



Xfinity xFi Wireless Gateway MediaAccess TC8717C User Manual

[Home](#) » [Xfinity](#) » Xfinity xFi Wireless Gateway MediaAccess TC8717C User Manual 

Contents

1	Xfinity xFi Wireless Gateway MediaAccess TC8717C User Manual
2	SAFETY INSTRUCTIONS AND REGULATORY NOTICES
3	Important safety instructions
4	RF-exposure statement
5	Restricted frequency band
6	Copyright
7	Trademarks
8	Document Information
9	About this Setup and User Guide
10	ABOUT THIS SETUP AND USER GUIDE
11	1. Getting started
11.1	1.1 Features at a glance
11.2	1.2 Getting to know the Gateway
11.3	1.3 Preparing for the installation
12	2. Setup
12.1	Setup procedure
12.2	Optional configuration
12.3	2.1 Connect the Gateway to your service provider's network
12.4	2.2 Power on the Gateway
12.5	2.3 Connect your wired devices
12.6	2.4 Connect your wireless devices
13	Troubleshooting
13.1	2.5 How to connect your phone
14	3. Admin Tool
14.1	3.1 Components
14.2	3.2 How to change the default Admin Tool password
14.3	3.3 How to backup or restore a configuration
15	4. The Gateway wireless access point
15.1	4.1 How to configure the wireless settings
15.2	4.2 How to start a WPS session via the Admin Tool
15.3	4.3 Prevent devices from accessing your wireless network
16	5. Sharing content
17	6. Internet security
17.1	6.1 Parental control
18	References
19	Related Posts

Xfinity xFi Wireless Gateway MediaAccess TC8717C User Manual



SETUP AND USER GUIDE

MediaAccess TC8717C

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.

Directive

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 overvoltages (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 mains 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, take it to a qualified service dealer.

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 that is 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 where 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 M(aximum) P(ermissible) E(xposure) 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 ©1999-2014 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

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.
- MoCA® and the MoCA logo are registered trademarks of the Multimedia over Coax Alliance.
- 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

About this Setup and User Guide

In this Setup and User Guide

The goal of this Setup and User Guide is to show you:

- 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 MediaAccess TC8717C will be referred to as Gateway in this Setup and User Guide.

Typographical conventions

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” on page 1.
- 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.

ABOUT THIS SETUP AND USER GUIDE

1. Getting started

Introduction

This chapter gives you 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.

Superior wireless performance

The integrated IEEE 802.11n 2.4 GHz 3×3 and IEEE 802.11ac 5 GHz 3×3 wireless access points are optimized for high-speed video and data transfer over wireless.

Each access point has multiple wireless transmitters and receivers. This allows it to handle multiple data streams at the same time and boost the wireless transmission rate and data stream reliability.

IPv6 Ready

Your Gateway is IPv6 ready. Internet Protocol version 6 (IPv6) is the next generation of Internet technologies aiming to effectively support the ever-expanding Internet usage and functionality, and also to address security concerns that exist in an IPv4 environment.

Internet connection features

- Broadband access via the integrated DOCSIS 3.0 (16×4) Cable Modem
- Parental control allows you to restrict access to specific websites, services or your network.

For more information, see “6.1 Parental control” on page 44.

- The Gateway has an integrated firewall to protect you from malicious attacks.

For more information, see “6.2 Firewall” on page 52.

- Advanced network tools like port forwarding, port triggering and DMZ.

For more information, see “7 Advanced configuration” on page 53.

Local networking features

- MoCA 2.0 to interconnect your local MoCA devices (for example, your set-top box) via your coax network.
- Wireless access for your local network devices via the integrated IEEE 802.11b/g/n 2.4 GHz and IEEE 802.11a/n/ac 5 GHz wireless access points. For more information, see “2.4 Connect your wireless devices” on page 19.

- Wired access for your local network devices via the Ethernet interface.
For more information, see “2.3 Connect your wired devices” on page 18.
- An integrated file and media server allowing you to share your media with media players and other network devices. For more information, see “5 Sharing content” on page 41.

Telephony features

- The Gateway offers connectivity for traditional phones and IP phones.
- The Gateway has a built-in DECT base station that allows you to connect up to five CAT-iq 2.0 compatible DECT phones.



The built-in DECT base station is only available for single line customers. Two line customers have to connect an external DECT base station to the Gateway to be able to use DECT phones.



Only CAT-iq 2.0 phones can connect to the built-in DECT base station.

Support for auto dial alarm systems

The Gateway offers support for auto dial alarm systems. When the alarm is triggered, the Gateway will terminate all calls to make the primary line available for the alarm call.



For connecting the alarm system to the Gateway, please contact your service provider for more information. This installation must be done by qualified technicians.

Battery backup (sold separately)

When the power is down the Gateway will automatically switch to the integrated rechargeable battery, if you purchased a battery.

This guarantees that the following functions will not be impacted:

- The connected phones or dial function for a connected alarm system
- The CAT-iq 2.0 phones
- All voice-related features

Easy configuration

The Admin Tool allows you to configure your Gateway and network via your web browser. For more information, see “3 Admin Tool” on page 29.

1.2 Getting to know the Gateway

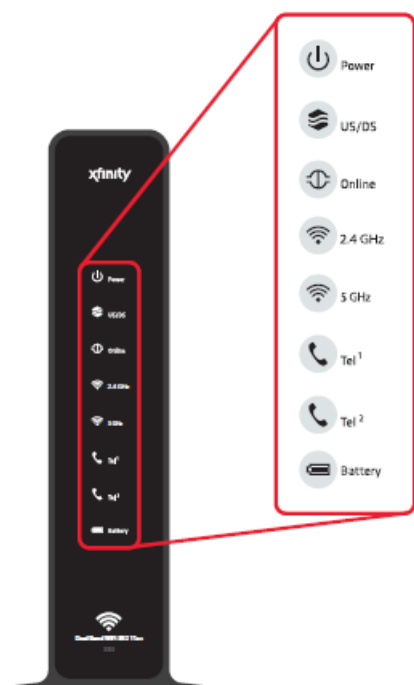
This section introduces you to the different components of the Gateway:

Topic	Page
1.2.1 Front panel	7
1.2.2 Top panel	10
1.2.3 Back panel	11
1.2.4 Bottom panel	13

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 LED

State	Description
Solid on	The Gateway is powered on from the electrical outlet.
Blinking	Power failure or running on battery.
Off	The Gateway is powered off.

US/DS LED

State	Description
Solid on	Upstream and downstream channel locked.
Blinking	Locking upstream or downstream channel.
Off	The Gateway is powered off.



Online LED

State	Description
Solid on	Connected to your service provider's network.
Blinking	Connecting to your service provider's network.
Off	Not connected to your service provider's network.



2.4 GHz LED

State	Description
Solid on	One or more wireless clients connected to the 2.4 GHz access point, no wireless activity.
Blinking	One or more wireless clients connected to the 2.4 GHz access point, wireless activity.
Off	The 2.4 GHz access point is disabled.



5 GHz LED

State	Description
Solid on	One or more wireless clients connected to the 5 GHz access point, no wireless activity.
Blinking	One or more wireless clients connected to the 5 GHz access point, wireless activity.
Off	The 5 GHz access point is disabled.



Tel1 LED

State	Description
Solid on	The telephone connected to the Tel1 port is on the hook.
Blinking	The telephone connected to the Tel1 port is off the hook or the home alarm is triggered.
Off	Voice service not provisioned.



