Fing

Fingbox

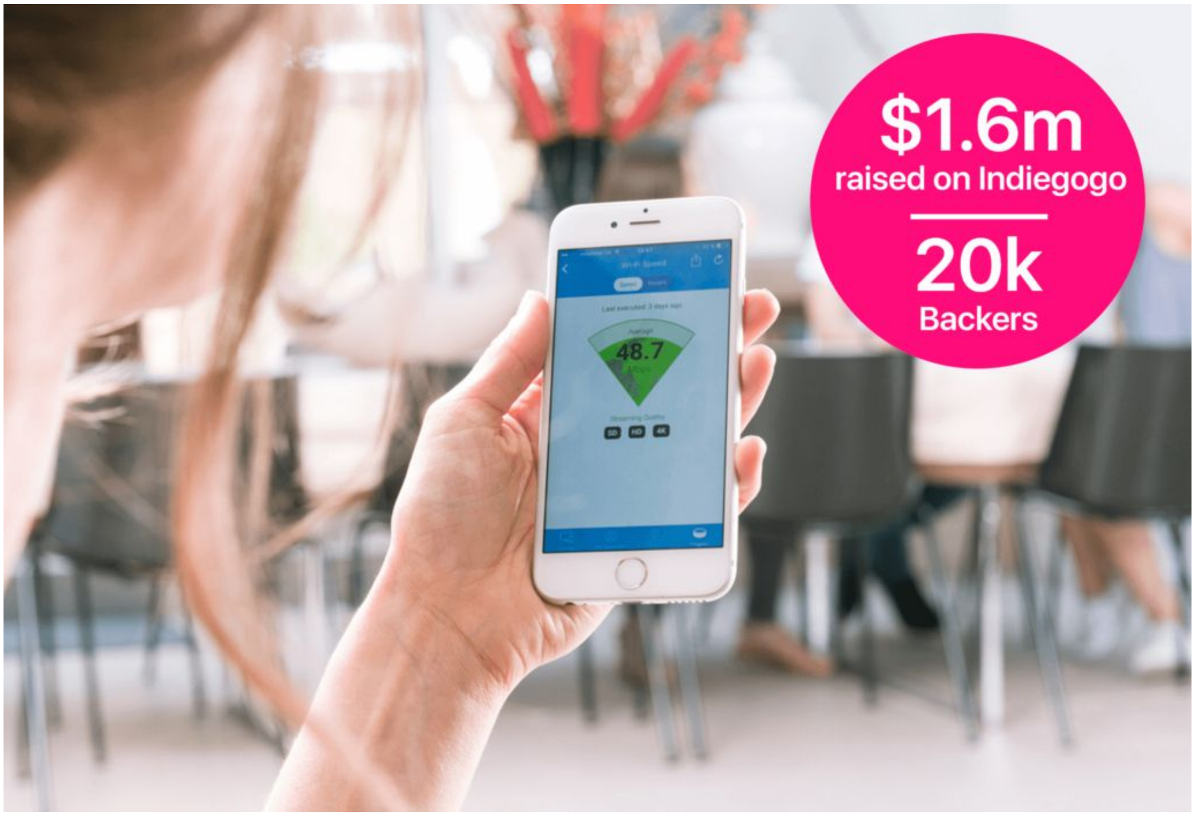
User’s Manual

Manual Version 1.4
Fing app v6.4.x
Rev.40 - November 27th, 2017

Welcome to Fingbox!

Thank you for purchasing Fingbox. With Fingbox you can see who and what is on your network, understand what to do when things slow down or don't work, limit the Internet access for your kids[1], block intruders and stay aware of network security risks.

Fingbox is the smart caretaker of your home network.

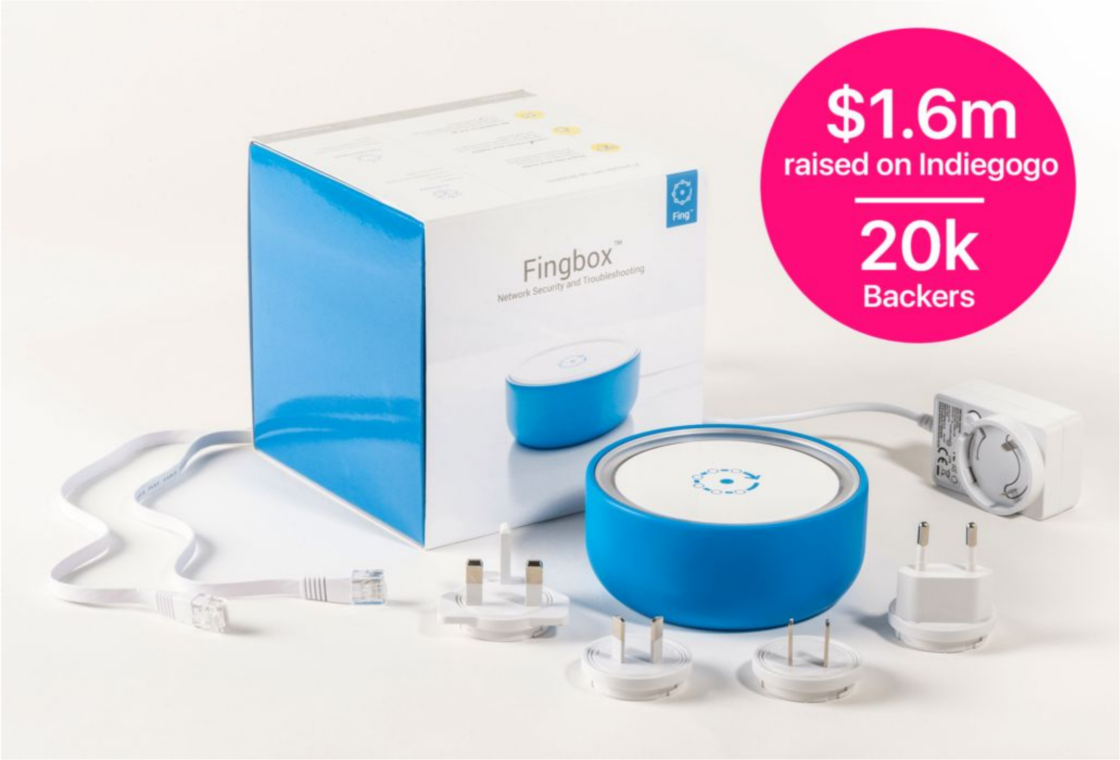


[1] Fingbox can limit Internet access only if the router allows it. With some routers the features of Internet Pause and Bandwidth Analysis may not work. Please, consult the Fing Knowledge Base for router compatibility information.

Table of Contents

Get started

Let's **activate** Fingbox using the Fing app. These are the **steps to follow**.



Unboxing and Assembling Fingbox

1. Extract the Fingbox and all the accessories from the original package.
2. Pass the included Ethernet cable through the hole in the blue case and connect it to your main router. Choose an Ethernet port labeled LAN (or sometimes INTERNAL, HOME or with a simple number). Connect the other end to the Fingbox.
3. Check that the power adapter has the right plug matching your country electrical standard. If needed, keep the button pressed while rotating and extracting the current plug. Then insert the right one until it's locked.
4. Pass the power cord through the hole in the blue case and attach it to the Fingbox micro-USB port (the small one).
5. Verify that your router is turned on and your Internet connection works well.
6. Connect the Fingbox power adapter to an electrical outlet.

7. At power-up, Fingbox top circle will show a single white/blue light for a few seconds. This means the power-up sequence has started.
8. Wait until the top circle lights becomes green. At this point Fingbox is ready for activation. If the top circle doesn't become green within 10 minutes, check the Troubleshooting section below.

Activation

1. Make sure your phone or tablet is connected to a Wi-Fi network that can reach the router where you attached the Fingbox.
2. Verify that the Fingbox top circle light is green (either steady or blinking).
3. Open the app store (Apple, Google or Amazon) and search for “Fing network”.
4. Install the Fing app
5. Open the Fing app
6. If you installed Fing for the first time, it will automatically scan your network. Wait a few seconds until it completes. The more devices you have, the longer it takes to complete a full scan. At the end of the scan, you may already see the prompt to activate the Fingbox. If you don't see the prompt, don't worry and read on.
7. At the bottom-right of the screen, tap on the Fingbox icon.
8. At the top-right of the screen, tap on the (+) icon to start searching for the Fingbox to activate. If needed, Fing will ask you to login into your Fing Account or to sign up for a new one.

Troubleshooting and Support for activation

Activation is a smooth process and it should take you no more than a few minutes. If you have problems during the activation, please check the following list of issues and solutions. If you still can't activate, send an email to our Customer Support Service: support@fing.io

I don't remember the password for my Fing Account

Password recovery is right here on the web: https://app.fing.io/recovery

The top circle light never gets green

Fingbox system is not starting up completely.

SOLUTION 1 - restart your router

Sometimes routers get stuck and don't recognize a new device. Turn off the Fingbox and your router; then turn them on in this order:

1. Power up the router
2. Wait until you can connect to the Internet again
3. Power up the Fingbox
4. Wait for the top circle to become green (up to 5 minutes)
5. Proceed with the activation

SOLUTION 2 - check the firewall configuration

Connect to your router configuration page (for example http://192.168.0.1)

Look for a section named Network Security or Firewall.

On many routers, you can find a simple setting like LOW, MEDIUM, HIGH. Fingbox cannot work on the HIGH setting. Try to set on MEDIUM or LOW, save the router settings and then power up the Fingbox to see if it gets to the green top circle.

If your router/firewall needs OUTBOUND filtering rules, set the following rules to allow Fingbox to reach the Fing services:

```
OUTBOUND - tcp/80 - to ANY Internet address
OUTBOUND - tcp/443 - to ANY Internet address
OUTBOUND - tcp/4443 - to ANY Internet address
OUTBOUND - tcp/5671 - to ANY Internet address
OUTBOUND - tcp/3001 - to ANY Internet address
OUTBOUND - tcp/3002 - to ANY Internet address
OUTBOUND - tcp/3003 - to ANY Internet address
```

The top circle light is orange

Fingbox cannot reach the Fing service on the Internet. Typically this happens because a firewall is blocking the access to Fing services.

SOLUTION - check the firewall configuration

Connect to your router configuration page (for example http://192.168.0.1)

Look for a section named Network Security or Firewall.

On many routers, you can find a simple setting like LOW, MEDIUM, HIGH. Fingbox cannot work on the HIGH setting. Try to set on MEDIUM or LOW, save the router settings and then power up the Fingbox to see if it gets to the green top circle.

If your router/firewall needs OUTBOUND filtering rules, set the following rules to allow Fingbox to reach the Fing services:

```
OUTBOUND - tcp/80 - to ANY Internet address
OUTBOUND - tcp/443 - to ANY Internet address
OUTBOUND - tcp/4443 - to ANY Internet address
OUTBOUND - tcp/5671 - to ANY Internet address
OUTBOUND - tcp/3001 - to ANY Internet address
OUTBOUND - tcp/3002 - to ANY Internet address
OUTBOUND - tcp/3003 - to ANY Internet address
```

When I try to activate, I get an “Authentication Error”

SOLUTION - delete the network from the Fing list

a. Launch the Fing app
b. At the bottom of the screen, tap on “My Networks”.
c. On the list, find the network that you’re currently connected to and then delete it with a swipe-left gesture.
d. At the bottom of the screen, tap on “Fingbox”.
e. At the top-right corner, tap on the (+) button to search for the Fingbox.
f. Follow the on-screen instructions.

When I try to activate, the app says it cannot find any Fingbox

Make sure your mobile phone (where you’re running the Fing app) is connected to a WiFi network that can reach the Fingbox (i.e. using the same router to connect to the Internet).

Login with your Fing account or sign up for a new one. To activate a Fingbox you have to be logged in before searching for a Fingbox.

When I try to activate, the app says the Fingbox has been already activated under another account

For security reason, a Fingbox is controllable only if you’re logged in with the same account used to activate the Fingbox.

Go to the account screen and login with the same account that activated the Fingbox.

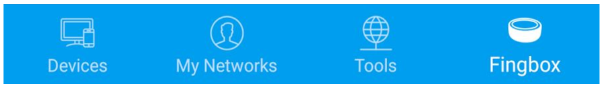
To access the account screen, go to “My Networks” and then tap on the icon in the top-right corner.

If you don’t remember which account you used to activate the Fingbox, write an email to support@fing.io specifying your name and the Fingbox MAC serial (as printed in a sticker under its white body).

Quick Tour

You can interact with Fingbox by using the Fing mobile app for smartphones and tablets as well as the website located at https://app.fing.io. Fingbox can also use the lights in its top circle to communicate some operational conditions with colors and motion patterns (look at the chapter on how to interpret the top circle lights).

The Fing mobile app has four main screens, quickly accessible from the buttons at the bottom of the screen.



Devices - shows the list of all the devices monitored by Fingbox. From this screen you can access device details and technical info about the network, sort devices in different ways and export the device list into various file formats.

Fingbox notifies you about devices when:

a new device appears on the network for the first time (enabled by default)

an existing device changes its status, e.g. online → offline and vice versa (you have to enable this alert for each device you want alerts for)

See the Devices section for detailed instructions on how to use each element on the screen.

My Networks - shows the list of all the networks belonging to your Fing account. A network can be of two types:

Unmanaged (manual scan only) - this is the *classic* Fing network, created and updated every time you run a manual scan from the Devices screen. Unmanaged networks are marked with any of the “context” icons for Home, Office, Rental, Public or Unclassified. You can delete an unmanaged network with a swipe-left gesture. All the customizations you made to devices will be lost.

Managed by Fingbox - this type of network has a Fingbox and can be managed from anywhere (locally or via Internet). Managed networks are displayed with an icon representing a small Fingbox. If you have **multiple Fingbox units** activated under your account, you’ll see them listed here. You can switch from one to another by simply tapping on the list item. If you swipe-left to **delete a managed network**, the associated **Fingbox will be deactivated** and its memory wiped out and reset to factory defaults. Because of this potential data loss, a pop-up will always ask you to confirm a deactivation.

Tools - this screen contains network tools **running locally** on your phone (not on the Fingbox). You can use them on any network, on any hostname or IP address to scan for open ports, ping, traceroute or send a Wake-on-LAN command. These tools are independent from Fingbox.

Fingbox - This is the Fingbox command center, also called the ***Dashboard***. Here you can see **who's at home now**, apply parental control by "pausing" Internet access, act on important **security warnings** and see what happened while you weren't watching. You can also find the tools to **troubleshoot your WiFi** and other network problems.

Look at the Dashboard section of this manual for a description of all its screen elements. Because this is the most important screen, we'll start right from here.

Fingbox Dashboard

The Fingbox Dashboard has multiple sections. They keep information easy to find for you.

Dashboard sections

People

At the top of the screen you can see **your family members**. A grayed out icon means they are not at home (or at least, their personal device is offline).

A small number under the face tells you **how long ago** their state changed (i.e. they left home or came back).

Tap on a face to see the **owned devices**, pause the Internet access for this person's devices or change anything about the person.

Attention required

Right under the people section, there is a recap of the global status (green or yellow shield) and how many devices are currently online. This area is where important notifications appear requiring for your immediate action. For example, when a new device is detected the notification will stay here until you take an action or simply acknowledge.

