteristics. Sorting devices makes it easier to select a large number of devices based on group, name, serial number and a number of other criteria.
Filter by group

- Use the Filter user group box to sort a large number of devices (fastest method)
- Requires devices to be already organized into more than one subgroup

Filter by search term

- Finds devices with a specific text string in any field

Filter by device status

- Use the Status filter field
- Finds devices based on the update status:
  - ✔ Up to Date: the device is provisioned with the assigned release of firmware or software
  - ! Needs Update: the device is not provisioned with the assigned release of firmware or software
  - ? Unknown: the device is not activated

Filter by name

- Finds devices with a specific text string in the Name field

Filter by type

- Finds either the North American or European CloudGate models using the type field

Filter by serial number

- Finds devices with a specific text string in the serial number field
Setting the Check-In Frequency

The check-in frequency is the interval at which a device connects to the CloudGate Universe and checks for updates.

To set the check-in frequency:

1. Click **Provisioning** in the menu.
2. Select the device(s) in the Device list.
3. In the Device Properties tab, select an option for **Check-in frequency**.

**IMPORTANT** Option recommends caution when setting the check-in frequency to **NEVER**. If **NEVER** is selected, the next time the device connects to the CloudGate Universe, the automatic check-in function will be turned off permanently. Even if the check-in frequency is changed later, the device will not connect with the CloudGate Universe and download the new setting.
4. Click **Save**.
Enabling Automatic Update

If you are responsible for managing M2M deployments of all sizes, keeping devices up to date with the correct version of firmware and software is time consuming. One of the most powerful features of the CloudGate Universe is the ability to automatically update devices with assigned, or preset, images.

You can specify the firmware, configuration, and developer images you want the CloudGate Universe to download to the device the next time it checks in. Each image occupies a release slot on the CloudGate.

There are four types of images and four release slots:

- CloudGate Firmware Image
- Config File
- Developer Image - only available to members of the Option Developer Program
- CloudGate Gobi Image

Tip: There are two ways to select images for automatic update. You can create a "default release" for a specific group of devices. Or, you can select one or more devices in the Device list and assign the images for download using the Release Slots tab. Follow the steps below.

To enable automatic update and select the images for download at the next device check-in:

1. Click Provisioning in the menu.
2. Select one or more devices.
3. Click the Release Slots tab
4. Ensure Ignore slot is NOT selected for each image you want to enable automatic update.
5. To assign a specific image, select the image from the "assigned release" drop down box.

Ignore slot

- Disables automatic update for the image.
Current release

- Displays the currently provisioned release for the selected device(s).

Assigned release

- Selects the specific image release for download to the selected device(s).

6. Click **Save**.
Disabling Automatic Update

You can disable the automatic update feature so that firmware, configuration and developer images are not downloaded when the device connects to the CloudGate Universe.

Each image can be disabled separately. For example, you can enable automatic updates for CloudGate Firmware but disable it for the Config File.

To disable automatic update:

1. Click **Provisioning** in the menu.
2. Select one or more devices.
3. Click the **Release Slots** tab.
4. Select **Ignore slot** for the image you want to disable. Remember to do this for each image in the Details pane.
5. Click **Save**.
Changing the Device Name and Description

When you activate a device, the CloudGate Universe adds a factory-set name and description to the device properties. Option recommends changing the name and description to something meaningful for your CloudGate deployment.

To change the device name and description:

1. Click **Provisioning** in the menu.
2. Edit the **Name** and **Description** fields as required.
3. Click **Save**.
Deactivating Devices

If you need to disassociate a device from the CloudGate Universe for some reason, for example the device is damaged, or will be provisioned through a different account, you can deactivate the device.

NOTE: Deactivation means you will no longer have access to the device through the CloudGate Universe.

To deactivate a device:

1. Click Provisioning in the menu.
2. Select a device.
3. Click the Deactivate button on the Device Properties tab.
4. In the confirmation dialog box, click Deactivate.
Managing Images

The CloudGate Universe allows you to manage the firmware and software images for the CloudGate base unit. Each image can have multiple releases.

You can do the following tasks:

- Manage CloudGate firmware provided by Option
- Manage developer images for controlling third party expansion cards or software
- Manage CloudGate configurations as well as upload a config file from a locally configured device
- Manage Gobi firmware for the 3G Gobi radio module
- Download images to laptop or hard drive

---

Note 1:
Developers images are only visible to persons which have a developers account!