Tel2 LED

State	Description
Solid on	The telephone connected to the Tel2port is on the hook.
Blinking	The telephone connected to the Tel2 port is off the hook or the home alarm is triggered.
Off	Voice service not provisioned.


Battery LED

State	Description
Solid on	Battery level is OK or recharging.
Blinking	If the Power LED is: < Solid on: bad battery. < Blinking: low battery.
Off	If the Power LED is: < Blinking: the battery level is OK. < Off: bad battery or no battery installed.


1.2.2 Top panel



WPS button (item A)

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” on page 20.

Page button (item B)

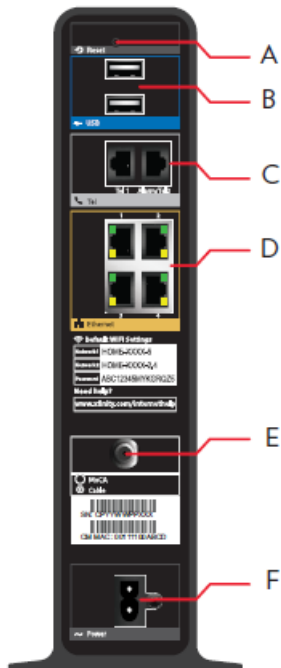
If you press the DECT pairing/paging  button:

- Briefly, the Gateway pages all connected CAT-iq 2.0 phones.
- For about 15 seconds, the Gateway switches to registration mode.

For more information, see “Connecting a CAT-iq 2.0 phone to your Gateway” on page 27.

1.2.3 Back panel

Overview



Reset button (item A)

The Reset button allows you to:

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


For more information, see “8.3 Gateway reset and restore options” on page 69.

USB ports (item B)


The USB () ports allow you to:

- Connect a USB mass storage device to share your content (for example, music, movies,...) on your local network. For more information, see “5 Sharing content” on page 41.
- Power or charge a USB device.

Tel ports (item C)

The Tel () ports allows you to connect a traditional phone or DECT base station to your 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” on page 27.

Ethernet switch (item D)

The Ethernet switch () allows you to connect an Ethernet device (for example, a computer) to your local network. For more information, see “2.3 Connect your wired devices” on page 18. All Ethernet ports on the Gateway are Gigabit Ethernet ports and have a maximum speed of 1 Gbps (Gigabit per second).

Each Ethernet port has two LEDs:.

LED	LED status	Description
Top LED (Green)	Solid on	Connected to a Gigabit Ethernet device.
	Blinking	Connected to a Gigabit Ethernet device and sending/receiving data.
	Off	Not connected to a Gigabit Ethernet device.
Bottom LED (Amber)	Solid on	Connected to a 100Mbps/10Mbps device.
	Blinking	Connected to a 100Mbps/10Mbps device and sending/receiving data.
	Off	Not connected to a 100Mbps/10Mbps device.

MoCA/Cable port (item E)

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

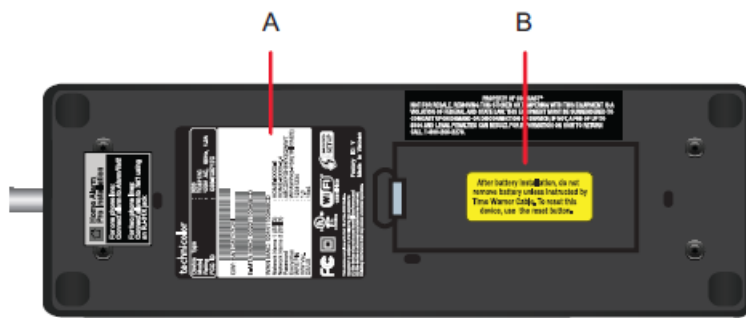
The MoCA LED indicates the status of the MoCA interface:

State	Description
Solid on	The MoCA interface is enabled, no MoCA activity.
Blinking	The MoCA interface is enabled, MoCA activity.
Off	The MoCA interface is disabled or the Gateway is powered off.

Power inlet (item F)

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

1.2.4 Bottom panel



Product label (item A)

The label on the bottom of the Gateway contains information about your Gateway, like:

- Device information
- Wireless security settings



For the network name, two values are available:

- Network Name 1 (SSID) is the network name of the 5 GHz access point and is of the following format:
HOME-XXXX-5 (where X is an alphanumeric character).
 - Network Name 2 (SSID) is the network name for the 2.4 GHz access point and is of the following format:
HOME-XXXX-2.4 (where X is an alphanumeric character).
- The other values are common for both access points.

Battery compartment (item B, optional)

During a power failure the Gateway can automatically switch to the auxiliary emergency power via the rechargeable battery (if installed). This is to guarantee that the following services are not interrupted during power failure:

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



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

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” on page 15.

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” on page 16.

2. Power on the Gateway.

For more information, see “2.2 Power on the Gateway” on page 17.

3. Connect your wired devices to the Gateway.

For more information, see “2.3 Connect your wired devices” on page 18.

4. Connect your wireless devices to the Gateway.

For more information, see “2.4 Connect your wireless devices” on page 19.

5. Connect your phones.

For more information, see “2.5 How to connect your phone” on page 27.

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” on page 29.

2.1 Connect the Gateway to your service provider’s network

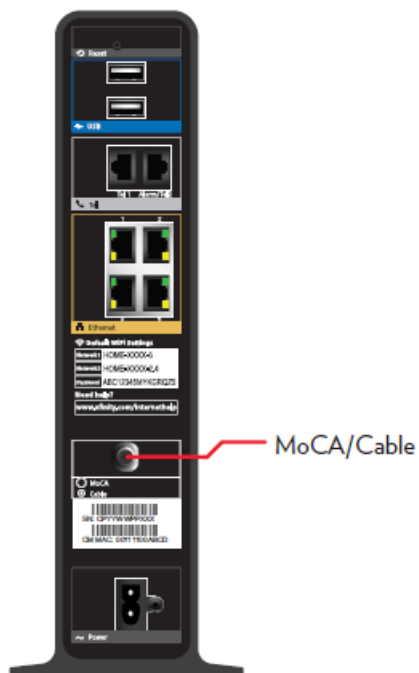
Introduction

This section helps you to 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 MoCA/Cable port of the Gateway.

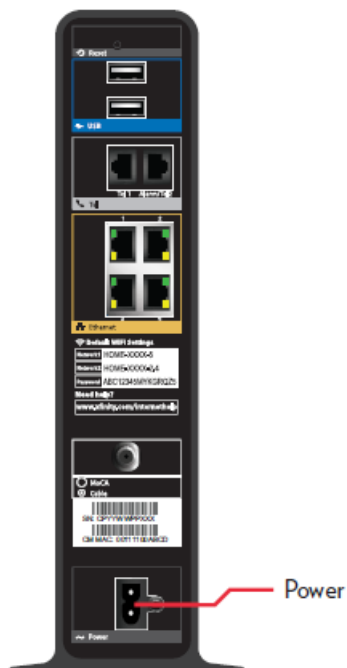


2.2 Power on the Gateway

Procedure

Proceed as follows:

1. Take 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 start up phase.

2.3 Connect your wired devices

Requirements

- Both your network device (for example, a computer, a gaming console, 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. Take the yellow Ethernet cable that is included in your box.
2. Plug one end of the Ethernet cable into one of the yellow 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 your other Ethernet devices (computers, network printers and so on).