On the right there is a button to access all the past events that happened in your network.

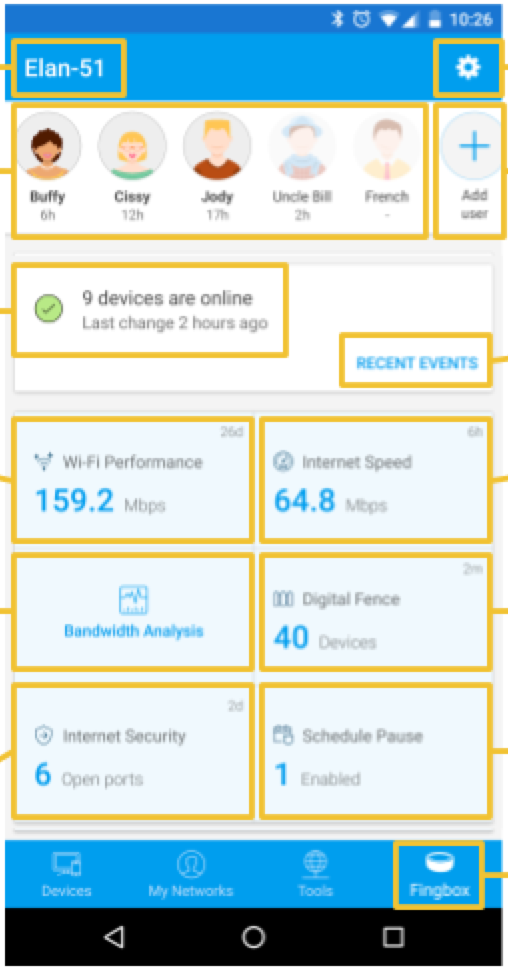
Tests and reports

In this section you have the "tiles" reporting the latest results from tools and checks such as Wi-Fi performance, Internet speed, DigitalFence, bandwidth usage analysis and Internet security. Tap on a tile to access the corresponding tool, test or report.

Paused and Blocked devices

This section appears at the bottom of the Dashboard screen, whenever a device or a person have been restricted access to the Internet (PAUSE) or to the whole network (BLOCK). Here you can quickly review the restricted devices and easily unpause or unblock them. You'll also see when an automatic schedule is active and a person is being restricted from accessing the Internet.

FINGBOX DASHBOARD



9 devices are online
Last change 2 hours ago

Name of this Fingbox

People at home or away, how long ago they left or arrived. Tap on a face to see their devices and other actions.

Recap of device status and area for important events requiring your attention (e.g. new device found).

Measure the speed of your local Wi-Fi. This tile shows the result of the last test run.

Find out who or what is slowing down your network.

Tap to see how your network is exposed to the public Internet. This tile shows how many open ports have been found and how long ago the test was performed.

Fingbox settings

Add family members, frequent visitors and even pets!

Event journal - Tap to see what happened in your network.

See how fast your service provider connects you to the "big" Internet.

See nearby devices that are not on your network but may interfere with your business.

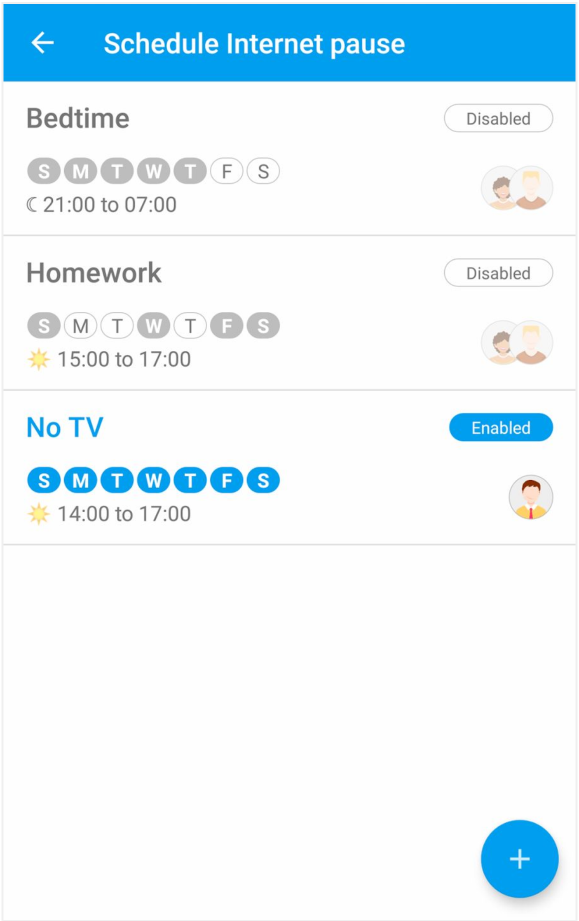
Set the automatic scheduling of Internet Pause

Tap here to get back to this screen, the Fingbox Dashboard

Scheduling Internet Pause

Instead of manually “pausing” the Internet access, you can set recurring schedules to automatically pause all the devices assigned to one or more family members.

From the Fingbox screen, tap on the tile “Schedule Pause” to see the available schedules or to create a new one.



To create a **new schedule**, tap on the big (+) button on the bottom-right corner.

Tap on an **existing schedule** to enable, disable, delete or modify it.

Here is how you can personalize a schedule to fit your needs:

Schedule’s name - Assign a name of your choice to this schedule.

Enabled - Determines if the schedule will be executed on the defined days and time. When you don’t want a schedule to be executed, disable it from this switch.

Days of the week - A schedule is by nature a recurring event. Choose the days of the week you want to run this schedule. Select the days in which the scheduled time starts, don't worry if the schedule ends on the next day.

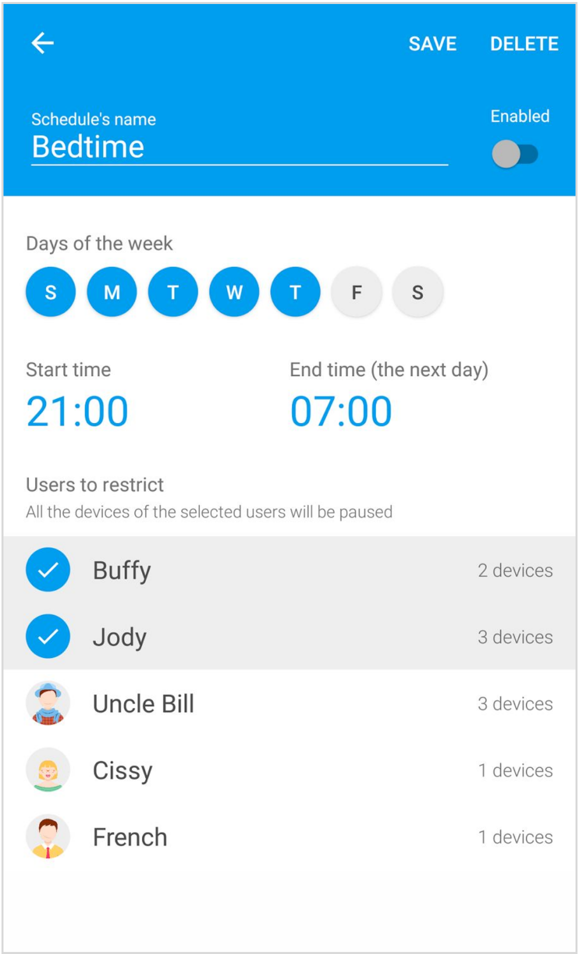
Start time - The time on which the Internet will be restricted.

End time - The time on which the Internet access will be restored. End time can occur on the next day. For example: from 9PM to 7AM (next day).

Users to restrict - The users that will be affected when this schedule is active.

SAVE - Remember to tap SAVE after you configure a schedule. If you don't tap SAVE, all the changes will be lost.

DELETE - To completely eliminate a schedule, tap on DELETE.



Schedule's name
Bedtime

Days of the week

Start time
21:00

End time (the next day)
07:00

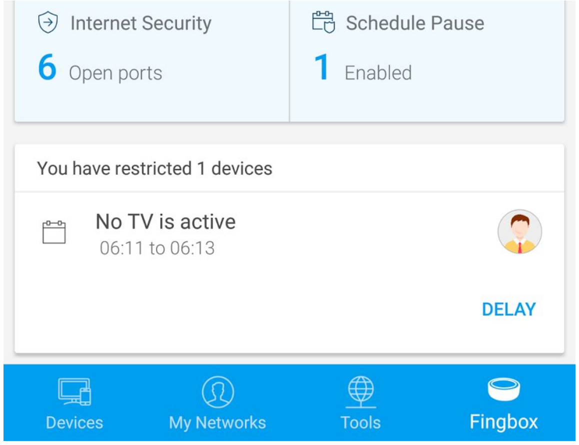
Users to restrict
All the devices of the selected users will be paused

✓	Buffy	2 devices
✓	Jody	3 devices
	Uncle Bill	3 devices
	Cissy	1 devices
	French	1 devices

Making exceptions: delay a scheduled pause

If you you want to make an exception and allow Internet usage, you can simply delay a scheduled execution. In this way you don't need to manually disable and re-enable a schedule just to skip a day.

When a schedule kicks in and you get a complain, open the Fing app, scroll down to the restricted device area and tap on DELAY.

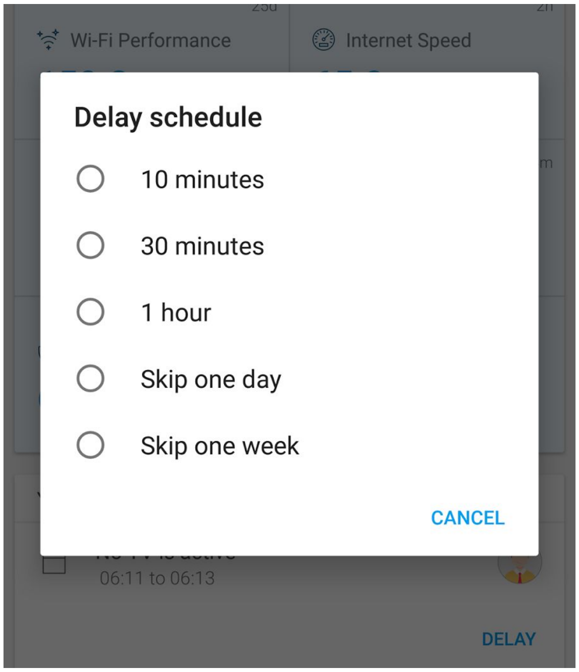


You have restricted 1 devices

No TV is active
06:11 to 06:13

After tapping on DELAY you'll be prompted to **choose for how long** you want to delay the scheduled pause.

You can choose "Skip one day" to skip the whole time interval or "Skip one week" if your kids are on holiday (enjoy!).



Delay schedule

○ 10 minutes

○ 30 minutes

○ 1 hour

○ Skip one day

○ Skip one week

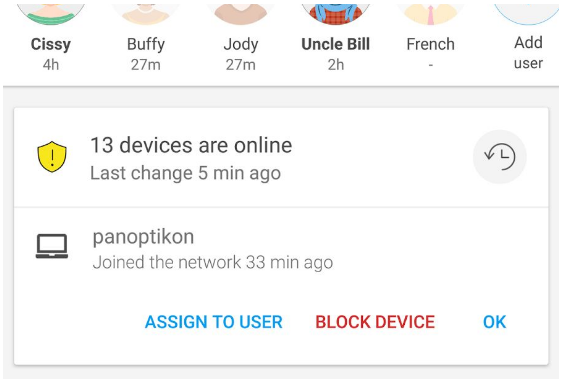
06:11 to 06:13

Alerts on new devices

Adding a new device to a network is not a frequent event (unless you run a coffee shop - or you're a gadget lover, are you?). One of the **most important security practice** is to avoid unauthorized people connecting their devices to your network.

Fingbox alerts you whenever a new device appears on the network for the first time. Such alerts can be sent as email messages or mobile notifications but you may be busy at that time and simply ignore them.

When a **new device** is detected, the Fingbox blue light circle will split in two blinking half-circles until you acknowledge the message in the Dashboard. See below an example of a new laptop that joined the network 33 minutes ago.



13 devices are online
Last change 5 min ago

panoptikon
Joined the network 33 min ago

The attention area with a message waiting for your action

When you see this message you can do any of these three actions.

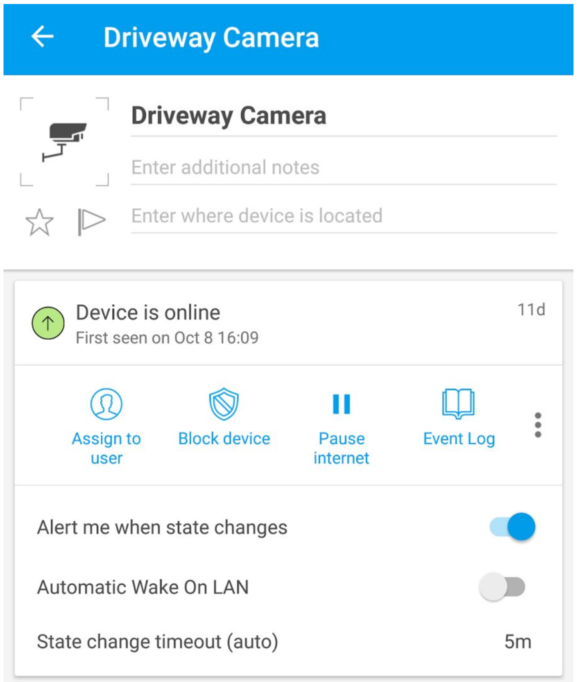
ASSIGN the new device to a family member (e.g. a new game console or a new phone or laptop).

BLOCK - If you didn't expect or don't recognize the device, you can immediately block it from accessing the network. You can come back later and unblock it from the bottom of the Dashboard screen.

ACKNOWLEDGE - You can tap **OK** to acknowledge without any special action. Fingbox top lights will get back to the normal blue circle.

Alerts on new devices are so important for network security that we chose to make them **active by default**. If you want to change the alert setting for New Devices, go to the Devices screen, tap on the List Manager icon (with the three lines, on the top-right corner) and then tap on Alerts.

See an example from a Device Details screen in the picture below. The “**Alert me when state changes**” setting is set to ON.



Driveway Camera

Driveway Camera

Enter additional notes

Enter where device is located

Device is online 11d
First seen on Oct 8 16:09

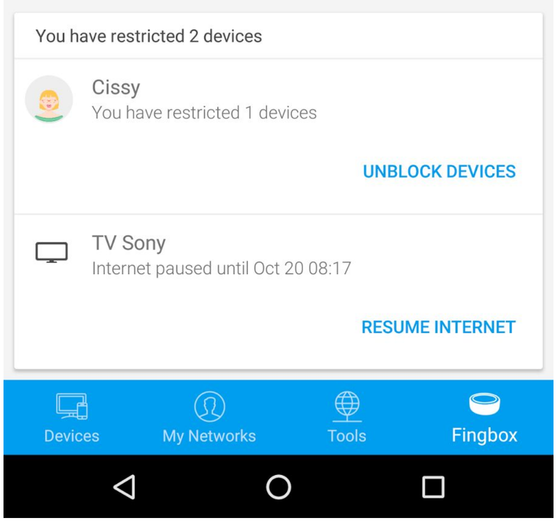
Alert me when state changes ●

Automatic Wake On LAN ○

State change timeout (auto) 5m

Paused and blocked devices

Whenever you PAUSE or BLOCK a device or a family member, they will be listed at the bottom of the Dashboard so you can quickly review and unpause them.