Note 2:
Gobi firmware images can only be changed on the "CloudGate WCDMA + EVDO" (=CG0192)
Managing CloudGate Firmware

The CloudGate Universe allows you to see a list of all CloudGate firmware releases. You can download images from this list to a hard drive if you need to update a device manually.

The list of CloudGate firmware is displayed by clicking Content in the menu, followed by the CloudGate Firmware button or tab. Below the tab, the Products list contains the collections of firmware or software available. Click Option Firmware (the only option in this case), to display the list of available releases and then select a release by clicking it. Note that the only action available is to Download the release to a hard drive.
Managing Developer Images

The ability to manage developer images is only available if you are a member of the Option developer program. To become member of the developer program, upgrade your account via the "upgrade to developer" setting.

For information on displaying and uploading developer images, log on to your developer account, click Developer tools in the menu, and select Software Developer Kit.
Managing Configurations

The CloudGate Universe allows you to maintain and organize CloudGate configurations (config files). Config files contain the 3G, Ethernet, firewall, software watchdog, and other system settings for the CloudGate base unit and expansion cards.

Config files are displayed by clicking Content in the menu followed by the CloudGate Config button or tab. Below the tab, the Products list shows the collections of config files available.

Learn more about uploading a custom config file to the CloudGate Universe

To display the available config files for your account:

1. Click Content in the menu.
2. Click CloudGate Config.
3. Click on one of the products available.
4. Select a release by clicking it and displaying the release details on the right.
Creating config files

Once you have downloaded a config file from a CloudGate you can upload this config file to other CloudGates. This allows you to create many identical CloudGates.

However before you can upload your config file to other CloudGates you will have to transform it a little bit.

To do this:

1. Download the configuration file via the "Download config" button in the system tab. This will generate a config.bin file.
2. Go to https://cloudgate.option.com:8443/static/cfgimg.html
3. You will see the next:

   ![Load configuration:](image)

   4. Press the "Choose file" button and select the file you downloaded in step 1
   5. Press the upload button.
   6. You will see the next:
7. Press the "Create config image" button.
8. This will generate a *.zip file.
9. This zip file you can upload on the provisioning server or on the WebGUI of the CloudGate.
Uploading a Config File

The config files are maintained in different "Products". The "Option default configs" is a "product" which contains all the configs delivered by Option. Next to this product you will also find a "Product" per usergroup you are allowed to see.

Before you can upload a config file you first have to create it properly. Go to Create Config Files for more information.

To upload a config file:

1. Click Content in the menu.
2. Click CloudGate Config.
3. Select the product of the usergroup in which you would like to upload your config file. (You can't upload to the "Option default configs" product!)
4. Click Upload release.
5. Select the file and enter a Version, Name and Description. (This is the file you have created in "Creating config files")
6. Click **Upload**.
7. If the upload is successful, the release name and version number appears in the list.

💡 **TIP** The Provisioning Server does not automatically increment version numbering. You must specify the correct version number in the Upload dialog box.
Managing Gobi Firmware

Gobi Firmware is the firmware by Qualcomm for the 3G Gobi radio module.

NOTE Releases of Gobi firmware are uploaded by Option. You cannot upload or download versions of Gobi firmware from the Provisioning Server.

Gobi firmware is displayed by clicking Content on the menu, followed by the CloudGate Gobi Firmware button on tab. Below the tab, click Option Gobi Firmware in the Products list.
Downloading Images

In some cases, you may have to manually update CloudGate base units. Manual updates require the image files to be downloaded to a laptop or hard drive.

To download all the firmware, config files and developer images assigned to a device at once:

1. Click **Provisioning** on the menu.
2. Select the device in the list that has the images you want to download.
3. Click **Download all releases** and save the file to another location.

To download each image separately:

1. Click **Content** on the menu.
2. Click the **CloudGate Firmware**, **CloudGate Developer Image**, or **CloudGate Config** button or tab.

   **IMPORTANT** The Gobi Firmware cannot be downloaded separately.

3. In the Products list, click the appropriate firmware, image or config product to display the releases.
4. Click a release to select it, and then click **Download** on the right and save the file to another location.
Learn about manually uploading an image to a device using the on-device web interface.
Managing Groups of Devices

For provisioning multiple devices at once, the CloudGate Universe allows you to organize CloudGate base units into groups. Groups have preset firmware and config file assignments. When a new device is added to the group, these presets are automatically assigned to the device. The next time the device checks in, the CloudGate downloads the images all at once.