2.4 Connect your wireless devices

Introduction

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

- The 5 GHz (3×3) IEEE 802.11ac access point offers superior transfer rates, is less sensitive to interference and allows you to connect IEEE802.11a/n/ac wireless clients.
- The 2.4 GHz (3×3) IEEE 802.11n access point allows you to connect IEEE802.11b/g/n wireless clients. Use this access point for wireless clients that don't 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:

- Via WPS, proceed with “2.4.1 How to connect your wireless client via WPS” on page 20.
- By manually entering the settings, proceed with “2.4.2 How to manually connect your wireless client” on page 22.

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 point of your Gateway support WPS.

Requirements

- Your wireless client must support WPS. Check the documentation of your wireless client for this.



Windows 8, Windows 7 and Windows Vista Service Pack 1 have native WPS support.

- 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):

You have to put both the wireless client and the Gateway in registration mode by pushing a hardware or software button.

- PIN code entry on the wireless client:

You have to 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” on page 38.

- PIN code entry on the Gateway:

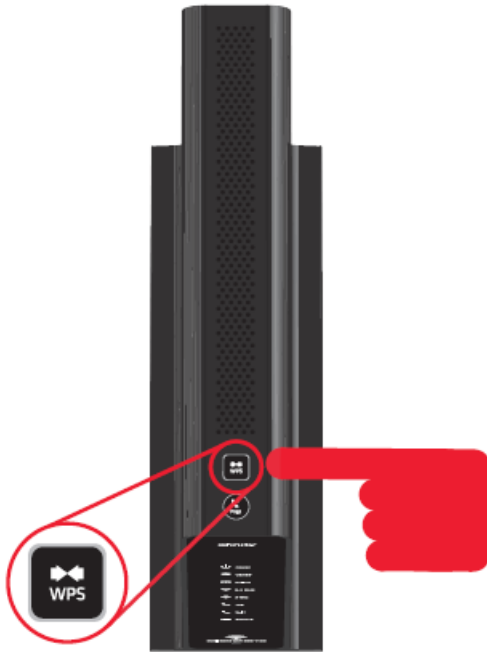
You have to enter the wireless client's WPS PIN code on the Admin Tool. For more information, see “Adding a

wireless client using WPS PIN entry on the Gateway” on page 39.

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 starts 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.
5. Your wireless client prompts you that it is now 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 can not be correctly executed:**

Configure your wireless manually. For more information, see “2.4.2 How to manually connect your wireless client” on page 22.

- **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

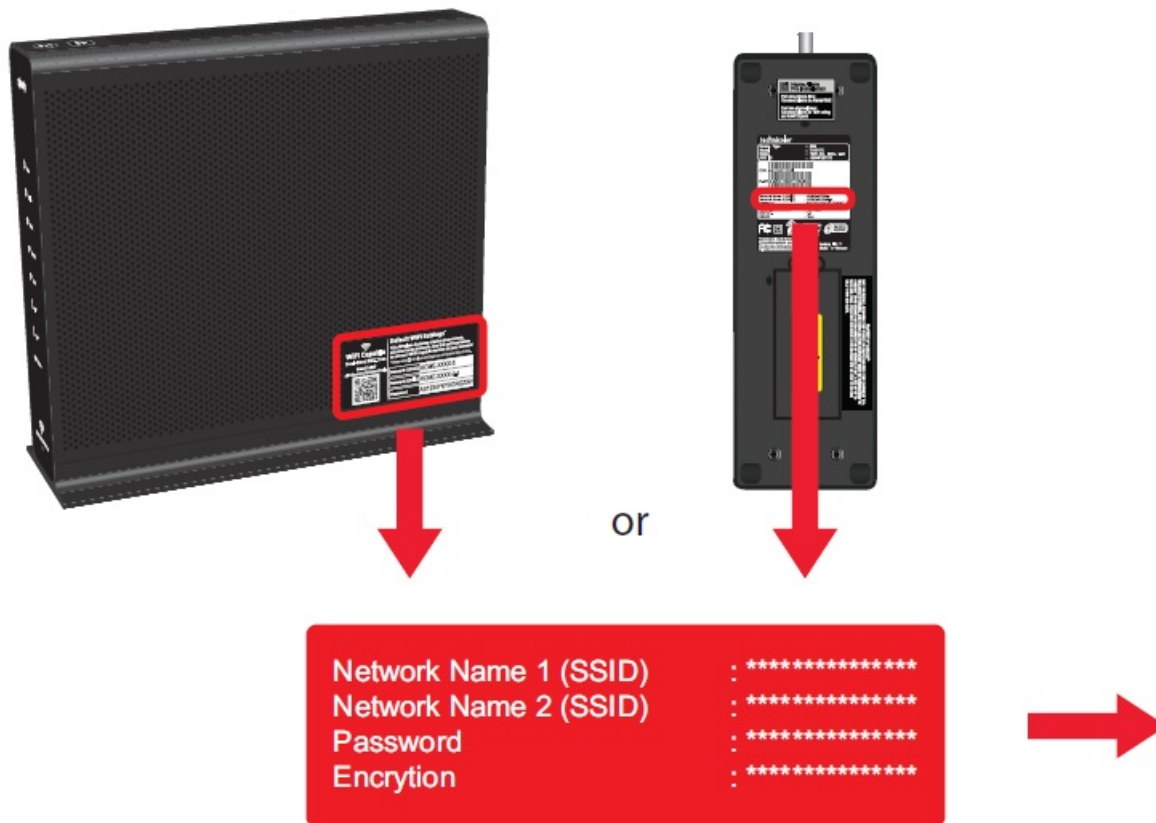
Requirements

- Your network device must be equipped with a Wi-Fi 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 side or back panel label.



For the network name, two values are available:


- Network Name 1 (SSID) is the network name of the 5 GHz access point and is of the following format: HOME-XXXX-5 (where X is an alphanumeric character).
- Network Name 2 (SSID) is the network name for the 2.4 GHz access point and is of the following format: HOME-XXXX-2.4 (where X is an alphanumeric character).

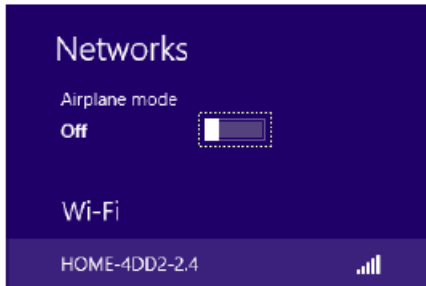
The other values are common for both access points.

To configure these settings on:

- Windows 8, proceed with “How to connect your computer on Windows 8” on page 23.
- Windows 7, proceed with “How to connect your computer on Windows 7” on page 23.
- Windows Vista, proceed with “How to connect your computer on Windows Vista” on page 24.
- Windows XP, proceed with “How to connect your computer on Windows XP” on page 25.
- Mac OS X, proceed with “How to connect your computer on Mac OS X” on page 26.
- On another operating system, consult the help of your wireless client or operating system.

How to connect your computer on Windows 8

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

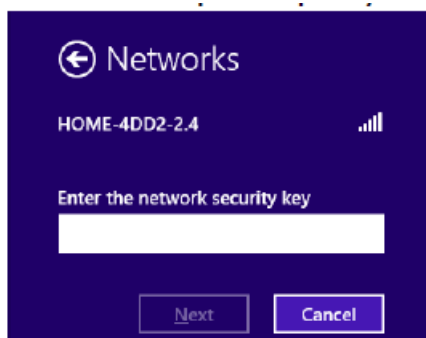


Double-click the Gateway access point.