You have restricted 2 devices

Cissy
You have restricted 1 devices

UNBLOCK DEVICES

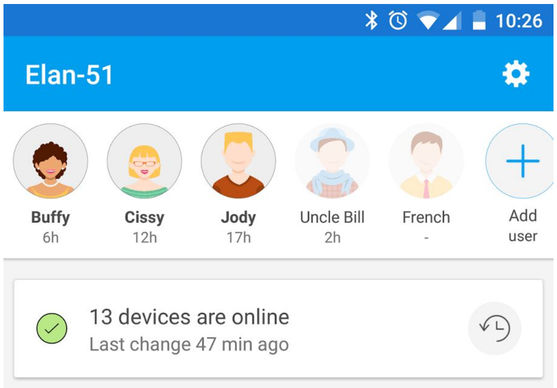
TV Sony
Internet paused until Oct 20 08:17

RESUME INTERNET

Adding a family member

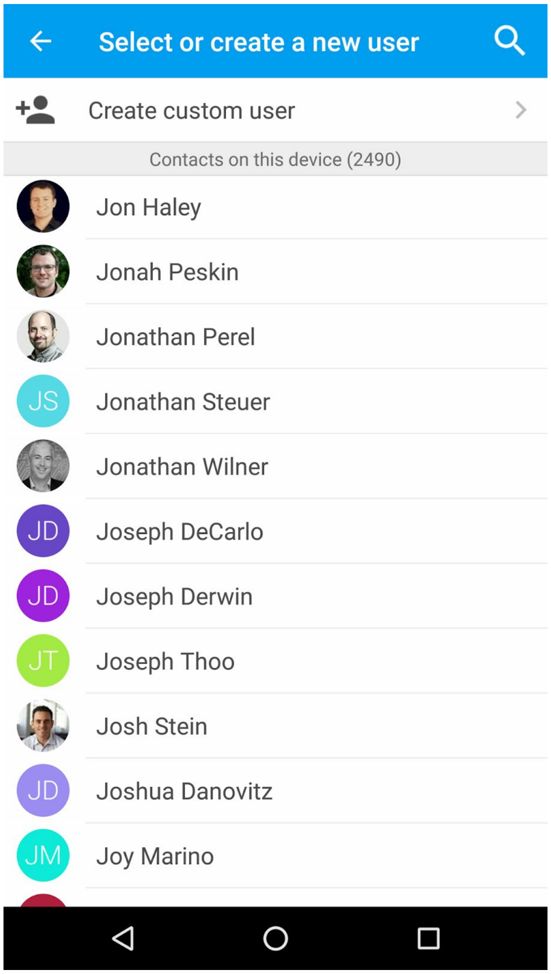
One of the key functions of Fingbox is **associating personal devices** to specific members of the household. In this way you can organize the devices in a natural way, see who's at home and, if you want, limit the Internet access for all the devices owned by a person, with a single command.

Tap on "Add user"



13 devices are online
Last change 47 min ago

Optionally, Fing can use the picture you already have in your phone contact list, otherwise tap on "Create custom user" to proceed without using your phone contacts. The latter works even if you don't allow Fing to access your contacts. Fing asks for Contacts only to make this user association easier - your contact details are not shared with the Fing service.



Select or create a new user

Create custom user

Contacts on this device (2490)

Jon Haley

Jonah Peskin

Jonathan Perel

Jonathan Steuer

Jonathan Wilner

Joseph DeCarlo

Joseph Derwin

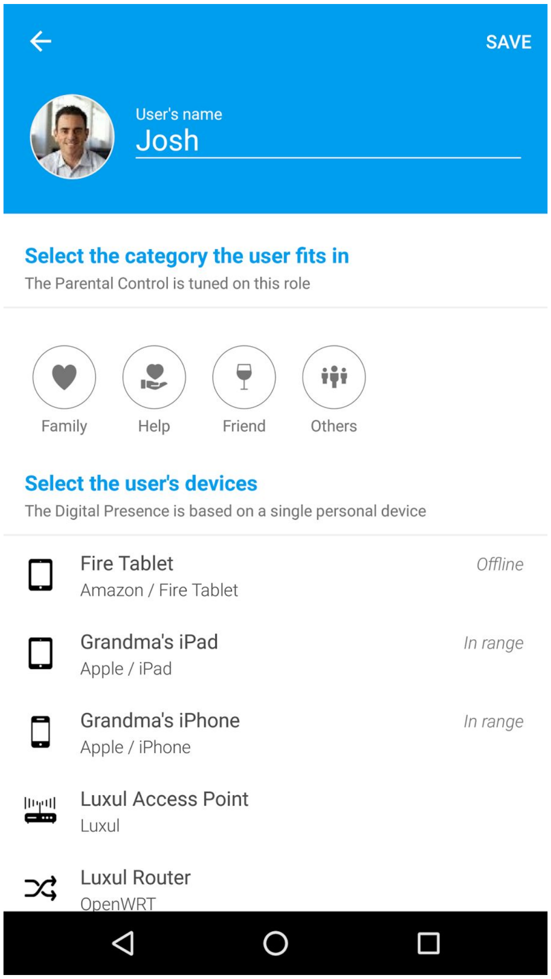
Joseph Thoo

Josh Stein

Joshua Danovitz

Joy Marino

Once you select a contact, modify the name if you wish, or tap on the picture to choose another image (or a simple graphical avatar). If you don’t add any picture, Fing will generate a colorful graphic with the initials.



SAVE

User's name

Josh

Select the category the user fits in

The Parental Control is tuned on this role

Select the user's devices

The Digital Presence is based on a single personal device

Fire Tablet — Amazon / Fire Tablet — *Offline*

Grandma's iPad — Apple / iPad — *In range*

Grandma's iPhone — Apple / iPhone — *In range*

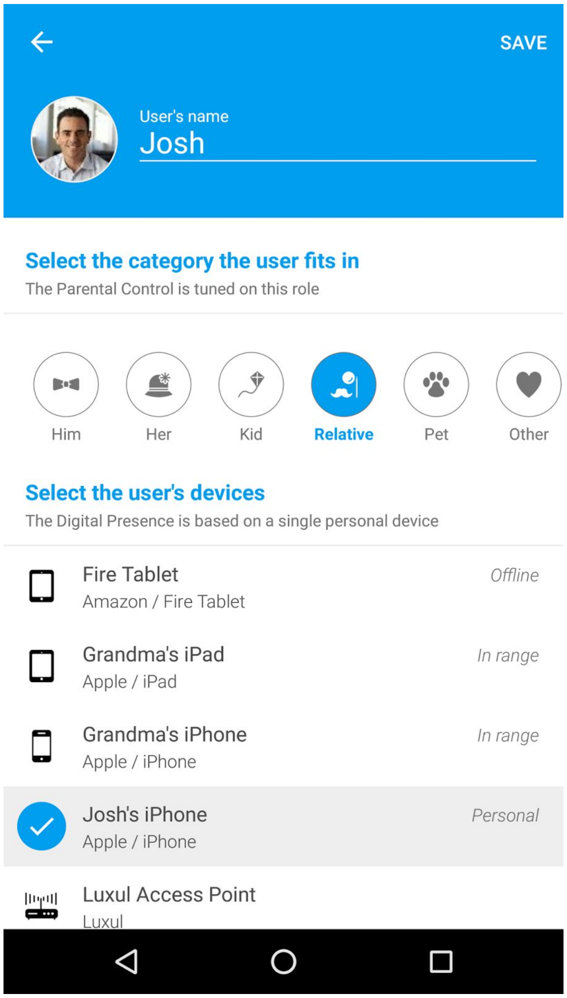
Luxul Access Point — Luxul

Luxul Router — OpenWRT

To allow Fing to adapt the parental control rules, tap on the **family member category**, such as Her, Kid, Relative or even Pet!

Then, tap on the device that will **determine the presence of this person** (usually a phone). Choose something that is with this person most of the time, like a phone or a wristwatch. The first pick will become the “Personal” device, the other devices you select will be associated to this person.

If you want **to change** the designated “Personal” device, **long-tap on another device** (already associated to the person) and Fing will ask to confirm.



Select the category the user fits in

The Parental Control is tuned on this role

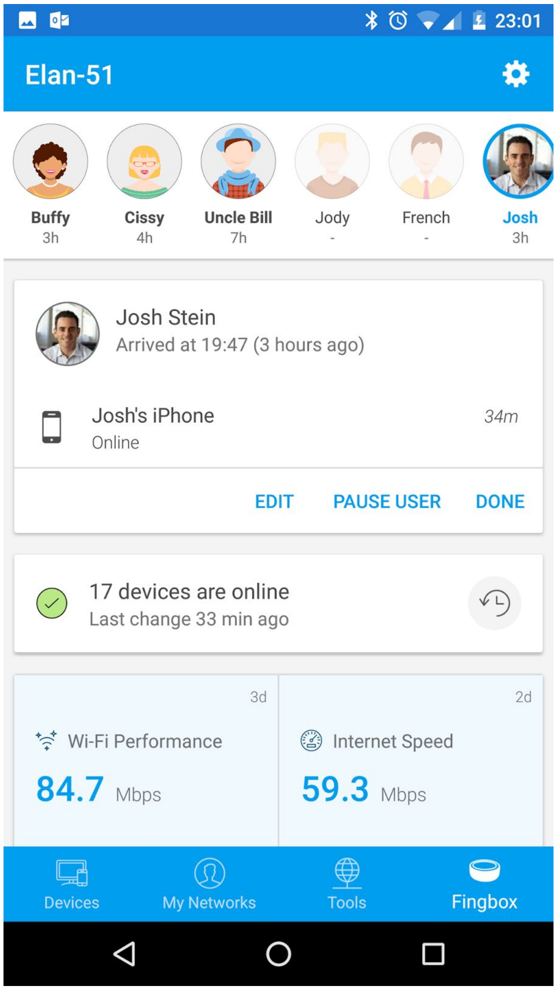
Select the user's devices

The Digital Presence is based on a single personal device

☐	Fire Tablet Amazon / Fire Tablet	*Offline*
☐	Grandma's iPad Apple / iPad	*In range*
☐	Grandma's iPhone Apple / iPhone	*In range*
✓	Josh's iPhone Apple / iPhone	*Personal*
☐	Luxul Access Point Luxul	

Tap on **SAVE** (top-right corner) and it's done! A new family member with his personal device.

To close the user's card, tap on DONE.



23:01

Elan-51

Buffy 3h | Cissy 4h | Uncle Bill 7h | Jody - | French - | Josh 3h

Josh Stein
Arrived at 19:47 (3 hours ago)

Josh's iPhone
Online
34m

17 devices are online
Last change 33 min ago

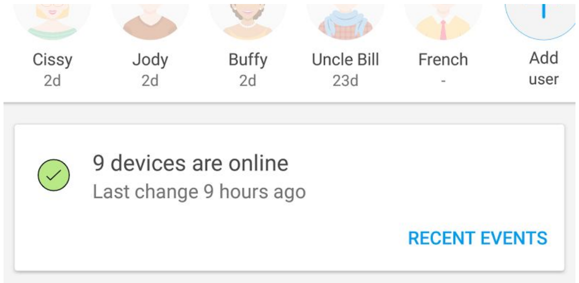
3d
Wi-Fi Performance
84.7 Mbps

2d
Internet Speed
59.3 Mbps

Recent Events

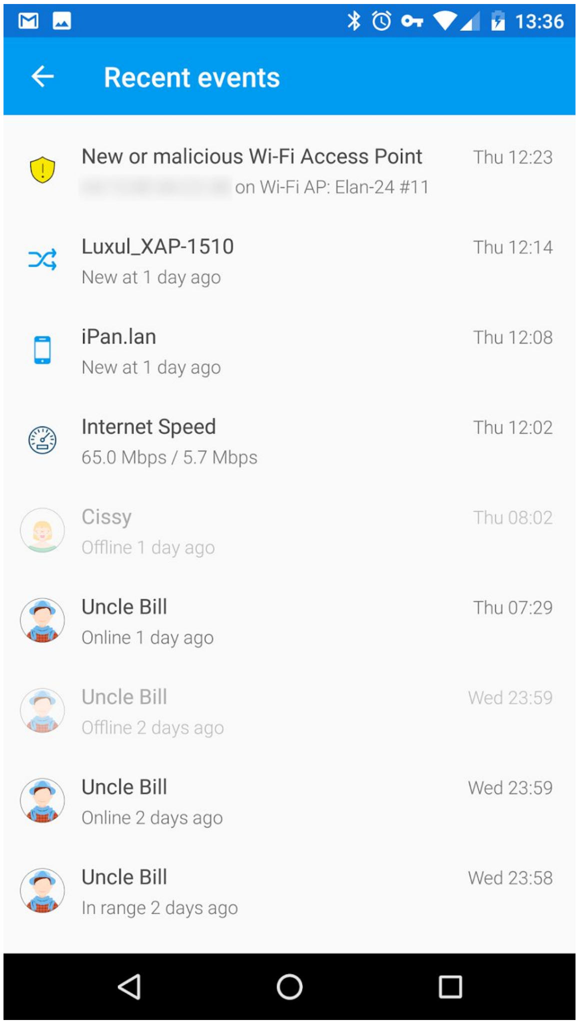
To see what happened while you weren't watching, tap on RECENT EVENTS.

You'll see all the relevant events that happened in your network, including family member presence, device status change, Internet Speed measurements and the Security Events.



Cissy 2d | Jody 2d | Buffy 2d | Uncle Bill 23d | French - | Add user

9 devices are online
Last change 9 hours ago



13:36

Recent events

New or malicious Wi-Fi Access Point — Thu 12:23
[redacted] on Wi-Fi AP: Elan-24 #11

Luxul_XAP-1510 — Thu 12:14
New at 1 day ago

iPan.lan — Thu 12:08
New at 1 day ago

Internet Speed — Thu 12:02
65.0 Mbps / 5.7 Mbps

Cissy — Thu 08:02
Offline 1 day ago

Uncle Bill — Thu 07:29
Online 1 day ago

Uncle Bill — Wed 23:59
Offline 2 days ago

Uncle Bill — Wed 23:59
Online 2 days ago

Uncle Bill — Wed 23:58
In range 2 days ago

Tap on an event to get more information, for example:

Person → see the person’s history of presence at home.

Device → see the history of the device status changes, including block/pause.

Security alert → see the details of the security alert (available for some events).

Internet Security → see the Internet Security report.

Internet Speed → see the Internet speed measured when the test was run.