Using the Groups, you can do the following tasks:

- Display the devices in each group and images provisioned to each device in the group
- Create new groups and subgroups
- Add devices to a group for provisioning
- Add users and administrators for managing or creating groups
- Create "Default releases"
Creating Groups

When you create an account, the Provisioning Server creates a personal user group for you. For example, Jim Doe Group. Any devices activated under your account are added to your personal user group by default.

You can then create subgroups within your personal user group to organize your devices more efficiently. For example, you may want to organize devices by customer (such as M2M Solutions and Sensor Solutions) or by department (such as Field Services and Development).

Besides your personal user group, you may have access to other top level groups. These appear in the group hierarchy at the same level as your personal user group. These are groups that another administrator has given you administrator access to. When you have admin access, you can add users to a group.

Your personal user group (and any other groups you have access to) are displayed by clicking Groups in the menu. A group can be selected from the list on the left by clicking the group to highlight it. The details pane on the right contains tools for displaying the devices in a group, adding users and administrators to a group, and creating default releases.

To create a subgroup:

1. Click Groups in the menu.
2. Select a group to highlight it.
3. Click Add Subgroup.

Enter a name and description, and then click Add. The subgroup appears in the hierarchy below your personal user group.
Add subgroup

This will add a new subgroup to **MyCloud's group - MyCloud's personal usergroup**.

Name

Description

[Cancel]  [Add]
Adding Devices to a Group

After creating the groups you want to use, you can add devices to them.

To add devices to a group:

1. Click **Provisioning** in the menu.
2. Select the devices to add to the group in the Device list.

   TIP If you have lots of devices, use the filters to sort the Device List first, then use the Select All checkbox at the top of the column to highlight all the sorted devices at once.

4. Click **User Groups** in the Details pane on the right.

5. Select the user groups you want to add the devices to. A device can belong to more than one group as long as it also belongs to the group immediately above it in the hierarchy.

   TIP If a group is greyed out in the list, it means that you do not have permission to add the selected device to that group.

6. Click **Save**.
Creating Default Releases

When provisioning a number of CloudGate base units with identical settings, you can create a default release to speed up the process.

A “Default Release” contains preset firmware, configuration and developer image assignments for a specific user group. By applying the "Default Release" to selected devices, you can easily provision a large number of devices at once.

For example, if you have a user group called Field Services, you can create a "Default Release" for that group that specifies a particular developer image. The developer image may contain customized software for your site application. You can then assign the "Default Release" to all the devices in Field Services. When the devices connect for the first time with the CloudGate Universe and check for updates, the contents of the "Default Release", in this case a new developer image, is automatically downloaded to all the devices in the group.

You can create "Default Releases" that specify a particular release of CloudGate firmware, developer image, config file, and Gobi firmware.

To create a Default Release:

1. Click Groups in the menu.
2. Select a group by clicking the name to highlight it.
3. Click the Default Releases tab.
4. Edit the change release options for each image and click Save to update the "Default Release" with the new presets.
### Details for JimDoe's group - JimDoe's personal usergroup

#### CloudGate Firmware
- Change release: 1.18.0

#### CloudGate Developer Image
- Change release: empty

#### CloudGate Config
- Change release: No preset

#### CloudGate Gobi Firmware
- Change release: Gobi image 30-06-2013
Displaying Group Content

To display the images assigned to a group in the device template:

1. Click **Groups** in the menu.
2. Select a group on the left by clicking to highlight it.
3. Click the **Content** tab on the right to display a list of images, including custom developer images (if any) and custom configuration files. Note you can only see the image name and type, not the specific release version. To display the release assignments, click **Default Releases**.

1. Click **Manage products** to go to the Content page where you can upload new config files and developer images (for members of the Option developer program).
Managing Users and Group Administrators

The CloudGate Universe supports two types of users: Users and Group Administrators.

Regular users include anyone who creates an account, such as developers (members of the Option developer program) and non-developers (field engineers and installers).

Group Administrators, or Admins are a special class of user with the ability to assign users to different groups. For example, an Admin can create a subgroup for field engineers and a subgroup for developers, and then assign users to each group as appropriate.