The Gateway is listed with the Network Name 1 and/or Network Name 2 which is printed on the Gateway's side or back panel label. For more information, see "Product label (item A)" on page 13.

3. Windows prompts you to enter the security key.




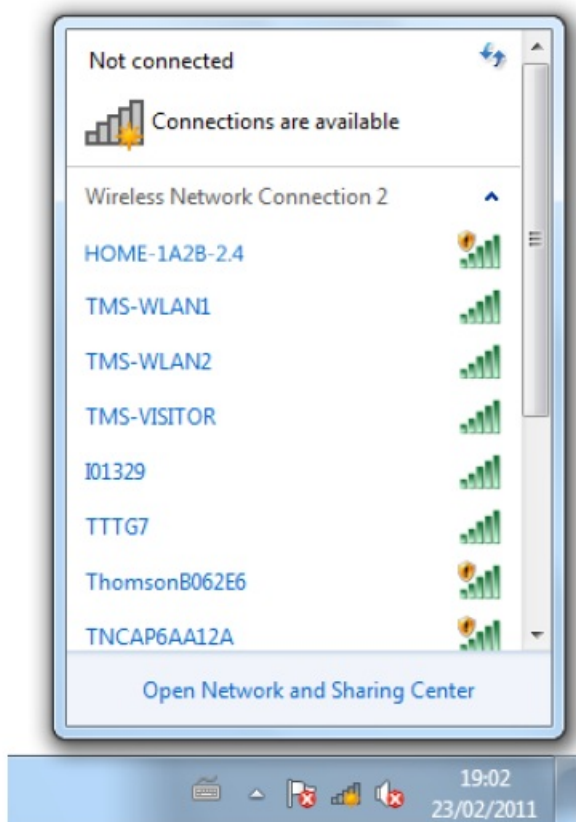
Type the Password which is printed on the Gateway's side or back panel label in the Enter the network security key box and click Next.

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.

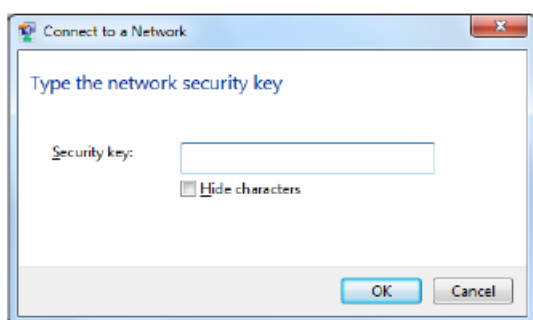


Double-click the Gateway access point.



The Gateway is listed with the Network Name 1 and/or Network Name 2 which is printed on the Gateway's side or back panel label. For more information, see "Product label (item A)" on page 13.

3. Windows prompts you to enter the security key.



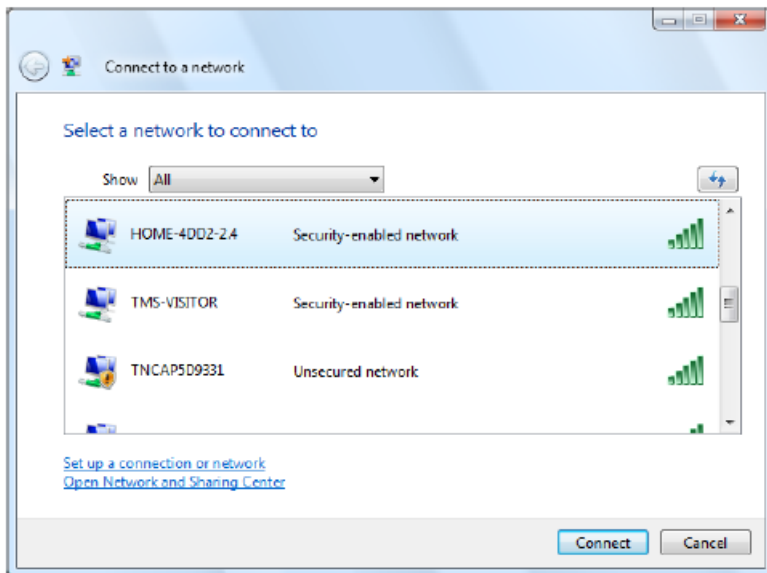
Type the Password which is printed on the Gateway's side or back panel label in the Security key and click OK.

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.

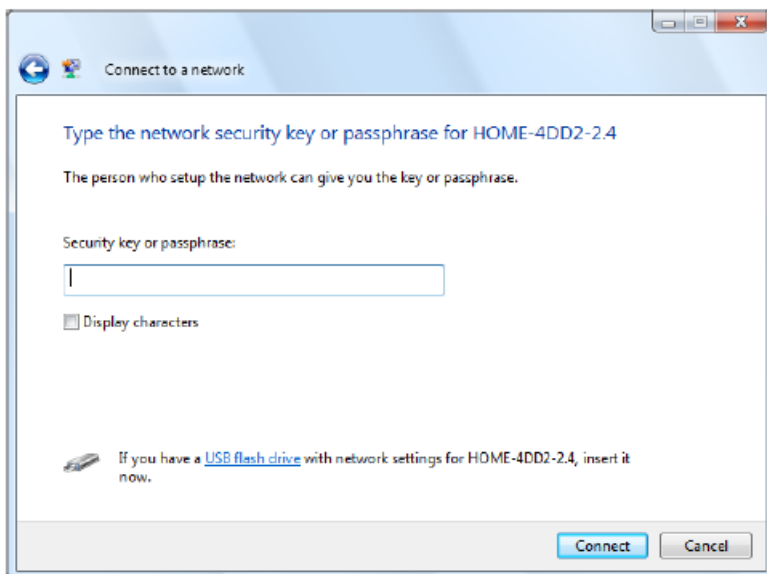


3. Double-click the Gateway access point.



The Gateway is listed with the Network Name 1 and/or Network Name 2 which is printed on the Gateway's side or back panel label. For more information, see "Product label (item A)" on page 13.



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



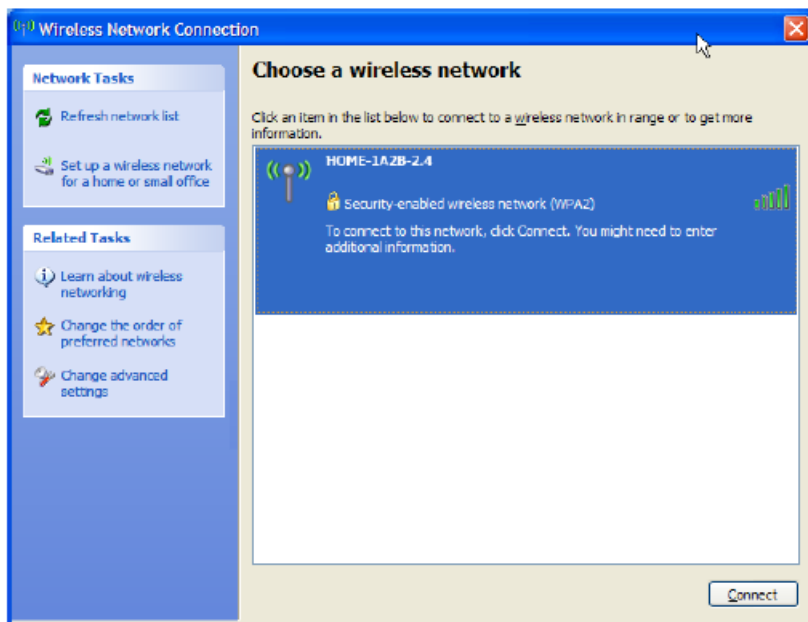
Type the Password which is printed on the Gateway's side or back panel label in the Security key or passphrase box and click Connect.

