

Comcast Business Router (CBR) Model- CGA4131COM

The Comcast Business Router (CBR) DOCSIS® 3.1 Cable Modem, with built-in 802.11ac Wi-Fi Router and voice eMTA



SETUP AND USER GUIDE

CBR CGA4131COM

SAFETY INSTRUCTIONS AND REGULATORY NOTICES

Before you start installation or use of this product, carefully read these instructions!





When using this product, always follow the basic safety precautions to reduce the risk of fire, electric shock and injury to persons, including the following:

- Always install the product as described in the documentation that is included with your product.
- Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.
- Do not use this product to report a gas leak in the vicinity of the leak.

Warranty Information

Unless express and prior approval by Technicolor in writing, you may not:

- Disassemble, de-compile, reverse engineer, trace or otherwise analyse the equipment, its content, operation, or functionality, or otherwise attempt to derive source code (or the underlying ideas, algorithms, structure or organization) from the equipment, or from any other information provided by Technicolor, except to the extent that this restriction is expressly prohibited by local law;
- Copy, rent, loan, re-sell, sub-license, or otherwise transfer or distribute the equipment to others;
- Modify, adapt or create a derivative work of the equipment;
- Remove from any copies of the equipment any product identification, copyright or other notices;
- Disseminate performance information or analysis (including, without limitation, benchmarks) from any source relating to the equipment.

Such acts not expressly approved by Technicolor will result in the loss of product warranty and may invalidate the user's authority to operate this equipment in accordance with FCC Rules.

Technicolor disclaims all responsibility in the event of use that does not comply with the present instructions.

Safety instructions

Climatic conditions

This product:

- Is intended for in-house stationary desktop use; the maximum ambient temperature may not exceed 40°C (104°F).
- Must not be mounted in a location exposed to direct or excessive solar and/or heat radiation.
- Must not be exposed to heat trap conditions and must not be subjected to water or condensation. Batteries (battery pack or batteries installed) shall not be exposed to excessive heat such as sunshine, fire or the like.
- Must be installed in a Pollution Degree 2 environment (Environment where there is no pollution or only dry, nonconductive pollution).

Cleaning

Unplug this product from the wall socket and computer before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.

Water and moisture

Do not use this product near water, for example near a bathtub, washbowl, kitchen sink, laundry tub, in a wet basement or near a swimming pool. Transition of the product from a cold environment to a hot one may cause condensation on some of its internal parts. Allow it to dry by itself before re-starting the product.

Secure handling and disposal of used batteries

NOTE: Only use the battery qualified for this equipment. Remember to dispose batteries properly according to local regulation, i.e. at a battery collection point. Batteries may not be disposed with domestic waste.

Interface classifications

The external interfaces of the product are classified as follows:

- Phone: TNV circuit, not subjected to over voltages (TNV-2)
- Cable, MoCA, RF: TNV circuit subject to over voltages (TNV-1)
- All other interface ports (e.g. Ethernet, USB, etc.), including the low voltage power input from the AC mains power supply: SELV circuits.

Electrical powering

The powering of the product must adhere to the power specifications indicated on the marking labels.

USB

The device is to be connected to an identified USB port complying with the requirements of a Limited Power Source.

Accessibility

The plug on the power supply cord serves as disconnect device. Be sure that the power socket outlet you plug the power cord into is easily accessible and located as close to the equipment as possible.

Overloading

Do not overload main supply socket outlets and extension cords as this increases the risk of fire or electric shock.

Servicing

To reduce the risk of electric shock, do not disassemble this product. None of its internal parts are user-replaceable; therefore, there is no reason to access the interior. Opening or removing covers may expose you to dangerous voltages. Incorrect reassembly could cause electric shock if the appliance is subsequently used.

If service or repair work is required, please contact a qualified service representative.

Damage requiring service

Unplug this product from the wall outlet and refer servicing to qualified service personnel under the following conditions:

- When the power supply or its plug are damaged.
- When the attached cords are damaged or frayed.
- If liquid has been spilled into the product.
- If the product has been exposed to rain or water.
- If the product does not operate normally.
- If the product has been dropped or damaged in any way.
- There are noticeable signs of overheating.
- If the product exhibits a distinct change in performance.

Immediately disconnect the product if you notice it giving off a smell of burning or smoke. Under no circumstances must you open the equipment yourself; you run the risk of electrocution.

Regulatory information

You must install and use this device in strict accordance with the manufacturer's instructions as described in the user documentation included with your product.

Before you start installation or use of this product, carefully read the contents of this document for device specific constraints or rules that may apply in the country in which you want to use this product.

In some situations or environments, the use of wireless devices may be restricted by the proprietor of the building or responsible representatives of the organization.

If you are uncertain of the policy that applies on the use of wireless equipment in a specific organization or environment (e.g. airports), you are encouraged to ask for authorization to use this device prior to turning on the equipment.

Technicolor is not responsible for any radio or television interference caused by unauthorized modification of the device, or the substitution or attachment of connecting cables and equipment other than specified by Technicolor. The correction of interference caused by such unauthorized modification, substitution or attachment will be the responsibility of the user. Technicolor and its authorized resellers or distributors are not liable for any damage or violation of government regulations that may arise from failing to comply with these guidelines.

North-America - United States of America

Important safety instructions

- The cable distribution system should be grounded (earthed) in accordance with ANSI/ NFPA 70, the National Electrical Code (NEC), in particular Section 820.93, Grounding of outer Conductive Shield of a Coaxial Cable.
- Leave 5 to 8 cm (2 to 3 inches) around the product to ensure proper ventilation to it.
- Never push objects through the openings in this product.

Federal Communications Commission (FCC) radio frequency interference statement

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

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



This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- 1 This device may not cause harmful interference, and



2 This device must accept any interference received, including interference that may cause undesired operation.

RF-exposure statement

When the product is equipped with a wireless interface, then it becomes a mobile or fixed mounted modular transmitter and must have a separation distance of at least 20 cm (8 inches) between the antenna and the body of the user or nearby persons. In practice, this means that the user or nearby persons must have a distance of at least 20 cm (8 inches) from the modem and must not lean on the modem in case it is wall-mounted. With a separation distance of 20 cm (8 inches) or more, the Maximum

Permissible Exposure limits are well above the potential this module is capable to produce. For operation within 5.15 ~ 5.25GHz frequency range, it is restricted to indoor environment. This device meets all the other requirements specified in Part 15E, Section 15.407 of the FCC Rules.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Restricted frequency band

This product is equipped with an IEEE802.11b/IEEE802.11g/IEEE802.11n wireless transceiver and may only use channels 1 to 11 (2412 to 2462 MHz) on U.S.A. territory.

Copyright

Copyright ©2017 Technicolor. All rights reserved.

Distribution and copying of this document, use and communication of its contents is not permitted without written authorization from Technicolor. The content of this document is furnished for informational use only, may be subject to change without notice, and should not be construed as a commitment by Technicolor. Technicolor assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

TECHNICOLOR WORLDWIDE HEADQUARTERS

1-5 rue Jeanne d'Arc

92130 Issy les Moulineaux

France

<http://www.technicolor.com>

Trademarks

The following trademarks may be used in this document

- AutoWAN sensing™ is a trademark of Technicolor.
- Qeo™ is a trademark of Qeo LLC, a subsidiary of Technicolor.
- Adobe®, the Adobe logo, Acrobat® and Adobe Reader® are trademarks or registered trademarks of Adobe Systems, Incorporated, registered in the United States and/or other countries.
- Apple® and Mac OS® are registered trademarks of Apple Computer, Incorporated, registered in the United States and other countries.
- Bluetooth® word mark and logos are owned by the Bluetooth SIG, Inc.
- CableLabs® and DOCSIS® are registered trademarks of CableLabs, Inc.
- DECT™ is a trademark of ETSI.
- DLNA® is a registered trademark, DLNA disc logo is a service mark, and DLNA Certified™ is a trademark of the Digital Living Network Alliance. Digital Living Network Alliance is a service mark of the Digital Living Network Alliance.
- Ethernet™ is a trademark of the Xerox Corporation.
- EuroDOCSIS™, EuroPacketCable™ and PacketCable™ are trademarks of CableLabs, Inc.
- HomePNA™ and HPNA™ are trademarks of HomePNA, Inc.
- Linux™ is a trademark of Linus Torvalds.
- Microsoft®, MS-DOS®, Windows®, Windows NT® and Windows Vista® are either registered trademarks or trademarks of the Microsoft Corporation in the United States and/or other countries.
- UNIX® is a registered trademark of UNIX System Laboratories, Incorporated.
- UPnP™ is a certification mark of the UPnP Implementers Corporation.
- Wi-Fi Alliance®, Wi-Fi®, WMM® and the Wi-Fi logo are registered trademarks of the Wi-Fi Alliance. Wi-Fi CERTIFIED™, Wi-Fi ZONE™, Wi-Fi Protected Access™, Wi-Fi Multimedia™, Wi-Fi Protected Setup™, WPA™, WPA2™ and their respective logos are trademarks of the Wi-Fi Alliance.

Other brands and product names may be trademarks or registered trademarks of their respective holders. All other logos, trademarks and service marks are the property of their respective owners, where marked or not.

Document Information

Status: v1.0 (May 2017)

Reference: CBR Data Sheet 5252017 COMCAST

Title: Setup and User Guide CBR CGA4131COM



Table of Contents

About this Setup and User Guide	8
1 Getting Started	9
1.1 Features at a glance	10
1.2 Getting to know the Gateway	11
1.2.1 Front panel.....	11
1.2.2 Top panel.....	12
1.2.3 Back panel	14
1.2.4 Bottom panel.....	15
1.3 Preparing for the installation	16
2 Setup	17
2.1 Connect the Gateway to your service provider's network	17
2.2 Power on the Gateway	18
2.3 Connect your wired devices.....	18
2.4 Connect your wireless devices	19
2.4.1 How to connect your wireless client via WPS.....	20
2.4.2 How to manually connect your wireless client.....	21
2.5 How to connect your phone	27
3 Admin Tool	28
3.1 Components	29
3.2 How to change the default Admin Tool password	31
3.3 How to backup or restore a configuration.....	31
3.4 Battery Behaviour	32
4 The Gateway wireless access point.....	34
4.1 How to configure the wireless settings	34
4.2 How to start a WPS session via the Admin Tool	37
4.3 Prevent devices from accessing your wireless network.....	39
5 Internet security	40
5.1 Content Filtering	40
5.1.1 Manage sites	40
5.1.2 Manage services.....	42
5.1.3 Manage devices.....	43
5.1.4 Reports	44
5.2 Firewall.....	45
6 Advanced configuration	46
6.1 Port configuration for applications and services.....	46
6.1.1 UPnP.....	48
6.1.2 Port forwarding	49
6.1.3 Port triggering	51
6.1.4 Port Management	52



6.1.5	Remote Management	53
6.1.6	Configure a DMZ Host	54
6.1.7	NAT	54
6.1.8	Static Routing	55
6.1.9	Dynamic DNS	56
6.2	Assigning a reserved IP to a device	57
7	Support	58
7.1	Wireless connection troubleshooting	58
7.2	Network diagnostic tools	60
7.3	Gateway reset and restore options	60

About this Setup and User Guide

In this Setup and User Guide

The goal of this Setup and User Guide is to:

- Set up your Gateway and local network
- Configure and use the main features of your Gateway.

For more advanced scenarios and features visit the documentation pages on www.technicolor.com.

Used symbols



The danger symbol indicates that there may be a possibility of physical injury.



The warning symbol indicates that there may be a possibility of equipment damage.



The caution symbol indicates that there may be a possibility of service interruption.



The note symbol indicates that the text provides additional information about a topic.

Terminology

Generally, the CBR CGA4131COM will be referred to as Gateway in this Setup and User Guide.

Typographical convention

Following typographical convention is used throughout this manual:

- This sample text indicates a hyperlink to a Web site.
Example: For more information, visit us at www.technicolor.com.
- This sample text indicates an internal link.
Example: If you want to know more about guide, see “About this Setup and User Guide”.
- This sample text indicates an important content-related word.
Example: To enter the network, you must authenticate yourself.
- This sample text indicates a GUI element (commands on menus and buttons, dialog box elements, file names, paths and folders).
Example: On the File menu, click Open to open a file.

1 Getting Started

Introduction

This chapter provides a brief overview of the main features and components of the Gateway. After this chapter, we will start with the installation.



Do not connect any cables to the Gateway until instructed to do so.

1.1 Features at a glance

Introduction

This section provides a brief overview of the main features of your Gateway.

