

CloudGate



CloudGate User Guide

CloudGate Setup Guide

Last updated on 18/06/2019

Table Of Content

1. CloudGate Setup Guide	3
1.1. Setup the Base Unit	4
1.1.1. Logging On	6
1.1.2. Home Tab	7
1.1.3. Interfaces Tab	12
1.1.3.1. Main Ethernet	15
1.1.3.2. Main Ethernet - WAN	22
1.1.3.3. LTE Connection	23
1.1.3.4. 3G Connection	30
1.1.4. Firewall Tab	42
1.1.5. Conn. Persistence Tab	50
1.1.6. Provisioning Tab	57
1.1.7. System Tab	60
1.1.8. VPN Tab	70
1.2. Setup Expansion Cards	76
1.2.1. Ethernet Switch Tab	77
1.2.2. WLAN Client Tab	81
1.2.3. WLAN Access Point Tab	87
1.2.3.1. WLAN Access Point Tab 1	88
1.2.3.2. WLAN Access Point Tab 2	94

CloudGate Setup Guide

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 CloudGate does automatically recognize the presence of an expansion card. The web interface is updated accordingly: it shows one or multiple additional tabs that allow the user to configure the parameters of the inserted expansion card(s).

The following subsections explain:

- how to configure the base unit
- how to configure the expansion cards

The web interface allows you to configure one device at a time.

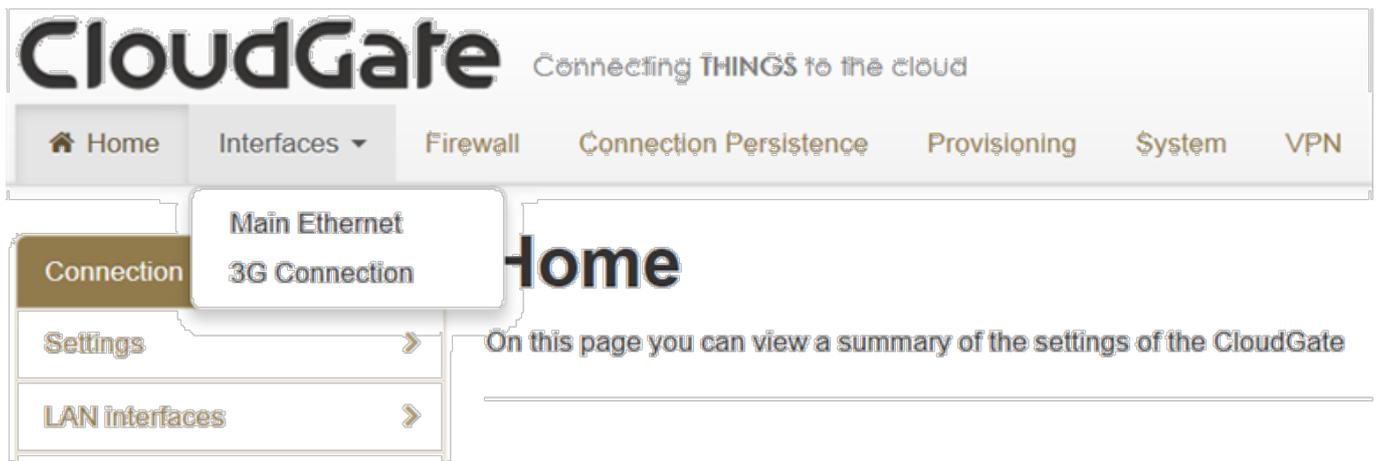
Setup and configure the Base Unit

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. The procedure how to do this is explained in the CloudGate Universe Guide.

In the Logging On section you can 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, Interfaces, Firewall, Connection Persistence, Provisioning, System and VPN. In the Interfaces tab you can select between Main Ethernet and 3G or LTE Connection.



Click this tab	To do these tasks
Home	<ul style="list-style-type: none"> - Verifying the Internet Connection - Checking the Firmware Version
Interfaces, then select Main Ethernet	<ul style="list-style-type: none"> - Disabling the WAN/LAN Switchover Feature - Managing IP Configuration Settings
Interfaces, then select 3G Connection ¹	<ul style="list-style-type: none"> - Configuring the WWAN Interface - Choosing a Wireless Operator - Setting Up SIM Parameters - Setting Up WWAN Connection Parameters - Choosing PIN Code Settings - Setting up Verizon Wireless or Sprint wireless operators

Click this tab	To do these tasks
Firewall	<ul style="list-style-type: none"> - Setting Default Firewall settings - Setting Up the DMZ - Setting Up Inbound Port Forwarding - Setting Up Outbound Port Filtering - Setting Up Outbound Trusted IPs - Setting Up Static Routing
Connection Persistence	<ul style="list-style-type: none"> - Configuring the Connection Watchdog - Configuring the Automatic Timed Reset
Provisioning	<ul style="list-style-type: none"> - Setting up Automatic updates
System	<ul style="list-style-type: none"> - Setting up the Time Zone - Setting up Remote Access to the CloudGate - Setting up a Dynamic DNS Service - Changing the Username and Password <ul style="list-style-type: none"> - Creating Log Files - Download a configuration file - Manually Resetting the CloudGate
VPN	<ul style="list-style-type: none"> - Setting up Tunnel Management

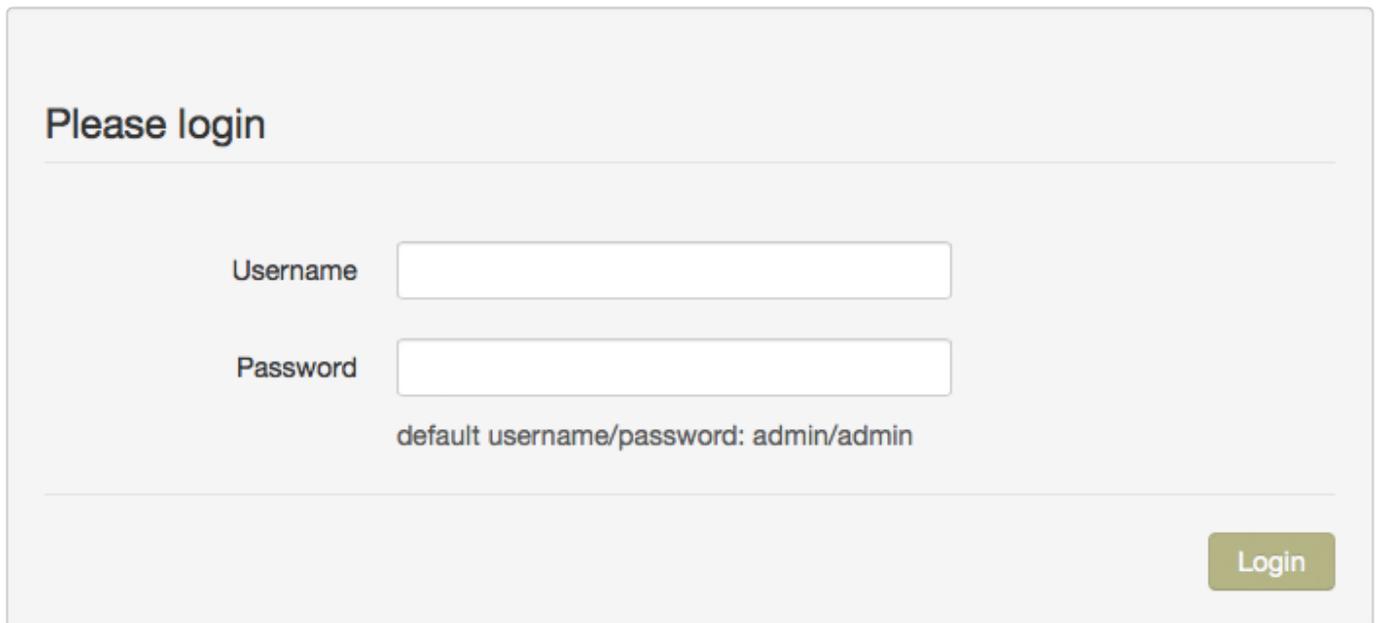
Note1:

The CloudGate Ethernet (CG0102) will not show a "3G connection" tab as it has no WWAN module. Newer CloudGate models have an LTE interface.

1.1.1. Logging On to the Base Unit

To log on to the on-device web interface:

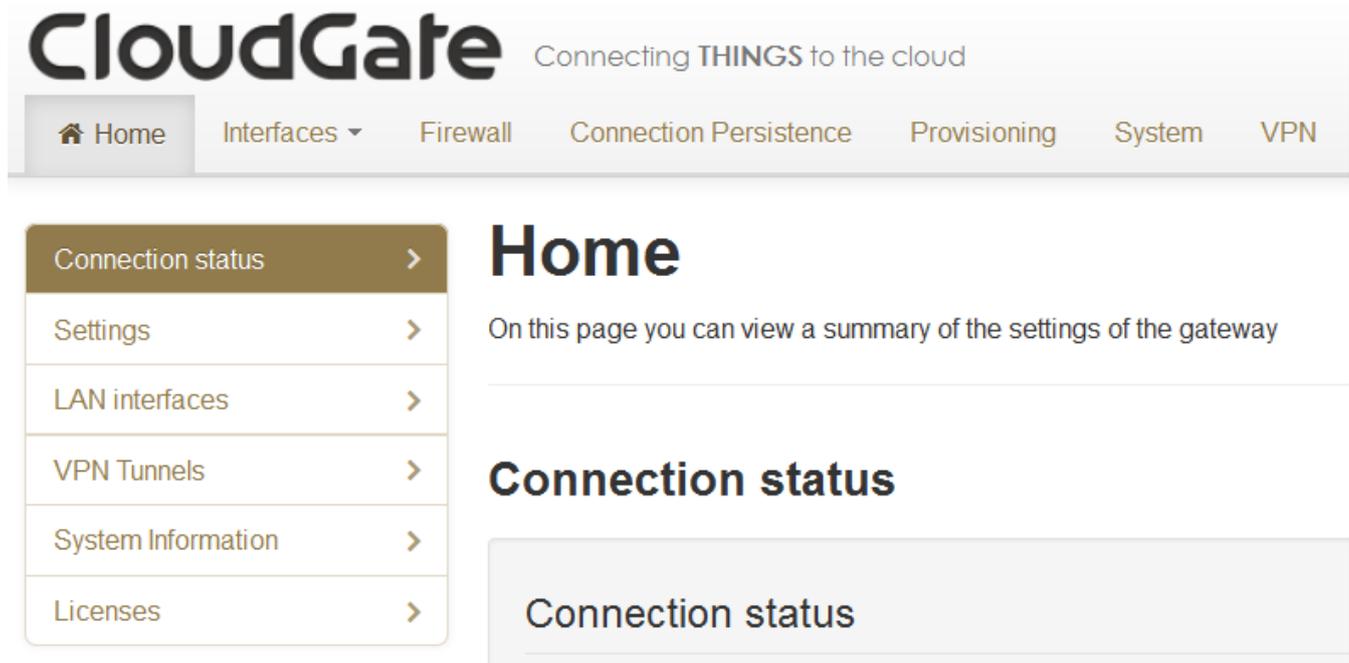
1. In a web browser, go to the URL: 192.168.1.1.
 2. Enter the username and password, and then click "Login".
- Use the default username "admin" and password "admin". It is strongly recommended to change the default username and password later via the System Tab, however.



The screenshot shows a web interface for logging in. At the top left, the text "Please login" is displayed. Below this, there are two input fields: "Username" and "Password". Underneath the password field, the text "default username/password: admin/admin" is shown. In the bottom right corner, there is a green "Login" button.

1.1.2. Home Tab

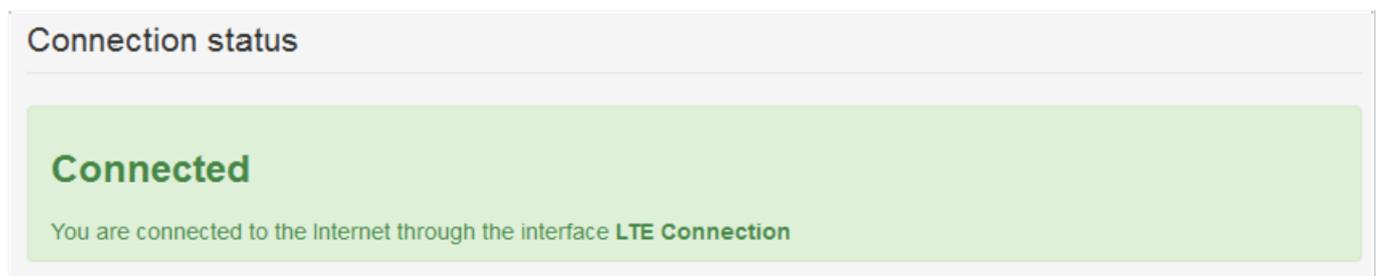
The Home tab displays the CloudGate connection status, the connection settings, the different available LAN interfaces, the VPN tunnels and the system information, like firmware and software versions installed.



Connection status

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

In case of a CloudGate LTE that is connected to the LTE network, the screen looks as follows:



In case of a CloudGate 3G that is connected to the 3G network, the screen looks as follows:

Connection status

Connected

You are connected to the Internet through the interface **3G Connection**

Connection settings

In case of a CloudGate LTE that is connected to the LTE network, the screen looks as follows:

Settings

Internet connection enabled Yes No

Connection strategy Manual Priority-based

#	Interface	Connection status	IP	Move up/down
1	LTE Connection	Connected	37.62.4.92	

For a CloudGate 3G the screen looks as follows:

Settings

Internet connection enabled Yes No

Connection strategy Manual Priority-based

#	Interface	Connection status	IP	Use for internet connection
1	3G Connection	Connected	92.48.145.253	<input checked="" type="checkbox"/>
2	WLAN Client			<input type="checkbox"/> Use this

Note: the WLAN client settings are not present if there is no WLAN expansion card (CG2101) inserted.

Internet connection enabled:

This parameter enables (yes) or disables (No) the WAN interface.