How to connect your computer on Windows XP

Proceed as follows:

1. Right-click the wireless network connection icon ( or ) in the notification area and then click View Available Wireless Networks.

2. A list of available wireless networks appears.

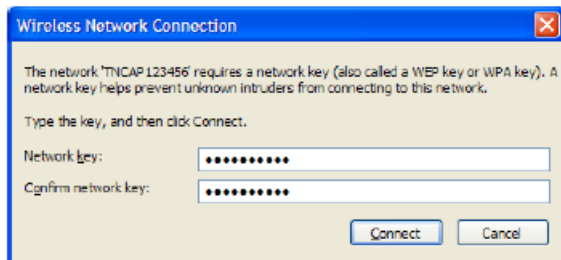


Double-click the Gateway access point..



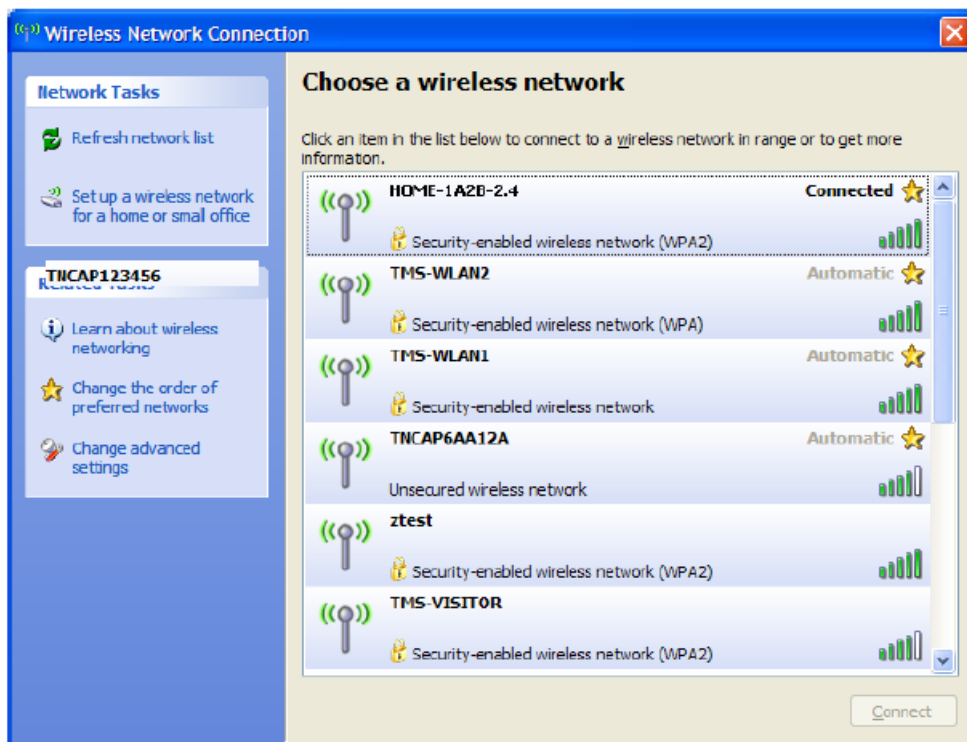
The Gateway is listed with the Network Name 1 and/or Network Name 2 which is printed on the Gateway's side or back panel label. For more information, see "Product label (item A)" on page 13.

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



Type the Password which is printed on the Gateway's side or back panel label in the Network key and Confirm network key box and click Connect.

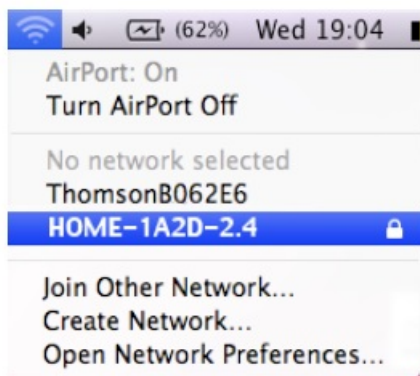
4. You are now connected to the Gateway:



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.

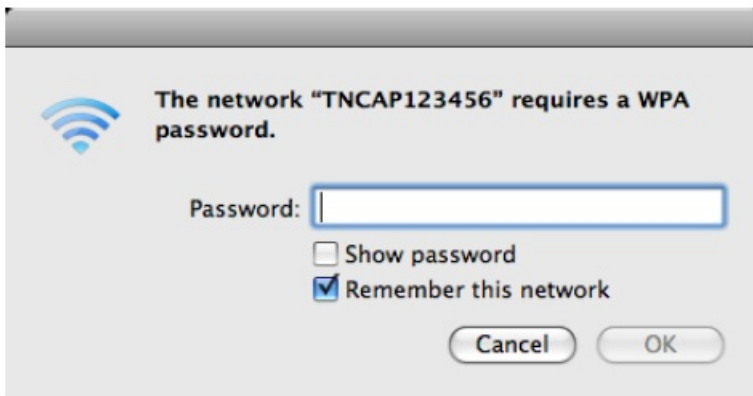


Select the Gateway from the list.



The Gateway is listed with the Network Name 1 and/or Network Name 2 which is printed on the Gateway's side or back panel label. For more information, see "Product label (item A)" on page 13.

3. The WiFi window prompts you to enter your WPA password.



In the Password box, type the Password which is printed on the Gateway's side or back 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 described how to connect the phones for single line customers.

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

Procedure

To set up your telephone network, follow these steps:

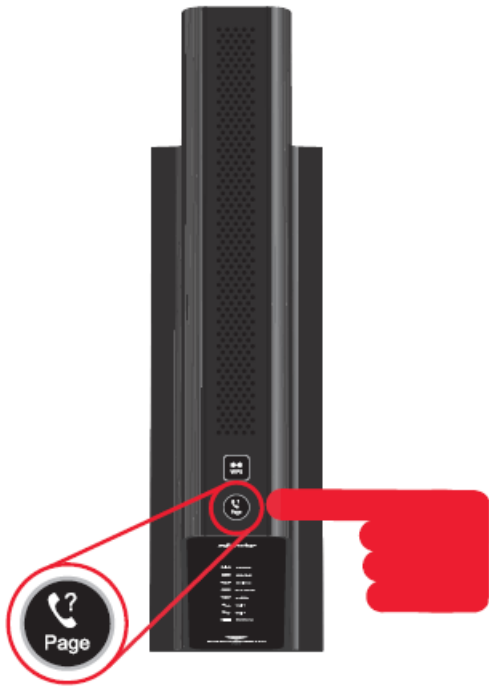
1. Connect your CAT-iq 2.0 compatible DECT phones to the built-in DECT base station.
For more information, see "Connecting a CAT-iq 2.0 phone to your Gateway" on page 27.
2. Connect your traditional phone, external DECT base station or fax to the Tel1 port on the back panel of your Gateway.