- DOCSIS® 3.1 Certified
- 2 DOCSIS® 3.1 OFDM downstream channels & 2 DOCSIS® 3.1 OFDM upstream channels
- DOCSIS® 3.0 Certified
- 32 x 8 bonded channels in DOCSIS 3.0 mode
- Switchable diplexer for upstream and downstream
- Eight IEEE 802.3 10/100/1000 Base-T Gigabit Ethernet LAN ports
- Wireless networking on-board
- IEEE 802.11n 2.4 GHz Wi-Fi (2x2)
- IEEE 802.11a/n/ac Wave 2 with MU-MIMO 5 GHz Wi-Fi (4x4)
- Eight FXS ports for phone or fax
- Battery back-up with 8 hours standby and 5 hours talk time
- PacketCable™ 2.0 and SIP compliant
- IPv6 DS-Lite enabled



1.2 Getting to know the Gateway

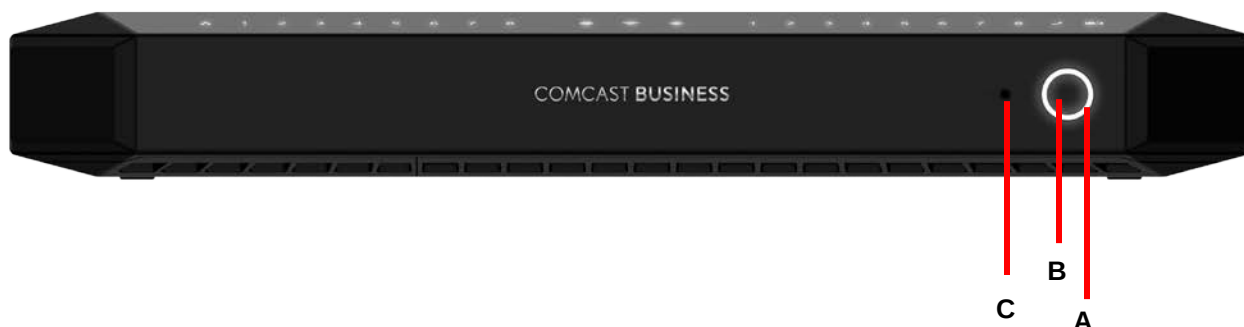
This section introduces you to the different components of the Gateway:

Topic	Page
1.2.1 Front Panel	11
1.2.2 Top Panel	12
1.2.3 Back Panel	14
1.2.4 Bottom Panel	15

1.2.1 Front panel

Introduction

On the front panel of your Gateway, you can find a number of LEDs that allow you to check the state of the services offered by the Gateway.



Power/WPS LED (item A)

The **Power/WPS** LED is lit when the gateway is powered on from the electrical outlet. It will turn off when the device is operational. The LED blinks when the WPS button is pressed. It will blink for 2 minutes or until the wireless client Wi-Fi is connected to the gateway, whichever is earlier. The LED will then turn solid white for 2 minutes and will turn Off thereafter.

For more information about WPS, see *"2.4.1 How to connect your wireless client via WPS"*.

WPS button (item B)

The **WPS** button allows you to add new wireless clients to your local network in a swift and easy way, without the need to enter any of your wireless settings (network name, wireless network key, encryption type).

For more information about WPS, see *"2.4.1 How to connect your wireless client via WPS"*.

Reset button (item C)

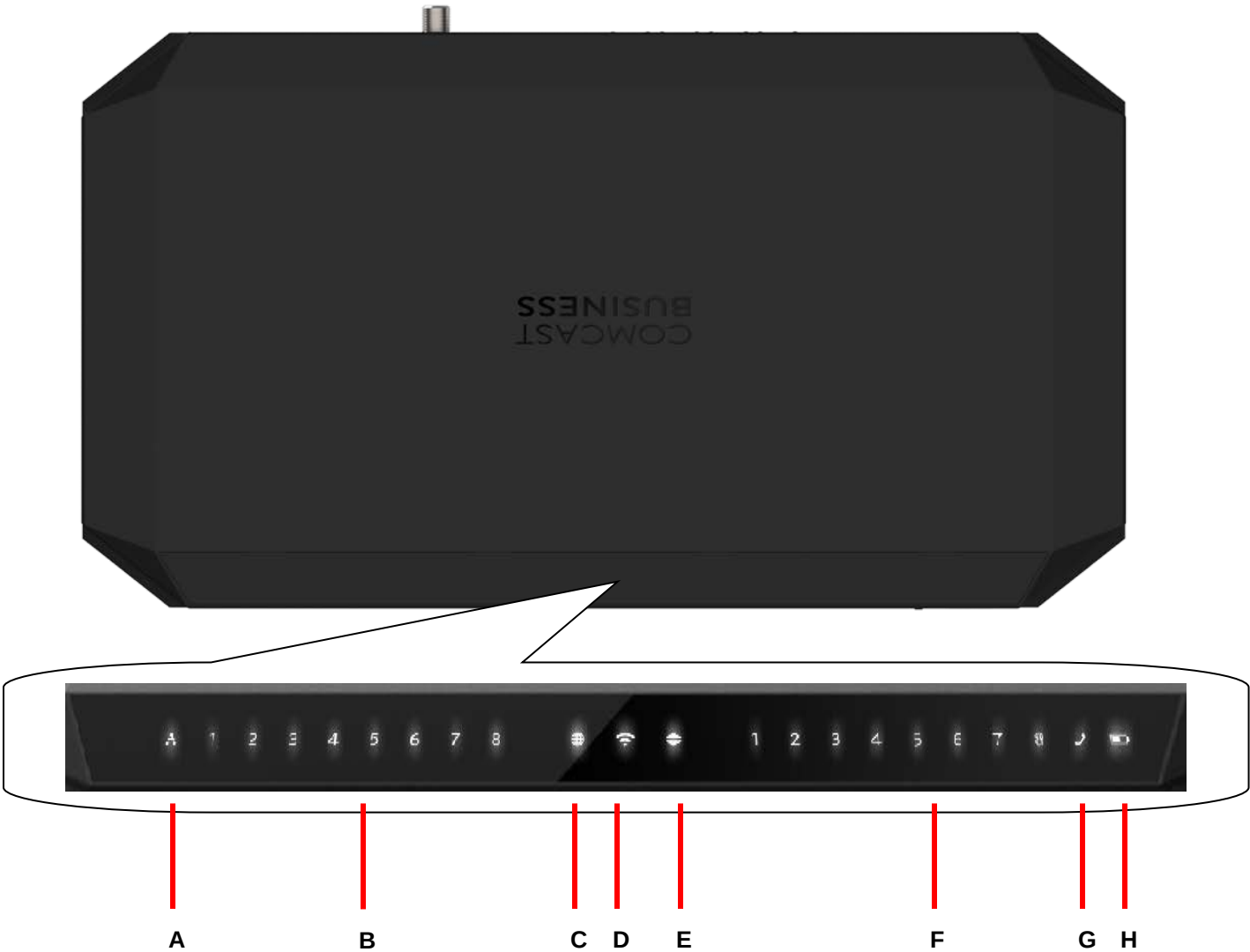
The **Reset** button allows you to:

- Restart the Gateway.
- Restore the factory defaults of the Gateway.

For more information, see *"7.3 Gateway reset and restore options"*.



1.2.2 Top panel



LED Legend:

State	Description
Solid on	Signifies steady state, or no action required
Blink (1X/second)	Signifies activity in progress or action required
Fast Blink (5X/second)	Fatal error, unrecoverable
Off	No activity, off

State	Description
Solid on	AC Power

Ethernet 1 to Ethernet 8 LED (item B)

State	Description
Solid on	Active Ethernet link
Blink (1X/second)	Active Traffic
Fast Blink (5X/second)	Port Error: physical connection error preventing traffic/activity
Off	No active Ethernet link

🌐 Online LED (item C)

State	Description
Solid on	Connection OK
Fast Blink (5X/second)	No internet connectivity (has block sync)
Off	No connection

📶 WiFi LED (item D)

State	Description
Solid on	On and OK
Blink (1X/second)	In Use (2.4 or 5G active)

📶 US/DS LED (item E)

State	Description
Solid on	Registration State Confirmed
Blink (1X/second)	Up/Down Stream registration or Non-deferred SW Download (when Online)

TEL 1 – TEL8 LED (item F)

State	Description
Solid on	Port Provisioned
Blinking (1X/second)	Call in Process
Blinking (5X/second)	Port Error: Tip & Ring shorts, foreign voltage detected, provisioning or registration error
Off	Port Not provisioned / Not enabled

Note: The CBR supports a total of 8 lines; the state is reflective of number of lines in use.

 TEL LED (item G)

State	Description
Solid on	AC Power

 Battery LED (item H)

LED	LED Status	Description
White	Solid on	On Battery Power
Amber	Solid	Battery at <=20% (Overrides AC / Battery Power States)
White and Amber	Blinking (1X/second)	Battery needs Replacement (Overrides AC/ Battery Power & Battery <=20% States)
Off	Off	Device is off or on AC Power or Battery not installed

1.2.3 Back panel



Tel port (item A)

The **Tel** () RJ-11 ports support up to eight traditional phones or DECT base station to connect to the Gateway. Single line customers can use the Tel 2/Alarm port to connect an auto dial alarm system. For more information, see “2.5 How to connect your phone”.

Ethernet switch (item B)

The RJ-45 Ethernet ports () support up to eight Ethernet connections (for example, a computer) to your local network. For more information, see “2.3 Connect your wired devices”.



All Ethernet ports on the Gateway support Gigabit Ethernet ports and have a maximum speed of 1 Gbps (Gigabit per second).

Each Ethernet port has two LEDs:

LED	LED Status	Description
Left LED (Green)	Solid on	1000MBPS Link
	Blinking (1X/second)	1000MBPS Link – Activity in progress
	Off	No Link
Right LED (Amber)	Solid on	10/100MBPS Link
	Blinking (1X/second)	10/100MBPS Link – Activity in progress
	Off	No Link

Cable port (item C)

The **Cable** port allows you to connect to your local coax network and the broadband network of your services provider.

USB ports (item D)

- Currently not supported.

Power inlet (item E)

The power inlet (**Power**) allows you to connect the power cord.

1.2.4 Bottom panel



Battery compartment (item A, optional)



A

B

During a power failure, the Gateway can automatically switch to the auxiliary emergency power via the rechargeable battery (if installed). The following capabilities are supported during a loss of power:

- The connected phones or dial function for a connected alarm system
- Basic voice features.



Do not remove the battery, unless instructed by your service provider.

Product label (item B)

The label on the bottom of the Gateway contains key manufacturing information, such as the part number, serial number, CM MAC address, MTA MAC address and WAN MAC address.

1.3 Preparing for the installation

Local connection requirements

Wireless connection

If you want to connect your computer using a wireless connection, your computer must be equipped with a Wi-Fi Certified wireless client adapter.

Wired connection

If you want to connect a computer using a wired connection, your computer must be equipped with an Ethernet Network Interface Card (NIC).

Start with the installation

You are now ready to start with the installation of your Gateway; proceed with “2 Setup”.



2 Setup

Setup procedure

Complete the following steps to setup the Gateway:

1. Connect your Gateway to your service provider's network.
For more information, see *"2.1 Connect the Gateway to your service provider's network"*.
2. Power on the Gateway.
For more information, see *"2.2 Power on the Gateway"*.
3. Connect your wired devices to the Gateway.
For more information, see *"2.3 Connect your wired devices"*.
4. Connect your wireless devices to the Gateway.
For more information, see *"2.4 Connect your wireless devices"*.
5. Connect your phones.
For more information, see *"2.5 How to connect your phone"*.

Optional configuration

After completing the setup procedure, the Gateway is ready for use. Optionally, you can further configure the Gateway to your needs (for example, change the wireless security) using the Gateway's Admin Tool.

For more information, see *"3 Admin Tool"*.

2.1 Connect the Gateway to your service provider's network

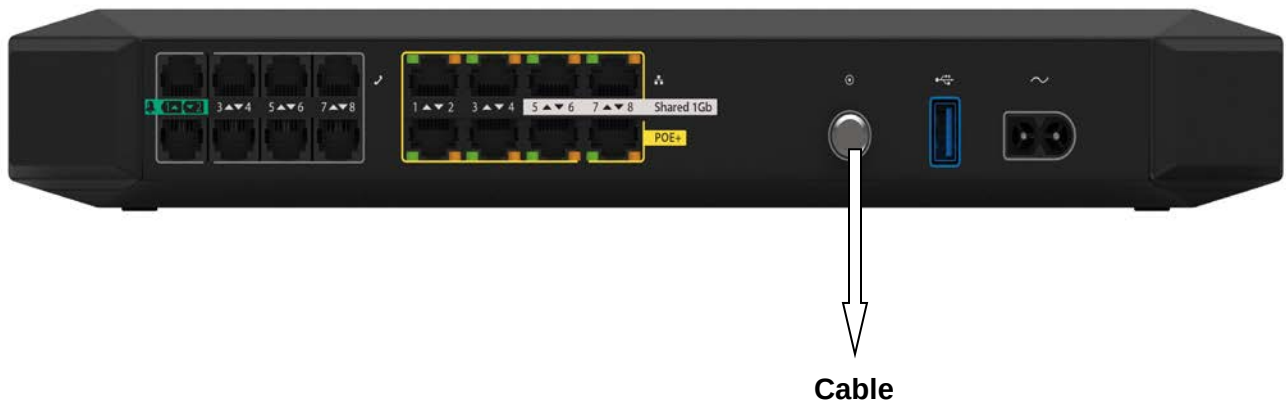
Introduction

This section helps you connect the Gateway to your service provider's network.

Connecting the cables

Proceed as follows:

1. Take one end of the coaxial cable and connect it to your cable splitter.
2. Connect the other end to the **Cable** port of the Gateway.