- default = Yes

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.

- default = Priority based

Important:

The CloudGate decides that he's not connected anymore when:

- For the Ethernet connection the cable is removed.
- For the Cellular 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 their IP address.

LAN interfaces			
#	Interface	Enabled	IP
1	Main Ethernet	✓	192.168.1.1
2	WLAN Access Point 1	✓	192.168.2.1
3	WLAN Access Point 2		192.168.3.1

Note: the WLAN interfaces are not present if there is no WLAN expansion card (CG2101) inserted.

VPN Tunnels

This is a list of the active VPN tunnels.

VPN Tunnels			
#	Interface	Connection status	Type

System information

System Information

Device serial number: **MX19D3C0JN**

There are no updates available on the CloudGate Universe server.

Firmware version: **Option Firmware - 1.43.0**

Image version: **No application - not set**

Configuration version: **Option Default Configs - empty**

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. More information can be found in the CloudGate Universe Guide.

1.1.3. Interfaces Tab

The interfaces menu groups the settings of all connection technologies.

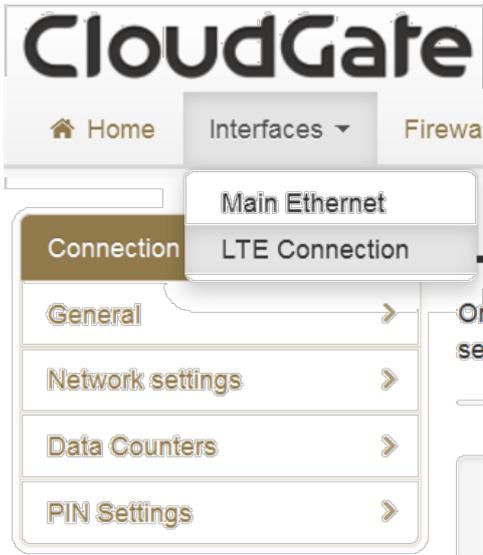
The content of this menu depends on the CloudGate model and on the expansion cards that are inserted.

CloudGate LTE WW

In case of a CloudGate LTE WW base unit the Interfaces Tab looks as follows:

- Main Ethernet
- LTE Connection

Note: the base unit is the CloudGate without expansion cards inserted.

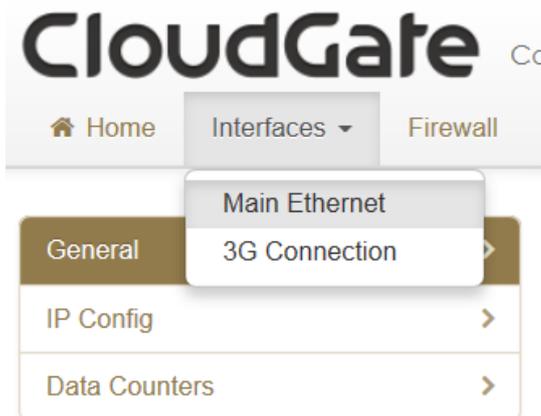


CloudGate 3G

For a CloudGate 3G base unit the Interface Tab shows the following list:

- Main Ethernet
- 3G Connection

Note: the base unit is the CloudGate without expansion cards inserted.

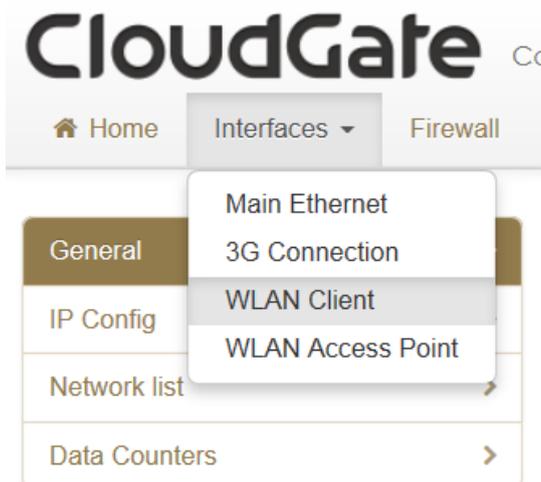


Depending upon the presence of expansion cards, the list can be expanded with one or more interfaces.

In case a WLAN expansion card (CG2101) is inserted in the CloudGate, the following interfaces are visible in the web interface:

- Main Ethernet
- 3G Connection
- WLAN Client
- WLAN Access point

The explanation about the WLAN Client and WLAN Access Point Tab settings can be found in the corresponding subsection of the "Setup Expansion Cards" chapter.

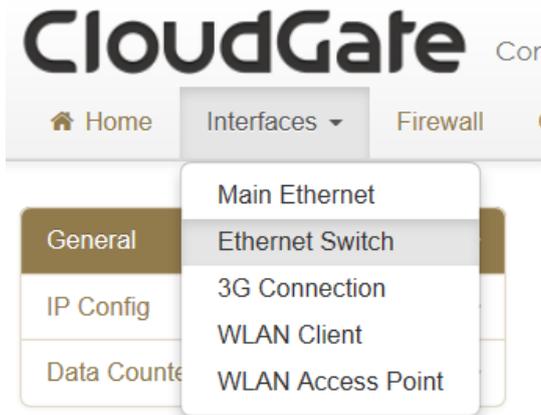


In case an Ethernet Switch (CG1103, CG1104 or CG1109) and a WLAN expansion card (CG2101) are inserted in the CloudGate, the following interfaces are visible in the web interface:

- Main Ethernet
- Ethernet Switch

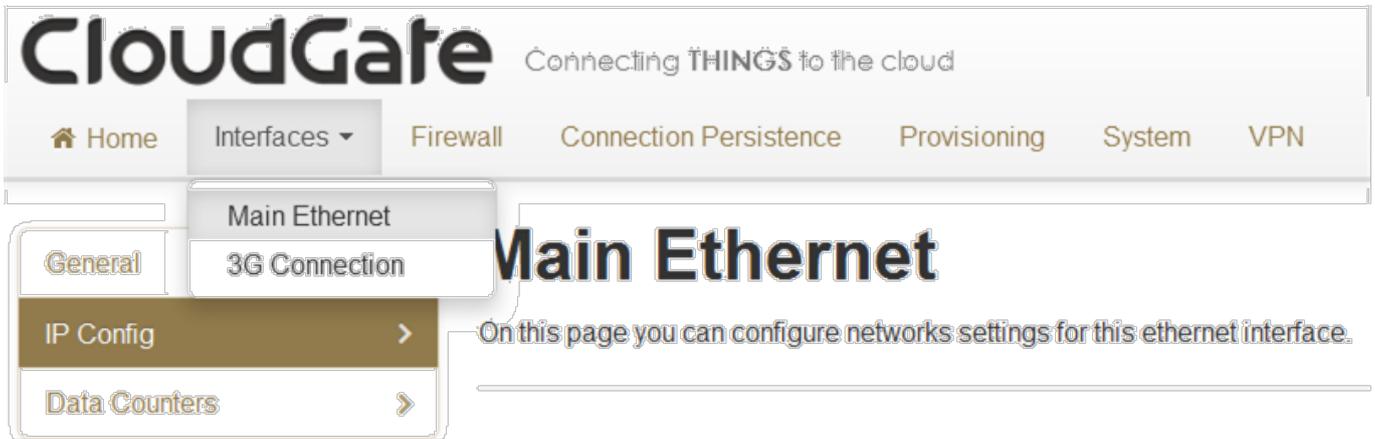
- 3G Connection
- WLAN Client
- WLAN Access point

The explanation about the Ethernet Switch Tab settings can be found in the corresponding subsection of the "Setup Expansion Cards" chapter.



1.1.3.1. Main Ethernet Tab

The Main Ethernet tab configures the behavior of the Ethernet port of the base unit at startup and manages IP network settings.



It includes the following sections:

- General
- IP Config
- Data Counters

General

Enabled Yes No

Mode LAN WAN PPPoE

WAN/LAN Switchover Yes No

MTU

IP Config

IP address
ex: 192.168.2.1

Netmask
ex: 255.255.255.0

Enable DHCP server Yes No

DHCP range to

Lease time

DNS 1

DNS 2

General

Enabled

- Enables (Yes) or disables (No) the Ethernet interface on the main board of the CloudGate
- default = Yes

Mode

- The Mode setting 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 table below.

- PPPoE: Point to Point Protocol over Ethernet

WAN/LAN Switchover

It is recommended to disable WAN/LAN switchover in a production environment

New CloudGate versions (4.0, mini, micro) do not have the WAN/LAN switchover feature. These devices have two ethernet ports that support both WAN and LAN)

- This setting enables or disables the WAN/LAN switchover feature
- By default, WAN/LAN switchover is enabled.
- 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 found, then the port switches to WAN mode and acts as a WAN interface.
- If there is no connection available, then 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.

Combination of Mode and WAN/LAN Switchover

Result of WAN/LAN switchover feature	State of "Mode"	End result
WAN	LAN	WAN
WAN	WAN	WAN
LAN	LAN	LAN
LAN	WAN	WAN

A more detailed explanation of the WAN/LAN switchover feature, together with a flowchart, can be found below.

IP Config

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.
- Default range is 100 to 250

Lease time

- Sets the lease time of the connection
- Default lease time is 12 hours

DNS 1 and DNS 2

- When the Ethernet interface 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 Ethernet interface 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 then 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

Hostname	MAC	Lease time	IP	Active	Actions
Option-Canada	00:15:b7:6d:f1:67	1d	192.168.1.237	✘	 
Option-US	00:23:32:da:de:52	1d	192.168.1.122	✔	 

Active leases

Hostname	MAC	IP	Actions
Option-US	00:23:32:da:de:52	192.168.1.122	<input type="button" value="+ Reserve"/>

WAN/LAN Switchover Feature

The Ethernet port can be in two states:

- WAN state: the Ethernet interface acts as a WAN interface. In this state the Ethernet port can be connected to the Internet, e.g. via an ADSL or a cable modem
- LAN state: the Ethernet interface acts as a LAN interface. In this state e.g. a PC can locally be connected to the Ethernet port and the CloudGate will act as DHCP server on this connection

The Cloudgate has a built in mechanism to maximize the internet connectivity via the Ethernet port. There are two elements in this mechanism:

- An automatic WAN/LAN switchover feature that determines the state of the port after power on
- A manual setting "Mode" by which the user can determine the state if the WAN/LAN switchover is disabled or can force the state to WAN even if the switchover mechanism determined the power-on state to be LAN

WAN/LAN detection at power up

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

If the feature is enabled then the following will happen each time the CloudGate is

powered on:

- CloudGate will check if he can reach the internet via the Ethernet port by sending 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. 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.

Manual selection of the Mode

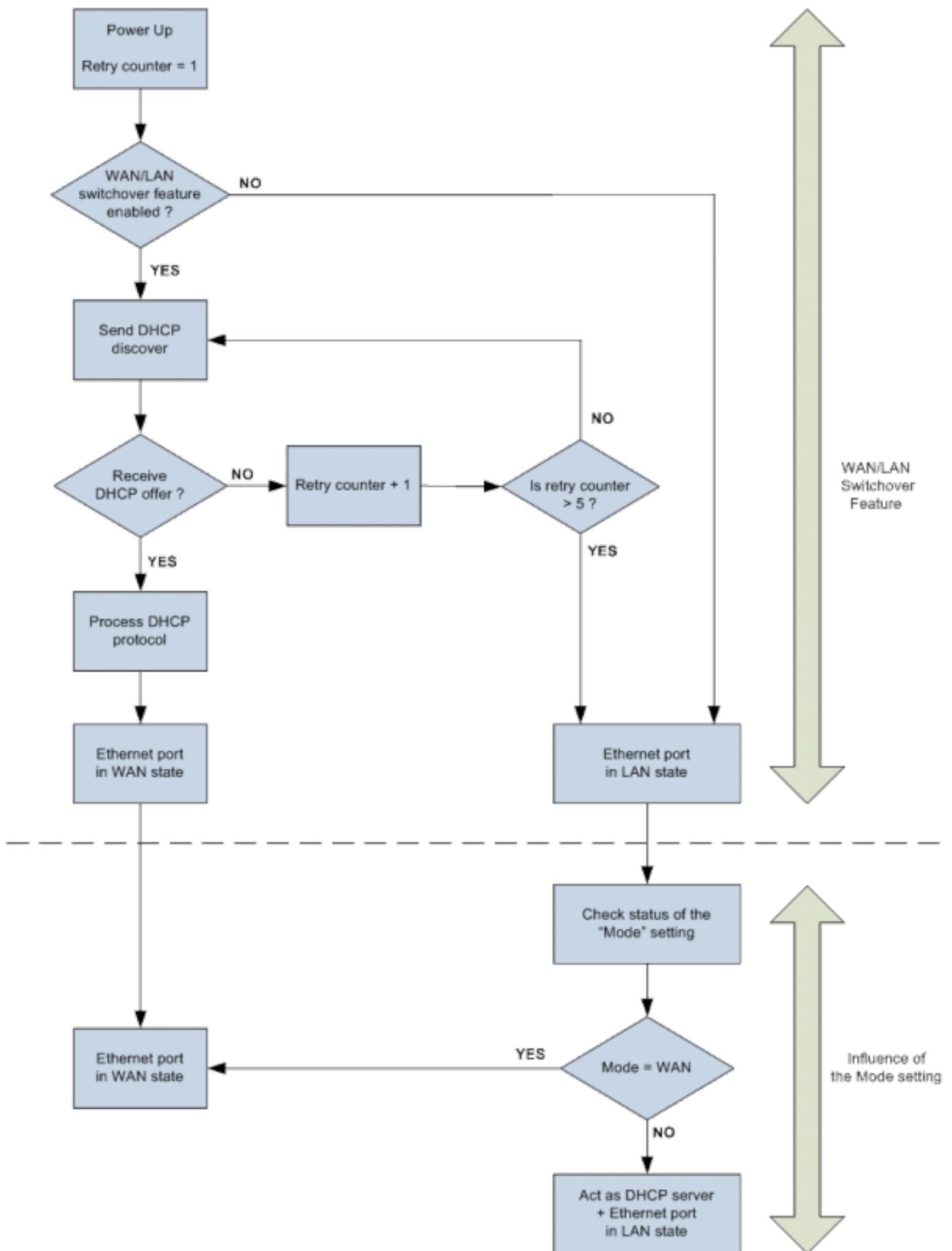
By setting the Mode parameter the user has the possibility to select the preferred state of the Ethernet port (LAN or WAN). By default the Mode is set to LAN. See above how to change the Mode setting.