Connecting a CAT-iq 2.0 phone to your Gateway

The Gateway is equipped with a DECT base station allowing you to connect up to five DECT phones. Any CAT-iq 2.0 certified DECT phone is able to connect.

Before you can start using your CAT-iq 2.0 phone, you first have to pair it with your Gateway. Proceed as follows:

1. On the top panel of the Gateway, press and hold the Page button until the button LED starts flashing (this will take approximately 15 seconds).



2. Put your CAT-iq 2.0 phone in pairing mode.

Consult your CAT-iq 2.0 phone's user documentation to register your CAT-iq 2.0 phone.

3. Your CAT-iq 2.0 phone prompts you that if the registration is successful, the message "Registered to base x" appears on the screen of your CAT-iq 2.0 phone.

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 browse to <http://10.0.0.1>, 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 "7.1.1 UPnP" on page 56.



10.0.0.1 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: admin) and password (default: password) and click OK.

Log In

Please log in to manage your router.

Username:

Password:

Xfinity.com • customerCentral • User Guide

3. The Admin Tool appears.

Hi admin • [Logout](#) • [Change Password](#)

0%
Internet
Wireless
MoCA
DECT
Low Security

Gateway
At a Glance
Connection
Firewall
Software
Hardware
Wizard
Connected Devices
Parental Control
Advanced
Troubleshooting

Gateway > At a Glance

TIP: See more information about any device. [more](#)

SAVE CURRENT CONFIGURATION
RESTORE SAVED CONFIGURATION

Home Network

- Ethernet
- WiFi
- MoCA

Firewall Security Level: Low

Connected Devices

- 10.0.0.150
- RANITESTPC
- INDYL25553N1

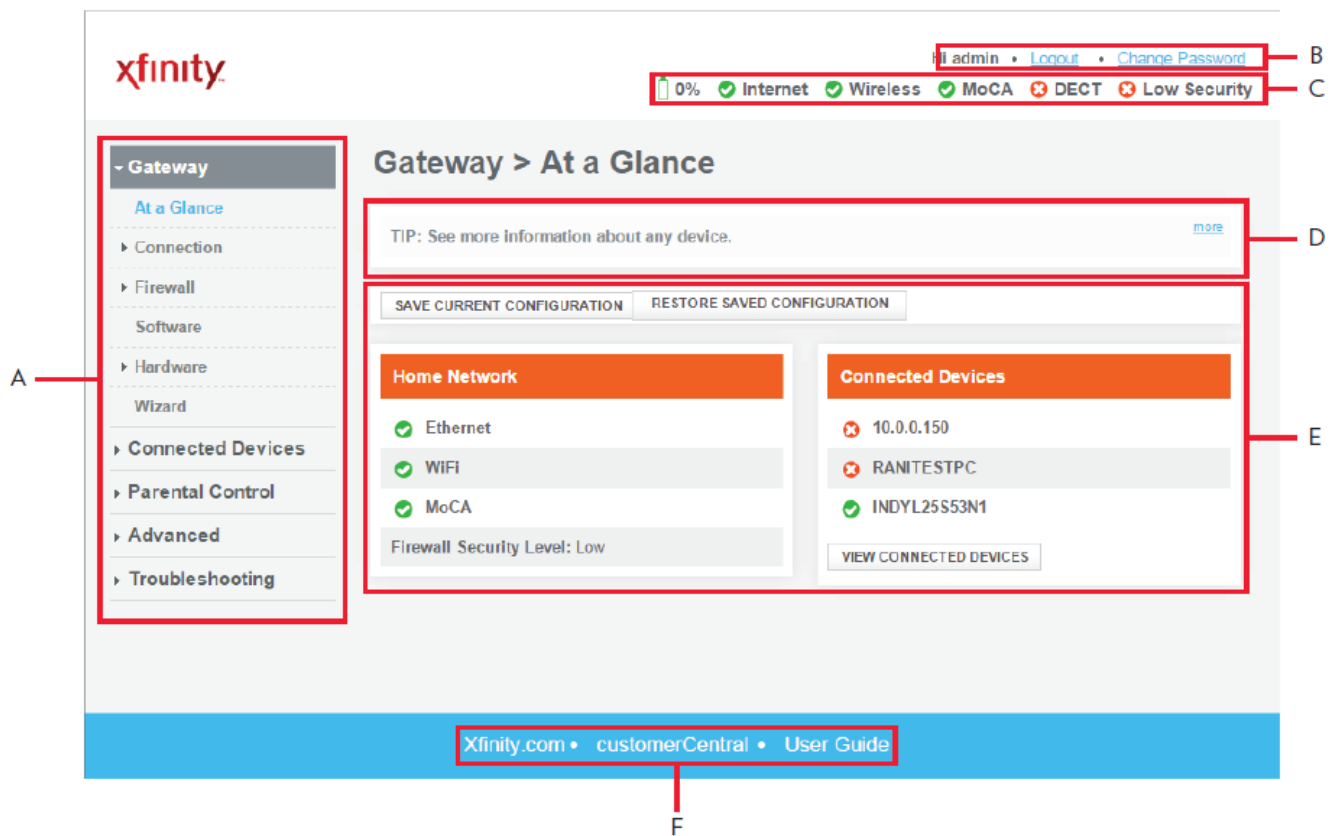
VIEW CONNECTED DEVICES

Xfinity.com • customerCentral • User Guide

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.
- **Parental Control:**
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)" on page 32.

Login section (item B)

In the login section you can see the following details:

- User Name
- Option to logout
- Option to change the Admin Tool password

Status section (item C)

The diagnostics section provides a quick overview of:

- The battery level
- The status of the Internet interface
- The status of the wireless interface
- The status of the MoCA interface
- The status of the DECT 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.

To expand the tip, click more.

Content panel (item E)

The content pane displays the actual configuration page.

Online support (item F)

The online support section provides links to the web sites where you can find additional information.

3.2 How to change the default Admin Tool password

We recommend changing the default password of the Gateway.



The default username is admin and the default password is password.

Procedure

1. Browse to the Admin Tool (<http://10.0.0.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly).
For more information, see “Accessing the Admin Tool” on page 29.
2. In the upper-right corner, click Change Password.
3. The Change Password page appears.

A screenshot of a web form titled "Password" in a blue header bar. The form contains three input fields: "Current Password:", "New Password:", and "Re-enter New Password:". At the bottom, there are two buttons: "SAVE" and "CANCEL".

Password	
Current Password:	<input type="text"/>
New Password:	<input type="text"/>
Re-enter New Password:	<input type="text"/>
<input type="button" value="SAVE"/> <input type="button" value="CANCEL"/>	

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



The default password is password.

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

Backing up your configuration

Proceed as follows:

1. Browse to the Admin Tool (<http://10.0.0.1>), using a computer or device that is currently connected to you Gateway (either wired or wirelessly).

For more information, see “Accessing the Admin Tool” on page 29.

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.

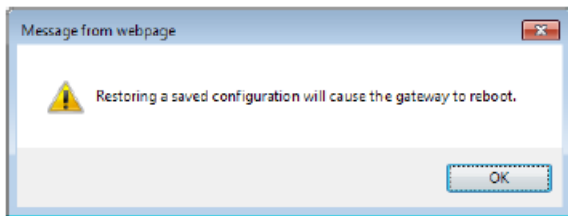
Proceed as follows:

1. Browse to the Admin Tool (<http://10.0.0.1>).

For more information, see “Accessing the Admin Tool” on page 29.