2.2 Power on the Gateway

Procedure

Proceed as follows:

1. Use the power cord that is included with your Gateway.
2. Connect the small end of the power cord to the Power port on the back of the Gateway.



3. Plug the other end of the power cord into an electrical outlet.
4. Wait at least two minutes to allow the Gateway to complete the startup phase.

2.3 Connect your wired devices

Requirements

- Both your network device (for example, a computer, a point of sale terminal, etc.) and Gateway must have a free Ethernet port.
- Your network device must be configured to obtain an IP address automatically. This is the default setting.

All Ethernet ports on the Gateway are Gigabit Ethernet ports and have a maximum speed of 1 Gbps (Gigabit per second).

Procedure

Proceed as follows:

1. It is recommended to use Category 5e or Category 6 Ethernet cables with the Gateway
2. Plug one end of the Ethernet cable into one of the RJ-45 Ethernet ports on the back of the Gateway:





3. Plug the other end of the Ethernet cable into the Ethernet port of your network device.
4. Your network device is now connected to your network. Use the same procedure to connect other Ethernet devices (computers, network printers and so on).

2.4 Connect your wireless devices

Introduction

The Gateway has two access points that allow you to connect wireless devices to your network:

- The 5 GHz IEEE 802.11a/n/ac access point offers superior transfer rates, is less sensitive to interference and allows you to connect IEEE 802.11a/n/ac wireless clients.
- The 2.4 GHz IEEE 802.11b/g/n access point allows you to connect IEEE 802.11b/g/n wireless clients. Use this access point for wireless clients that do not support 5 GHz.



If you want to connect your wireless client to the 5 GHz access point, make sure that your wireless client supports 5 GHz connections.

Procedure

To connect your device:

- Via WPS, proceed with *"2.4.1 How to connect your wireless client via WPS"*.
- By manually entering the settings, proceed with *"2.4.2 How to manually connect your wireless client"*.

2.4.1 How to connect your wireless client via WPS

WPS

Wi-Fi Protected Setup (WPS) allows you to add new wireless clients to your local network in a swift and easy way, without the need to enter any of your wireless settings (network name, wireless network key, encryption type).

Both the 2.4 GHz as the 5 GHz access points of your Gateway support WPS.

Requirements

- Your wireless client must support WPS. Check the documentation of your wireless client for this.
- Your Gateway must use **WPAWPA2-PSK (TKIP/AES)** encryption (default encryption) or **WPA2-PSK (AES)** encryption.

WPS methods

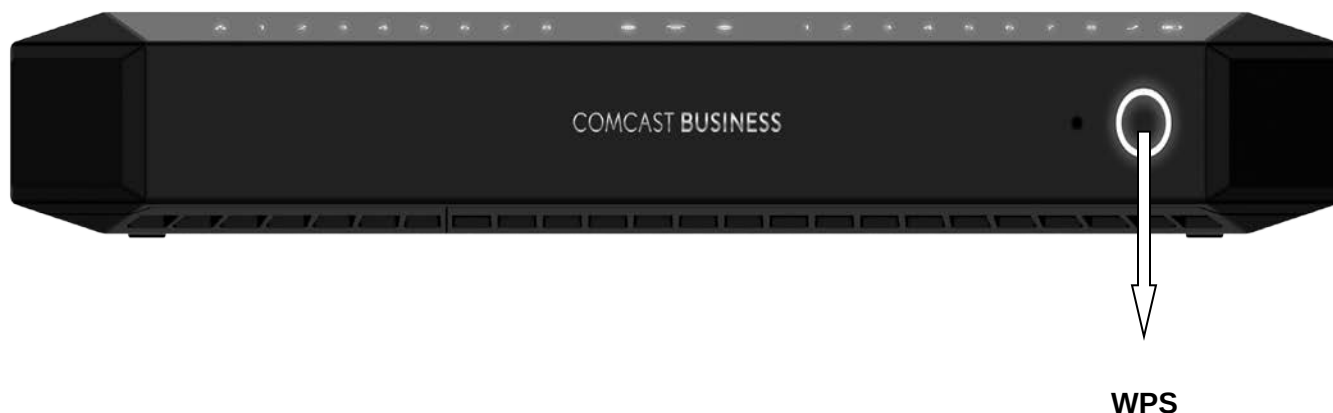
The following WPS methods are supported by your Gateway:

- Push Button Configuration (PBC):
Place both the wireless client and the Gateway in registration mode by pushing a hardware or software button.
- PIN code entry on the wireless client:
Enter the Gateway's WPS PIN code on the wireless client. For more information, see *"Adding a wireless client using WPS PIN entry on the wireless client"*.
- PIN code entry on the Gateway:
Enter the wireless client's WPS PIN code on the Admin Tool. For more information, see *"Adding a wireless client using WPS PIN entry on the Gateway"*.

Procedure for PBC

Proceed as follows:

1. Start WPS on your wireless client.
2. On the Gateway, press and hold the **WPS** button for at least 5 seconds and then release it.



3. The **WPS** button LED will start blinking. This indicates that the Gateway is now searching for wireless clients that are in registration mode.
4. The Gateway is now exchanging the security settings with the wireless client.
5. Your wireless client will prompt you when it is connected to the access point.



Troubleshooting

If you are having trouble connecting your wireless client via WPS, this may be caused by one of the following reasons:

- WPS cannot be correctly executed:
Configure your wireless manually. For more information, see “2.4.2 How to manually connect your wireless client”.
- Your wireless client is out of range:
If possible, move your wireless client closer to your Gateway or use a wireless repeater to extend the range of your wireless network.

2.4.2 How to manually connect your wireless client

Requirements

- Your network device must be equipped with a WiFi Certified wireless client.
- Your network device must be configured to obtain an IP address automatically. This is the default setting.

Procedure

If you want to connect a computer using the wireless network, configure the wireless client on your computer with the wireless settings printed on the Gateway's back panel label.



The Gateway's back panel contains two items needed to establish a Wi-Fi connection:

- **Network Name (SSID)** is the default network name. This network name is used by both the 2.4GHz and 5 GHz access points and is in the following format:

CBCI-XXXX (where X is last 4 octets of CM MAC).
- **Password (Key)** is the default password used for both the 2.4 GHz and 5 GHz access points



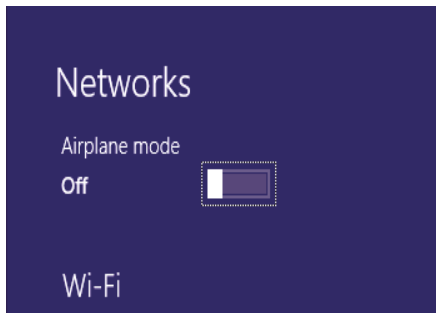
To configure these settings on:

- Windows 10, proceed with *"How to connect your computer on Windows 10"*.
- Windows 8, proceed with *"How to connect your computer on Windows 8"*.
- Windows 7, proceed with *"How to connect your computer on Windows 7"*.
- Windows Vista, proceed with *"How to connect your computer on Windows Vista"*.
- Windows XP, proceed with *"How to connect your computer on Windows XP"*.
- Mac OS X, proceed with *"How to connect your computer on Mac OS X"*.
- On another operating system, consult the help of your wireless client or operating system.

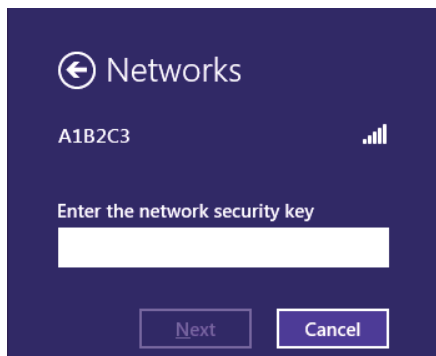
How to connect your computer on Windows 10

Proceed as follows:

1. Click the wireless network icon () in the notification area.
2. A list of available wireless networks appears.



3. Double-click the Gateway's Network Name (SSID).
 - Use the Gateway's Network Name (SSID) as printed on the bottom panel label.
4. Windows prompts you to enter the security key.



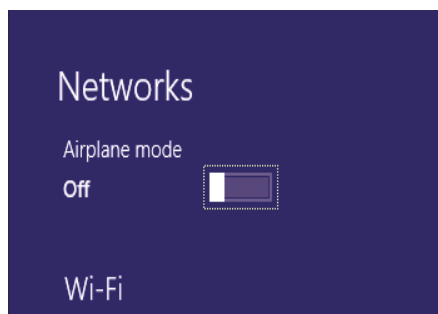
5. Type the **Password (Key)** from the Gateway's bottom panel label in the **Enter the network security key** box and click **Next**.
6. Windows prompts you if it should turn on sharing. Click **Yes**.



How to connect your computer on Windows 8

Proceed as follows:

1. Click the wireless network icon () in the notification area.
2. A list of available wireless networks appears.

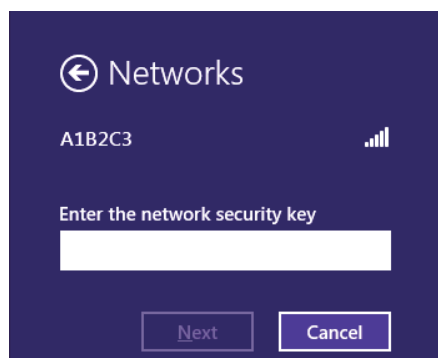


Double-click the Gateway's Network Name (SSID).



Use the Gateway Network Name as listed on the Gateway's back panel label. For more information, see "*Product label (item B)*".

3. Windows prompts you to enter the security key.



Type the **Password (Key)** from the Gateway's bottom panel label in the **Enter the network security key** box and click **Next**.

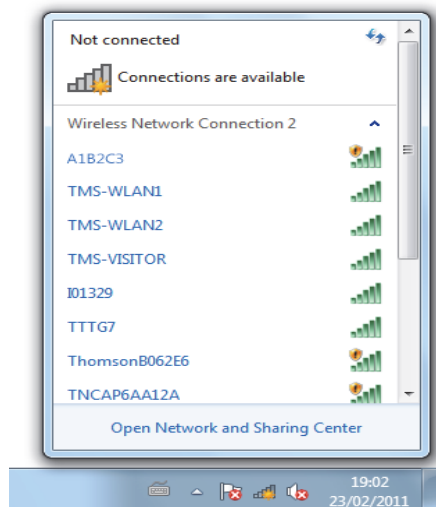
4. Windows prompts you if it should turn on sharing. Click **Yes**.

How to connect your computer on Windows 7

Proceed as follows:

1. Click the wireless network icon () in the notification area.
2. A list of available wireless networks appears.

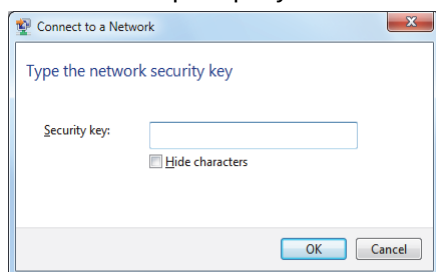




Double-click the Gateway's Network Name (SSID) access point.

 The Gateway's Network Name from the Gateway's back panel label. For more information, see *"Product label (item B)"*.

3. Windows prompts you to enter the security key.

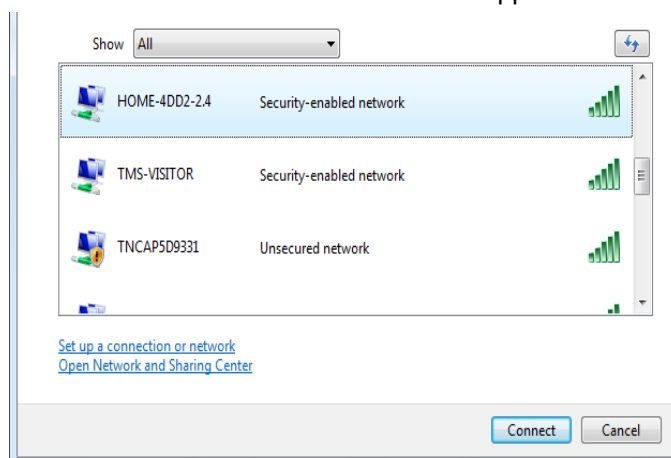


Type the **Password (Key)** which is printed on the Gateway's bottom panel label in the **Security key** box and click **OK**.

How to connect your computer on Windows Vista

Proceed as follows:

1. Click **Start**  and click **Connect To**.
2. A list of available wireless networks appears.

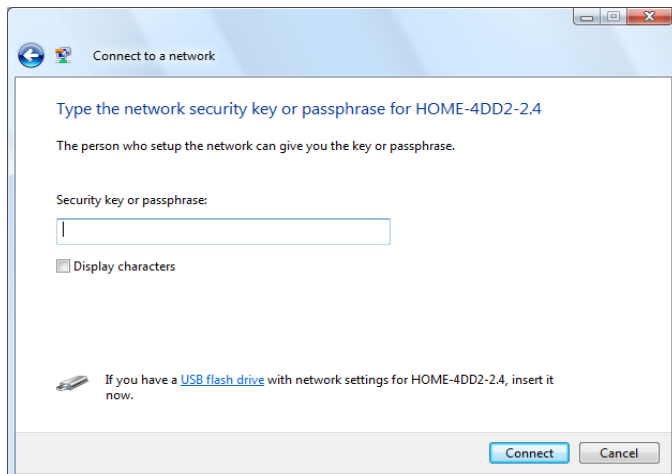


3. Double-click the Gateway's Network Name (SSID).



The Gateway's Network Name (SSID) is listed on the Gateway's back panel label. For more information, see *"Product label (item B)"*.