If the WAN/LAN switchover feature is disabled, then the state of the Ethernet port is determined by the Mode setting.

If the WAN/LAN switchover feature is enabled, then the state is determined by this feature, unless the user has set the Mode to WAN. In that case the result of the switchover feature is overruled by the Mode setting.

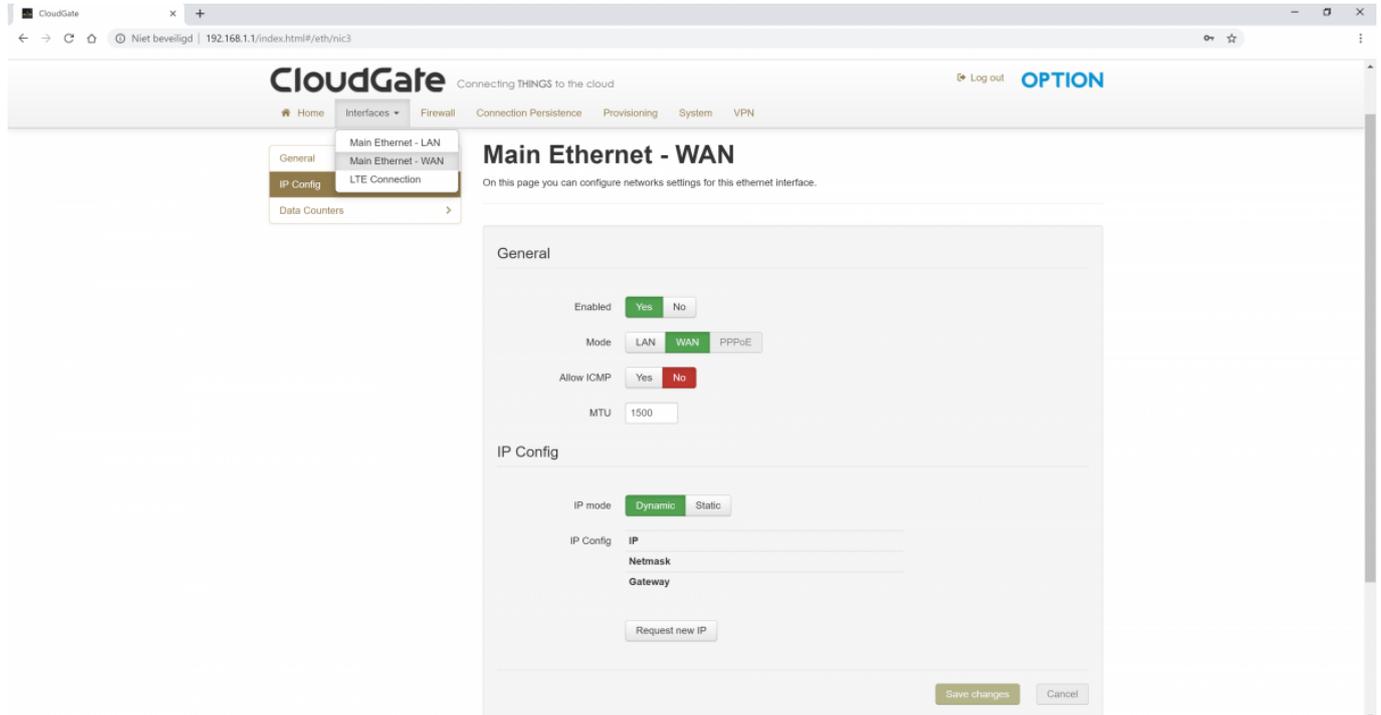
Final state of the Ethernet port

Following flow diagram shows how the WAN/LAN switchover feature works and what the influence is of the Mode setting.



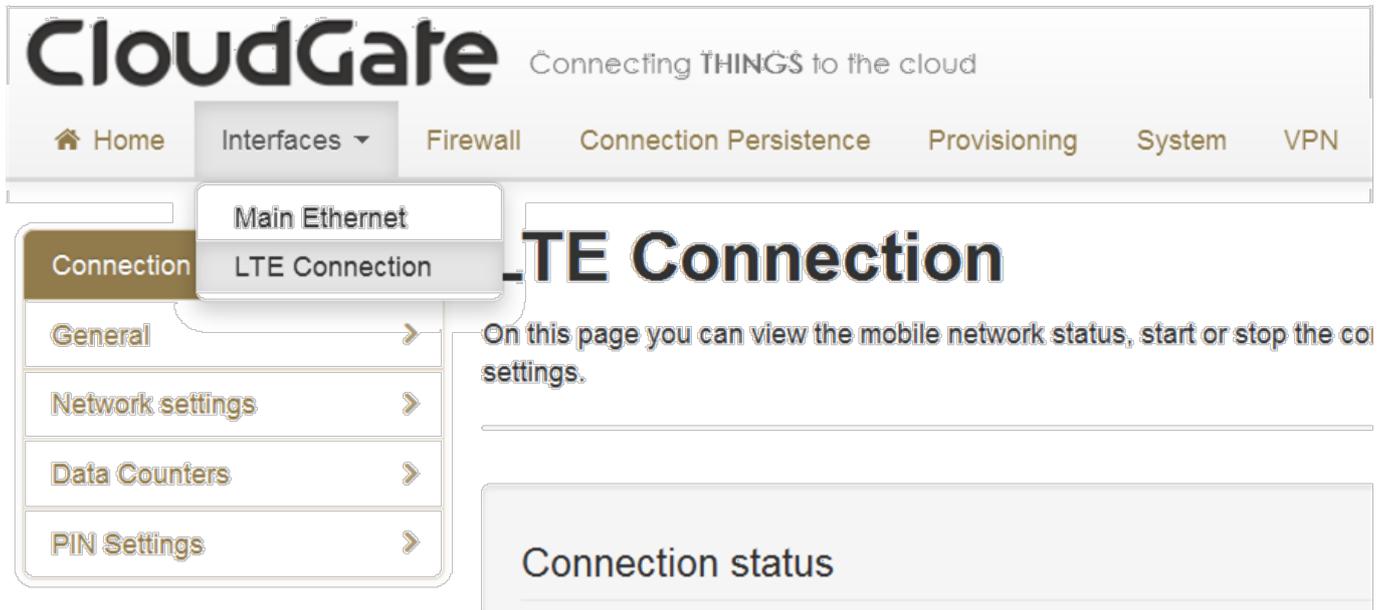
Main Ethernet - WAN

CloudGate 4.0 family devices, which include mini and micro, feature two ethernet ports. By standard these are configured as WAN (left) and LAN (right). Each port can be configured as the other type as well. This means the WAN/LAN switchover feature does not exist on these devices.



1.1.3.2. LTE Connection Tab

The LTE Connection tab configures the CloudGate WWAN interface, as well as LTE network settings.



It includes the following sections:

- Connection Status
- General
- Network Settings
- Data counters
- PIN Settings

Connection Status

The Connection status section provides information about the LTE wireless WWAN network.

Connection status

Connected

The gateway is connected to the mobile network

Operator BEL PROXIMUS

RSRP -109 dBm

Technology LTE

Voice number +32473539612

IP configuration

IP	37.185.206.69
Netmask	255.255.255.0
Gateway	37.185.206.1
DNS 1	80.201.237.239
DNS 2	80.201.237.238

Operator Name

- Displays the name of the wireless operator the CloudGate is connected to.

Signal Strength

- When the CloudGate is connected to an LTE network it will show the RSRP value in dBm.
- When the CloudGate is connected to a 3G network it will show the RSCP value in dBm.
- When the CloudGate is connected to a 2G network it will show the RSSI value in dBm.

Technology

- Displays the technology used by the wireless operator.

Voice number

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

General

The General section configures the LTE WWAN interface on the CloudGate.

General

Enabled Yes No

Only upon traffic Yes No

Connect while on international roaming Yes No

WWAN Passthrough mode Yes No

Allow ICMP Yes No

Radio firmware selection AT&T LTE Generic LTE* Verizon LTE

Cancel Save changes

Enabled

- Enables and disables the WWAN (LTE) interface,
- Set to Yes (default) to enable the WWAN interface.
- Set to No to disable the the WWAN interface.

IMPORTANT: the fact that the LTE interface is enabled, does not necessarily mean that a connection will be set up via this LTE interface. The CloudGate will select one of the available interfaces, depending upon the "Manual" or "Priority-based" settings as described in the Home Tab

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 afterwards. 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 international roaming

- Manages international roaming settings for a device installed in a vehicle.
- If set to Yes, international roaming is enabled.
- If set to No (default), 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 international roaming" feature only has an impact on international roaming behaviour.

WWAN Passthrough Mode

- By default, the 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.

Allow ICMP

- By default, ICMP (Ping) is disabled (set to No) and the CloudGate will not respond to Ping messages.
- If set to Yes, the CloudGate will respond on Ping messages.

Radio firmware selection

- Different network operators require a different firmware. With the radio buttons you can select a network operator and then the corresponding firmware will be selected automatically.
- AT&T LTE
- Generic LTE
- Verizon LTE

Network Settings

Network settings

APN

Authentication method Automatic PAP CHAP None

Username

Password

Network selection method Automatic Manual

You can configure the following 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 (default): 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 manually.

Data counters

Data Counters [?](#)

Data received: **147080 bytes**

Packets received: **540**

Data transmitted: **120030 bytes**

Packets transmitted: **936**

PIN Settings

Change PIN

Enter current PIN

Choose new PIN

Confirm new PIN

Enable PIN

Enabled Yes No

Enter PIN

Save PIN

Enabled Yes No

Enable PIN

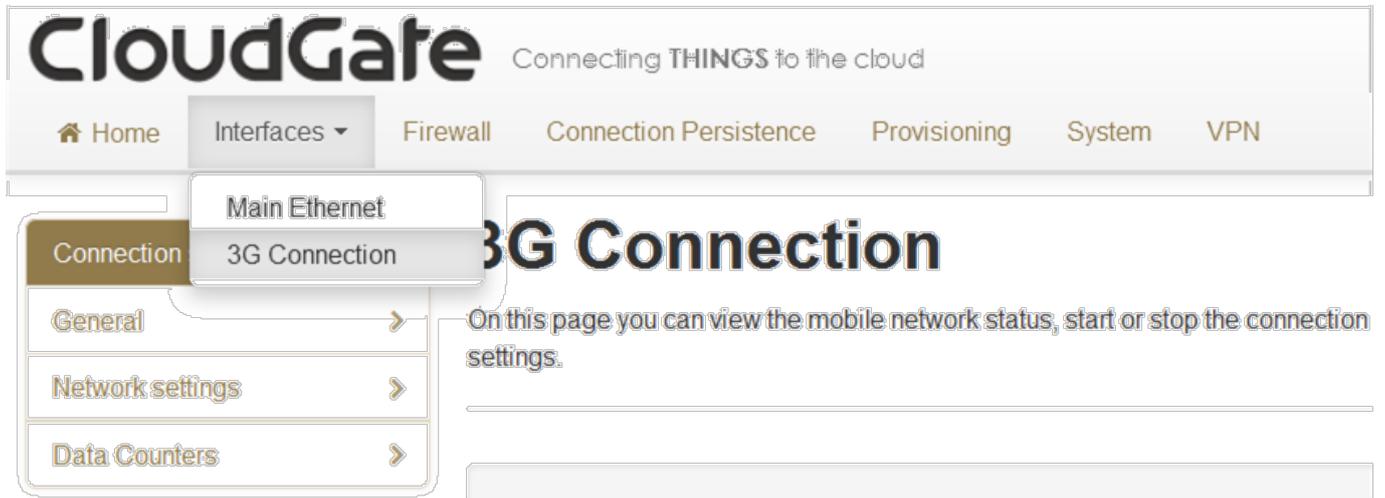
- Enables the PIN code and displays a field for entering the value.

Save PIN

- Automatically saves the PIN code.

1.1.3.3. 3G Connection Tab

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



It includes the following sections:

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

Connection Status

The Connection status section provides information about the 3G wireless WWAN network.

Connection status

Connected

CloudGate is connected to the mobile network

Operator

Signal strength dBm

ECIO dB

Technology

Voice number

IP configuration

IP	109.140.77.230
Netmask	255.255.0.0
Gateway	109.140.77.229
DNS 1	80.201.237.239
DNS 2	80.201.237.238

Operator Name

- Displays the name of the wireless operator the CloudGate is connected to.

Signal Strength

- When the CloudGate is connected to a 3G network it will show the RSCP value in dBm.
- When the CloudGate is connected to a 2G network it will show the RSSI value in dBm.

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.

The list of parameters depends on the CloudGate model. For the CloudGate 3G Americas the settings are indicated in the screenshot below:

General

Enabled Yes No

Only upon traffic Yes No

Connect while on international roaming Yes No

WWAN Div antenna present Yes No

WWAN Passthrough mode Yes No

Allow ICMP Yes No

Limit Wireless Mode

MTU

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

Radio firmware selection

- Sprint
- Verizon Wireless
- UMTS Generic
- AT&T A SIM requiring different radio firmware was detected.