💡 TIP When you create an account, you are automatically made Admin of your own personal group.

For managing users and admins, you can do the following tasks:

- Assign users to a group
- Remove users from a group
- Create a group admin
Assigning Users to a Group

Only users assigned to a group can provision of the devices in that group.

ℹ️ NOTE: To assign users to a group, you must be an Admin for that group.

To assign users to a group:

1. Make sure you are an Admin for the group. Learn more about creating an Admin user.
2. Click Groups in the menu.
3. Select a group on the left by clicking to highlight it.
4. Click the Users tab on the right to display the list of users with provisioning access to the devices in the selected group.

1. Click Invite user by email.

💡 TIP: If the Invite button is not displayed, you may not be the Admin for the selected group. Only Admins can assign users. If you are an Admin and the Invite button is still not available, try refreshing your browser.

1. Enter the user's email address. Click Make admin to make the user an administrator. Click Send Invitation.
1. If the user already has an account, the user will be added immediately. Refresh your browser window to see the user added to the list. If the invited user does not have an account, a confirmation email is sent with a link to the CloudGate Universe sign up form. Once the user completes the sign up process and logs on to the CloudGate Universe, he or she is added to the group.
Creating a Group Admin

A Group Admin, or administrator, is a user who has the ability to assign users to a group.

¡NOTE: To assign users to a group, you must be an Admin for that group.

To create an Admin for a group:

1. Follow the steps for assigning a user.
2. Make sure you click Make admin in the Add User dialog box.
Removing Users from a Group

To remove a user from a group of devices:

1. Click **Groups** in the menu.
2. Select a group on the left by clicking to highlight it.
3. Click **Edit users**.
4. Uncheck the user(s) you want to remove, and click **Save**.

**NOTE:** Removing a user from a group does not delete the user or the account from the CloudGate Universe.
Troubleshooting

What is the priority order between port forwarding rules, DMZ and remote login in the internal routing table?

How does the automatic upgrade feature work on the CloudGate Universe?

Why does the page display incorrectly?

How does connection priority work in conjunction with connection persistence?

How to configure CloudGate to switch automatically to 3G when the fixed DSL connection is offline?
How does connection priority work in conjunction with connection persistence

First off all it is crucial to understand both features run as separate services on the CloudGate although their output is heavily linked.

In essence the **connection priority** feature is responsible to make sure the CloudGate is **connected** to the best available communications link. **Connection Persistence** however is ensuring that the **service** required for proper operation is reachable.

The CloudGate will first attempt to connect to the highest priority network selected in the connection priority table. In case after 15 seconds this does not yield in a connected state the next interface will be started to try and connect in parallel to the primary interface. If after an additional 15 seconds none of the previously started interfaces is in connected state the next interface in line will be started. It is important to understand Cloudgate will keep checking higher priority interfaces for their connection status.

Example: Connection priority is configured in following order: 1. Ethernet; 2. WLAN; 3. 3G interface. At startup CloudGate will check is the Ethernet is connected, if not the WLAN interface will be started; at that point Cloudgate will check both WLAN and Ethernet. When WLAN is in a connected state Cloudgate will keep checking the Ethernet interface in the background and will switch back to the Ethernet interface incase the state is changed to connected.

Example: Connection priority is configured in following order: 1. WLAN; 2. Ethernet; 3. 3G interface. The WLAN interface reports it is connected although connection persistence reports it cannot resolve the requested destination address. (e.g. Cloudgate is connected to a WLAN network with a captive portal active). CloudGate will start the Ethernet interface. When Ethernet is connected and connection persistence reports the link is accepted Cloudgate will start using the Ethernet interface.

⚠️ The 3G interface has additional reset options: When connection persistence detects the 3G interface is not connected to its appropriate service the interface will initially get a soft reset as all the other interfaces can get but if this is unsuccessfull the 3G interface will be rebooted without having to rebooting the CloudGate.
How to configure CloudGate to switch automatically to 3G when the fixed DSL connection is offline?

This is how it works:

1.) Click on the ‘Move up/down’ arrows to set the ‘Main ethernet’ interface as the #1 interface the CloudGate uses to connect to the internet. (See screenshot above)

2.) Click on the ‘Move up/down’ arrows to set the ‘3G Connection’ interface as the #2 interface the CloudGate uses to connect to the internet. (See screenshot above)

3.) Make sure the CloudGate is connected via fixed DSL line.