4. Windows prompts you to enter the network security key.

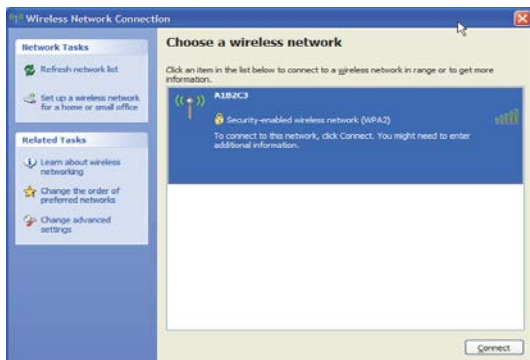


Type the **Password** from the Gateway's back panel label in the **Security key or passphrase** box and click **Connect**.

How to connect your computer on Windows XP

Proceed as follows:

1. Right-click the wireless network connection icon () in the notification area and then click **View Available Wireless Networks**.
2. A list of available wireless networks appears.

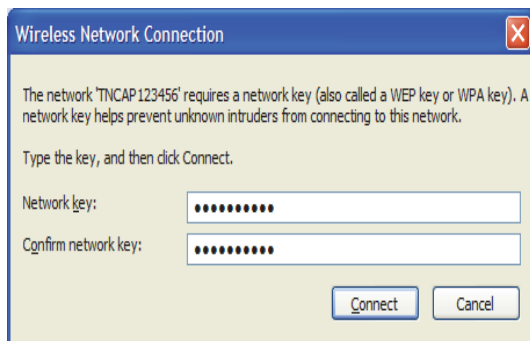


Double-click the Gateway's Network Name (SSID) access point.



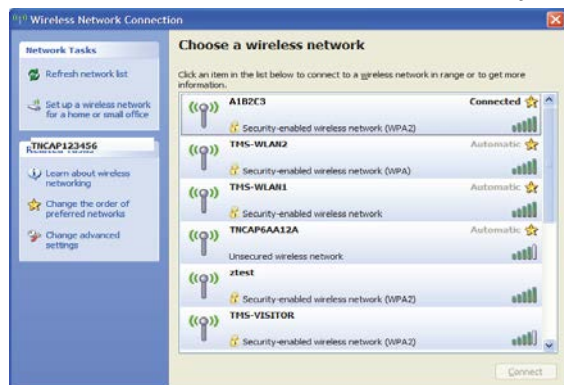
The Gateway's Network Name (SSID) is listed on the Gateway's back panel label. For more information, see *"Product label (item B)"*.

3. Windows prompts you to enter the network security key.



Type the **Password (Key)** which is printed on the Gateway's bottom panel label in the **Network key** and **Confirm network key** boxes and click **Connect**.

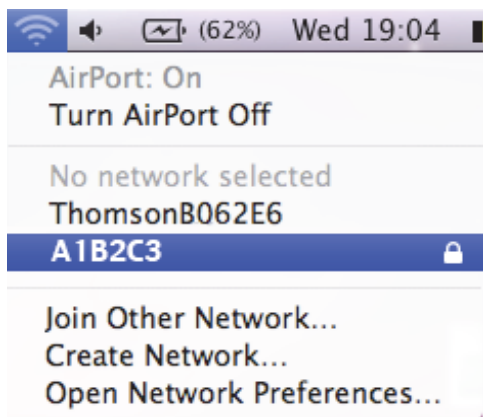
4. You are now connected to the Gateway:



How to connect your computer on Mac OS X

Proceed as follows:

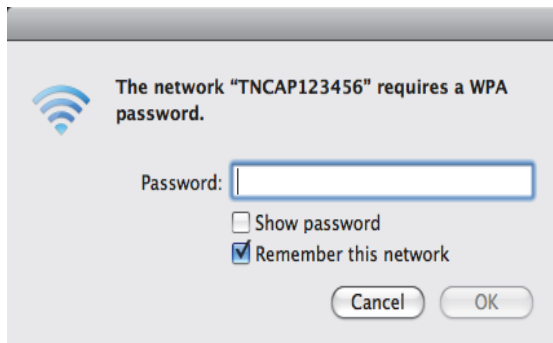
1. Click the **WiFi** icon on the menu bar.
2. A list of available wireless networks appears.



Double-click the Gateway' Network Name (SSID).



-  The Gateway's Network Name (SSID) is printed on the Gateway's side or back panel label. For more information, see *"Product label (item B)"*.
- 3. The **WiFi** window prompts you to enter your WPA password.



In the **Password** box, type the **Password (Key)** which is printed on the Gateway's bottom panel label and select the **Remember this network** box and click **OK**.

- 4. You are now connected to the Gateway network.

2.5 How to connect your phone

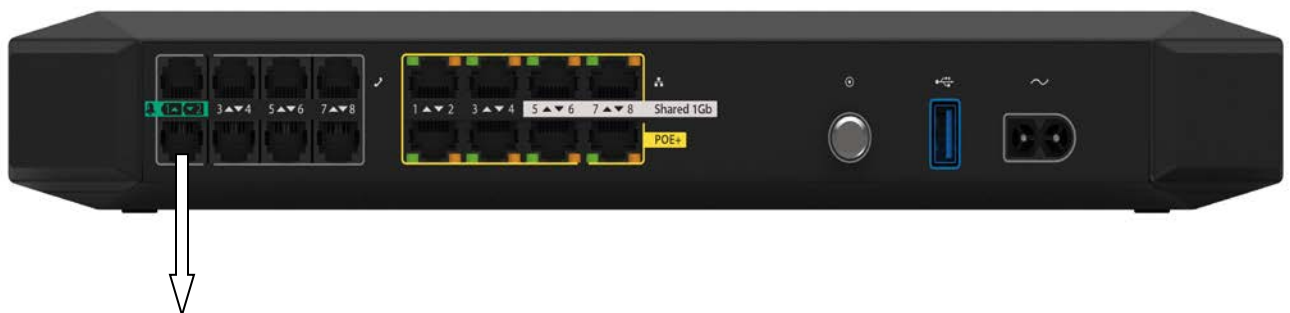
Introduction

This section describes how to connect the phones for single line customers.

If you have a two-line setup or a setup involving an alarm, please contact your service provider. This setup must be done by qualified technicians.

Procedure

Connect your traditional phone, external DECT base station or fax to an active RJ-11 Telephone jack on the back panel of your Gateway.



Telephone Port

1. Plug the other end of the telephone cable into the telephone device.
2. You must use connect Alarms dialers to either port 1 or 2. You are responsible to ensure that Alarms dialer is connected to an active telephone port connected to the phone network.
3. You must verify that each phone line is active by first checking for dial tone, and then by placing a call to an active telephone number and checking that both parties can properly hear one another.



3 Admin Tool

Introduction

The Admin Tool allows you to configure the settings of your Gateway via your web browser, using a computer or device that is currently connected to your Gateway (either wired or wirelessly).

Requirements

JavaScript must be enabled on your browser (this is the default setting). For more information, consult the help of your web browser.

Accessing the Admin Tool

Proceed as follows:

1. Open your web browser and go to <http://10.1.10.1>, using a computer or device that is currently connected to your Gateway (either wired or wirelessly).



On Windows, it is also possible to access the Admin Tool using UPnP. For more information, see “6.1.1 UPnP”.



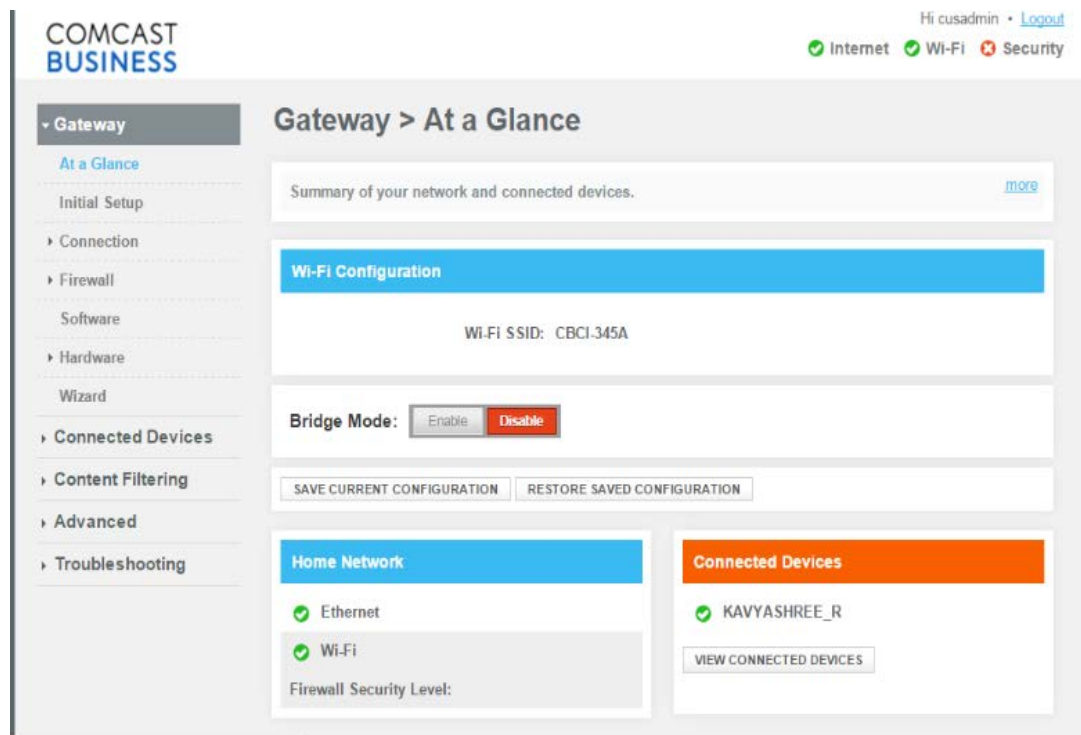
10.1.10.1 is the default IP address of the Gateway. If at some point you changed the IP address of the Gateway, use the new IP address instead.

2. The Gateway prompts you to enter the username and password. Enter your user name (default: **cusadmin**) and password (default: **highspeed**) and click **OK**.

The image shows the Comcast Business Admin Tool Login page. At the top is the Comcast Business logo. Below it is a grey header bar with the text 'Admin Tool Login'. Underneath the header, there is a light grey box containing the text 'Please login to manage your router.' followed by two input fields. The first field is labeled 'Username:' and contains the text 'cusadmin'. The second field is labeled 'Password:' and contains a series of dots. Below the password field is a button labeled 'LOGIN'.

3. The *Admin Tool* appears.

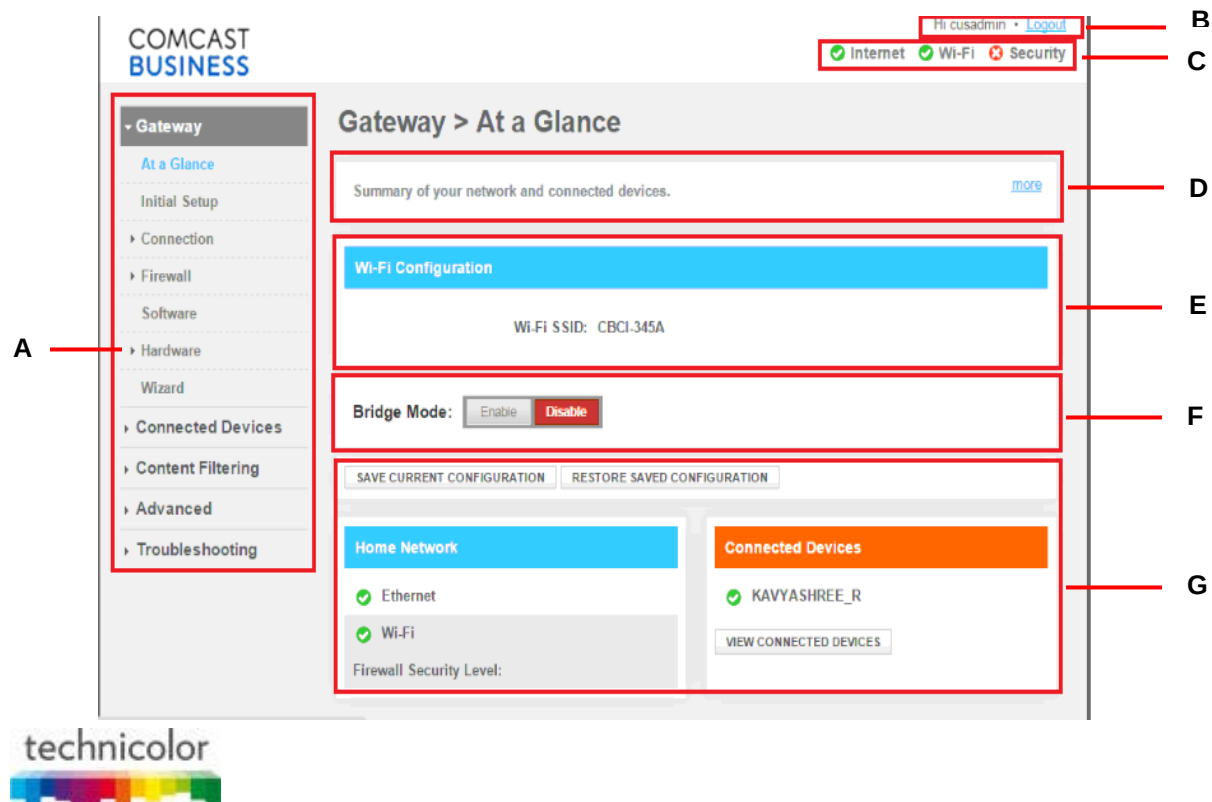




3.1 Components

Components overview

The following diagram identifies the sections of the Admin Tool:



Menu (item A)

The menu consists of the following menu items:

- **Gateway:**
Provides basic information about the Gateway and allows you to configure the basic settings.
- **Connected Devices:**
Allows you to manage the access settings of the devices in your network.
- **Content Filtering:**
Allows you to manage the access rights for Internet access.
- **Advanced:**
Allows you to configure more advanced Internet services.
- **Troubleshooting:**
Allows you to perform some basic troubleshooting on the Gateway and network connections.