Connection hunting Yes No

For the CloudGate 3G EMEA the settings are indicated in the screenshot below:

General

Enabled Yes No

Only upon traffic Yes No

Connect while on international roaming Yes No

WWAN Div antenna present Yes No

WWAN Passthrough mode Yes No

Allow ICMP Yes No

Limit Wireless Mode ▼

MTU ▲▼

Cancel

Save changes

For the CloudGate 3G JP/APAC the settings are indicated in the screenshot below:

General

Enabled	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Only upon traffic	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Connect while on international roaming	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
WWAN Div antenna present	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Allow ICMP	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
MTU	<input type="text" value="1500"/>

Cancel

Save changes

Enabled

- Enables and disables the WWAN (3G) interface,
- Set to Yes (default) to enable the WWAN interface.
- Set to No to disable the the WWAN interface.

IMPORTANT: the fact that the 3G interface is enabled, does not necessarily mean that a connection will be set up via this 3G interface. The CloudGate will select one of the available interfaces, depending upon the "Manual" or "Priority-based" settings as described in the Home Tab

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 afterwards. 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 international roaming

- Manages international roaming settings for a device installed in a vehicle.
- If set to Yes, international roaming is enabled.
- If set to No (default), 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 international 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 (default), then the RX diversity is disabled.

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.

WWAN Passthrough Mode

- 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 send to port 80 will always redirect to the WebGui of the CloudGate!

Allow ICMP

- By default, ICMP (Ping) is disabled (set to No) and the CloudGate will not respond to Ping messages.

- If set to Yes, the CloudGate will respond on Ping messages.

Limit Wireless Mode

- This parameter allows to limit the unit to register (and connect) on 2G or 3G networks
- Possible settings are: "2G only", "3G only" and "No limit"
- Default setting is "No limit"

Image configuration (Radio firmware selection)

- These settings are applicable for the CloudGate 3G Americas
- Different network operators require a different firmware. With the radio buttons you can select a network operator and then the corresponding firmware will be selected automatically.
- If Verizon Wireless or Sprint is selected, the web interface jumps to the CDMA section. Click "Update profile" 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.
- In case a non-AT&T SIM is inserted, a warning message "A SIM requiring different radio firmware was detected" next to the AT&T radio button and the AT&T firmware cannot be selected

IMPORTANT: When using the CloudGate 3G EMEA (CG0112) base unit, you don't have to select the wireless operator. The device uses the UMTS Generic setting.

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.

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 period during which the CloudGate will try to a network from the list before trying the next network.

Connection hunting Yes No

Connection hunting

Connection hunting configuration

- Verizon Wireless
- UMTS Generic
- Sprint
- AT&T
- Aeris

Fallback time minutes

IMPORTANT: The connection hunting feature is only available on CloudGate 3G Americas (CG0192).

Network Settings

Network settings

APN

Authentication method Automatic PAP CHAP None

Username

Password

Network selection method Automatic Manual

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.

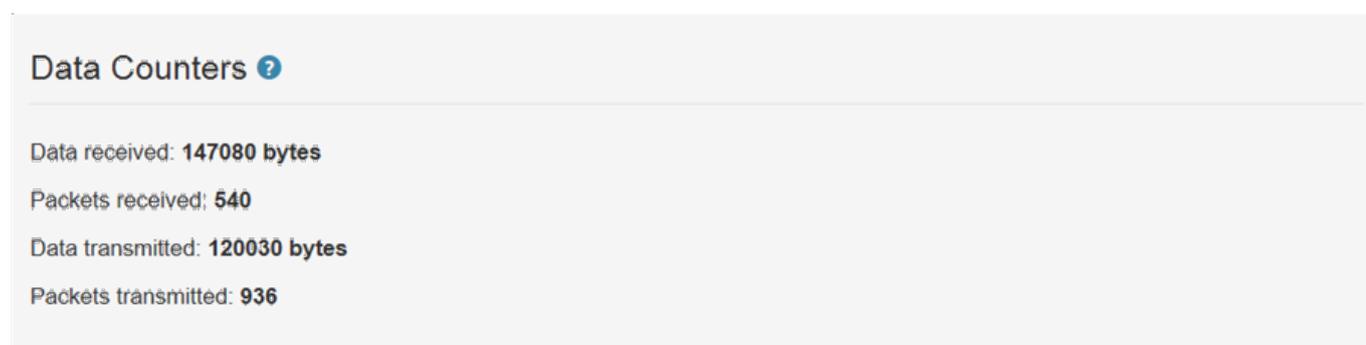
Password

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

Network selection method

- Sets the network selection method when roaming:
 - Automatic (default): 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 manually.

Data counters



Data Counters ?

Data received: **147080 bytes**

Packets received: **540**

Data transmitted: **120030 bytes**

Packets transmitted: **936**

PIN Settings

Change PIN

Enter current PIN

Choose new PIN

Confirm new PIN

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

Enable PIN

Enabled Yes No

Enter PIN

Save PIN

Enabled Yes No

Enable PIN

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

Save PIN

- Automatically saves the PIN code.

CDMA

This paragraph is only applicable for CloudGate 3G Americas.

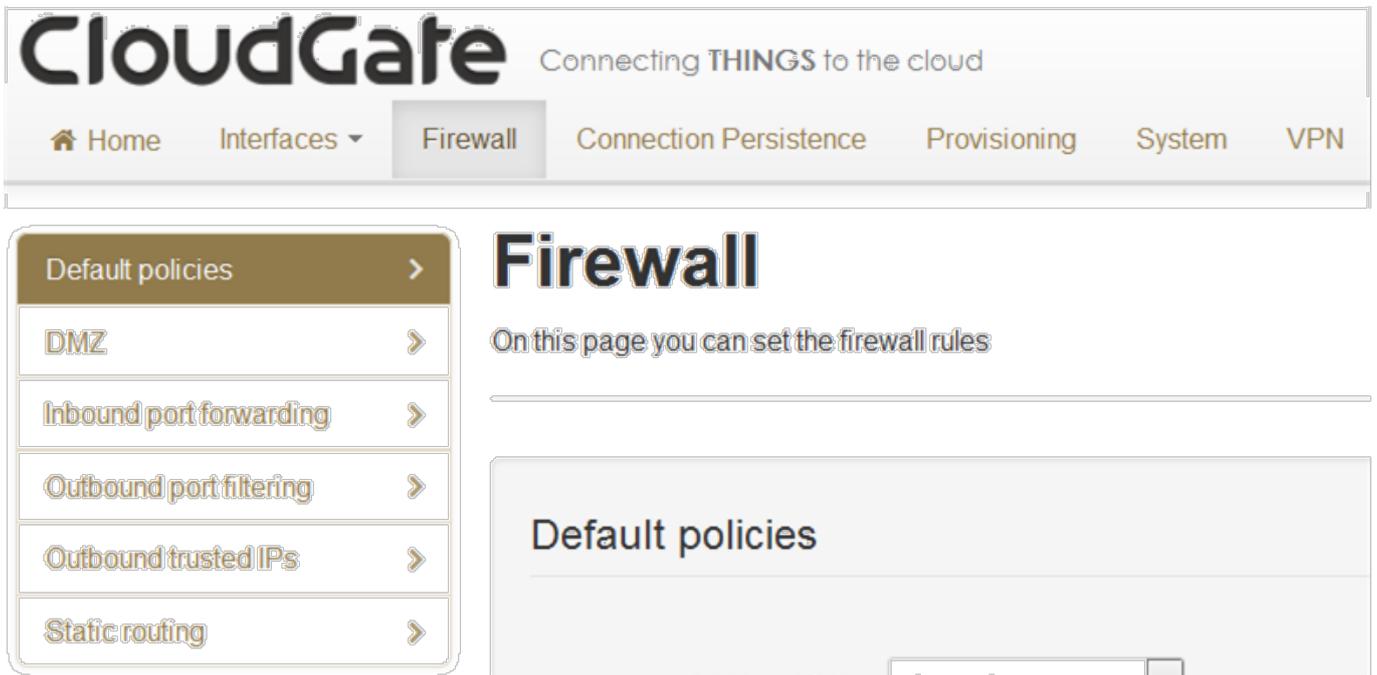
If Verizon Wireless or Sprint is the chosen wireless operator, click Update profile to provision the CloudGate.

CDMA

Programming in progress

[PRL Update](#) [Update profile](#)

1.1.4. 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 Main Ethernet interface (this is the Ethernet interface of the base unit) behaves as a WAN or LAN depending on the mode configured through the WAN/LAN Switchover feature, as described in section about the Main Ethernet tab.

The firewall tab includes 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.

Default policies

LAN -> WAN	<input type="text" value="Accept"/>	▼
LAN -> LAN	<input type="text" value="Accept"/>	▼
LAN -> Local	<input type="text" value="Accept"/>	▼
WAN -> Local	<input type="text" value="Drop"/>	▼

In order for the changes to take effect, please reboot your gateway after saving.

- 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 incoming traffic from the internet can enter the CloudGate. It is extremely important not to set the 'WAN to Local' firewall policy of the CloudGate to 'accept' at any time when your CloudGate is equipped with a public routable IP-address! This can lead to data consumptions of 10's of GB's in just a few days when hackers are trying to access your CloudGate via SSH!

DMZ

The DMZ section configures the demilitarized zone.

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

DMZ

Enabled Yes No

WAN Interface

IP Address Required
ex: 192.168.1.1

Enabled

- Enables the DMZ.
- The default status is No

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

Protocol	Inbound interface	Source IP	Dest. port	Target IP : port	Actions
----------	-------------------	-----------	------------	------------------	---------

Note: Inbound port forwarding is priority based. The first line has the highest priority.

- 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".

Edit inbound port forwarding rule ×

Protocol

Inbound interface

Source IP Any Specific:

Destination port Required

Target IP address Required

Target destination port Required

Outbound Port Filtering

The Outbound Port Filtering section defines the data allowed to pass from the Local or LAN interface to the WAN interface.

Outbound port filtering

Outbound WAN interface

Port range

Policy

Actions

+ Add

- 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".

Edit outbound port filtering rule

Outbound WAN interface

-- ALL --

Port range

to

Both values must be in range 1 to 65535 and the second value must be greater than or equal to the first one

Policy

Accept

Cancel

Add

Outbound Trusted IPs

The Outbound Trusted IP list is disabled when "LAN -> WAN" policy is set to "Accept" (this is the factory default setting).

Outbound trusted IPs

The outbound trusted IP list is disabled when LAN -> WAN Policy is set to 'accept'
You may click on the button below to change it

Change LAN -> WAN Policy to 'reject'

Cancel

Save changes

When the "LAN -> WAN" policy is set to "reject", you can give a list of Outbound trusted IP's. These IP addresses that can be contacted even when LAN-to-WAN traffic is not allowed.

Outbound trusted IPs

new IP

Add

Cancel

Save changes

- 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

Interface	Target	Netmask	Gateway	Actions
<input type="button" value="⊕ Add"/>				
				<input type="button" value="Cancel"/> <input type="button" value="Save changes"/>

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.

When clicking the "Add" button the following window pops up. Fill out the required fields and tap "Add" to confirm.

Edit static routing ✕

Interface

Target Required

Netmask Required

Gateway Required

Priority scheme of the different firewall rules

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

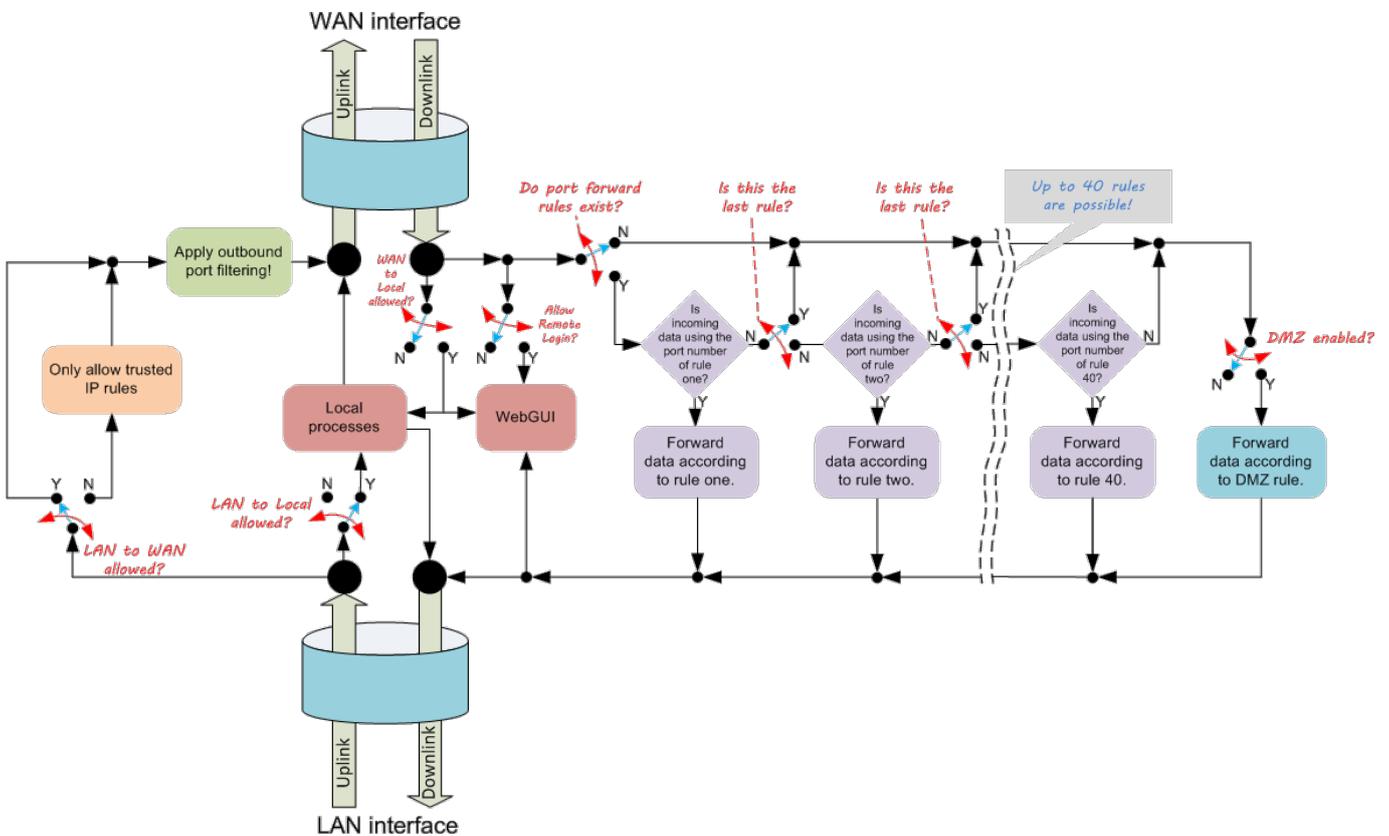
-
Priority example: If you enable HTTPS and DMZ, you can still use the HTTPS because those port forwarding's are processed before the DMZ redirect.