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.

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:

- A 5 GHz (3×3) IEEE 802.11ac access point that offers superior transfer rates, is less sensitive to interference and allows you to connect IEEE802.11a/n/ac wireless clients.
- A 2.4 GHz (3×3) IEEE 802.11n access point that allows you to connect IEEE802.11b/g/n wireless clients. Use this access point for wireless clients that don't 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.

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 computer if you are not sure if your computer 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” on page 20
- “2.4.2 How to manually connect your wireless client” on page 22

4.1 How to configure the wireless settings

1. Browse to the Admin Tool (<http://10.0.0.1>), using a computer or device that is currently connected to you Gateway (either wired or wirelessly).

For more information, see “Accessing the Admin Tool” on page 29.

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.

4. The Edit page appears:

Private WiFi Network Configuration (2.4 GHz)

Wireless Network: ☒ Enabled ☐ Disabled

Network Name for 2.4 GHz (SSID):

Mode:

Security Mode:

Channel Selection: ☐ Automatic ☒ Manual

Channel:

Network Password:

Show Network Password: ☒

WPA2 requires a 8-63 ASCII character or a 64 hex character password. Hex means only the following characters can be used: ABCDEF0123456789.

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).

- **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 you not to change this setting.

- **Channel:**

The channel that is currently used for your wireless communication.

- **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.

- 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. Browse to the Admin Tool (<http://10.0.0.1>), using a computer or device that is currently connected to you Gateway (either wired or wirelessly).
- For more information, see “Accessing the Admin Tool” on page 29.
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.

Add WiFi Client (WPS)

WiFi Protected Setup (WPS): **Enabled** Disabled

AP PIN: 44129941

WPS Pin Method: Enabled **Disabled**

Connection Options: Push Button ▼

To pair, select the Pair button and your wireless device will connect within two minutes. You may also press the [pair] button on this device.

PAIR **CANCEL**

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. Browse to the Admin Tool (<http://10.0.0.1>), using a computer or device that is currently connected to you Gateway (either wired or wirelessly).
- For more information, see “Accessing the Admin Tool” on page 29.
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.

Add WiFi Client (WPS)

WiFi Protected Setup (WPS): **Enabled** Disabled

AP PIN: 44129941

WPS Pin Method: Enabled **Disabled**

Connection Options: Push Button ▼

To pair, select the Pair button and your wireless device will connect within two minutes. You may also press the [pair] button on this device.

PAIR **CANCEL**

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. Browse to the Admin Tool (<http://10.0.0.1>), using a computer or device that is currently connected to you Gateway (either wired or wirelessly).
- For more information, see “Accessing the Admin Tool” on page 29.
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.

Add WiFi Client (WPS)

WiFi Protected Setup (WPS): **Enabled** Disabled

AP PIN: 44129941

WPS Pin Method: **Enabled** Disabled

Connection Options: Push Button ▼

To pair, select the Pair button and your wireless device will connect within two minutes. You may also press the [pair] button on this device.

PAIR CANCEL

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. Browse to the Admin Tool (<http://10.0.0.1>), using a computer or device that is currently connected to your Gateway (either wired or wirelessly).
For more information, see “Accessing the Admin Tool” on page 29.
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.

Mac Filter Setting

The TC8706C can allow the wireless client stations to connect to your TC8706C in any of these ways:

SSID: HOME-4DD2-2.4 ▼

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.

Device Name	MAC Address
My Neighbour	12 34 56 78 9A BC
<input type="button" value="ADD"/>	
<input type="button" value="SAVE FILTER SETTING"/>	

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

6. Click SAVE FILTER SETTING.

5. Sharing content

Introduction

The Gateway allows you to share the content on your USB storage device(s) with other devices that are connected to your local network (mostly computers).

These devices have read and write access to this USB device(s).

Features

- The Gateway has two USB 2.0 ports
- The following file systems are supported:

NTFS

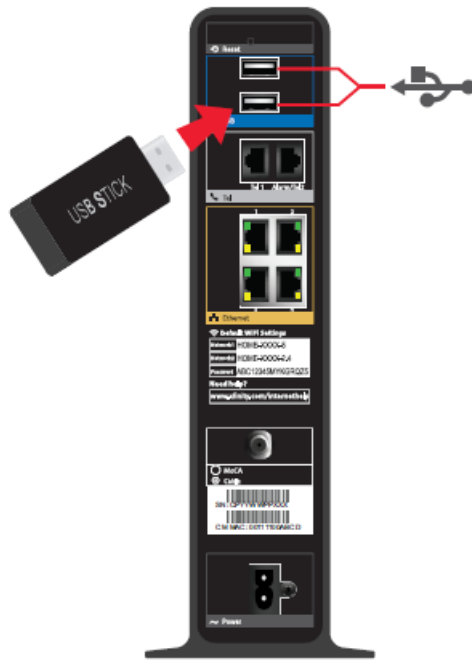
FAT32

FAT16

EXT3/EXT4

Configuration

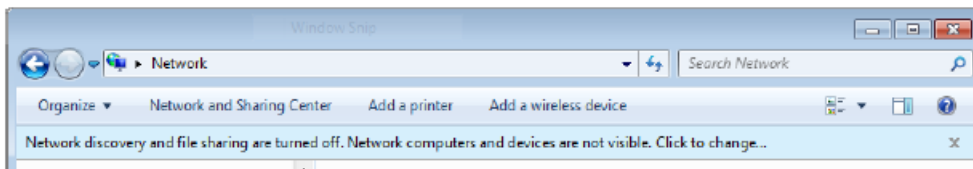
The only thing that you need to do is to plug your USB memory stick or external hard disk in (one of) the USB port(s) of your Gateway.



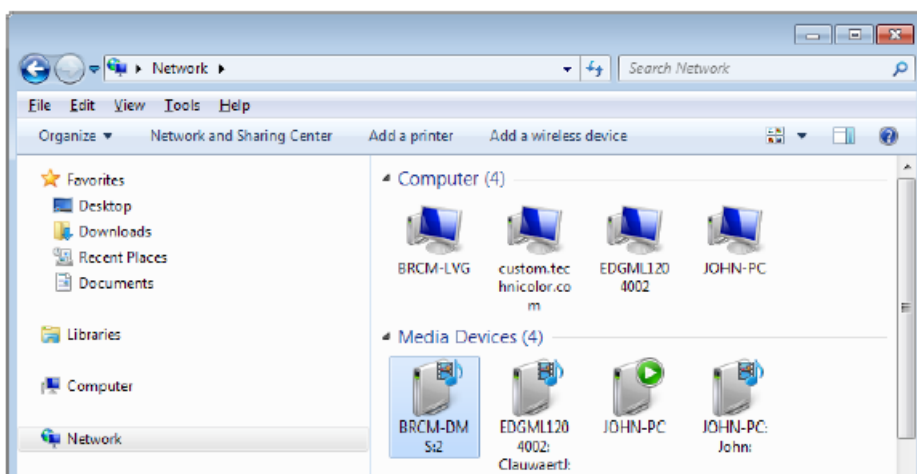
Accessing the shared content on Windows

Proceed as follows:

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.