Each of these items contain a number of sub-menu items.

More detailed information about the pages can be found in the tips section of each page. For more information, see *“Tips section (item D)”*.

Login section (item B)

In the login section, you can see the following details:

- User Name
- Option to logout

Status section (item C)

The diagnostics section provides a quick overview of the following:

- The status of the Internet interface
- The status of the wireless interface
- The selected firewall level



Move your mouse pointer over one of these items to view additional information.

Tips section (item D)

The tips section provides helpful information about the settings displayed on the current page.

Summary of your network and connected devices. [more](#)

To expand the tip, click **more**.

Summary of your network and connected devices. [less](#)

Select **VIEW CONNECTED DEVICES** to manage devices connected to your network.

WiFi Configuration (item E)

The WiFi configuration section displays the Network name (SSID) for both 2.4GHZ and 5GHz.

Bridge Mode (item F)

The Bridge mode section provides the option to Enable/Disable the Bridge mode.

Content panel (item G)

The content pane displays the actual configuration page.



3.2 How to change the default Admin Tool password

We recommend changing the default password of the Gateway.



The default username is **cusadmin** and the default password is **highspeed**.

Procedure

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *"Accessing the Admin Tool"*.
2. Enter default username and Password.
3. A pop-up message is displayed to change the password; click on "Yes" option **which re-directs the page to Change default Password.**

4. In the **Current Password** box, type your current password.



The default password is **highspeed**.

5. In the **New Password** and **Re-enter New Password** box, type your new password.



Your new password must be at least 8 characters long. It may include letters, numbers, or a combination of both (no symbols). For better security, try using at least one number and a mix of upper and lower-case letters.

6. Click **SAVE**.
7. The Gateway prompts you to login with your new password.

3.3 How to backup or restore a configuration

Introduction

Once you have configured the Gateway to your needs, it is recommended to backup the configuration for later use. This way, you can always return to the last working configuration in case of problems.

Backing up your configuration

Proceed as follows:

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *"Accessing the Admin Tool"*.
2. The **At a Glance** page appears. Click **SAVE CURRENT CONFIGURATION**.
3. Your browser prompts you to save or open the backup file. Save your file to a location of your choice.





Do not edit the backup files; this may result in corrupt files making them worthless as configuration backup.

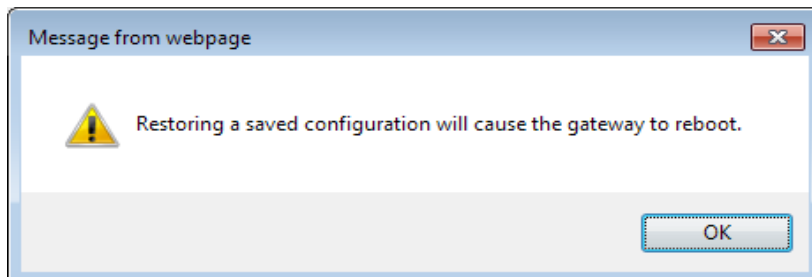
Restoring a previously saved configuration



Restoring a saved configuration will require the Gateway to restart. The reboot will cause a short service interruption of the services provided by the Gateway.

Proceed as follows:

1. Go to the Admin Tool (<http://10.1.10.1>). For more information, see *“Accessing the Admin Tool”*.
2. The “At a Glance” page appears. Click **RESTORE SAVED CONFIGURATION**.
3. The Gateway prompts you that restoring a saved configuration will cause the Gateway to reboot.



Click **OK** and then open your backup file.



A backup file usually has a **.cfg** extension.

4. The Gateway restores your configuration.

3.4 Battery Behaviour

Introduction

It displays the current status of connected battery.

Battery Status

Proceed as follows:

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *“Accessing the Admin Tool”*.
2. On the **Gateway** menu, click **Connection** and then click **Hardware**.
3. Click on **Battery**.
4. The Battery page appears:

Battery Status (As per GUI)	Description
Power Status	AC - When running on AC power with battery installed AC - When running on AC power with no battery installed
Battery Installed	Yes No
Battery Condition	Good (Awaiting Comcast Product Team's Reply) Low (Awaiting Comcast Product Team's Reply)



Battery Status	Charging (When Device is on AC power and battery charge is < 100%) Discharging (When Device is on Battery power) Idle (When Battery is neither 'Charging' nor 'Discharging')
Battery Life	Good (Awaiting Comcast Product Team's Reply) Need Replacement (Awaiting Comcast Product Team's Reply)
Total Capacity	Displays Battery Capacity
Actual Capacity	Displays Battery Capacity
Remaining Charge	Displays Remaining Charge left in the Battery
Remaining Time	Displays Remaining Time left for Battery Usage
Number of cycles to date	Displays Total no. of Cycles till date
Battery Model Number	Displays Battery Model Number
Battery Serial Number	Displays Battery Serial Number

4 The Gateway wireless access point

Introduction

This section will help you set up your wireless network.

What you need to set up a wireless network

To set up a wireless network, you need the following components:

- A *Wireless access point* (already integrated into your Gateway)
- A *Wireless client*: the device that you want to connect (for example, a computer, smartphone, network printer)

Wireless access point

The wireless access point is the heart of your wireless network. The wireless access point:

- Connects different wireless clients.
- Secures the data sent over wireless connection.

The Gateway has two access points:

- The 5 GHz access point enables superior transfer rates for 802.11a/n/ac wireless devices that are closer to the AP.
- The 2.4 GHz access point provides connectivity to 802.11b/g/n wireless clients that are farther from the AP. Use this access point for legacy wireless clients.



If you want to connect your wireless client to the 5 GHz access point, make sure that your wireless client supports 5 GHz connections.

Wireless client

The wireless client allows you to connect a wireless client to a wireless access point. Both built-in and external (for example via USB) wireless clients are available.



Devices like tablets, smart TVs and smartphones usually have a built-in wireless client. Check the documentation of your device for more information.

Check the documentation of your device if you are not sure if your device is equipped with a wireless client.

Configuring your wireless clients

For more information on how to establish a wireless connection to the Gateway, see:

- *"2.4.1 How to connect your wireless client via WPS"*
- *"2.4.2 How to manually connect your wireless client"*

4.1 How to configure the wireless settings

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *"Accessing the Admin Tool"*.
2. On the Gateway menu, click Connection and then click WiFi.
3. The WiFi page appears. In the Private WiFi Network table, click the EDIT button next to the access point that you want to modify (2.4GHz or 5GHz).



4. The Edit page appears:

Private Wi-Fi Network Configuration (2.4 GHz)

Wireless Network:

Network Name (SSID):

Mode:

Security Mode:

Please note 802.11 n mode only compatible with AES and None encryption!!

Channel Selection: ☒ Automatic ☐ Manual

Channel:

Channel Bandwidth: ☐ 20 ☒ 20/40

Network Password:

WPA requires an 8-63 ASCII character password.

Show Network Password: ☐

Broadcast Network Name (SSID): ☒ Enabled

or

Private Wi-Fi Network Configuration (5 GHz)

Wireless Network:

Network Name (SSID):

Mode:

Security Mode:

Please note 802.11 n/ac mode only compatible with AES and None encryption!!

Channel Selection: ☒ Automatic ☐ Manual

Channel:

Channel Bandwidth: ☐ 20 ☐ 20/40 ☒ 20/40/80

Network Password:

WPA requires an 8-63 ASCII character password.

Show Network Password: ☐

Broadcast Network Name (SSID): ☒ Enabled



The following fields are available for configuration:

Wireless Network:

Allows you to enable or disable this access point.

Network Name (SSID):

To distinguish one wireless network from another, each wireless network has its own network name, often referred to as Service Set Identifier (SSID). All your wireless clients on your network must use this network name (SSID).

Note: By default, the 2.4 GHz and 5 GHz APs have the same Network Name (SSID). This is so that dual mode clients can easily attach to the best AP best on rate and distance from the AP. You can choose to use different Network Names (SSIDs) for the 2.4 GHz and 5 GHz APs, if desired.

Mode:

The standards that are allowed for wireless communication. Only devices that support one of the selected modes can connect to the Gateway.

Security Mode:

The encryption type used to secure your wireless communication. We recommend using the default encryption, **WPAWPA2-PSK (TKIP/AES)** as it is compatible with most of the Wi-Fi devices and offers an excellent level of security. **Open** and **WEP** are to be avoided because of their own security flaws and should not be used in normal conditions.

Channel Selection:

The default setting is **Automatic**; the Gateway automatically selects the best channel for your wireless communication. We recommend that you not change this setting.

Channel:

The channel that is currently used for your wireless communication.

Channel bandwidth:

Allows you to select the channel bandwidth from the available option.

Network Password:

The wireless network key that is used for encrypting your wireless communication.

Show Network Password:

When you select the **Show Network Password** check box, the text in the **Network Password** will no longer be masked.

Broadcast Network Name (SSID):

By default, the Gateway broadcasts its network name. Wireless clients can then detect the presence of your network and inform the users that this network is available.



Enabling SSID broadcast does not mean that everyone can connect to your network. They still need the correct wireless network key (password) to connect to the Gateway network. It only informs them that your network is present.



SSID broadcasting is required for WPS.

5. Click **SAVE SETTINGS**.



4.2 How to start a WPS session via the Admin Tool

Adding a wireless client using WPS PBC

1. Make sure that the WPS button of your wireless client is accessible. This button can be a hardware button or a software button.
2. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *"Accessing the Admin Tool"*.
3. On the **Gateway** menu, click **Connection** and then click **WiFi**.
4. The **WiFi** page appears, click **ADD WIFI PROTECTED SETUP (WPS) CLIENT**.
5. The **Add WiFi Client** page appears.

Gateway > Connection > Wi-Fi > Add Wi-Fi Client

If a Wi-Fi device supports Wi-Fi Protected Setup (WPS), use the Gateway's WPS feature to simplify connection to your network. [more](#)

Add Wi-Fi Client (WPS)

Wi-Fi Protected Setup (WPS):

AP PIN: 06803308

WPS Pin Method:

Connection Options:

To pair, select the Pair button and your wireless device will connect within two minutes.

6. Click **PAIR**.
7. Within two minutes, press the PAIR button of your wireless client.

Adding a wireless client using WPS PIN entry on the wireless client

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *"Accessing the Admin Tool"*.
2. On the Gateway menu, click Connection and then click WiFi.
3. The WiFi page appears, click ADD WIFI PROTECTED SETUP (WPS) CLIENT.
4. The Add WiFi Client page appears.

Gateway > Connection > Wi-Fi > Add Wi-Fi Client

If a Wi-Fi device supports Wi-Fi Protected Setup (WPS), use the Gateway's WPS feature to simplify connection to your network. [more](#)

Add Wi-Fi Client (WPS)

Wi-Fi Protected Setup (WPS):

AP PIN: 06803308

WPS Pin Method:

Connection Options:

To pair, select the Pair button and your wireless device will connect within two minutes.

5. Write down the number displayed in **AP PIN**.
6. In the **WPS Pin Method** list, click **Enabled**.
7. Open the WPS PIN page of your wireless client and enter the PIN that you wrote down.

Adding a wireless client using WPS PIN entry on the Gateway

1. Locate and write down the WPS PIN of your wireless client. For more information, consult the documentation of your wireless client.
2. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *"Accessing the Admin Tool"*.
3. On the **Gateway** menu, click **Connection** and then click **WiFi**.
4. Click **ADD WIFI PROTECTED SETUP (WPS) CLIENT**.
5. The **Add WiFi Client** page appears.

Gateway > Connection > Wi-Fi > Add Wi-Fi Client

If a Wi-Fi device supports Wi-Fi Protected Setup (WPS), use the Gateway's WPS feature to simplify connection to your network. [more](#)

Add Wi-Fi Client (WPS)

Wi-Fi Protected Setup (WPS):

AP PIN: 87188301

WPS Pin Method:

Connection Options:

To pair, select the Pair button and your wireless device will connect within two minutes.