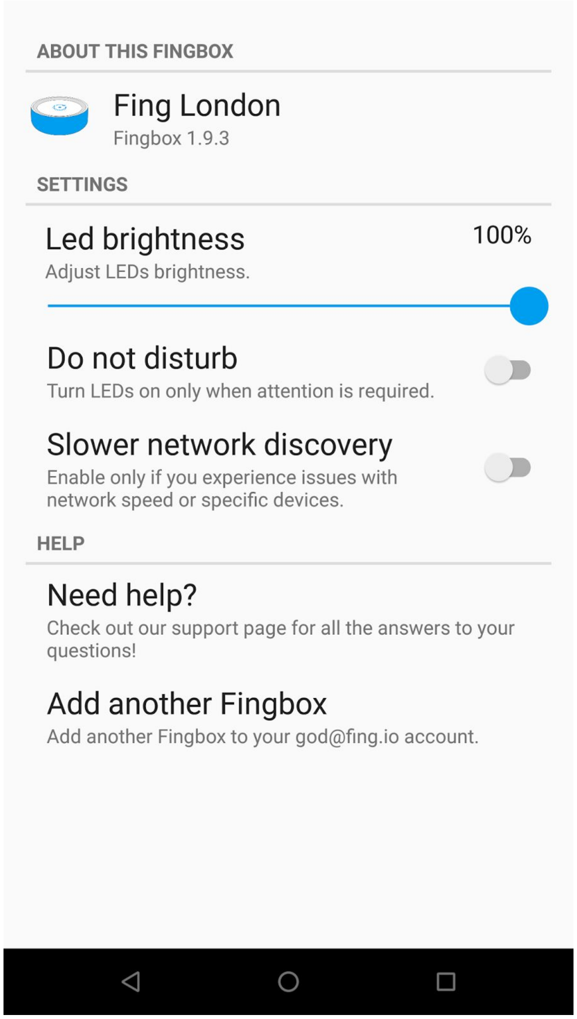
Wi-Fi Performance → see the Wi-Fi speed measured when the test was run.

Bandwidth Analysis → see the bandwidth usage report generated when you ran the analysis.

DigitalFence → The event reports the number of devices nearby.

Fingbox settings

To access Fingbox Settings, tap on the “wheel” icon in the top-right corner of the Dashboard.



ABOUT THIS FINGBOX

Fing London
Fingbox 1.9.3

SETTINGS

Led brightness — 100%
Adjust LEDs brightness.

Do not disturb
Turn LEDs on only when attention is required.

Slower network discovery
Enable only if you experience issues with network speed or specific devices.

HELP

Need help?
Check out our support page for all the answers to your questions!

Add another Fingbox
Add another Fingbox to your god@fing.io account.

The top section ABOUT THIS FINGBOX tells you the **Fingbox name** and the **firmware version** currently running on this Fingbox. To change the Fingbox name, go to the screen Devices and tap on the name at the top.

Led brightness - Use this slider to dim the lights on the top circle. Set to 0% to turn them off.

Do not disturb - When this is ON, Fingbox lights will stay dimmed when in normal operations and will turn at full brightness only when Fingbox wants to signal an important warning (new device, security alerts, configuration change).

Slower network discovery - When you set this to ON, Fingbox will slow down the rate of the “broadcast” discovery packets sent to monitor your devices. Use this only if you have a device having issues when Fingbox is active (for example, the device slows down, loses Internet connectivity or reboots).

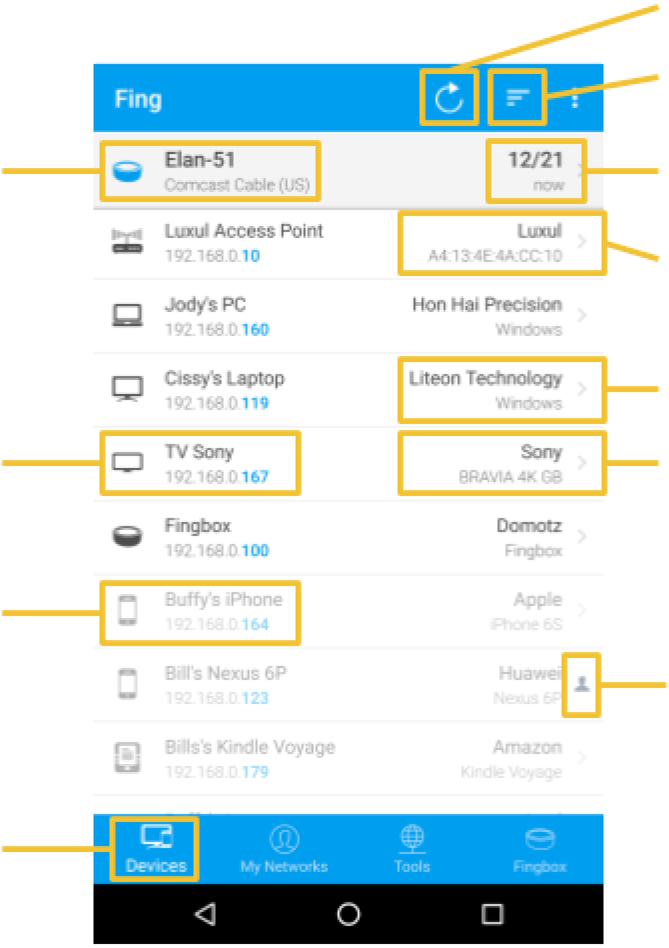
Add another Fingbox - Tap on this to add another Fingbox to the current account. The new Fingbox must be non-activated and with a **green top circle**, connected on the same home network as the phone you’re using right now.

This function **will not find** Fingbox units that are **already activated**.

Devices screen

This screen contains the “inventory” of all the devices ever seen on your network (online and offline) plus the *off-network* devices you chose to “watch” from the DigitalFence lists.

DEVICES



Elan-51 Comcast Cable (US) 12/21 now

Luxul Access Point 192.168.0.10 Luxul A4:13:4E:4A:CC:10

Jody's PC 192.168.0.160 Hon Hai Precision Windows

Cissy's Laptop 192.168.0.119 Liteon Technology Windows

TV Sony 192.168.0.167 Sony BRAVIA 4K GB

Fingbox 192.168.0.100 Domotz Fingbox

Buffy's iPhone 192.168.0.164 Apple iPhone 6S

Bill's Nexus 6P 192.168.0.123 Huawei Nexus 6P

Bills's Kindle Voyage 192.168.0.179 Amazon Kindle Voyage

Name of this Fingbox and service provider. Tap here to access Network info, device list sorting and global notification settings.

Online device with type icon, name and current IP address

Offline device with type icon, name. The displayed IP address is the last known address.

Tap on this icon to get back to this screen

Manual Scan is disabled for Fingbox-managed networks.

Search, Sort, Filter Devices. Set alert notifications.

Number of devices currently online and total number of devices ever seen.

When model is not available, the MAC address is shown.

For some devices, the operating system is shown.

Device brand and model (where available).

This icon marks the device you're currently using.

States of a device

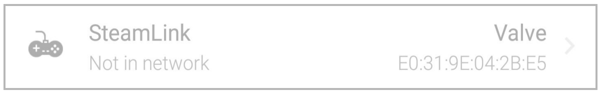
Beside the **ONLINE** and **OFFLINE** states, a device can be displayed in a few other conditions:

NOT DETECTED - The device stopped responding to the Fingbox heartbeat messages, but the timeout defined for declaring this device offline has not passed yet. If the device keeps staying silent, the status will eventually become OFFLINE.

NOT IN NETWORK - A device that was previously seen by Fingbox is “talking” on the network but doesn’t have an IP address on the same subnet as Fingbox. Possible reasons for this state are:

1. The device has been assigned an IP address in another subnet (e.g. because of manual IP address configuration or multiple DHCP servers are active on the same ethernet segment).
2. The device is trying to get an IP address but the DHCP server is not assigning one (because the device is blacklisted or the DHCP server is not working properly and need to be re-configured or simply restarted).

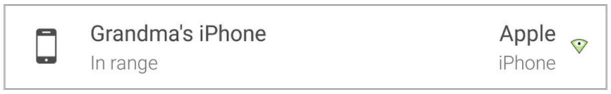
A device in this status can be deleted with a swipe-left gesture.



SteamLink Valve
Not in network E0:31:9E:04:2B:E5

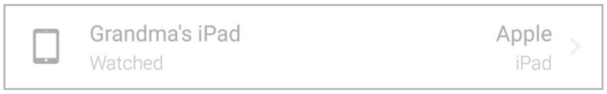
IN RANGE - A device that you selected in DigitalFence is active nearby (the WiFi sensor of the Fingbox has a range of about 100 feet, although this may be reduced by concrete walls and metallic obstacles).

▽ The small green triangle on the right marks a device watched with DigitalFence. A device in this status can be deleted with a swipe-left gesture.



Grandma's iPhone Apple
In range iPhone

WATCHED - A device that you selected in DigitalFence is not active in the vicinity of your Fingbox (the WiFi sensor of the Fingbox has a range of about 100 feet, although this may be reduced by concrete walls and metallic obstacles). A device in this status can be deleted with a swipe-left gesture.

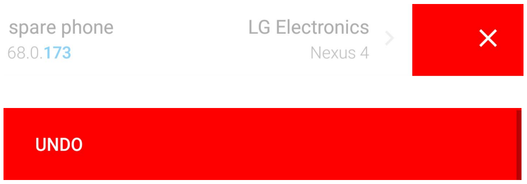


Grandma's iPad Apple
Watched iPad

Deleting a device

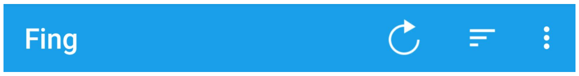
You can delete any device that is OFFLINE, IN RANGE or WATCHED. To delete, **swipe-left** with your finger. As an alternative, if you're using Android, you can long-tap on the row.

After deleting a device, Fing will offer the UNDO option for 3 seconds. If you deleted the device by mistake, tap on UNDO to restore the device entry.

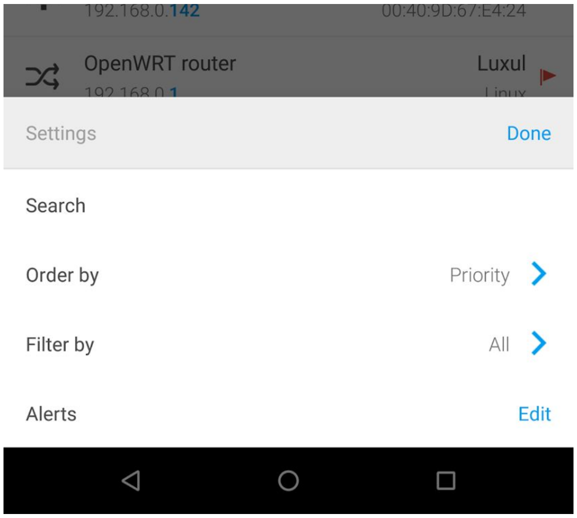


Searching devices

To search for a device, go to the Devices screen and tap on the List Manager **icon with three lines**, in the top-right corner of the screen.



This will open a menu at the bottom, tap on “Search”.



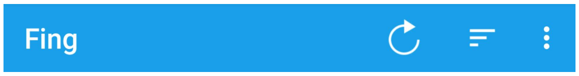
You can search devices by entering any text. Fing will search your text within the following device attributes:

- **Device name** (e.g. driveway, Cissy, TV)
- **IP address** (e.g. 150, 1.254)
- **MAC address** (e.g. A4:13, 18:B4:30)

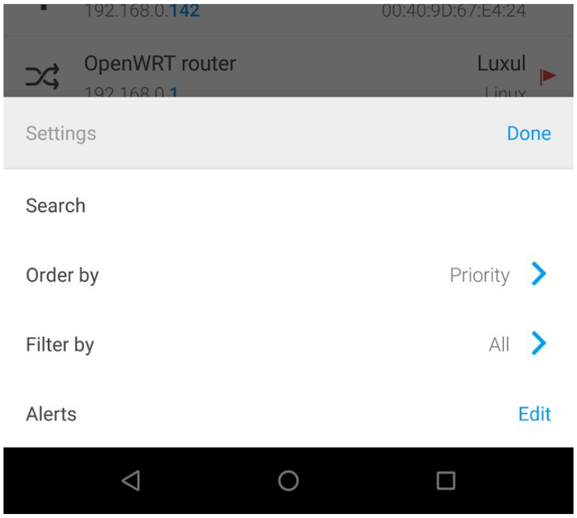
- **Device brand** (e.g. Apple, Samsung, Sony)
- **Device model** (e.g. Bravia, Nexus, Galaxy)
- **Device type** (e.g. mobile, tablet, printer, doorbell)

Sorting devices

To sort devices, go to the Devices screen and tap on the List Manager **icon with three lines**, in the top-right corner of the screen.



This will open a menu at the bottom, tap on “Order by”. You’ll see the available device sorting criteria.



Settings Done

Search

Order by Priority

Filter by All

Alerts Edit

Device sorting criteria

IP address - Sort devices by IP address.

State - Active devices on top. Offline devices are at the bottom of the list.

Name - Devices by name, in alphabetical order.

Vendor - Devices by brand name, in alphabetical order.

MAC address - Sort devices by MAC address.

Last change - Put on top the devices that changed status most recently (went offline or online).

Priority - Put on top the devices with the highest “device order score”. The *device order score* is higher if:

- The device is currently online
- The device is used to determine a user’s presence
- You set the device to send an alert when its status changes

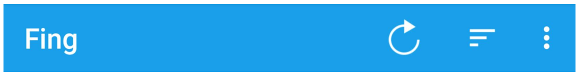
If the score is the same, then Fing will sort by:

- Most recent status change
- IP address
- MAC address

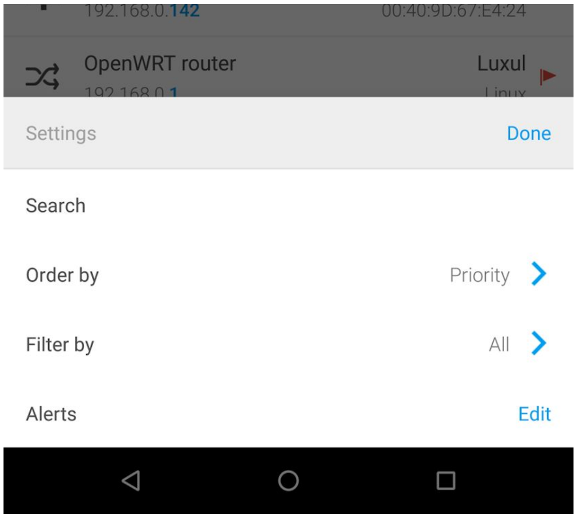
Filtering the device view

If you have a lot of devices, reviewing the list may become overwhelming. You can narrow the device list by using the filter.

To filter the device list, go to the Devices screen and tap on the List Manager **icon with three lines**, in the top-right corner of the screen.



This will open a menu at the bottom, tap on “Filter by”.



192.168.0.142 00:40:9D:67:E4:24

OpenWRT router Luxul
192.168.0.1 Linux

Settings Done

Search

Order by: Priority

Filter by: All

Alerts: Edit

You'll see the available filtering criteria.

All - Show all the devices (remove the filter).

Online - Show only the active devices.

Offline - Show only the offline devices (they stopped responding to Fingbox messages for longer than the device timeout).

Unrecognized - Show only the devices requiring manual identification. Fing couldn't understand what they are and needs a little help.

Alerted - Show only the devices you set to send an alert when their status changes.

Important ⚑ - Show only devices you marked with the little flag.

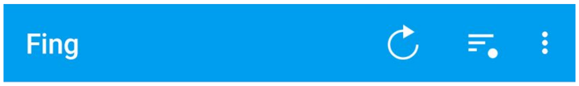
Favorite ★ - Show the devices you marked with the star.