Outbound Rules LAN -> WAN

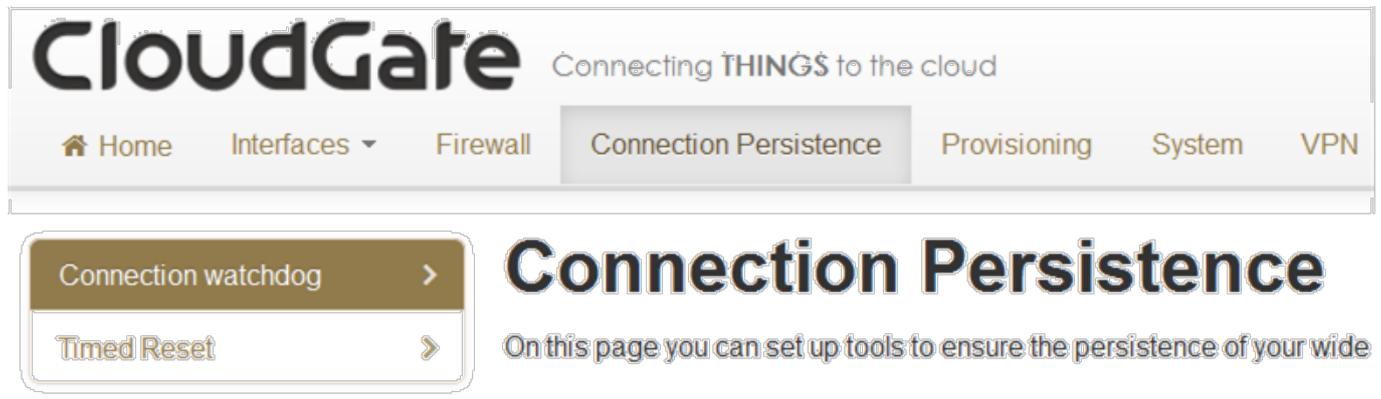
-
Outbound rules in order of priority:

-
- 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)

The following scheme (also attached as PDF) gives the overview:



Connection Persistence Tab



The screenshot shows the CloudGate web interface. At the top, the logo "CloudGate" is displayed with the tagline "Connecting THINGS to the cloud". Below the logo is a navigation menu with the following items: Home, Interfaces, Firewall, Connection Persistence (highlighted), Provisioning, System, and VPN. On the left side, there is a sidebar menu with "Connection watchdog" and "Timed Reset" options, both with right-pointing arrows. The main content area features the heading "Connection Persistence" and a sub-heading "On this page you can set up tools to ensure the persistence of your wide".

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 action is based on a connection persistence algorithm that 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.
- The priority list can be found and configured in the Home Tab under "Connection Settings".

Timed reset:

- This feature will reset the CloudGate after a period of time.

Connection Watchdog

Algorithm:

- The connection persistence algorithm will regularly check whether it still has internet access. If no data is received after a certain period of time the algorithm will try to lookup a list of up to 5 URLs and/or IP addresses at regular intervals.
- For each URL in the list a DNS request will be sent to verify whether the URL can be resolved. Optionally also a PING request can be sent to that URL.
- For each IP address in the list a PING request will be sent.
- The algorithm will run through the list 3 times.
- If all the above checks fail, the conclusion will be that there is no internet

connection any more and the watchdog action will be executed: the next WAN interface in the priority list will be taken and if the current WAN interface was the 3G interface, then the 3G module will be either reset or just re-connected

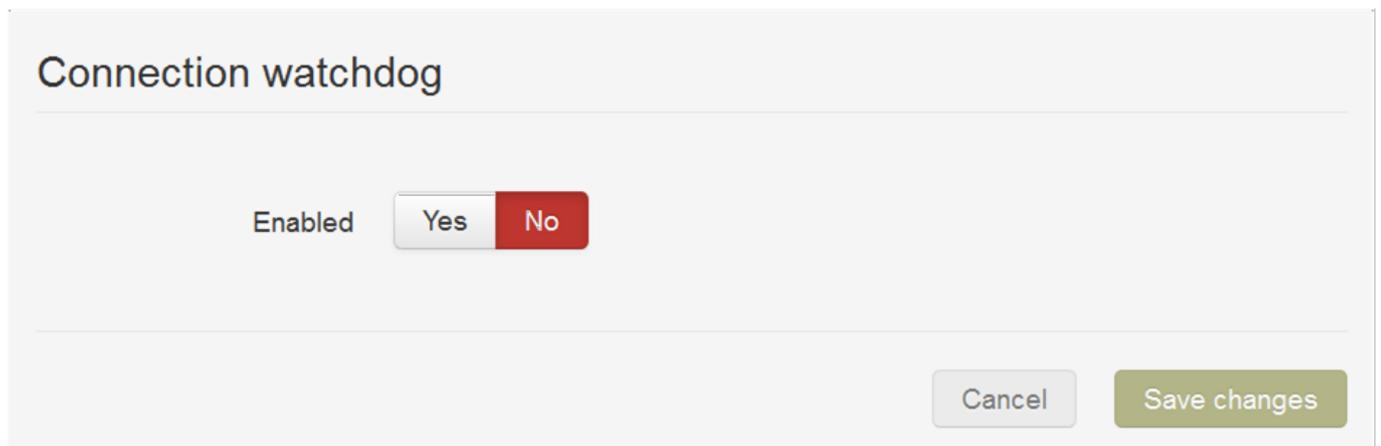
- A flow chart of the connection persistence algorithm can be found below

Notes:

- in the current SW versions the connection persistence algorithm will start to lookup the URL/IP addresses when no data is received during a certain period of time (being the checking interval)
- in future SW versions the algorithm will monitor the internet access continuously, this means independent whether data is received or not. The URL/IP lookup will be checked periodically, after the checking interval

Watchdog configuration

- After factory reset the watchdog is disabled and the screen looks as follows:



Connection watchdog

Enabled Yes No

Cancel Save changes

Enabled

- Set to No (= default status) to disable the watchdog
- Set to Yes to enable the connection watchdog and to monitor the active WAN interface for data received.

If set to "Yes" the following screenshot appears:

Connection watchdog

Enabled Yes No

Addresses to check No addresses defined

Use PING in addition to DNS Yes No

Checking interval seconds

Watchdog action Reset interface Re-establish 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

- If set to No (= default status), then the URL/IP lookup feature will just send a DNS request for each URL
- If set to Yes, then the URL/IP lookup feature will send a DNS request plus a PING
- Note: this parameter has only impact for the URL addresses. For the IP addresses in the list, there will always be a PING sent

Checking interval

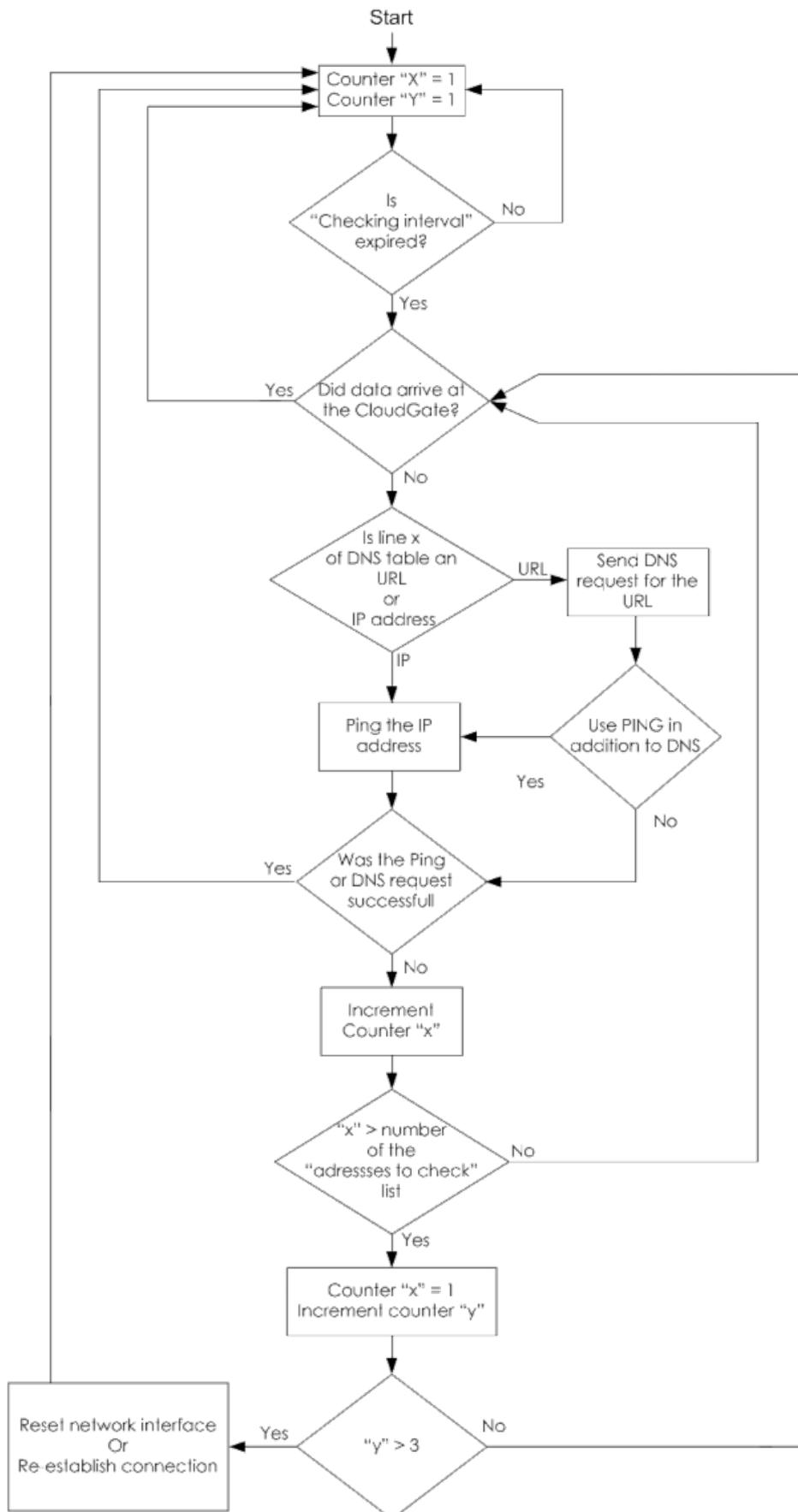
- If no data is received during a time equal to the "checking interval" the connection persistence algorithm will start the URL/IP lookup feature.
- The factory default checking interval is 900 seconds

Watchdog action

- If set to "Reset interface" (= default status) then the watchdog will reset the WWAN module.
Resetting the WWAN module can take about 2 minutes
- If set to "Re-establish connection" then the watchdog will just try to re-establish the connection to the wireless network.
Reconnecting to the wireless network will take about 20 seconds.

Flowchart of the connection persistence algorithm

Connection persistence watchdog

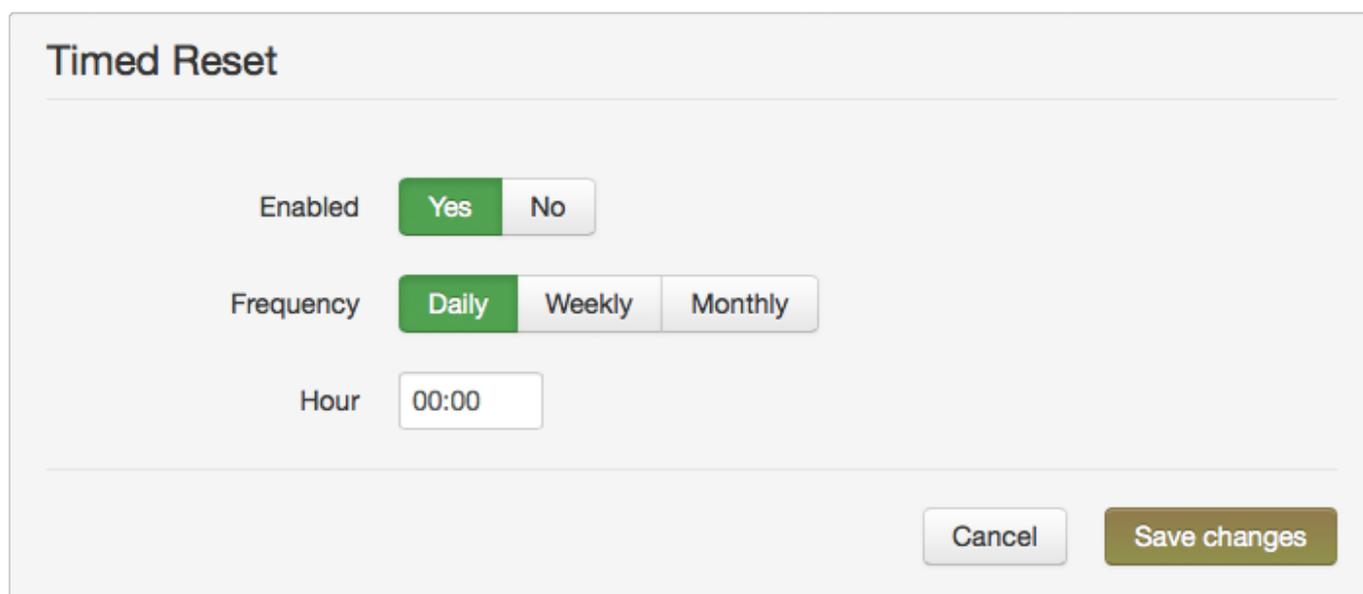


Timed Reset

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

The default status after factory reset is "No".