Wireless Client's PIN:



6. In the **WPS Pin Method** list, click **Enabled**.
7. In the **Connection Options** list, select **Pin Number**.
8. Enter the PIN from your wireless client in the **Wireless Client's PIN** box.
9. Click **PAIR**.

4.3 Prevent devices from accessing your wireless network

MAC address

A MAC (Media Access Control) address is a unique hexadecimal code that identifies a device on a network. Each network-enabled device has at least one unique MAC address.

For example, if your computer is equipped with an Ethernet and a wireless network adaptor, each of these interfaces will have its own MAC address.

MAC filtering

When using MAC filtering, you allow or deny devices to access your network based on their MAC address.

How to set up MAC filtering

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *"Accessing the Admin Tool"*.
2. On the **Gateway** menu, click **Connection** and then click **WiFi**.
3. The **WiFi** page appears. In the **SSID** list under **MAC Filter Setting**, select the access point for which you want to set up the MAC filter.

4. In the **MAC Filtering Mode** list, click:
 - **Allow-All** to allow all wireless clients. The **Wireless Control List** will not be used.
 - **Allow** to block wireless clients by default, except if they are listed in the **Wireless Control List**.



If you are currently connected via this access point, you must add your device to the exceptions in the **Wireless Control List** before clicking **SAVE FILTER SETTING** (this will be done in the next step). If you do not do this, you will be disconnected from the access point.

- **Deny** to allow wireless clients by default, except if they are listed in the **Wireless Control List**.
5. Add the exception on the default action, by doing one of the following:
 - Under **Auto-Learned wireless clients**, select the device and click **ADD**.
 - Under **Manually-Added wireless clients**, type the device name and MAC address and click **ADD**.

Manually-Added Wi-Fi Devices

Repeat this step for each exception that you want to add.

6. Click **SAVE FILTER SETTING**.



5 Internet security

Overview

The Gateway offers various options to secure your Internet connection:

Topic	Page
5.1 Content Filtering	40
5.1.1 Managed Sites	40
5.1.2 Managed Services	42
5.1.3 Managed Devices	43
5.1.4 Reports	44
5.2 Firewall	45

5.1 Content Filtering

Introduction

The Content Filtering function:

- Prevents access to specific website based on the URL or keywords.
For more information, see *"5.1.1 Manage sites"*.
- Prevents access to specific application or services (for example, FTP).
For more information, see *"5.1.2 Manage services"*.
- Prevents devices from accessing your network.
For more information, see *"5.1.3 Manage devices"*.

5.1.1 Manage sites

Introduction

The **Managed Sites** page allows you to:

- Block specific websites (always or for a specific time frame).



The Gateway does not block websites that use HTTPS.

- Block keywords (always or for a specific time frame).
- Mark devices as trusted.

When a device is marked as trusted, all **Managed Sites** rules will be ignored.

How to access the Managed Sites page

1. Go to Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *"Accessing the Admin Tool"*.
2. On the left menu, click **Content Filtering**.
3. The **Managed Sites** page appears.
4. In the **Enable Managed Sites** list, click **Enable**.



How to block a specific website

Proceed as follows, from the **Managed Sites** page:

1. Under **Blocked Sites**, click **+ ADD**.
2. The **Add Blocked Domain** page appears.

The screenshot shows the 'Add Site to be Blocked' form. The URL field contains 'http://'. The 'Always Block?' toggle is set to 'Yes'. The 'Set Block Time' section shows 'Start from: 12:00 AM' and 'End on: 11:59 PM'. The 'Set Blocked Days' section shows checkboxes for Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday, all of which are checked. There are 'SAVE' and 'CANCEL' buttons at the bottom.

3. In the URL field type the address of the website (for example, **facebook.com**).
 4. If you want this rule only to be applied at specific time frames, click **No** in the **Always Block** list and define when to apply the rule:
 - a. Under **Set Block Time**, enter a start time and end time.
 - b. Under **Set Block Days**, select the days for which the selected block time should be applied.
-  If you want to have different time schedules depending on the day, you will have to group these in separate rules:
- One rule for weekdays (for example, access to Facebook from 8:00 PM until 10:00 PM).
 - One rule for the weekend (for example, access to Facebook from 4:00 PM until 10:00 PM).
 - If you want to create rules that run overnight, you must create two rules (for example, one rule from Monday 8:00 PM until 11:59PM and second rule from Tuesday 12:00 AM until 6:00 AM).
5. Click **SAVE**.

How to block websites based on keywords

Proceed as follows, from the **Managed Sites** page:

1. Under **Blocked Sites**, click **+ ADD**.
2. The **Add Keyword to be Blocked** page appears.



3. In the **Keyword** box type the keyword that you want to block (for example, the **webmail** keyword will block all URLs that contain the word **webmail** in the URL).
4. If you want this rule only to be applied at specific time frames, click **No** in the **Always Block** list and define when to apply the rule:
 - Under Set Block Time, enter a start time and end time.
 - Under Set Block Days, select the days for which the selected block time should be applied.
-  If you want to have different time schedules depending on the day, you must group them in separate rules:
 - One rule for weekdays (for example, rule active from 8:00 PM until 10:00 PM).
 - One rule for the weekend (for example, rule active from 4:00 PM until 10:00 PM).
5. Click **SAVE**.

Mark computers as trusted for all websites

When a device is marked as trusted, all Managed Sites rules will be ignored.

Proceed as follows:

1. Under **Trusted Computers**, look for your device and click **Yes** in the **Trusted column**.
2. The device is now able to access all web sites unless prevented by other parental control functions that you configured.

5.1.2 Manage services

Introduction

The **Managed Services** page allows you to:

- Create a service-specific rule to block specific Internet services.



Optionally, you can provide a time schedule for a rule. The rule will then only be activated within the specified time frame.

- Mark computers as trusted. For trusted computers, all service rules will be ignored.

How to create a service rule

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *"Accessing the Admin Tool"*.
2. On **Content Filtering** menu, click **Managed Services**.
3. The **Managed Services** page appears.
4. In the **Enable Managed Services** list, click **Enable**.



Managed Services:

Enable

Disable

5. In the Blocked Services table, click **+ ADD**.
6. The **Add Service to be Blocked** page appears.
7. Complete the following fields:
 - In the **User Defined Service** box, type a name for the rule (for example, FTP).
 - In the **Protocol** list, click on the protocol that is used (for example, TCP).
 - In the **Start Port** box, type the start port of the port range (for example, 21).
 - In the **End Port** box, type the end port of the port range. If the service only uses one port, enter the same value as in the **Start Port** box (for example, 21).
-  If the port range is not a contiguous range of numbers, you must spread them over multiple service rules.
8. If you want this rule only to be applied at specific time frames, click **No** in the **Always Block** list and define when to apply the rule:
 - Under **Set Block Time**, enter a start time and end time.
 - Under **Set Block Days**, select the days for which the selected block time should be applied.
-  If you want to have different time schedules depending on the day, you must group them in separate rules:
 - One rule for weekdays (for example, block the service from 10:00 PM until 8:00 PM).
 - One rule for the weekend (for example, block the service from 10:00 PM until 8:00AM).
9. Click **SAVE**.

Mark computers as trusted for all services

When a device is marked as trusted, all managed services rules will be ignored.

Proceed as follows:

1. Under **Trusted Computers**, look for your device and click **Yes** in the **Trusted column**.
2. The device is now able to use all web services unless prevented by other parental control functions that you configured.

5.1.3 Manage devices

On the **Managed Devices** page, you can create a device-specific rule to prevent a device from accessing your network.



Optionally, you can provide a time schedule for a rule. The rule will then only be activated within the specified time frame.

Procedure

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *"Accessing the Admin Tool"*.
2. On the **Content Filtering** menu, click **Managed Devices**.
3. In the **Enable Managed Devices** list, click **Enable**.
4. In the **Access Type** list, click:
 - **Allow All** to allow all devices by default. In this case you must create a rule for each device that you want to block on your network.



- **Block All** to block all devices by default. In this case you must create a rule for each device that you want to allow on your network.

Adding allowed devices

If you selected **Block All** in the **Access Type** list, proceed as follows:

1. In the **Allowed Devices** table, click **+ADD ALLOWED DEVICE**.
2. **The Add Device to be Allowed page appears.**
3. Under **Set Allowed Device**, select your device from the **Learned Device(s)** list. If your device is not listed, enter the computer name and MAC address under **Custom Device**.
4. If you want this rule only to be applied at specific time frames, click **No** in the **Always Allow** list and define when to apply the rule:
 - Under **Set Allow Time**, enter a start time and end time.
 - Under **Set Allow Days**, select the days for which the selected block time should be applied.



If you want to have different time schedules depending on the day, you must group them in separate rules:

- One rule for weekdays (for example, allow the device from 10:00 PM until 8:00 PM).
 - One rule for the weekend (for example, allow the device from 10:00 PM until 8:00 AM).
5. Click **SAVE**.

Adding blocked devices

If you selected **Allow All** in the **Access Type** list, proceed as follows:

1. In the **Blocked Devices** table, click **+ADD BLOCKED DEVICE**.
2. **The Add Device to be Blocked page appears.**
3. Under **Set Blocked Device**, select your device from the **Learned Device(s)** list. If your device is not listed, enter the computer name and MAC address under **Custom Device**.
4. If you want this rule only to be applied at specific time frames, click **No** in the **Always Block** list and define when to apply the rule:
 - Under **Set Block Time**, enter a start time and end time.
 - Under **Set Block Days**, select the days for which the selected block time should be applied.



If you want to have different time schedules depending on the day, you must group them in separate rules:

- One rule for weekdays (for example, block the device from 8:00 PM until 10:00 PM).
 - One rule for the weekend (for example, block the device from 8:00 AM until 10:00 PM).
5. Click **SAVE**.

5.1.4 Reports

Introduction

The **Reports** page allows you to generate reports on possible infringements of the parental control rules.

Procedure

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *"Accessing the Admin Tool"*.
2. On the **Content Filtering** menu, click **Reports**.
3. The **Report** page appears.



The screenshot shows a web interface for generating reports. At the top, there's a 'Report Filters' section with two dropdown menus: 'Report Type' set to 'All' and 'Time Frame' set to 'Today'. A 'GENERATE REPORT' button is to the right. Below this is a 'Generated report' section with a blue header. Under the header, it says 'All Logs for today'. There is a table with four columns: 'Date', 'MAC', 'Rule Type:Rule Name', and 'Comments'. Below the table are two buttons: 'PRINT' and 'DOWNLOAD'.

Under **Report Filters**, select a report type and time frame and click **GENERATE REPORT**.

4. The **Generated report** table now lists all log entries.
5. Optionally, you can:
 - Click **PRINT** to print the log entries.
 - Click **DOWNLOAD** to save the log entries as a text file.

5.2 Firewall

Introduction

The Gateway comes with an integrated firewall that helps you protect your network from attacks from the Internet. This firewall has a number of predefined levels to allow you to adjust the firewall to your needs. The default Firewall setting is **Minimum Security (Low)**. This means that *all* traffic passing through the Gateway (from and to the Internet) is allowed.

Predefined security levels

The Gateway has a number of predefined security levels. The following levels are available:

- **Maximum Security (High):**

Blocks all the applications including IP-driven voice applications (such as Gtalk, Skype) and P2P applications. Allows Internet browsing, email, VPN, DNS and iTunes services.



Although BlockAll will block all connections, some mandatory types of traffic such as DNS will still be relayed between LAN and WAN by the Gateway.

- **Typical Security (Medium):**

Blocks P2P applications and Ping to the Gateway, allows all other traffic.

- **Minimum Security (Low):**

Allows all secure applications. This is the default configuration.



The firewall levels only have impact on traffic passing through your Gateway. This means that the handling of traffic directly appointed from and to the Gateway is independent of the selected firewall level.

- **Custom Security:**

Allows you to create your own security level.

Changing the security level

Proceed as follows:

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *"Accessing the Admin Tool"*.
2. On the **Gateway** menu, click **Firewall**.
3. The **Firewall** page appears. Under **Firewall Security Level**, select one of the predefined levels or select **Custom Security** to create a custom level.
4. Click **SAVE SETTINGS**.