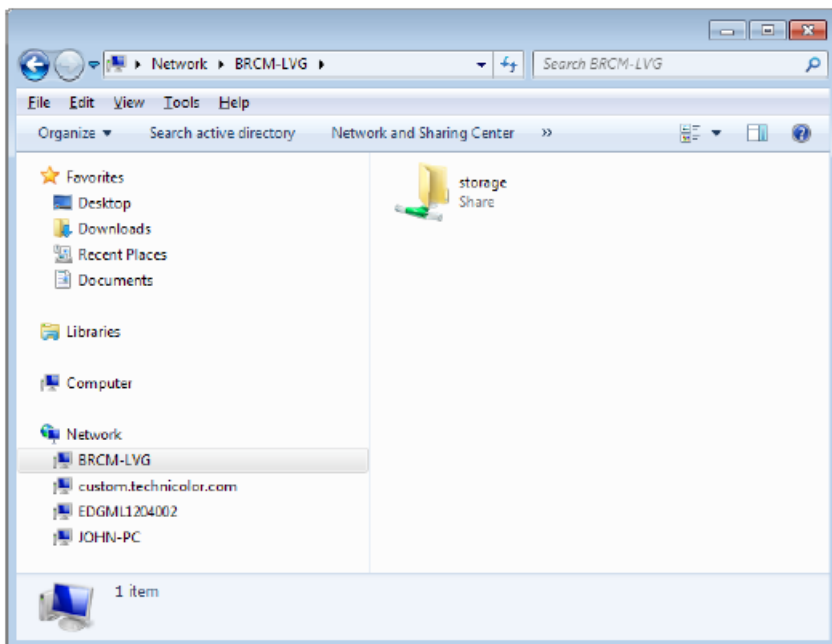


4. Explorer displays a list of detected devices.



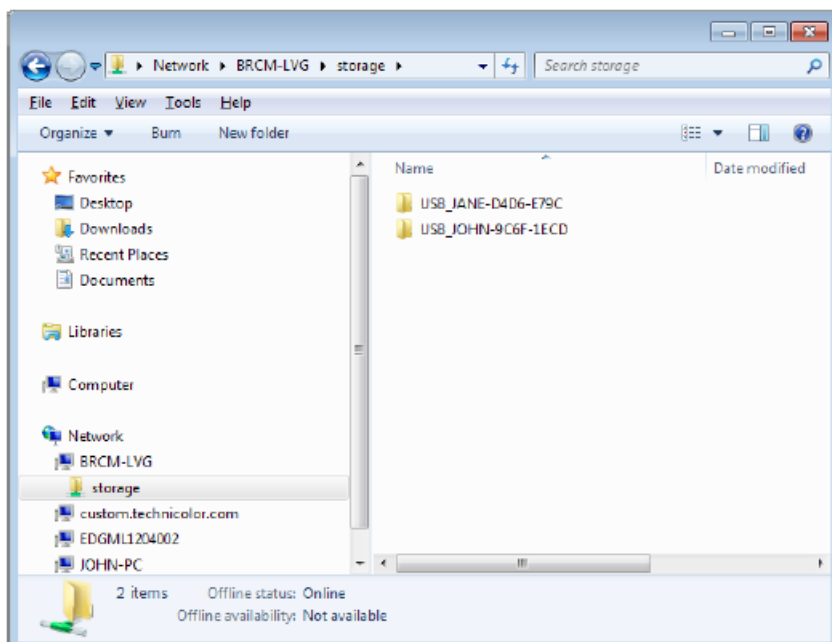
Double-click BRCM-LVG (this is the Gateway's file server).

5. The following window appears:



Double-click the storage folder.

6. Your connected USB devices are now displayed as a folders.



Double-click one of the folders to access the content files stored on the USB device.

6. Internet security

Overview

The Gateway offers various options to secure your Internet connection:

Topic	Page
6.1 Parental control	44
6.1.1 Manage sites	45
6.1.2 Manage services	47
6.1.3 Manage devices	49
6.1.4 View parental control reports	51
6.2 Firewall	52

6.1 Parental control

Introduction

The parental control function:

- Prevents access to specific website based on the URL or keywords.
For more information, see “6.1.1 Manage sites” on page 45.
- Prevents access to specific application or services (for example, FTP).
For more information, see “6.1.2 Manage services” on page 47.
- Prevents devices from accessing your network.
For more information, see “6.1.3 Manage devices” on page 49.

6.1.1 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.

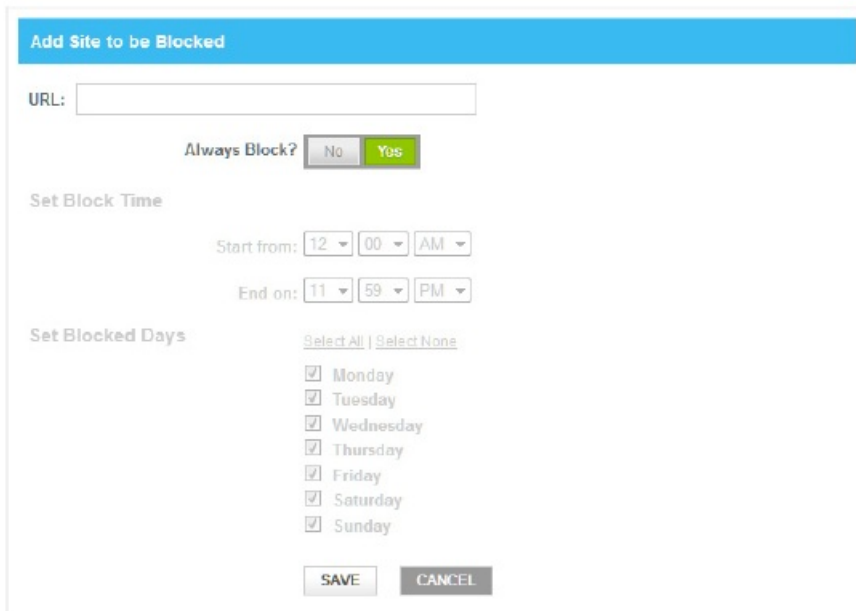
How to access the Managed Sites page

1. Browse to the Admin Tool (<http://10.0.0.1>), using a computer or device that is currently connected to you Gateway (either wired or wirelessly).
For more information, see “Accessing the Admin Tool” on page 29.
2. On the left menu, click Parental Control.
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 a web form titled "Add Site to be Blocked" with a blue header bar. Below the header, there is a text input field labeled "URL:". Underneath the URL field, there is a section labeled "Always Block?" with two buttons: "No" and "Yes". Below this is a section labeled "Set Block Time" containing two rows of time pickers. The first row is labeled "Start from:" and has dropdowns for "12", "00", and "AM". The second row is labeled "End on:" and has dropdowns for "11", "59", and "PM". Below the time pickers is a section labeled "Set Blocked Days" with links for "Select All" and "Select None". Under these links is a list of days of the week, each with a checked checkbox: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. At the bottom of the form are two buttons: "SAVE" and "CANCEL".

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).

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:
 - 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 have to 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.

6.1.2 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 computer all service rules will be ignored.

How to create a service rule

1. Browse to the Admin Tool (<http://10.0.0.1>), using a computer or device that is currently connected to you Gateway (either wired or wirelessly).

For more information, see “Accessing the Admin Tool” on page 29.

2. On Parental Control menu, click Managed Services.

3. The Managed Services page appears.

4. In the Enable Managed Services list, click Enable.



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 have to 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 have to 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.

References

- [User Manual](#)

Manuals+.