When clicking "Yes" the following screenshot appears.



The screenshot shows a configuration window titled "Timed Reset". It contains three settings:

- Enabled:** A toggle switch with "Yes" selected (highlighted in green) and "No" unselected.
- Frequency:** Three radio buttons: "Daily" (selected and highlighted in green), "Weekly", and "Monthly".
- Hour:** A text input field containing "00:00".

At the bottom right, there are two buttons: "Cancel" and "Save changes".

Enabled

- Default status is No
- 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. Also select the time of the day. Selected days are green.

Timed Reset

Enabled Yes No

Frequency Daily Weekly Monthly

Weekdays Monday Tuesday Wednesday Thursday Friday
 Saturday Sunday

Please select at least one weekday

Hour

Cancel

Save changes

- Set to Monthly and enter the day of the month and the time of the day.

Timed Reset

Enabled Yes No

Frequency Daily Weekly Monthly

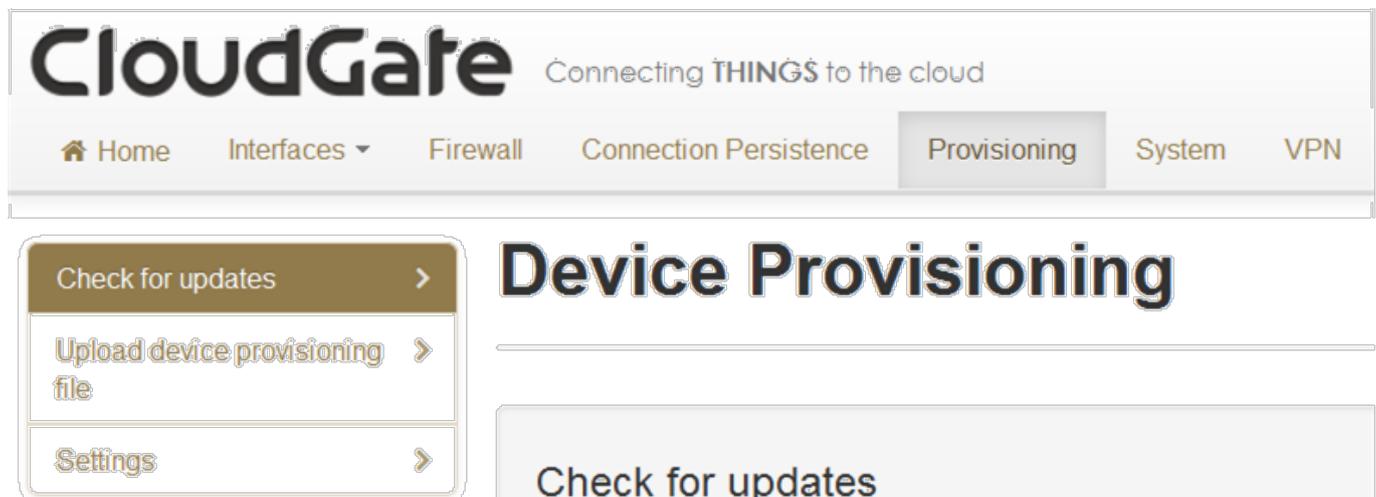
Day of the month

Hour

Cancel

Save changes

Provisioning Tab



The Provisioning tab configures how and when the CloudGate checks for image updates from the CloudGate Universe server (also called "Provisioning server"), and explains how an image can be uploaded locally.

A CloudGate image contains the following files:

- the firmware provided by Option,
- the radio firmware for the radio module, also provided by Option,
- the configuration file,
- the application software.

The upgrade with a new image can happen:

- either locally from a PC directly connected to the CloudGate via a network cable,
- or remotely over the WAN interface.

Upgrades can be triggered manually or will be driven automatically. The following cases are possible:

- via the WAN interface after CloudGate power on,
- via the WAN interface at regular and configurable time intervals,
- via the WAN interface, but triggered manually via the local web interface,
- locally from a PC connected to CloudGate via a network cable.

The Provisioning Tab explains the configuration screens that are available via the web interface of the device.

The section "Check-in frequency" in the CloudGate Universe Guide explains how to configure the check in frequency for periodic upgrade checks.

At CloudGate power on

- By default, the CloudGate base unit connects to the CloudGate Universe server 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

Check for updates

Note: this will automatically install updates to the gateway, even when automatic provisioning has been disabled. "Check for updates" can cause data traffic on your wireless operator subscription.

[Check for updates](#)

- By this method the user can trigger the CloudGate to check the CloudGate Universe server for firmware, developer image, and configuration file updates
- Click the "Check for Updates" button to check for updates even if "Enable automatic provisioning" (see below) is disabled.

Upload Option Provisioning File

Upload device provisioning file

Select file No file selected.

[Upload](#)

- This allows the user to upgrade the unit with an image from a PC that is locally connected via a network cable.
- Click "Browse" to select the file and then click "Upload".

Settings

Settings

Note: activate "Enable automatic provisioning" can cause data traffic on your wireless operator subscription.

Enable automatic provisioning Yes No

- This setting controls automatic updates from the CloudGate Universe.
- Default value of this parameter (= after factory reset) is "Yes".
- 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. For more details on how to configure this parameter, please refer to the "Check-in frequency" section in the CloudGate Universe Guide
- Set to No to disable automatic provisioning.
 - In this case the CloudGate will not check for updates any more, neither at periodic intervals, nor at power up,
 - But nevertheless the user can connect his PC locally to the CloudGate and manually trigger an upgrade check via the "Check for updates" button (see above).

Related topics

- Check-in frequency section in the CloudGate Universe Guide
- Managing software section in the CloudGate Universe Guide

1.1.7. System Tab

The screenshot shows the CloudGate web interface. At the top, the logo "CloudGate" is followed by the tagline "Connecting THINGS to the cloud". Below this is a navigation menu with items: Home, Interfaces, Firewall, Connection Persistence, Provisioning, System (highlighted), and VPN. On the left side, there is a sidebar menu with the following items: Time Settings (highlighted), Power Savings, Data Counters, Remote Access, Static DNS, Dynamic DNS, Username & Password, Logging, Config export, System reboot, and Factory reset. The main content area is titled "System" and contains the text: "On this page you can configure general settings, remote access etc." Below this text is a configuration panel for "Time Settings". This panel has two input fields: "Timezone" with the value "UTC+00:00 Abidjan, Dakar, Monrovia," and "NTP server" with the value "pool.ntp.org".

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

It includes the following sections:

- Time Settings
- Power Savings
- Data Counters
- Remote Access
- Static DNS
- Dynamic DNS
- Username and Password
- Logging
- Config Export
- System Reboot
- Factory Reset

Time Settings

Time Settings

Timezone

NTP server

Sets the timezone used by the unit for the "Timed Reset" watchdog. The description of the "Timed Reset" feature is given in the Connection Persistence Tab.

Power Savings

Power Savings

Turn off LEDs

Turn off LEDs

- Default status is "No", which means the LEDs indicate the status of the CloudGate
- Select "Yes" and "Save changes" to turn off all the LEDs

Data Counters

Data Counters

Reset all data counters

Reset

Remote Access through HTTPS

The Remote Access section configures a port on the CloudGate for remote access. With remote access, you can log on to the on-device web interface from a remote PC or laptop.

Remote access through HTTPS

Remote access

Yes

No

Port

1800

Cancel

Save changes

Default status after factory reset is "No".

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 (default is 1800) 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.

Warning: the default port number is 1800. You may change this but make sure that you

take a port number that does not conflict with any rules or limitations that are imposed by the mobile operator.

Static DNS

Static DNS settings

Nameserver 1

Nameserver 2

Dynamic DNS

Dynamic DNS

Enabled Yes No

Service provider

Host Name

User Name

Password

Use HTTPS Yes No

Status

Enabled

- Default status is "No"
- 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

- Set to "Yes" to enable HTTPS login.

Status

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

Username and Password

The image shows a web interface with two main sections: 'Username' and 'Password'. The 'Username' section has a text input field with the value 'admin' and a 'Save changes' button highlighted in green. The 'Password' section has three text input fields labeled 'Old password', 'New password', and 'Confirm password', and a 'Save changes' button also highlighted in green. Both sections have a 'Cancel' button next to the 'Save changes' button.

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.

Logging

Enable logging Yes No

Maximum log file size kB

Select log levels

- Info
- Warning
- Error
- Debug

Download log file

Clear log file

To create a log file:

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 2048 kB.

Select log levels

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

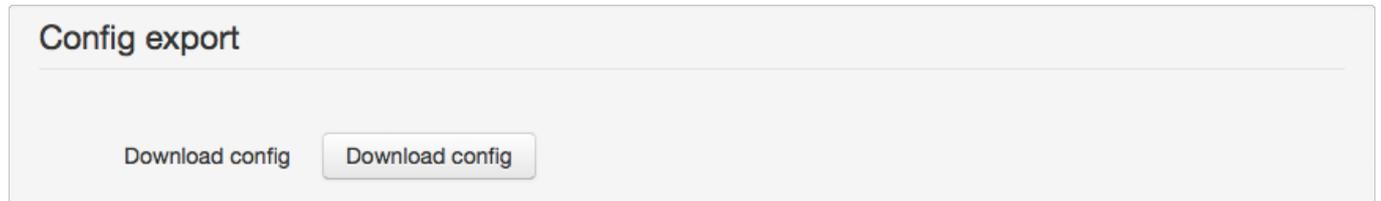
Download log file

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

Clear log file

- Removes the log file from the unit's memory.

Config Export



- Click "Download config" to save the device configuration to a file on a laptop. The configuration file can then be uploaded to the CloudGate Universe and used for provisioning multiple devices.

System Reboot and Factory Reset

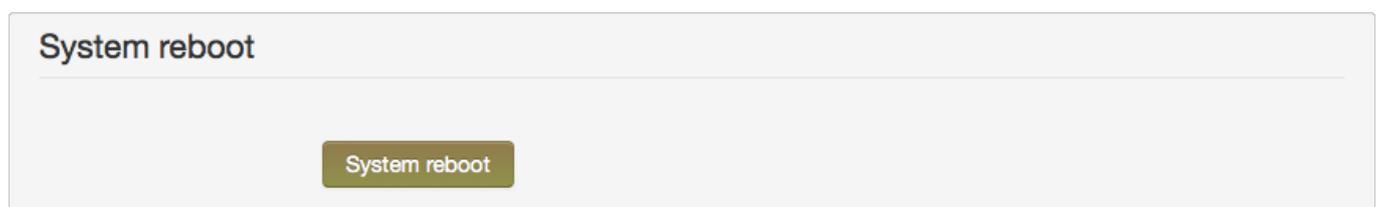
Two different manual resets are possible on the CloudGate: system reboot and factory reset.

TIP:

Automatic resets of the WWAN interface are managed by the connection watchdog feature.

Automatic resets of the CloudGate are managed by the timed reset feature.

System reboot



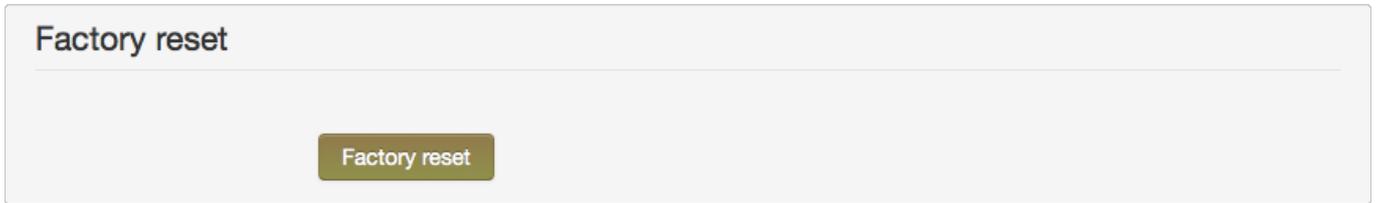
To reboot the CloudGate:

1. Click "System reboot".
2. In the confirmation dialog box, click "System reboot" to confirm.

During the reboot there is a "Rebooting" count down timer window visible which goes back to the login page when the CloudGate is operational again.

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 configuration settings and overwrite all custom configuration changes:

1. Click "Factory Reset"
2. In the confirmation dialog click "Factory reset" to confirm, in order to restart the device with the original configuration settings version from the factory.

During the factory reset there is a "Resetting" count down timer window visible which goes back to the login page when the CloudGate is operational again.

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.