Blocked - Show the devices currently blocked or paused.

Watched - Show only the off-network devices you picked from the DigitalFence list.

Partial list warning

When some devices are hidden because of a filter, the list manager icon shows a "dot" to warn you're looking at a partial device list.

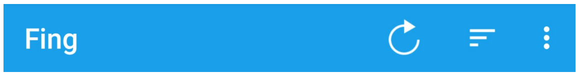


Setting alerts on a device status change

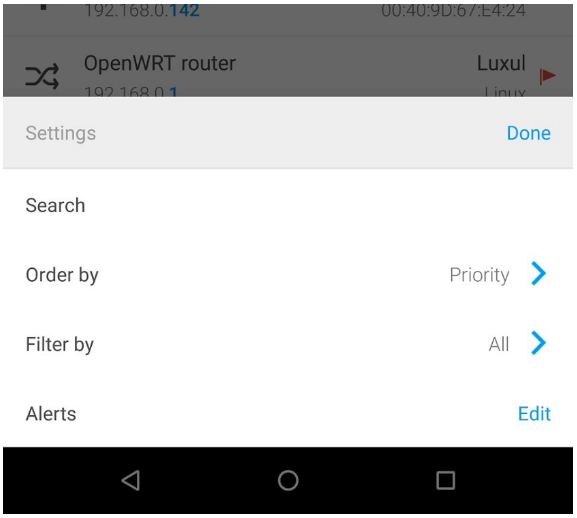
The usual way to set an alert on a device status change is to enter the Device Details screen and set the alert for each device.

To quickly review and change alert settings on devices, you can use the Alerts screen introduced with app release v6.4.

To access the global alerts view, go to the Devices screen and tap on the List Manager **icon with three lines**, in the top-right corner of the screen.



This will open a menu at the bottom, tap on "Alerts".


192.168.0.142 00:40:9D:67:E4:24

OpenWRT router Luxul
192.168.0.1 Linux

Settings Done

Search

Order by Priority

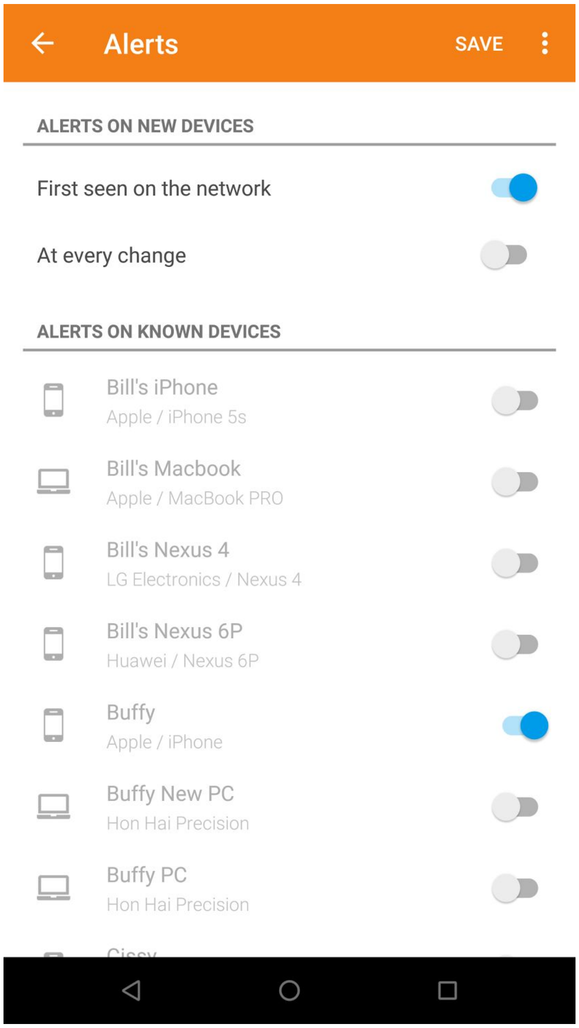
Filter by All

Alerts Edit

This will open the Alerts screen, displaying all your devices with the setting of the alert on the device status change (i.e. when the device status changes to offline or online).

Blue switch - You'll receive an alert every time the device changes it status to offline or online.

Gray switch - You'll not receive any alert when this device status changes.



Alerts SAVE

ALERTS ON NEW DEVICES

First seen on the network ●

At every change ○

ALERTS ON KNOWN DEVICES

Bill's iPhone Apple / iPhone 5s	○
Bill's Macbook Apple / MacBook PRO	○
Bill's Nexus 4 LG Electronics / Nexus 4	○
Bill's Nexus 6P Huawei / Nexus 6P	○
Buffy Apple / iPhone	●
Buffy New PC Hon Hai Precision	○
Buffy PC Hon Hai Precision	○
Cissy	

In the top section ALERTS ON NEW DEVICES, you can set the Fingbox behavior when it sees a device on the network for the first time.

A device is NEW when its MAC address has never been seen on the network. **If you manually delete a device**, it will be considered NEW when it is detected again by Fingbox.

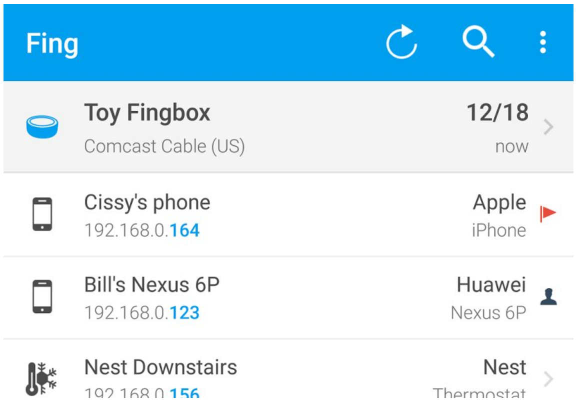
First seen on the network - Fingbox will send an alert every time it sees a device for the first time. *As a good network security practice, we recommend to keep this set to ON. In this way you'll be alerted whenever someone connects a new device to your network (you may want to set this to OFF if you run a cafe or a public place where everybody is allowed to connect).*

At every change - All the new devices will have the Status Change alert set to ON. To avoid being flooded with alerts, we recommend to keep this set to OFF.

Remember to tap on **SAVE** after you change the alert settings. If you go back, all changes will be lost.

Network details

To access the Network details, go to the Device list screen and tap on the Fingbox name at the top of the screen. In the example below, the Fingbox name is “Toy Fingbox”.



Fing

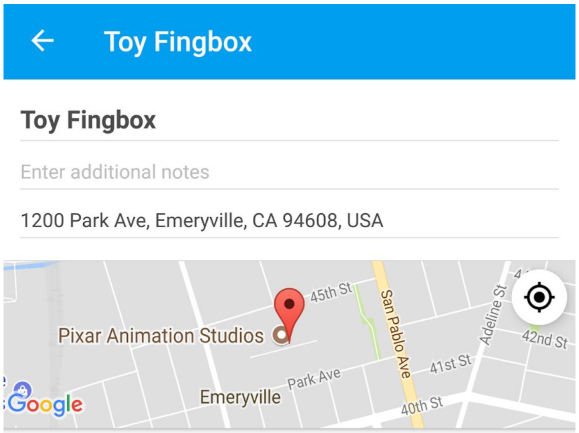
Toy Fingbox 12/18
Comcast Cable (US) now

Cissy's phone Apple
192.168.0.164 iPhone

Bill's Nexus 6P Huawei
192.168.0.123 Nexus 6P

Nest Downstairs Nest
192.168.0.156 Thermostat

The top section allows you to change the Fingbox name and set the location address. You can use the GPS to set the current phone location as the Fingbox location.



Toy Fingbox

Toy Fingbox

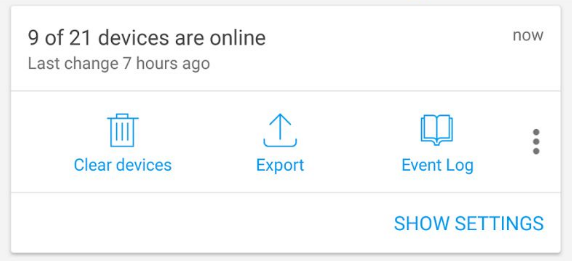
Enter additional notes

1200 Park Ave, Emeryville, CA 94608, USA

The next section allows you to perform several actions on the device list (tap on the vertical three dots to access the hidden menu items).

- **Clear devices** - Delete all the offline devices
- **Export** - Export the list to a file (CSV, HTML or XML)
- **Event Log** - See the history of state changes for all the devices

- **Share** - Share the device list (e.g. via email or chat)
- **Sync names and icons** - Synchronize your customized device icons and names across all the networks in your Fing account (show the same name and type wherever the device appears).



9 of 21 devices are online

Last change 7 hours ago

Tap on SHOW SETTINGS to see the context setting.

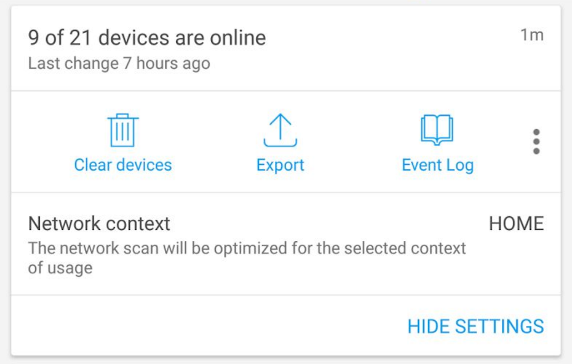
Change the **network context** to the appropriate value. Fingbox adapts the user interface and the automatic configurations to fit in any of these contexts.

HOME - for a residential household

RENTAL - a house for short rental periods, where devices change frequently

OFFICE - an office network with employees and contractors

PUBLIC - a public place, for example a coffee shop, where many people come and go



9 of 21 devices are online

Last change 7 hours ago

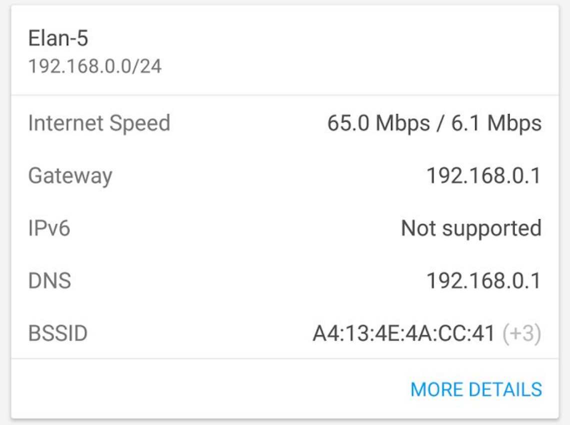
Network context: HOME

The network scan will be optimized for the selected context of usage

The next section recaps the key technical information about this network.

- The **Wi-Fi name (SSID)** used to **activate** this Fingbox (in the example below: Elan-5).
- The **IP network address** (ex: 192.168.0.0) and the network mask (ex: 24 bit).

- The most recent measurement of **Internet Speed** (download / upload).
- The IP address of the **default gateway** (the router used to reach the Internet).
- The allocation of **IPv6** addresses in the local network.
- The **DNS servers** indicated by the DHCP server.
- The MAC address of the **first Wi-Fi access point** (BSSID). The example shows that there is more than one BSSID in this network. Tap MORE DETAILS to get the whole list.

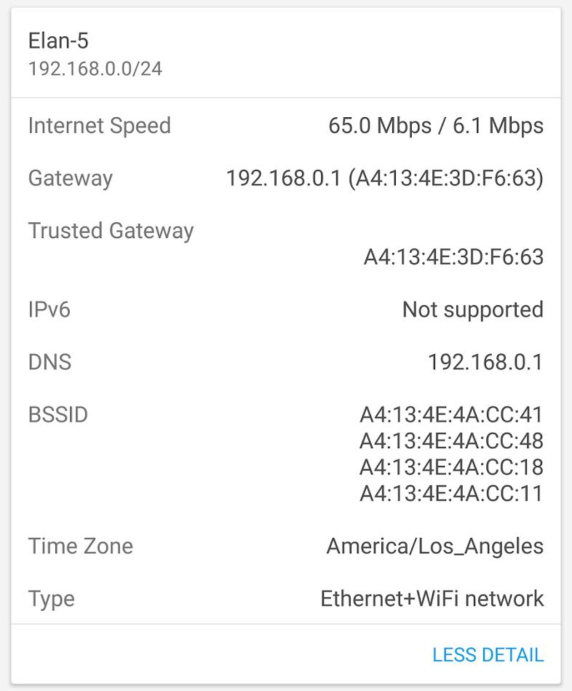


Elan-5
192.168.0.0/24

Internet Speed	65.0 Mbps / 6.1 Mbps
Gateway	192.168.0.1
IPv6	Not supported
DNS	192.168.0.1
BSSID	A4:13:4E:4A:CC:41 (+3)

Tapping on MORE DETAILS you can view additional information about this network:

- The full list of the Wi-Fi access point **BSSIDs known to Fingbox** (their number may exceed the number of physical access points because each 2.4 and 5GHz Wi-Fi network has a separate BSSID address).
- The **time zone** where the Fingbox is operating (e.g. America/Los_Angeles)
- The name of the **Internet service provider** with the city, state or country.
- The **public IP address** as seen by the Fing cloud service.
- The **hostname** associated to the public IP address as determined by a DNS reverse lookup.



Elan-5
192.168.0.0/24

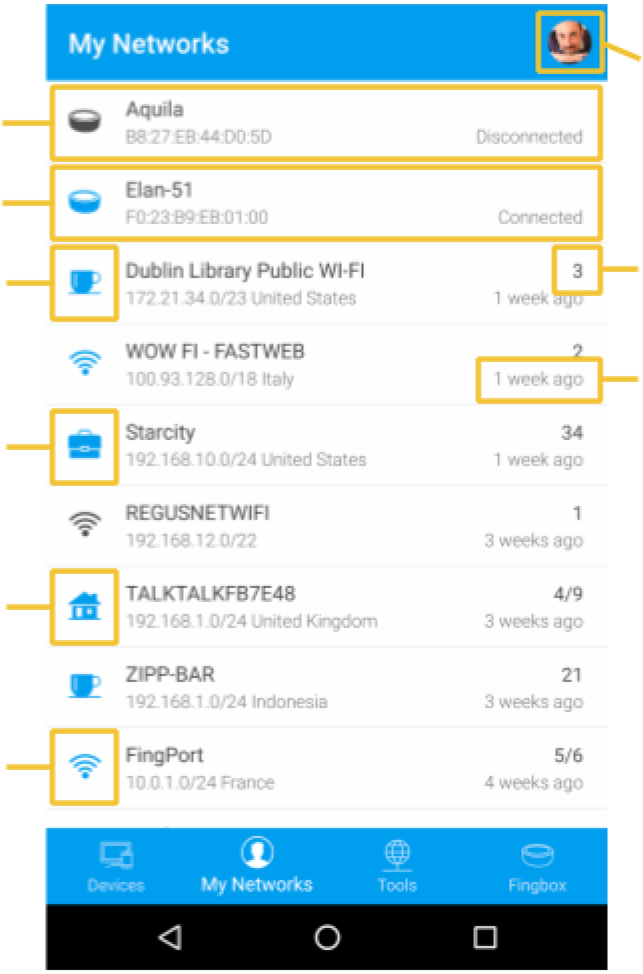
Internet Speed	65.0 Mbps / 6.1 Mbps
Gateway	192.168.0.1 (A4:13:4E:3D:F6:63)
Trusted Gateway	A4:13:4E:3D:F6:63
IPv6	Not supported
DNS	192.168.0.1
BSSID	A4:13:4E:4A:CC:41 A4:13:4E:4A:CC:48 A4:13:4E:4A:CC:18 A4:13:4E:4A:CC:11
Time Zone	America/Los_Angeles
Type	Ethernet+WiFi network

My Networks

This screen shows the list of all the networks belonging to your Fing account. A network can be of two types:

Unmanaged (manual scan only)
This is the *classic* Fing network, created and updated every time you run a manual scan from the Devices screen. Unmanaged networks are marked with any of the "context" icons for Home, Office, Rental, Public or Unclassified. You can **delete an unmanaged network** with a swipe-left gesture. All the customizations you made to devices will be lost.