4.) Reboot the CloudGate. (this will cause the ‘Main Ethernet’ interface to act as a WAN interface instead of a LAN interface)
5.) The main Ethernet port will act as a WAN interface and the CloudGate will receive an IP address from the fixed DSL network DHCP server automatically.

6.) Once the fixed DSL line’s internet connection is lost, the CloudGate will automatically connect to the 3G network for as long as the fixed DSL connection is offline.

7.) When the fixed DSL connection is back online, all traffic will be routed through the ‘Main Ethernet’ interface once again.
Priority Order Between Remote Login, DMZ, and Port Forwarding Rules

An internal routing table gives priority for different routing rules like remote login, DMZ, and port forwarding rules.

IMPORTANT: The first line of this table has the highest priority.

Default

By default, the DMZ and remote login are not active, and the CloudGate rejects all external IP traffic wanting access to the unit. This is also the reason why the WAN -> Local default policy is set to Reject in the firewall rules.

In this case, the routing table looks like:

- Reject everything

Remote Login Enabled

If remote login is enabled, you make a hole in this firewall at port 443. (Even when you do not enter “443” in the port list!)

In this case, the routing table looks like:

- Port 443 is open for HTTPS
- Reject everything

TIP These two lines are always at the bottom of the routing table.

If you add port 1800 in the remote login port field, both port 443 and port 1800 will be open.

In this case, the routing table looks like:

- Port 1800 is open for HTTPS
- Port 443 is open for HTTPS
- Reject everything

DMZ

The DMZ has a lower priority than the remote login and port forwarding rules, so activating the DMZ results in the next routing table:

- Port 1800 is open for HTTPS
• Send all incoming data to the address specified in the DMZ
• Port 443 is open for HTTPS
• Reject everything

**Port Forwarding Rules**

Adding port forwarding rules results in the next routing table:

• Port 1800 is open for HTTPS
• IP forwarding rule 1
• IP forwarding rule 2+
• Send all incoming data to the address specified in the DMZ
• Port 443 is open for HTTPS
• Reject everything
When Do Automatic Updates Occur?

The CloudGate tries to connect to the CloudGate Universe every time it powers on, and when it is configured to reset at regular time intervals.

Automatic updates occur when the following settings are enabled:

- On-device web interface:
  - Provisioning tab -> Enable automatic provisioning is set to Yes
- CloudGate Universe:
  - Devices tab -> Device Properties tab, Check-in frequency is set to every day, hour, week or month.
  - Devices tab -> Release Slot tab, Ignore Slot checkbox is unchecked; and there is an update available.

Manual updates occur when:

- On-device web interface:
  - Provisioning tab -> Check for updates button
- CloudGate Universe:
  - Devices tab -> Release Slot tab, Ignore Slot checkbox is unchecked; and there is an update available.

Automatic Update Flow Chart
Press "Check for updates" in WebGUI.

Automatic check for update at power on and at "check-in frequency".

"Check in frequency" = Never

Is "enable automatic provisioning" active in WebGUI?

Yes

Upgrade if available and allowed by the "ignore" box.

No

Do nothing
Why Does the Page Display Incorrectly?

If the CloudGate Universe or CloudGate on-device web interface does not display correctly, reports error messages, or does not display at all, make sure that your PC meets the following minimum browser requirements:

For the CloudGate universe:

- Chrome 27.0(.1453.110 m)
- Firefox 21.0
- Internet Explorer 9(.0.8112.16421)
- Internet Explorer 10(.0.9200.16540)

For the CloudGate one-device web interface:

- Internet Explorer 9
- Safari 5.1
- Firefox (Windows 21.0, Mac 12.0)
- Chrome (Windows 27.0.1453.110, Mac 26.0.1410.65)
- Opera (Windows 12.02, Mac 12.10)
Licenses

Most of the source code used in the CloudGate is available under free, open source license.

The following licenses are used:

- GPLv2
- GPLv3
- LGPLv2
- LGPLv2.1
- DROPBEAR
- GOBISERIAL
- LIBCURL
- LIBGCC
- LIBJSON
- LIBUUID
- LIGHTTPD
- OPENSSH
- OPENSSL
- PCRE
- ZLIB
Copyright (c) 2004, 2005 Metaparadigm Pte Ltd

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.