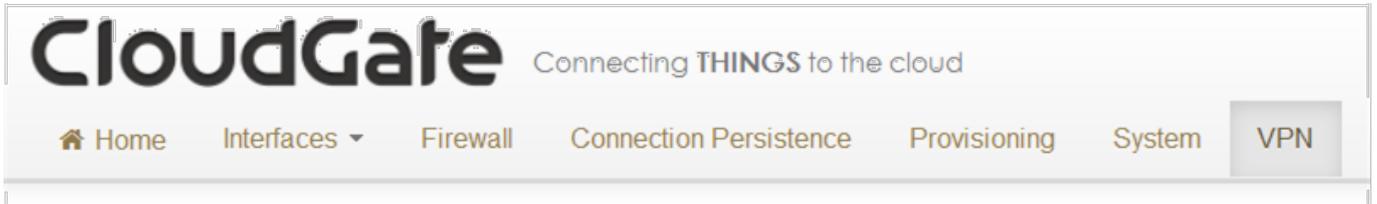


When the user performs a factory reset by pushing the reset button for more than 5 seconds, he will get visual feedback via a specific LED sequence as follows:

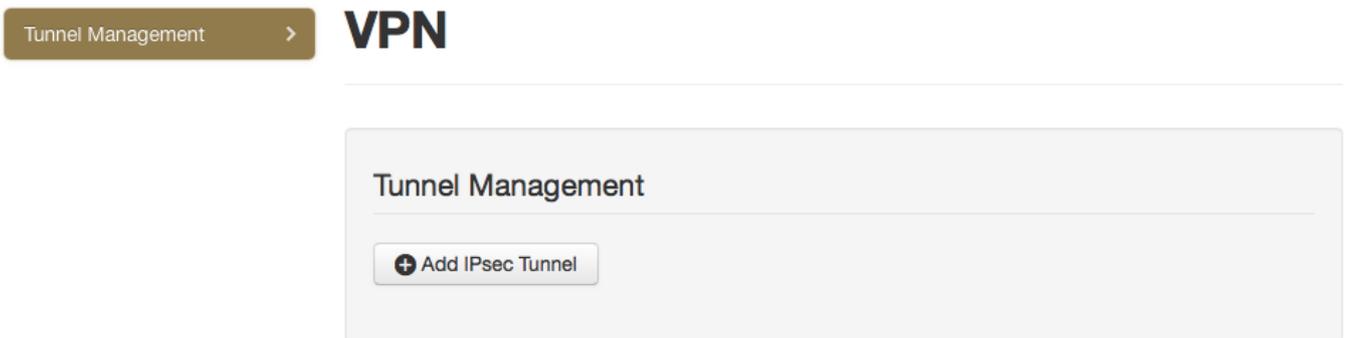
- the LEDs will quickly turn on red one by one (from the left to the right) until all LEDs are red

- then all LEDs will quickly turn on green
- finally all LEDs will quickly turn on orange and will remain orange for a while, until the CloudGate is ready to boot up again

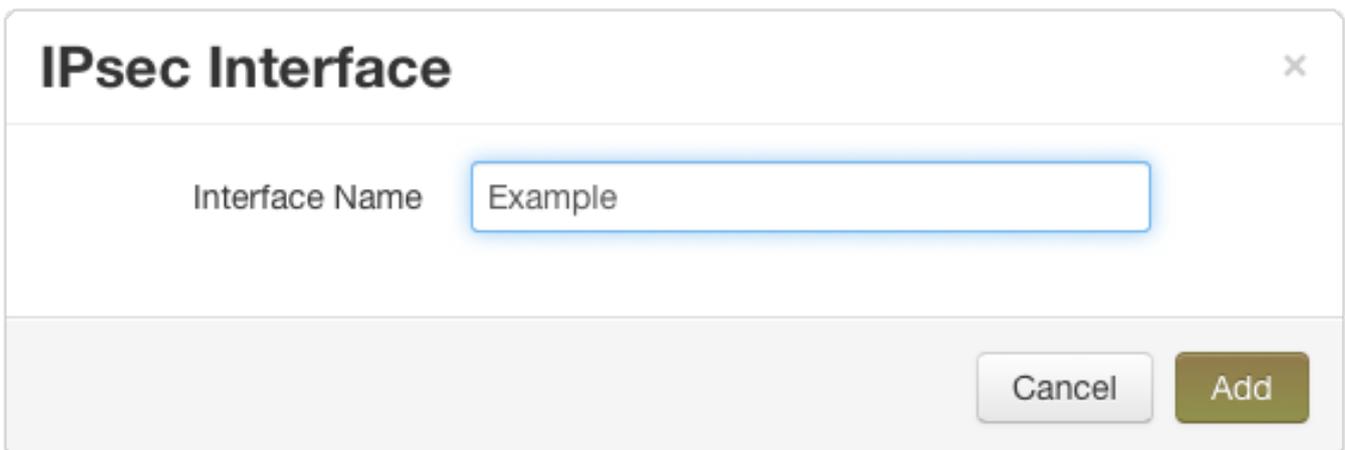
1.1.8. VPN Tab



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.

- Tunnel Management >
- Example - IPsec >

VPN

Tunnel Management

[+ Add IPsec Tunnel](#)

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

There are two modes.

Client Mode:

Identity

Mode

Server

Client

Authentication Method

PSK

Pre-shared Key

WAN Interface

Remote Host

Remote Peer Identity

Local Peer Identity

Local Subnet

ex: 192.168.1.1/24

Remote Subnet

ex: 192.168.1.1/24

Server mode:

Identity

Mode Server Client

Authentication Method

Pre-shared Key

WAN Interface

Remote Peer Identity

Local Peer Identity

Local Subnet
ex: 192.168.1.1/24

Remote Subnet
ex: 192.168.1.1/24

The identity section provides the ability to configure:

- Authentication Method: currently only PSK is available,
- Pre-shared Key,
- WAN Interface: 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.

The local subnet is the subnet's traffic that you want to port through the VPN tunnel. Option implemented this because sometimes only a part of a subnet (f.e. /24, /28, ...) needs to be ported or perhaps only the WLAN subnet and not the ethernet (LAN) subnet.

IKE Settings

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

IKE Settings

IKE Version V1 V2

Negotiation Mode Main Aggressive

IKE Encryption

IKE Authentication

IKE Key Group

IKE SA Lifetime seconds

IKE Settings

IKE Version V1 V2

IKE Encryption

IKE Authentication

IKE Key Group

IKE SA Lifetime seconds

- IKE Version: V1,V2
- Negotiation Mode (only for IKE V1): Main & Aggressive
- IKE Encryption: 3DES, AES128, AES256

- IKE Authentication: MD5, SHA1, SHA256
- IKE Key Group: DH1, DH2, DH5, DH14
- IKE SA Lifetime: must be a value between 60 - 86400

Wikipedia: Internet Key Exchange

IPsec Settings

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

The screenshot shows a configuration window titled "IPsec Settings". It contains four input fields:

- IPsec Encryption:** A dropdown menu.
- IPsec Authentication:** A dropdown menu.
- IPsec Key Group:** A dropdown menu.
- IPsec SA Lifetime:** A numeric input field with a spinner icon and a unit label "seconds".

At the bottom right of the window, there are three buttons: "Delete Tunnel", "Cancel", and "Save changes".

- IPsec Encryption: NULL, 3DES, AES128, AES256
- IPsec Authentication: MD5, SHA1, SHA256
- IPsec Key Group: DH1, DH2, DH5, DH14
- IPsec SA Lifetime: must be a value between 60 - 86400

Setup and configure Expansion Cards

If the CloudGate contains an Option expansion card, the device automatically detects and identifies the card and displays the appropriate configuration tab(s) in the Interfaces Tab.

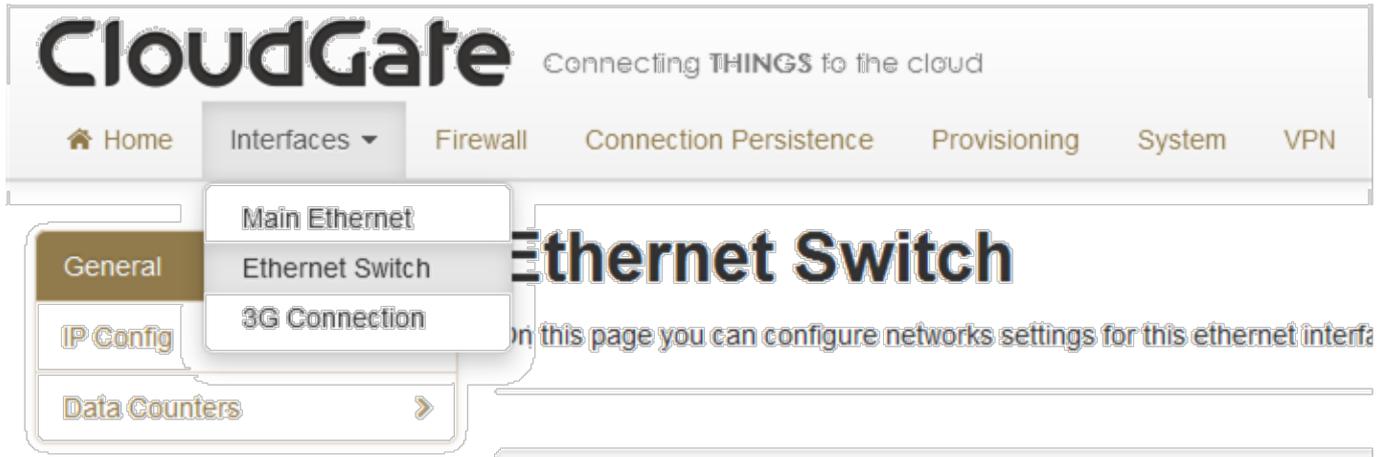
The additional configuration tabs are:

Click this tab	To do these tasks
Ethernet Switch	<ul style="list-style-type: none">• Enable the Ethernet Switch• Set the MTU• Configure the IP parameters
WLAN Client	<ul style="list-style-type: none">• Enable the WLAN client• Connect the device to a WLAN network• Disconnect the device from a WLAN network
WLAN Access Point	<ul style="list-style-type: none">• Enable the WLAN access point• Configure the SSID of the WLAN access point• Configure WLAN card IP address information

1.2.1. Ethernet Switch Tab

When the Ethernet expansion card is inserted into the CloudGate an additional item "Ethernet Switch" will be visible in the Interfaces tab.

The Ethernet expansion card can only provide LAN functionality, no WAN functionality.



3 fields are available in this tab:

- General
- IP Config
- Data Counters

General

The image shows a screenshot of the "General" configuration section for the Ethernet Switch. It features a header "General" and two settings: "Enabled" with a radio button set to "Yes" (highlighted in green) and "No", and "MTU" with a text input field containing the value "1500".

In the general section of the Ethernet Switch Tab the following settings can be selected :

- Enabled: Yes / No
Default status is "Yes"
- The MTU packet size: value range 68 to 1500
Default value is 1500

IP Config

IP Config

IP address
ex: 192.168.2.1

Netmask
ex: 255.255.255.0

Enable DHCP server Yes No

DHCP range to

Lease time

DNS 1

DNS 2

Reserved leases

Hostname	MAC	Lease time	IP	Active	Actions
<input type="button" value="+ Add"/>					

Active leases

Hostname	MAC	IP	Actions
----------	-----	----	---------

The IP configuration field allows to set:

- IP address: this is the IP address on which the CloudGate will be reachable from the Ethernet expansion card network

By default the CloudGate uses subnet 4 on the Ethernet expansion 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 expansion card. When enabled the address range can be selected
- DNS 1 & 2: these fields allow specification of custom primary and secondary DNS servers using their IP address

Reserved and active leases

The reserved and active leases table allow to manage the devices able to connect to ports of the Ethernet expansion 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.

Edit DHCP Reservation ✕

Host name	<input style="width: 95%;" type="text"/>	Required
MAC Address	<input style="width: 95%;" type="text"/>	Required
IP Address	<input style="width: 95%;" type="text"/>	Required
Lease time	<input style="width: 40px; text-align: center; border: 1px solid #ccc;" type="text" value="1"/> <input style="width: 20px; border: 1px solid #ccc;" type="button" value="↑"/> <input style="width: 20px; border: 1px solid #ccc;" type="button" value="↓"/> <input style="width: 100px; border: 1px solid #ccc;" type="text" value="Day(s)"/> <input style="width: 20px; border: 1px solid #ccc;" type="button" value="▼"/>	

Cancel
Add

Data counters

Data counters will trace the incoming & outgoing traffic of the Ethernet expansion card outputs since last start.

Data Counters [?](#)

Data received: **4540027 bytes**

Packets received: **34910**

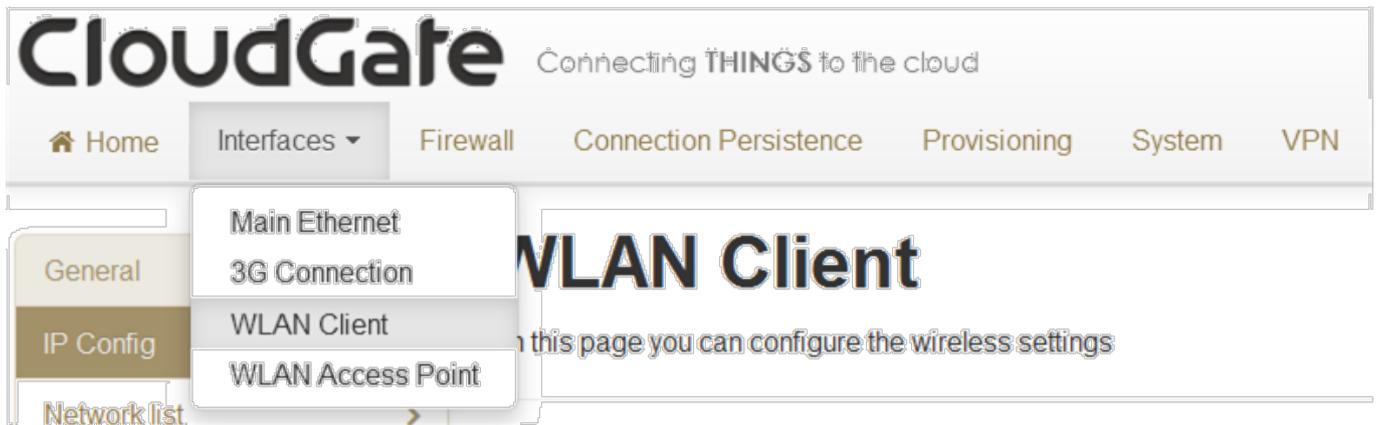
Data transmitted: **18199127 bytes**

Packets transmitted: **26729**

1.2.2. WLAN Client Tab

The WLAN expansion card (CG2101) acts as both a WLAN client and WLAN access point. 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.

When this card is inserted into the CloudGate, then two additional items "WLAN Client Tab" and "WLAN Access Point Tab" will be visible in the interfaces tab.



The WLAN Client tab allows the device to send and receive data over a WLAN network.

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

General

By default and after factory reset the WLAN Client is disabled.