Managed (by Fingbox)
This type of network has a Fingbox and can be managed from anywhere (locally or via Internet). Managed networks are displayed with an icon representing a small Fingbox. If you have **multiple Fingbox units** activated under your account, you'll see them listed here. You can switch from one to another by simply tapping on the list item. If you swipe-left to **delete a managed network**, the associated **Fingbox will be deactivated** and its memory wiped out to factory defaults. Because of this potential data loss, a pop-up will always ask you to confirm a deactivation.



My Networks

Aquila
B8:27:EB:44:D0:5D Disconnected

Elan-51
F0:23:B9:EB:01:00 Connected

Dublin Library Public WI-FI 3
172.21.34.0/23 United States 1 week ago

WOW FI - FASTWEB 2
100.93.128.0/18 Italy 1 week ago

Starcity 34
192.168.10.0/24 United States 1 week ago

REGUSNETWIFI 1
192.168.12.0/22 3 weeks ago

TALKTALKFB7E48 4/9
192.168.1.0/24 United Kingdom 3 weeks ago

ZIPP-BAR 21
192.168.1.0/24 Indonesia 3 weeks ago

FingPort 5/6
10.0.1.0/24 France 4 weeks ago

My account. Tap here to logout and switch to another Fing account.

A Fingbox-managed network. Fingbox is offline

A fully working Fingbox-managed network

A manually scanned network in a “public” place

Number of devices found after scanning this network

When this network was scanned

A manually scanned “office”

A manually scanned “home”

A manually scanned network, unclassified

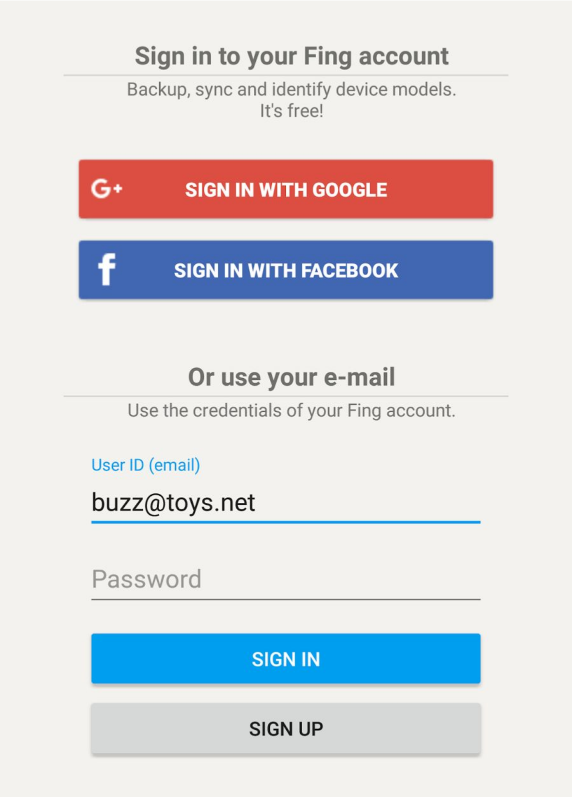
My account

Fingbox and the Fing app communicate via the Fing Secure Account Service. You can control a Fingbox from multiple mobile devices at the same time. Simply login with the same Fing Account and all the changes will be automatically synchronized.

Creating a Fing account

You can **create a Fing account** using your email address and a password (long, random and never written anywhere, right?).

If you have a Google or Facebook account and you **don't want another password to remember**, Fing works with **Google** and **Facebook authentication** to quickly create a Fing Account. No need for another password to remember. And we only read your email address and your picture. We don't post, we don't read your messages and we don't download your friends list (technically, we never get access to them). We promise.



Sign in to your Fing account

Backup, sync and identify device models.
It's free!

Or use your e-mail

Use the credentials of your Fing account.

User ID (email)
buzz@toys.net

Fing works with Google and Facebook authentication.
No need for another password to remember.

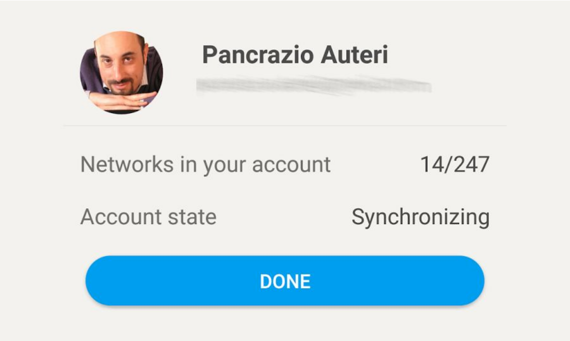
Once you sign in, you'll see the number of **networks synchronized** between your phone and the Fing Secure Account Service. In this way you can use **Fing on multiple devices** under the same account and see the same things from all of them. If you have a lot of networks, it may take a while. You can tap on DONE, synchronization will continue in the background.

Lost password

If you **forgot your password**, you can easily set a new one using the **password recovery** page:

https://app.fing.io/recovery

Just enter the email address of the Fing Account and we'll send you an email with a link to set a new password. Of course, you have access to that email account, right?



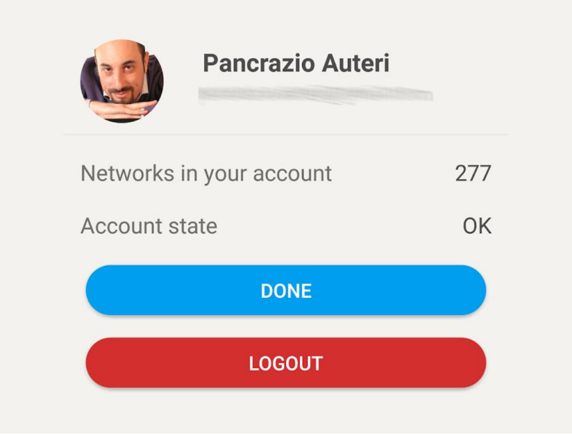
Pancrazio Auteri
[redacted]

Networks in your account 14/247

Account state Synchronizing

Logout

To **logout** from your account, just tap on LOGOUT. Please, be aware that, upon logout, all the scanned networks will remain saved locally on the phone (because you can still use Fing in anonymous mode, without being logged in).



Pancrazio Auteri

[redacted]

Networks in your account	277
Account state	OK

Tools

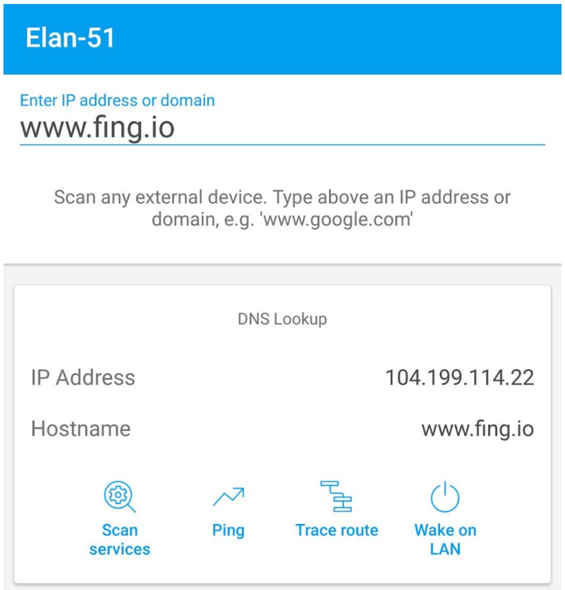
The tools in this screen run from the mobile device where you’re using the Fing app. **These tools don’t run from the Fingbox**, so all their measurements are affected by the connectivity of your phone or tablet.

Scan services - This performs a port scan on the target address. It tests only the TCP ports listed in the section “Edit TCP Services” of the Fing app settings. You can modify this list to fit your needs.

Ping - This will run a continuous ping to the target address, showing the round-trip time and the packet loss between your phone and the target address.

Trace route - This will show all the routers and the “hops” between your phone and the computer at the target address.

Wake on LAN - This will send a Wake-on-LAN packet to wake up the target device (if it supports the Wake-on-LAN functionality).



Elan-51

Enter IP address or domain: www.fing.io

Scan any external device. Type above an IP address or domain, e.g. 'www.google.com'

DNS Lookup

IP Address 104.199.114.22

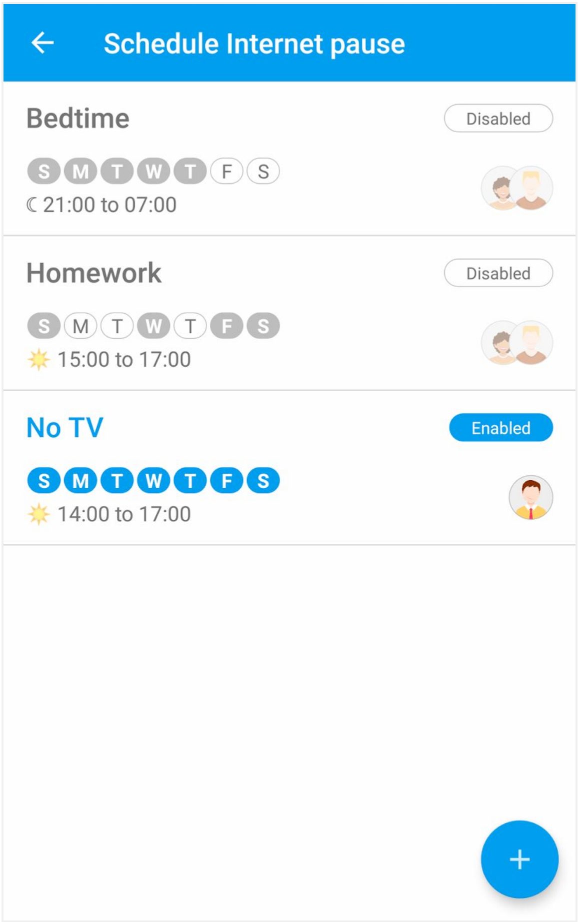
Hostname www.fing.io

Parental Control (scheduling Internet Pause)

Scheduling Internet Pause

Instead of manually “pausing” the Internet access, you can set recurring schedules to automatically pause all the devices assigned to one or more family members.

From the Fingbox screen, tap on the tile “Schedule Pause” to see the available schedules or to create a new one.



Schedule Internet pause

Bedtime Disabled
S M T W T F S
21:00 to 07:00

Homework Disabled
S M T W T F S
15:00 to 17:00

No TV Enabled
S M T W T F S
14:00 to 17:00

+

To create a **new schedule**, tap on the big (+) button on the bottom-right corner. Tap on an **existing schedule** to enable, disable, delete or modify it.

Here is how you can personalize a schedule to fit your needs:

Schedule’s name - Assign a name of your choice to this schedule.

Enabled - Determines if the schedule will be executed on the defined days and time. When you don't want a schedule to be executed, disable it from this switch.

Days of the week - A schedule is by nature a recurring event. Choose the days of the week you want to run this schedule. Select the days in which the scheduled time starts, don't worry if the schedule ends on the next day.

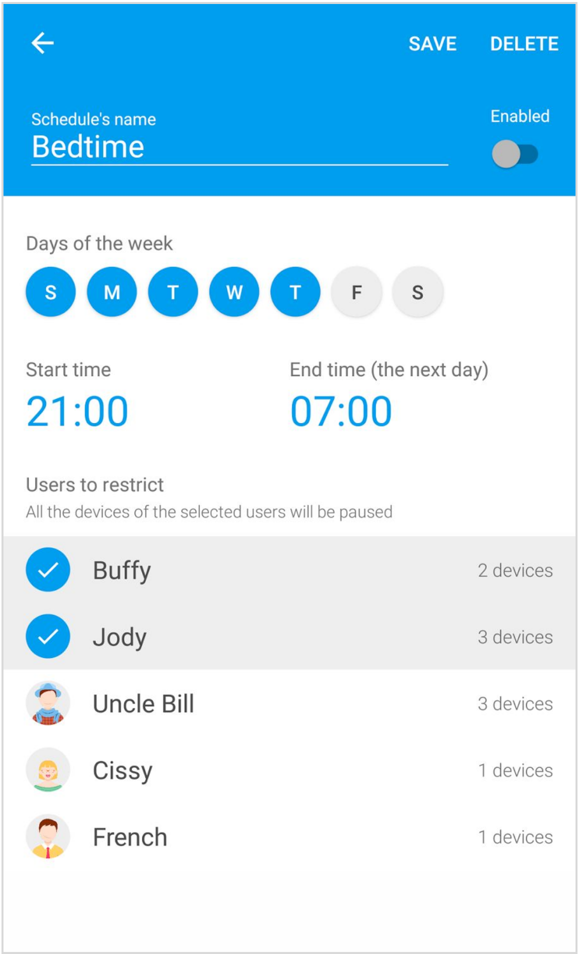
Start time - The time on which the Internet will be restricted.

End time - The time on which the Internet access will be restored. End time can occur on the next day. For example: from 9PM to 7AM (next day).

Users to restrict - The users that will be affected when this schedule is active.

SAVE - Remember to tap SAVE after you configure a schedule. If you don't tap SAVE, all the changes will be lost.

DELETE - To completely eliminate a schedule, tap on DELETE.



Schedule's name
Bedtime

Enabled

Days of the week
S M T W T F S

Start time
21:00

End time (the next day)
07:00

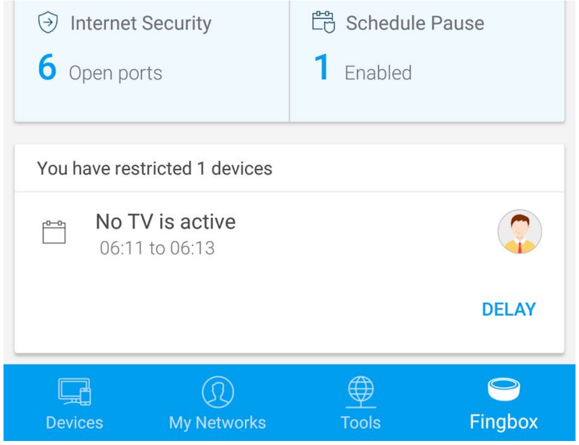
Users to restrict
All the devices of the selected users will be paused

✓	Buffy	2 devices
✓	Jody	3 devices
	Uncle Bill	3 devices
	Cissy	1 devices
	French	1 devices

Making exceptions: delay a scheduled pause

If you you want to make an exception and allow Internet usage, you can simply delay a scheduled execution. In this way you don't need to manually disable and re-enable a schedule just to skip a day.