6 Advanced configuration

Introduction

This chapter covers the more advanced features. The following topics are available:

Topic	Page
6.1 Port configuration for applications and services	46
6.1.1 UPnP	48
6.1.2 Port Forwarding	49
6.1.3 Port Triggering	51
6.1.4 Port Management	52
6.1.5 Remote Management	53
6.1.6 Configure a DMZ Host	54
6.1.7 NAT	54
6.1.8 Static Routing	55
6.1.9 Dynamic DNS	56
6.2 Assigning a Reserved IP to a Device	57

6.1 Port configuration for applications and services

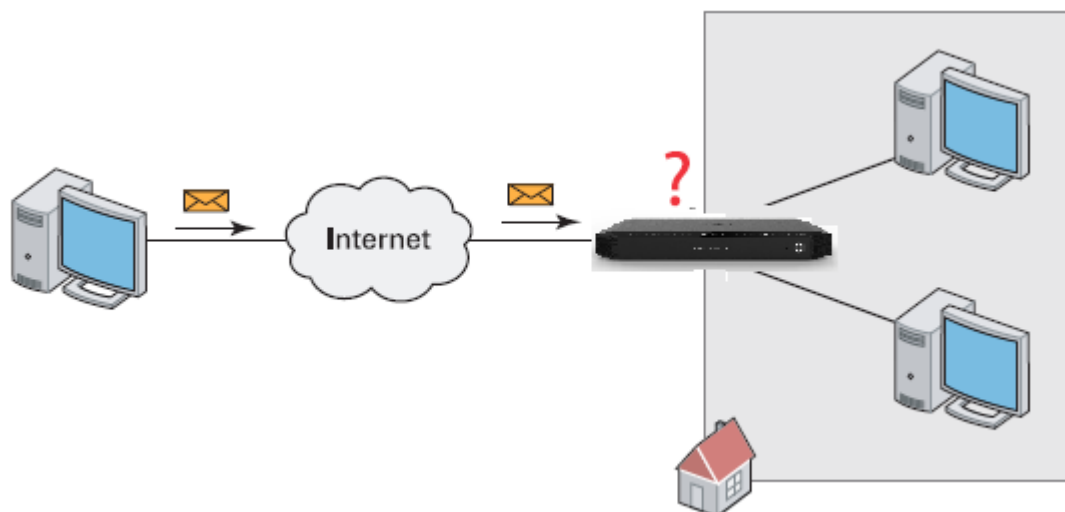
Introduction

The Gateway allows you to use one Internet connection for multiple computers. This means that all your computers share one public IP address, as if only one computer were connected to the outside world.

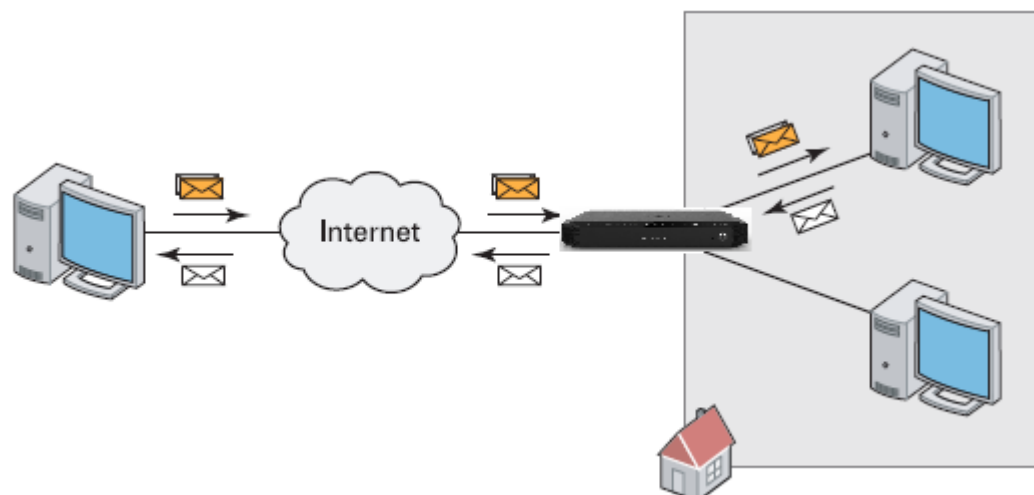
Issue

When the Gateway receives an incoming message, the Gateway must decide to which computer it should send this message.

If the incoming message is a response to an outgoing message originating from one of your computers, the Gateway sends the incoming message to this computer.



But the Gateway will not be able to resolve the destination if:



- The incoming message arrives on a different port as the outgoing message. Then the Gateway will not know that the two messages are related.
- There is no outgoing message.

Solutions

To avoid this problem, the Gateway offers the following solutions:

- The Gateway supports automatic device discovery and port configuration for UPnP-enabled devices. For more information, see [“6.1.1 UPnP”](#).
- The Gateway allows you to assign a port to a device. For more information, see [“6.1.2 Port forwarding”](#).
- The Gateway allows you to define a number of trigger ports. When a device sends data over one of these ports, the Gateway will automatically assign a number of related ports to the device. For more information, see [“6.1.3 Port triggering”](#).

6.1.1 UPnP

Introduction

UPnP is designed to automate the installation and configuration of a (small) network as much as possible. This means that UPnP-capable devices can join and leave a network without any effort of a network administrator.

Supported operating systems

The following operating systems support UPnP:

- Windows 10
- Windows 8
- Windows 7
- Windows Vista
- Windows XP



If your computer is running Windows XP, you first must install the UPnP component. For more information, see Windows help.

UPnP and the Gateway

UPnP offers you the following functions:

- You do not have to manually create port mappings to run services on a computer. The automatic port configuration mechanism for UPnP-enabled applications will do this for you. If the application is UPnP-enabled, UPnP will create these entries automatically.
- You can access the *Admin Tool* without having to remember the address of the Gateway.

Enable UPnP on the Gateway

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *"Accessing the Admin Tool"*.
2. On the **Advanced** menu, click **Device Discovery**.
3. The **Device Discovery** page appears.

In the **Enable UPnP** list, select **Enabled**.

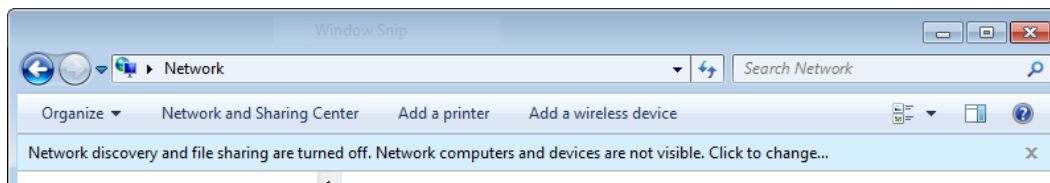
4. Click **SAVE**.

How use UPnP to access your Gateway on Windows 7/Vista

If your computer runs Windows 7/Vista:

1. On the Windows **Start** menu, click **Computer**.
2. An Explorer window appears. In the panel, click **Network**.
3. If Explorer prompts you that network discovery and/or file sharing are turned off, click on the message and turn it on.





4. Right-click **Technicolor CGA4131COM** and click **View device web page**.
5. The Admin Tool appears.

How to use UPnP to access your Gateway on Windows XP

If your computer runs Windows XP:

1. Go to **My Network Places**.
2. The **My Network Places** window appears.
3. Double-click **Technicolor CGA4131COM**.
4. The Admin Tool appears.

6.1.2 Port forwarding

Introduction

Port forwarding allows you to forward incoming Internet traffic arriving on a specific port to an internal IP address. For example, if you are running a web server and the Gateway receives a request on port 80, this request should be forwarded to your web server.

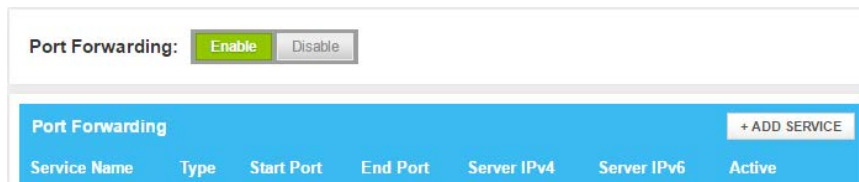
Use a reserved IP address

The target device of the port forwarding rules will be specified by an IP address. Make sure that your device uses a fixed IP address. If you do not do this, the device might get a new IP address after some time and the port forwarding rule will no longer be applied to the device. For more information, see *6.2 Assigning a reserved IP to a device*.

Procedure

Proceed as follows:

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *"Accessing the Admin Tool"*.
2. On the left menu, click **Advanced**.
3. The **Port Forwarding** page appears.



In the **Enable Port Forwarding** list, click **Enabled**. In the **Port Forwarding** table, click **+ADD SERVICE**.

4. The **Add Service** page appears.



Advanced > Port Forwarding > Add Service

Add a rule for port forwarding services by user. [more](#)

Add Port Forward

Common Service: Other ▼

Service Name:

Service Type: TCP/UDP ▼

Server IPv4 Address:

Server IPv6 Address:

Start Port:

End Port:

Select a device to add IPv4 and IPv6 address

CONNECTED DEVICE

SAVE CANCEL

5. In the Common Services list, select the service you want to run on the computer or select Other if the service is not listed.
6. If you selected Other, complete the following fields:
 - In the **Service Name** box, type a name for the services that you want to configure.
 - In the **Service Type** list, select the protocol that is used by the service.
 - In the **Starting Port** box, type the start port number of the port range.
 - In the **End port** box, type the last port number of the port range. If you only want to specify one port, use the same number as in the **Starting Port** box.
7. In the Server IPv4 Address box, type the IP address of the computer to which you want to assign the service.
8. In the Server IPv6 Address box, type the IP address of the computer to which you want to assign the service.
9. If you don't want to type in any of the IP address box then click on Connected Device tab, select the IP address of the computer to which you want to assign the service. Click on Add

Advanced > Port Forwarding > Add Service

Add a rule for port forwarding services by user. [more](#)

Add Port Forward

Common Service: Other ▼

Service Name:

Select from below Connected Devices:

Device Name	IPv4 Address	IPv6 Address	Add
durgeshn	10.1.10.19		+

Add Close

Start Port:

End Port:

Select a device to add IPv4 and IPv6 address

CONNECTED DEVICE

10. Click **SAVE**
11. Your service is now listed in the Port Forwarding table. All incoming requests for the selected service will now be directed to the selected device. The Gateway also automatically configures its firewall to allow this service.

6.1.3 Port triggering

Introduction

Port triggering allows you to define a set of dynamic port forwarding rules that will be activated as soon as a device sends traffic to the Internet over a specific port(s), the **trigger port(s)**.

The difference compared to the port forwarding function described in “6.1.2 Port forwarding” is that:

- Port triggering rules will only be activated if a local device is sending traffic over one of the trigger ports. There must be outbound traffic first.
- Port triggering rules forward the traffic to any device that has initiated the communication while port forwarding only forwards to a specific fixed IP.
- Port triggering rules allow you to translate the port numbers. This means that the incoming port can differ from the target port.

Procedure

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see “Accessing the Admin Tool”.
2. On the **Advanced** menu, click **Port Triggering**.
3. The **Port Triggering** page appears.

In the **Enable Port Triggering** list, click **Enabled**. In the **Port Triggering** table, click **+ADD PORT TRIGGER**.

4. The **Add Port Trigger** page appears.

Complete the following fields:

- In the **Service Name** box, type a name for the rule (for example, FTP).
 - In the **Service Type** list, click on the protocol that is used (for example, TCP).
 - In the **Trigger Port From** box, type the start port number of the trigger port range.
 - In the **Trigger Port To** box, type the end port number of the trigger port range. If you only want to specify one port, use the same number as in the **Trigger Port From** box.
 - In the **Target Port From** box, type the start port number of the target port range.
 - In the **Target Port To** box, type the end port number of the target port range. If you only want to specify one port, use the same number as in the **Target Port From** box.
5. Click **SAVE**.
 6. Your service is now listed in the **Port Triggering** table. All incoming requests for the selected service will now be directed to the selected device. The Gateway also automatically configures its firewall to allow this service.



6.1.4 Port Management

Introduction

Port management allows you to define a set of port management rules that restrict certain inbound traffic to specific computers on the True Static IP network. This gateway supports up to 100 True Static IP Port Management rules.

Procedure

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *"Accessing the Admin Tool"*.
2. On the **Advanced** menu, click **Port Management**.
3. The **Port Management** page appears.

In the **Enable Port Management**, uncheck the **Disable all rules and allow all Inbound traffic through**; click **OK** on the pop up window.

4. Select the Port Management from the list **Block all ports but allow exceptions below** or **Open all ports but block exceptions below**; click **OK** on the pop up window.
5. Click **+ADD NEW**
6. The **Add rule** page appears.

Complete the following fields:

- In the **Application Name** box, type a name for the rule (for example, FTP).
- In the **Protocol** list, click on the protocol that is used (for example, TCP).
- In the **Start True Static IP** box, type the start IP address of the IP range.
- In the **End True Static IP** box, type the end IP address of the IP range.
- In the **Start Port** box, type the start port number of the port range. If you only want to specify one port, use the same number as in the **End Port** box.
- In the **End Port** box, type the end port number of the port range.
- If you don't want to type in any of the IP address boxes then click on **Connected Device** tab, select the connected device for which you want to set the rule and Click **Add**.



7. Click **SAVE**.
8. Your service is now listed in the **Port Management** table.

6.1.5 Remote Management

Introduction

Remote management allows the gateway to be accessed remotely by a customer account representative to perform troubleshooting or maintenance. This can be used via HTTP and HTTPS.

Procedure

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *"Accessing the Admin Tool"*.
2. On the **Advanced** menu, click **Remote Management**.
3. The **Remote Management** page appears.

In the **Enable Remote Management**, click **Enable** for HTTP, click **OK** on the pop up window. It will display both IPv4 and IPv6 address which will be used to access the device remotely.