General

Enabled Yes No

To enable the client mode, set the "Enabled" parameter to "Yes" and tap "Save changes". Then the screen will look as follows:

General

Enabled Yes No

Allow ICMP Yes No

MTU

IP Config

IP mode Dynamic Static

IP Config **IP**

Netmask

Gateway

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.
- Default value is "Dynamic"

IP Config

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

IP Config

IP mode Dynamic Static

IP address Required

Netmask Required
ex: 255.255.255.0

Gateway

DNS 1 Required

DNS 2

Network list

- 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.

Network list

Available & Known networks 

Signal quality	SSID	Status	Encryption type
<div style="width: 100%; height: 10px; background-color: green;"></div>	CloudGate-SPB5		WPA2 PSK 
<div style="width: 50%; height: 10px; background-color: orange;"></div>	Guest		None 
<div style="width: 50%; height: 10px; background-color: orange;"></div>	Internal		WPA Enterprise 

[Manual connection](#)

Connecting to a WLAN Network

To connect to a WLAN network:

1. Click the network name.

CloudGate-SPB5

Password

Required

Cancel

Connect

2. Enter the network password and click "Connect".

3. Note the status change to "Connected" in the Available & Known Networks list.

Network list

Available & Known networks ↻

Signal quality	SSID	Status	Encryption type
★ 	CloudGate-SPB5	Connected	WPA2 PSK 
	Guest		None 
	Internal		WPA Enterprise 

Manual connection

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".

✕

SSID

Required

Encryption type

WPA PSK
▾

Password

Required

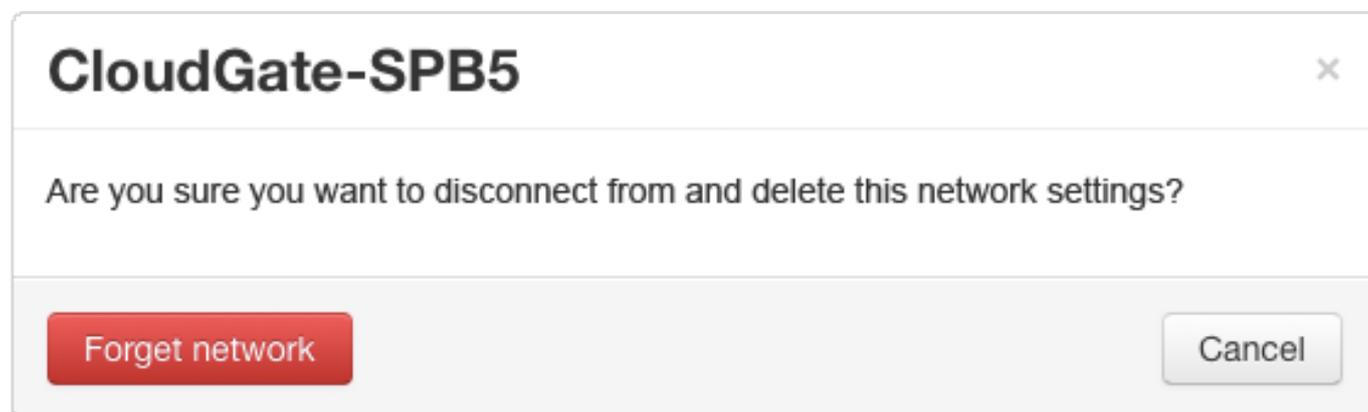
Cancel
Save

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 WLAN network to disconnect.



2. Click "Forget network".

Data counters

1.2.3. WLAN Access Point Tab

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.

The WLAN Access Point Tab looks slightly different, depending on which type of WLAN card is inserted in the CloudGate.

The WLAN expansion card (CG2101) acts both as a WLAN client and as a WLAN access point.

When this card is inserted into the CloudGate, then two additional items will be visible in the interfaces tab:

- WLAN Client Tab
- WLAN Access Point Tab

The WLAN Access Point Card (CG2102) will only act as a WLAN access point, it has no WLAN client functionality.

When this card is inserted into the CloudGate, the following additional item will be visible in the interfaces tab:

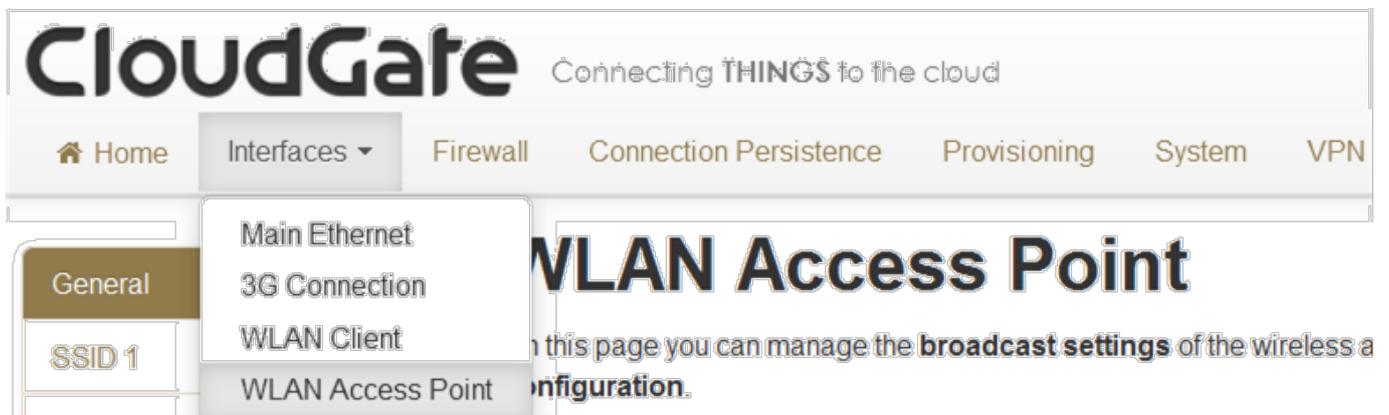
- WLAN Access Point Tab

WLAN Access Point Tab for WLAN Expansion Card CG2101

The WLAN expansion card (CG2101) acts as both a WLAN client and WLAN access point. 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.

When this card is inserted into the CloudGate, then two additional items "WLAN Client Tab" and "WLAN Access Point Tab" will be visible in the interfaces tab.

This section explains how the WLAN Access Point Tab looks like when the WLAN Expansion Card (CG2101) is inserted in the CloudGate.



The WLAN Access Point tab lets you to manage the broadcast settings of the wireless access point.

General

A screenshot of the 'General' configuration page for the WLAN Access Point. The page title is 'General'. It contains four settings: 'Enabled' with a toggle set to 'Yes'; 'WLAN Mode' with a dropdown menu set to '2.4 GHz'; 'Channel' with a dropdown menu set to '11'; and 'Enable second SSID' with a toggle set to 'No'. At the bottom right, there are 'Cancel' and 'Save changes' buttons.

Enabled

- Enables the WLAN access point
- Default value after factory reset is "Yes"

WLAN Mode

- Selects a 2.4Ghz or 5GHz access point

Warning: the 5GHz band is currently not supported

Channel

- Selects the WLAN channel on which the access point has to work.
- Default setting after factory reset is "auto"

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
- Default setting is "No"

SSID 1

General

General

Network name (SSID)
ex: MyNetwork

Broadcast SSID Yes No

Encryption

Password

MTU

Network name (SSID)

- The WLAN expansion card is shipped from the factory with a pre-defined, random SSID, which is different for each WLAN card. The pre-defined SSID is visible on the label that was delivered together with the expansion card
- The user can change this pre-defined SSID

Broadcast SSID

- If set to Yes, the SSID will be broadcasted.
- Default setting is "Yes"

Encryption

- Allows you to choose the type of encryption.
Possible choices are: "None", "WPA PSK", "WPA PSK2" and "Mixed PSK"
- Default setting is "Mixed PSK"

Password

- The WLAN expansion card is shipped from the factory with a pre-defined, random password, which is different for each WLAN card. The pre-defined password is visible on the label that was delivered together with the expansion card
- The user can change the password.

MTU

- the MTU packet size: value range from 68 to 1500
- default setting is 1500

IP Config

IP Config

IP address
ex: 192.168.2.1

Netmask
ex: 255.255.255.0

Enable DHCP server Yes No

DHCP range to

Lease time

DNS 1

DNS 2

IP address

- Sets the IP address of the WLAN access point.
- Default IP address is 192.168.2.1

Netmask

- Sets the netmask of the WLAN access point.
- Default setting is 255.255.255.0

Enable DHCP server

- Enables the DHCP server.
- Default setting is "Yes"

DHCP range

- Sets the DHCP range for the DHCP server.
- Default range is 100 to 250

Lease time

- Sets the lease time
- Default setting is 12 hours

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 then the other IP address will be used for the DNS server.

Reserved leases

Reserved leases					
Hostname	MAC	Lease time	IP	Active	Actions
<input type="button" value="+ Add"/>					

- 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

Active leases			
Hostname	MAC	IP	Actions

- Lists the active DHCP leases of the devices connected to the WLAN access point.
- Click "Reserve" to add the lease to the Reserved leases list.

Data counters

Data Counters [?](#)

Data received: **88971 bytes**

Packets received: **703**

Data transmitted: **146630 bytes**

Packets transmitted: **378**

SSID2

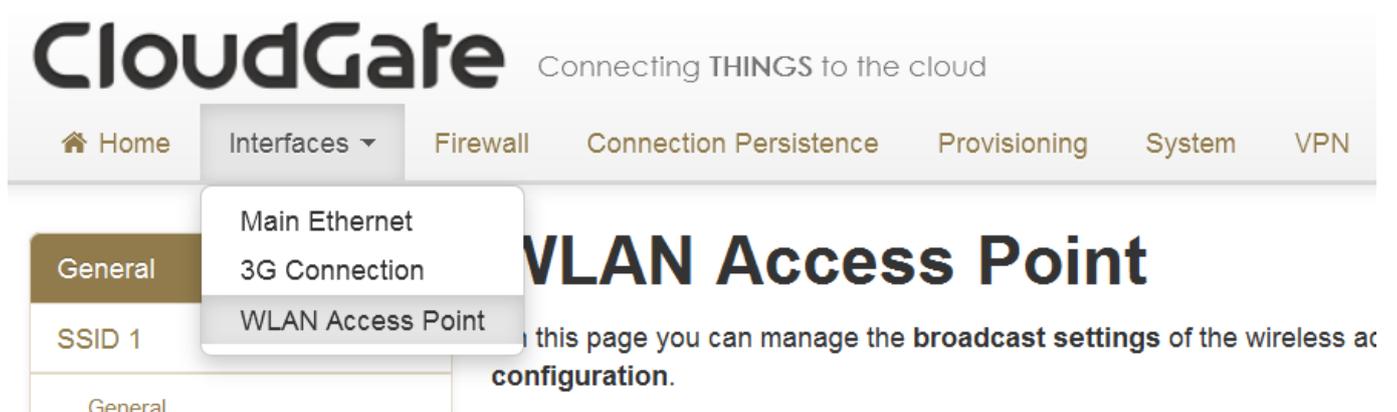
The SSID2 tab allows you to set or change some parameters for the second SSID. These parameters are identical as the parameters for the first SSID.

WLAN Access Point Tab for WLAN Access Point Card CG2102

The WLAN Access Point Card (CG2102) acts as a WLAN access point only. The WLAN access point allows the CloudGate to connect other wireless devices to a wired or 3G network.

When this card is inserted into the CloudGate, then an "WLAN Access Point Tab" will be visible in the interfaces tab.

This section explains how the WLAN Access Point Tab looks like when the WLAN Access Point Card (CG2102) is inserted in the CloudGate.



The WLAN Access Point tab lets you to manage the broadcast settings of the wireless access point.

General

General

Enabled Yes No

WLAN Mode

Channel

Cancel

Save changes

Enabled

- Enables the WLAN access point
- Default value after factory reset is "Yes"

WLAN Mode

- Selects a 2.4Ghz or 5GHz access point

Channel

- Selects the WLAN channel on which the access point has to work.
- Default setting after factory reset is "auto"

SSID 1

General

General

Network name (SSID)
ex: MyNetwork

Broadcast SSID Yes No

Encryption

Password

MTU

Network name (SSID)

- The WLAN Access Point Card is shipped from the factory with a pre-defined, random SSID, which is different for each WLAN card. The pre-defined SSID is visible on the label that was delivered together with the expansion card
- The user can change this pre-defined SSID

Broadcast SSID

- If set to Yes, the SSID will be broadcasted.
- Default setting is "Yes"

Encryption

- Allows you to choose the type of encryption.
Possible choices are: "None", "WPA PSK2" and "Mixed PSK"
- Default setting is "Mixed PSK"

Password

- The WLAN Access Point Card is shipped from the factory with a pre-defined, random password, which is different for each WLAN card. The pre-defined password is visible on the label that was delivered together with the expansion card
- The user can change the password.

MTU

- the MTU packet size: value range from 68 to 1500
- default setting is 1500

IP Config

IP Config

IP address
ex: 192.168.2.1

Netmask
ex: 255.255.255.0

Enable DHCP server Yes No

DHCP range to

Lease time

DNS 1

DNS 2

IP address

- Sets the IP address of the WLAN access point.
- Default IP address is 192.168.2.1

Netmask

- Sets the netmask of the WLAN access point.
- Default setting is 255.255.255.0

Enable DHCP server

- Enables the DHCP server.
- Default setting is "Yes"

DHCP range

- Sets the DHCP range for the DHCP server.
- Default range is 100 to 250

Lease time

- Sets the lease time
- Default setting is 12 hours

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 then the other IP address will be used for the DNS server.

Reserved leases

Reserved leases						
Hostname	MAC	Lease time	IP	Active	Actions	
<div style="border: 1px solid #ccc; border-radius: 5px; padding: 5px; display: inline-block;"> + Add </div>						

- 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

Active leases			
Hostname	MAC	IP	Actions

- Lists the active DHCP leases of the devices connected to the WLAN access point.
- Click "Reserve" to add the lease to the Reserved leases list.

Data counters

Data Counters

Data received: **0 bytes**

Packets received: **0**

Data transmitted: **0 bytes**

Packets transmitted: **0**



OPTION

WIRELESS TECHNOLOGY