When a schedule kicks in and you get a complain, open the Fing app, scroll down to the restricted device area and tap on DELAY.



Internet Security

6 Open ports

Schedule Pause

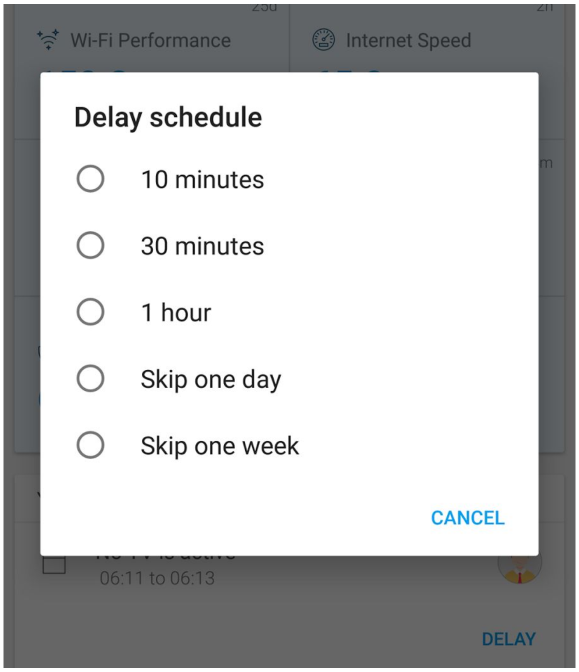
1 Enabled

You have restricted 1 devices

No TV is active
06:11 to 06:13

After tapping on DELAY you'll be prompted to **choose for how long** you want to delay the scheduled pause.

You can choose "Skip one day" to skip the whole time interval or "Skip one week" if your kids are on holiday (enjoy!).



Delay schedule

○ 10 minutes

○ 30 minutes

○ 1 hour

○ Skip one day

○ Skip one week

Solving network speed problems

Sometimes your network slows down or stops working (and you need to send that huge slide deck for tomorrow's presentation). Or maybe the connection is good during the day, but unusable at night (right when you were finally ready to catch up with Game of Thrones).

It's not easy to understand where the problem is. Calling your Internet provider often implies a long wait, a bunch of trivial questions and no problem solved.

What's the cause of the slow down? Is it your new neighbor's Wi-Fi? Should you move your Wi-Fi access point to a better position? Is your Wi-Fi extender messing up with your new doorbell? Or should you buy a Wi-Fi mesh system to cover the dark spots in your home?

Fingbox empowers you to understand what's happening and take the right actions. It all starts by measuring the following things:

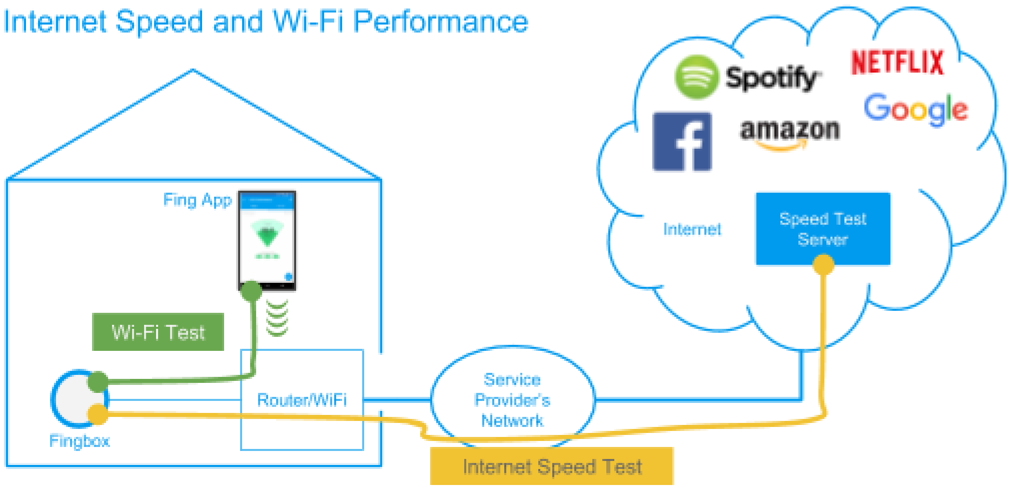
- The Wi-Fi speed at your phone location
- How fast your service provider connects you to the "Big Internet"
- How much bandwidth is being used by each device and who's "hogging" the connection

First, let's see how each test works. Then we'll use them all to troubleshoot a "slowness" issue.

The big difference between the Wi-Fi and the Internet speed test is this:

- the **Wi-Fi test** runs entirely **within your home** and is not affected by the Internet connection speed;
- the **Internet speed test** runs **between the Fingbox and** a test server on **the Internet** and doesn't use Wi-Fi.

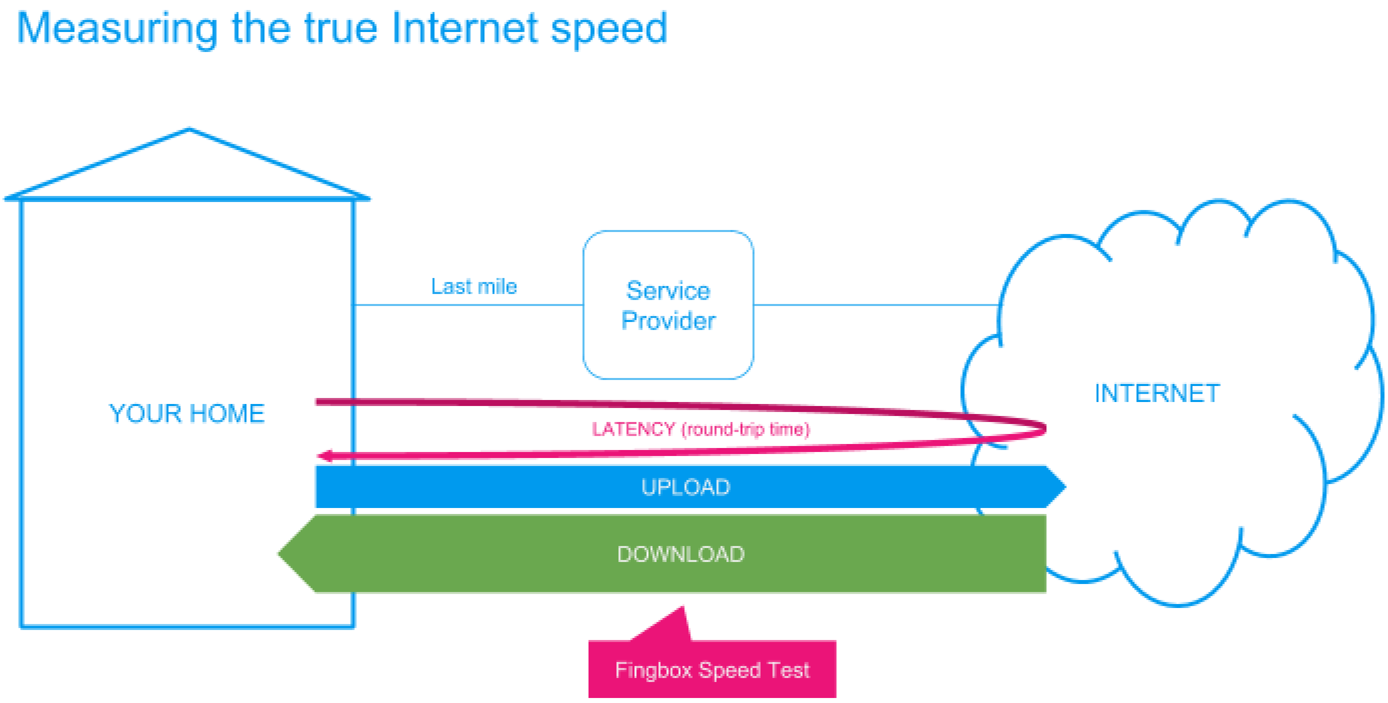
See the next diagram to have a better idea:



- The **Wi-Fi test** (green line) is all done within your home: it measures a data stream flowing between the Fingbox and the phone you're using to run the Fing app. Data flows through your home wireless and wired infrastructure. It accurately measures the Wi-Fi speed at the location of your phone. You can run the Wi-Fi test from different rooms and see where sweet and dark spots are located. This WiFi test is not affected by the speed of your service provider connection. Its results depend on the performance of your Wi-Fi access point, the local intensity of the Wi-Fi signal and the level of interference from other Wi-Fi systems nearby.
- The **Internet speed test** (yellow line) runs between the Fingbox and a test server located in an Internet data center as close as possible to your home. Because Fingbox is wired, this test is not affected by your home Wi-Fi. Of course, if someone is using a significant portion of the Internet connection, the test results may be affected. So, to have the most accurate measure, it's better to **run the Internet speed test when no other devices are using Internet significantly** (for example watching a video, uploading pictures or sending a large email attachment).

Internet Speed Test

The Internet Speed Test measures how fast your service provider connects you to the big "global" Internet. We selected M-Lab as the best partner to run this type of speed test because M-Lab has test servers in most of the important Internet Exchange points around the planet. It's right where most of the online services and connectivity providers run their systems. Moreover, M-Lab has a scientific approach without any commercial bias.



Other Internet speed tests you may find online, typically measure the speed between you and the service provider's network. We call this approach a "last mile" test. It is a valid approach to verify that your provider is honoring the speed promised in your contract. But it doesn't tell the whole story on how fast you can watch movies, send large attachments or make HD video calls with your grandchildren (or nieces), because these services are typically outside the network of your Internet provider (think sending a package on the other side of the world: you ship it at the local post office but the Postal Service will choose someone else to deliver it outside of the country. How good is this someone? And what delivery speed class has been asked by the Postal Service?)

With this Fingbox test you'll find out if your Internet provider is selling you a 100 Mbit/s "last mile" connection, but takes you to the Internet backbone with less (very, very common, especially during prime time, because to be economically viable, the service provider applies some degree of "overbooking" to the expensive Big Internet connection).

The Fingbox Internet Speed Test

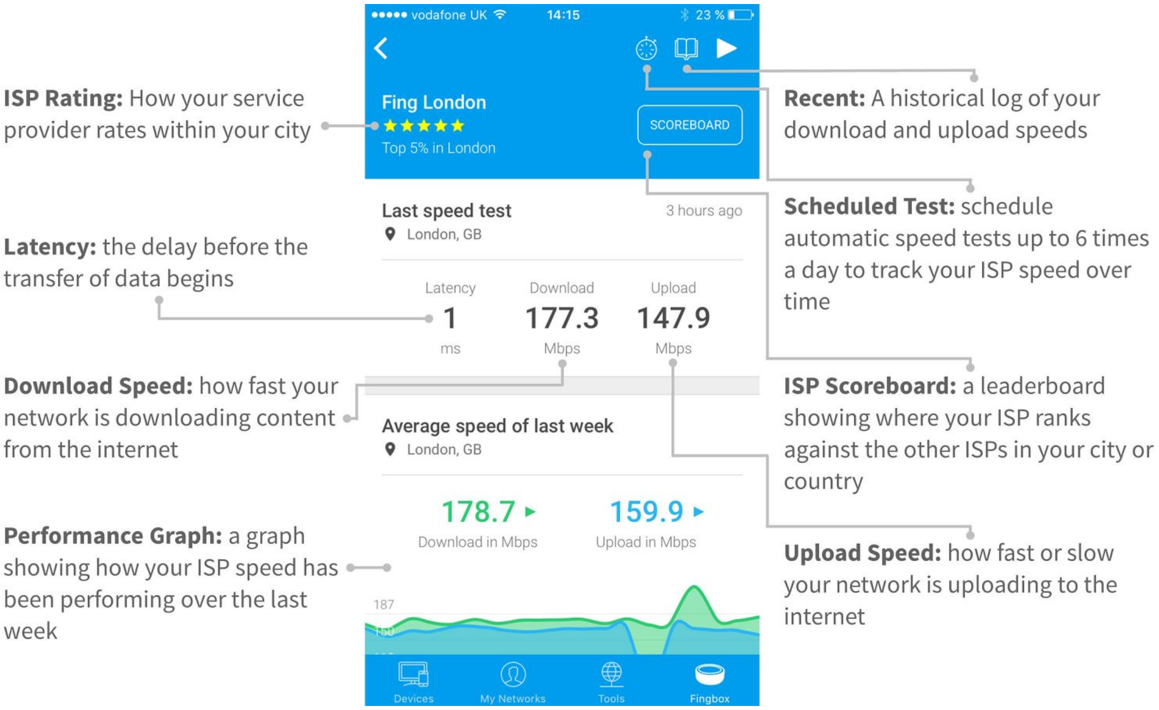
The Internet Speed Test shows how well your Internet Service Provider connects you to the big "global" Internet. The Internet Speed Test is made up of:

- **Latency** - This measures the time needed to send a short message to the test server and receive it back. This **round-trip time** is measured in milliseconds (1/1000th of a second). **The lower the better.** Values under 20 ms are great for hard-core online gamers. In general, values under 60 ms are acceptable for general use. Values above 100 ms can impact the comfort of an audio/video call and add some slugginess to interactive applications.
- **Download** - This measures how fast you can **fetch data** from the Internet backbone. The value is expressed in Megabits-per-second.

  > 1 Mega**byte** = 8 Mega**bit** - For example, if you measure a speed of 8 Mbps (Megabits per second) you can download one Megabyte of data in 1 second or one Gigabyte in 1000 seconds (16 minutes). Sorry for this silly math!

- **Upload** - This measures how fast you can **send data** to the Internet backbone. It's expressed in Mbps (Megabits per second).
- **Recent -** A table with a historical overview of your download, upload speed and latency. Values diverging from usual readings are boxed in red (worse than usual) or green (better than usual).
- **ISP Scoreboard -** a leaderboard showing where your network and your ISP rank against the other ISPs in your city, state or country.
- **Test scheduling -** schedule automatic speed tests up to 6 times a day to track your ISP speed over time.

- **Performance Graph -** a graph showing how your ISP speed has been performing over time.



ISP Rating: How your service provider rates within your city

Latency: the delay before the transfer of data begins

Download Speed: how fast your network is downloading content from the internet

Performance Graph: a graph showing how your ISP speed has been performing over the last week

Recent: A historical log of your download and upload speeds

Scheduled Test: schedule automatic speed tests up to 6 times a day to track your ISP speed over time

ISP Scoreboard: a leaderboard showing where your ISP ranks against the other ISPs in your city or country

Upload Speed: how fast or slow your network is uploading to the internet

How to Run an Internet Speed Test

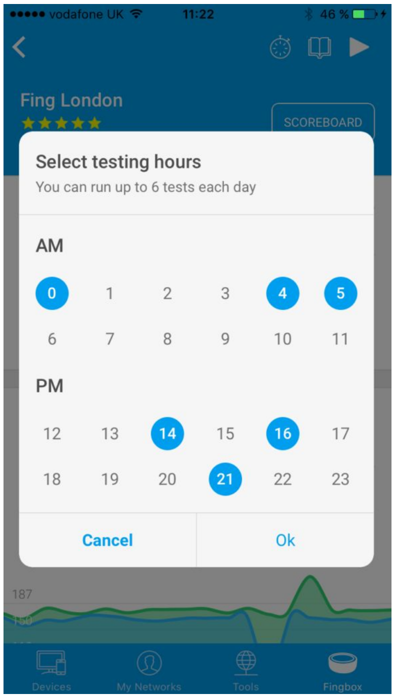
- From the Fingbox dashboard click on “Internet Speed” – this will take you through to the Internet Speed Dashboard (pictured above)
- For iOS, click the triangular Play icon in the top right-hand corner of the screen (bottom right on Android)
- Fingbox will automatically start running the test to give you your current latency, upload and download speeds (the test typically takes 30 seconds).