4. Select the Remote management Access from the list. The **Remote Access Allowed From** appears:

5. Select **Single Computer**.



- In the **Server IPv4 Address** box, type the IP address of the computer from which you want to access the gateway.
 - In the **Server IPv6 Address** box, type the IP address of the computer from which you want to access the gateway.
6. Select **Range Of IPs**.
 - In the **Start IPv4 Address** box, type the start IP address of the range from which you want to access the gateway.
 - In the **End IPv4 Address** box, type the end IP address of the range from which you want to access the gateway.
 - In the **Start IPv6 Address** box, type the start IP address of the range from which you want to access the gateway.
 - In the **End IPv6 Address** box, type the end IP address of the range from which you want to access the gateway.
 7. Select **Any Computer**. This option will allow any computer to access your network.

6.1.6 Configure a DMZ Host

Introduction

The Gateway allows you to configure one local device as a De-Militarized Zone (DMZ) host. This means that:

- None of the Gateway firewall rules will be applied to this device.
- All traffic originating from the Internet will be forwarded to this device unless there is a port forwarding rule defined for this type of traffic. Port forwarding rules always have higher priority.

Use a reserved IP address for the DMZ host

Make sure that your DMZ host uses a fixed IP address. If not, the device might get a new IP address after some time through DHCP and the port forwarding rule will no longer be applied to the device and another device may suddenly be acting as DMZ host. For more information, see *6.2 Assigning a reserved IP to a device*.

How to configure a device as DMZ host

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *“Accessing the Admin Tool”*.
2. On the Advanced menu, click DMZ.
3. The DMZ page appears:

Complete the following fields:

- In the **Enable DMZ** list, click **Enabled**.
 - In the **DMZ v4 Host** box, type the IP address of the device.
 - In the **DMZ v6 Host** box, type the IP address of the device.
4. Click **SAVE**.

6.1.7 NAT

Introduction

NAT manages 1-to-1 Network Address Translation.



Procedure

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to you Gateway (either wired or wirelessly). For more information, see *“Accessing the Admin Tool”*.
2. On the Advanced menu, click NAT.
3. The NAT page appears.

☐ Disable All

#	Public IP Address	Private IP Address	Enable
No entries!			

+ ADD NEW

In the **NAT**, uncheck the **Disable All**; click **OK** on the pop up window

4. Click +ADD NEW
5. The Add NAT page appears:

Advanced > NAT > Add Network Address Translation

Add a rule for 1-to-1 Network Address Translation.

Add Network Address Translation	
Public IP Address:	
Private IP Address:	
SAVE CANCEL	

6. In the Public IP Address box, type the IP address of the computer for which you want to add the rule for 1-to-1 NAT.
7. In the Private IP Address box, type the IP address of the computer for which you want to add the rule for 1-to-1 NAT.
8. Click SAVE.
9. Your service is now listed in the NAT table.

6.1.8 Static Routing

Introduction

Static Routes allow the users to manually add static routes to create specific paths to the destined networks.

Procedure

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *“Accessing the Admin Tool”*.
2. On the **Advanced** menu, click **Static Routing**.
3. The **Static Routing** page appears.

Static Routing				
Static Routing Entry				
Name				
Destination Subnet				
Subnet Mask				
Gateway IP				
ADD				
Static Routing Table				
Name	Destination Subnet	Subnet Mask	Gateway IP	Active

Complete the following fields:

- In the **Name** box, type a name.



- In the **Destination Subnet** box, type destination subnet. (example – 192.168.4.20)
 - In the **Subnet Mask** box, type the subnet mask (example – 255.255.255.0)
 - In the **Gateway IP** box, type the IP address of the gateway.
4. Click ADD.
 5. Your service is now listed in the Static Routing table.

6.1.9 Dynamic DNS

Introduction

Configures the Gateway's router functionality as a Dynamic DNS client.

Procedure

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *"Accessing the Admin Tool"*.
2. On the Advanced menu, click Dynamic DNS.
3. The Dynamic DNS page appears.

In the **Dynamic DNS** list, click **Enabled**. In the **Dynamic DNS** table, click **+ADD DDNS**.

4. The **Add DDNS** page appears:

Complete the following fields:

- In the **Service Provider** list, select your service provider.
 - In the **User Name** box, type username of the gateway.
 - In the **Password** box, type the password of the gateway.
 - In the **Host Name** box, type the host name.
5. Click ADD.
 6. Click Save Settings.
 7. Your service is now listed in the Dynamic DNS table.



6.2 Assigning a reserved IP to a device

Introduction

By default, each device will get an IP address from the Gateway's DHCP server. When a device leaves, is turned off or the lease time of the address has expired, the IP address becomes available and can be re-used for other devices.

When you want to run a service on a network device (for example, a web server, network printer, etc.), it is advised to assign a reserved IP to the device. This way, the device will always be reachable on the same address and there is no risk that you are accessing the wrong device.

How to assign a reserved IP

Proceed as follows:

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *"Accessing the Admin Tool"*.
2. On the left menu, click **Connected Devices**.
3. The **Devices** page appears.
 - If your device is already listed in one of the tables, proceed as follows:
 - o Click **Edit**.
 - o The **Edit Device** page appears.

Connected Devices > Devices > Edit Device

Change the IP address assignment method for Online Devices. [more](#)

Edit Device

Host Name: durgeshn

Connection: Ethernet

Configuration: ☐ DHCP ☒ **Reserved IP**

MAC Address: 48:4D:7E:D6:03:33

Reserved IP Address:

Comments:

- o In the **Configuration** list, click **Reserved IP**.
- o If needed, change the value in the **Reserved IP Address** box **3**.
- If your device is not listed, proceed as follows:
 - o On the **Device**, click **ADD DEVICE WITH RESERVED IP**.
 - o The **Add Device** page appears.

Connected Devices > Devices > Add Device

Connect a Device using a Reserved IP address. [more](#)

Add Device with Reserved IP Address

Host Name:

MAC Address:

Reserved IP Address:

Comments:

- o Enter the settings of your choice.

4. Click **Save**.



7 Support

Introduction

This chapter suggests solutions for issues that you may encounter while installing, configuring or using your Gateway. If the suggestions do not resolve the problem, look at the support pages on www.technicolor.com or contact your service provider.

Topics

This chapter describes the following topics:

Topic	Page
7.1 Wireless Connection Troubleshooting	58
7.2 Network Diagnostic Tools	60
7.3 Gateway Reset and restore Options	60

7.1 Wireless connection troubleshooting

No wireless connectivity

Try the following:

- Make sure that the wireless client is enabled (message like “radio on”).
- Make sure that the wireless client is configured with the correct wireless settings (Network Name, security settings).
- If the signal is low or not available, try to reposition the Gateway.
- Make sure that the wireless client supports the wireless band, protocol and the selected wireless security that are currently used by the access point.
- *Change the wireless channel.*
- Make sure that the access point is enabled.

For more information, see *“Make sure that the wireless access point is enabled”*.

Poor wireless connectivity or range

Try the following:

- Check the signal strength, indicated by the wireless client manager. If the signal is low, try to reposition the Gateway.
- If you are connected to the 5 GHz access point, try connecting to the 2.4 GHz access point instead.
- *Change the wireless channel.*
- Use **WPAWPA2-PSK (TKIP/AES)** as encryption.

For more information, see *“4.1 How to configure the wireless settings”*.

Change the wireless channel

Proceed as follows:

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *“Accessing the Admin Tool”*.
2. Under Gateway, click Connection and then click WiFi.
3. The WiFi page appears. Click the EDIT button next to the access point that you want to modify.
4. The Edit page appears.



Private Wi-Fi Network Configuration (2.4 GHz)

Wireless Network:

Enable

Disable

Network Name (SSID):

CBCI-3036-2.4

Mode:

802.11 g/n

Security Mode:

WPA2-PSK (AES)

Please note 802.11 n mode only compatible with AES and None encryption!!

Channel Selection:

☒ Automatic
☐ Manual

Channel:

1

Channel Bandwidth:

☒ 20
☐ 20/40

Network Password:

.....

WPA requires an 8-63 ASCII character password.

Show Network Password:

☐

Broadcast Network Name (SSID):

☒ Enabled

SAVE SETTINGS

5. In the **Channel Selection** list, click **Manual**.
6. In the **Channel** list, click on one of the channels.
7. Click **SAVE SETTINGS**.

Make sure that the wireless access point is enabled

Proceed as follows:

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *"Accessing the Admin Tool"*.
2. Under **Gateway**, click **Connection** and then click **WiFi**.
3. The **WiFi** page appears. Click the **EDIT** button next to the access point that you want to modify.
4. The **Edit** page appears.

Private Wi-Fi Network Configuration (2.4 GHz)

Wireless Network:

Enable

Disable

Network Name (SSID):

CBCI-3036-2.4

Mode:

802.11 g/n

Security Mode:

WPA2-PSK (AES)

Please note 802.11 n mode only compatible with AES and None encryption!!

Channel Selection:

☒ Automatic
☐ Manual

Channel:

1

Channel Bandwidth:

☒ 20
☐ 20/40

Network Password:

.....

WPA requires an 8-63 ASCII character password.

Show Network Password:

☐

Broadcast Network Name (SSID):

☒ Enabled

SAVE SETTINGS

5. In the **Wireless Network** list, click **Enabled**.
6. Click **SAVE SETTINGS**.

Cannot connect via WPS



If you are having trouble connecting your wireless client via WPS, try to configure it manually. For more information, see “2.4.2 How to manually connect your wireless client”.

7.2 Network diagnostic tools

Introduction

The Admin Tool offers a number of diagnostic tools to test your network connectivity.

How to access the network diagnostic tools

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see “*Accessing the Admin Tool*”.
2. On the **Troubleshooting** menu, click **Diagnostic Tools**.
3. The **Network Diagnostic Tools** page appears. The following tools are available:
 - Test Connectivity Results
 - Check for IPv4 Address Results
 - Check for IPv6 Address Results

7.3 Gateway reset and restore options

Reset

By performing a **reset**, you will restart a specific set of services (or the complete Gateway).

Restore

By performing a **restore** you will reset a specific set of services (or the complete Gateway) **and** reapply their factory default settings.



A reset to factory default settings deletes all configuration changes you made. Therefore, after the reset a reconfiguration of your Gateway or a restore of a previously saved configuration (see “*Restoring a previously saved configuration*”) will be needed.

Also, your wireless clients will have to be re-associated, as described in “2.4 Connect your wireless devices”.

Methods

You can choose between:

- *Performing a reset (restart)/restore via the Admin Tool.*
With this method, you can choose to only reset (restart) or restore a specific module of the Gateway or perform a complete reset/restore of the Gateway.
- *Reset/restore the Gateway via the Reset button*
With this method, you can only perform a complete reset (restart) or restore of the Gateway.

Performing a reset (restart)/restore via the Admin Tool

Proceed as follows:

1. Go to the Admin Tool (<http://10.1.10.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see “*Accessing the Admin Tool*”.
2. On the **Troubleshooting** menu, click **Reset/Reboot Gateway**.
3. The **Reset/Reboot Gateway** page appears. Click:
 - **RESET** to restart the Gateway.
 - **RESET WIFI MODULE** to restart just the wireless module only.
 - **RESET WIFI ROUTER** to restart the wireless and router modules.
 - **RESTORE WIFI SETTINGS** to activate the Gateway default settings for wireless only. All changes to the default wireless settings will be undone.
 - **RESTORE FACTORY SETTINGS** to activate all Gateway default settings. All changes to the default settings will be undone.

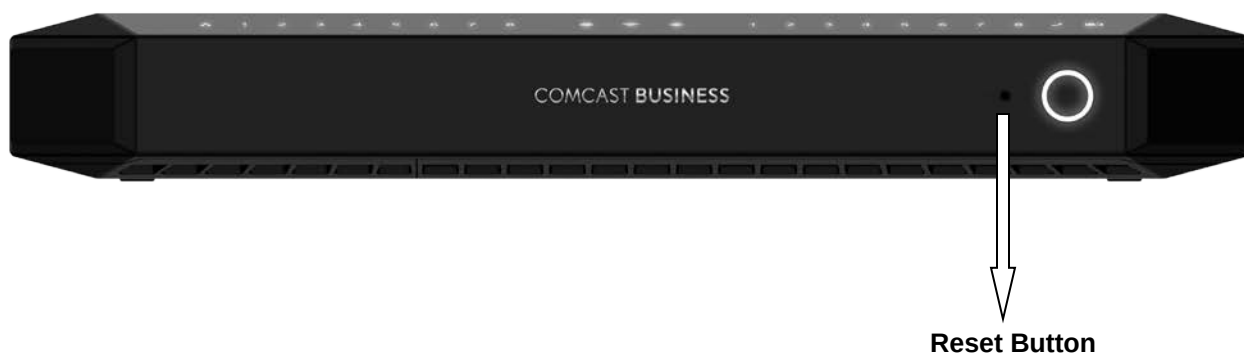


4. The Gateway prompts you to confirm your choice. Click **OK**.
5. If you selected **Restore Factory Settings**, the Gateway will restart. In all other cases, no restart is needed.

Reset/restore the Gateway via the Reset button

Proceed as follows:

1. Make sure that the Gateway is turned on.
2. If you want to:
 - Reset the Gateway, use a pen or an unfolded paperclip to push the recessed **Reset** button on the front panel of the Gateway for approximately 5 seconds and then release it.
 - Restore the factory default settings of the Gateway, use a pen or an unfolded paperclip to push the recessed **Reset** button on the front panel of the Gateway for at least 15 seconds and then release it.



3. Restart the Gateway.