How to Schedule Internet Speed Tests

Automated Internet Speed tests are set as a default for all Fingbox users, so if you wish to remove them or change their schedule you will need to do the following:

- On the Internet Speed Dashboard, tap on the stopwatch icon in the top right-hand corner
- Select the daily hours, either AM and/or PM, that you would an automatic speed test to run. Deselect all to remove the automated speed tests.
- The speed test will then take place within the hour you have selected. **Note: The reason you cannot select exact times to run a speed test is because Fingbox needs to**

randomize the execution during that hour in order to make sure the M-Lab servers are not overloaded by too many concurrent requests.



Select testing hours

You can run up to 6 tests each day

AM

● 0	1	2	3	● 4	● 5
6	7	8	9	10	11

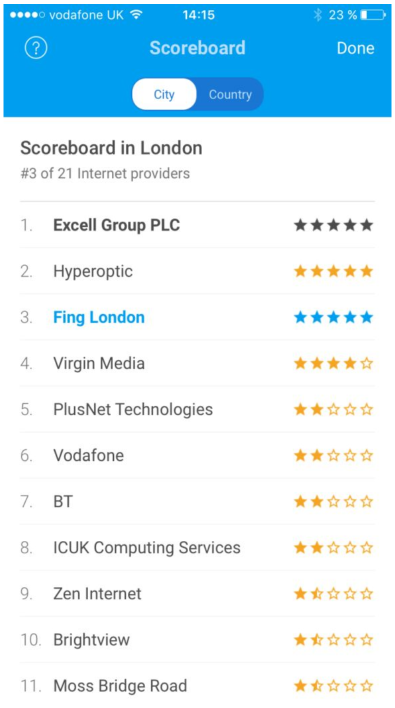
PM

12	13	● 14	15	● 16	17
18	19	20	● 21	22	23

- You can run up to 6 automatic tests a day
- Once you have selected the hours click OK

How to Check Where Your ISP Ranks

- On the Internet Speed Dashboard, tap on Scoreboard
- Here you will see a list of how **your own network**, highlighted in **blue**, and **your ISP's average**, in bold **black**, compare to others in your city. Your network name and ranking are visible to you only.
- Tap the Country label at the top to see how your ISP compares on a national level (this applies only to certain countries, you may not see the city/country switch in your territory).
- You can also tap on any of the ranked ISPs to see further statistics about that provider (maximum and average speeds as well as the ISP market penetration showing the popularity of the ISP in your area).



Scoreboard in London

#3 of 21 Internet providers

1.	**Excell Group PLC**	★★★★★
2.	Hyperoptic	★★★★★
3.	**Fing London**	★★★★★
4.	Virgin Media	★★★★☆
5.	PlusNet Technologies	★★☆☆☆
6.	Vodafone	★★☆☆☆
7.	BT	★★☆☆☆
8.	ICUK Computing Services	★★☆☆☆
9.	Zen Internet	★⯪☆☆☆
10.	Brightview	★⯪☆☆☆
11.	Moss Bridge Road	★⯪☆☆☆

What is the Science Behind the ISP ranking?

The Fing servers create ISP scoreboards by using Internet speed and quality measurements taken from the Fing app and the Fingbox units. The final rank is an easy to read summary of aggregated percentiles, z-scores and other statistics, grouped by geographical area and ISP.

Wi-Fi Performance Test

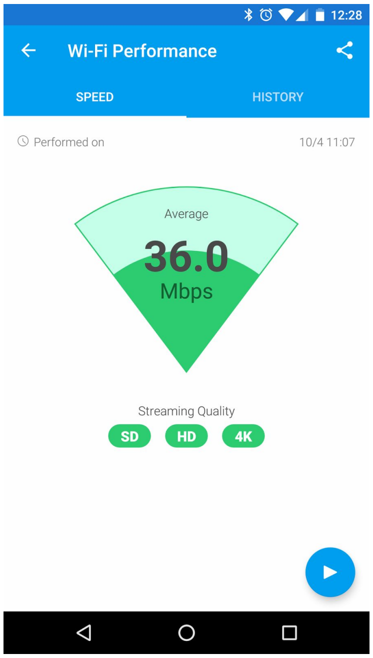
The Wi-Fi performance test measures the speed between the Fingbox and your phone (where you're running the Fing app).

The Wi-Fi signal (good) and the radio interference (bad!) vary from place to place across your house. The speed measured by this test is specific for the location where you are with your phone. For this reason, it's a good idea to **initially run this test very close to the Wi-Fi access point**. You'll likely get the maximum speed with the best signal and use this value as a reference to evaluate how speed decreases in other rooms and find the "dark" spots.

To run the Wi-Fi test, tap on the "play" arrow. You can stop the test at any time after you see a stable value (fluctuating within ±1 Mbps). The measured value will be memorized in the HISTORY section.

The Streaming Quality scale is just a hint to show that the measured Wi-Fi speed can support standard definition, HD or 4k-UltraHD streaming.

After this first “close-up” measurement, move to another room and re-run the Wi-Fi test. Fingbox will remember all the tests you run. You can access them in the HISTORY section.



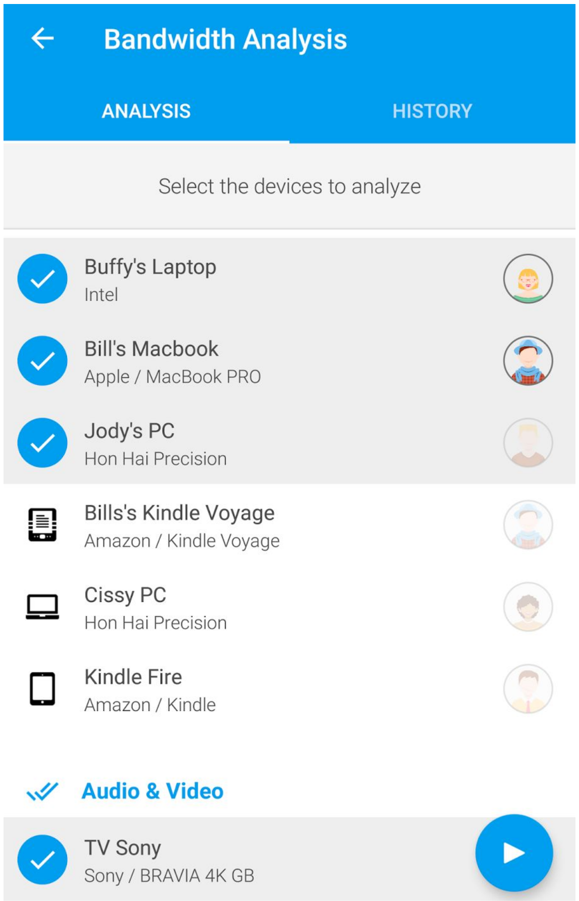
Bandwidth Analysis

If you still have “slowness” issues and you ruled out the Internet provider and the Wi-Fi performance, let’s try to find out who or what is using the bandwidth.

The Bandwidth Analysis tool can tell you how much bandwidth is being used by a device and how much traffic has been generated by each device while the test is running.

First, select the devices you want to monitor for bandwidth consumption. You can select a few of them (the usual suspects?) or you can select whole categories such as Personal devices, Audio & Video equipment, Home Office or Smart Home gear.

Start the analysis by tapping on the button with the “play” triangle. In a few seconds, Fingbox will start counting the packets each device is sending or receiving.



Bandwidth Analysis

ANALYSIS HISTORY

Select the devices to analyze

✓	Buffy's Laptop Intel	
✓	Bill's Macbook Apple / MacBook PRO	
✓	Jody's PC Hon Hai Precision	
	Bills's Kindle Voyage Amazon / Kindle Voyage	
	Cissy PC Hon Hai Precision	
	Kindle Fire Amazon / Kindle	

Audio & Video

✓	TV Sony Sony / BRAVIA 4K GB	▶

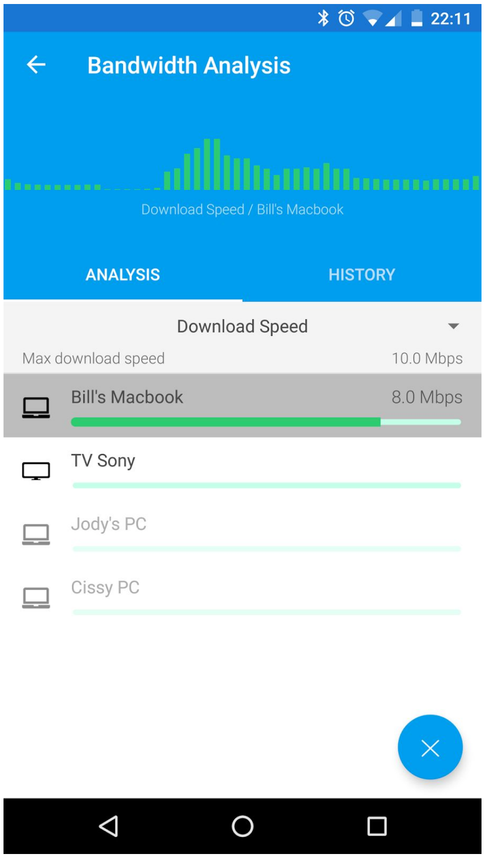
The devices will be **continuously sorted** by Download Speed. You can switch to other criteria by tapping on the small arrow near the Download Speed label. The available sorting criteria are as follows:

Download Speed - the download bandwidth used by the device, expressed in **Megabit/sec** (average of the last 5 seconds)

Upload Speed - the upload bandwidth used by the device.

Download Size - the cumulated amount of data downloaded since the test was started. Expressed in **Megabytes**.

Upload Size - the cumulated amount of data uploaded since the test was started.



22:11

Bandwidth Analysis

Download Speed / Bill's Macbook

Download Speed

Max download speed 10.0 Mbps

Bill's Macbook 8.0 Mbps

TV Sony

Jody's PC

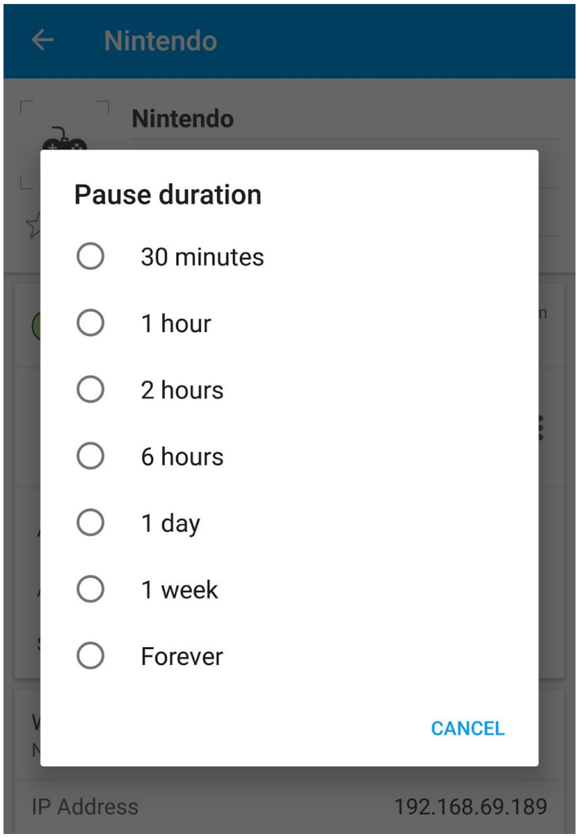
Cissy PC

Tapping on a device will show a **chart** of the measured value over time for the device. The chart is updated every second. You can tap on other devices to see their time chart of the last minute.

Stopping the bandwidth hogger

Once you find the device (or person) that is hogging your bandwidth, you can *politely* ask to stop doing that and finally upload your huge slide deck (and then go watch Game of Thrones).

If you are *not in the mood*, you can use Fingbox to “pause” the Internet access for the hogging device. Go to the Devices screen, tap on the device you found with the Bandwidth Analysis and then tap on Pause Internet. You can choose for how long you want to pause it, so you don’t need to remember to manually restore the connection.



Nintendo

IP Address 192.168.69.189

Megabit/sec vs. Megabytes

Talking about **network speed** and **cumulated data traffic** has a good analogy with your **car speed and traveled distance**.

Car speed is expressed in miles-per-hour or kilometers-per-hour while **network speed** and **bandwidth** are expressed in bits-per-second or its multiples like Megabit/sec (Mbps).

Traveled distance is expressed in **miles** or **kilometers**. For data traffic we talk about **Bytes** or multiples like kB (kilobyte), MB (Megabyte) or GB (1 Gigabyte = 1024 MB).

Internet Security Check

The Internet Security Check looks for potential vulnerabilities on the *public* side of your Internet connection.

Such vulnerabilities can be rooted into devices and applications that, to work well, need to be *exposed* directly on the public Internet.

It’s perfectly normal to expose home devices if they are designed to securely work on the public Internet, such as surveillance cameras and game consoles or applications like Skype and

BitTorrent. Unfortunately, many devices and applications have software defects that, when exposed to the Internet, may put your network at risk of unauthorized access. We strongly recommend that you regularly update the software of all the devices and applications you want to expose. Fingbox Security Check helps to be aware of what gets exposed to the Internet.

If you're not familiar with concepts like IP routing and port forwarding, you can read the following section "Meet the router".

Meet the router

Your home network is connected to the Internet through a special device called ***router***. It acts as the ***default gateway*** used by all the other devices and software applications to reach services and computers over the Internet. Your router has usually two "sides", technically called interfaces: an **internal interface** (typically labeled LAN) facing your home network and an **external interface** (sometimes labeled WAN or Internet), connecting to your Internet service provider (directly to cable, DSL, fiber or wireless or indirectly via a modem device). Your router is the bridge between the global internet and your home.

The external interface will be assigned by your provider a **Public IP address.** This is the equivalent of your home address in the global internet, used to deliver data to your devices.

Your devices on the other hand will be assigned **Internal IP Addresses** not visible from the outside world. The size of your internal network (ie. how many internal devices can be addressed) is called a **Subnet**. A typical subnet is 255.255.255.0 and it can include up to 254 devices. Internal IP addresses can be assigned manually or by a service called **DHCP Server** which often runs on the router itself.

The router acts as a forwarder of data between your devices on the internal interface and the global internet on the external interface via a process called **NAT** (Network Address Translation).

Router with integrated WiFi

If your router also acts as the **WiFi access point**, the WiFi network is typically attached to the internal interface and all the wireless devices will usually be in the same subnet as the ones *wired* to the ethernet ports of the router.

Guest WiFi

In case your router offers the (wise) option of creating a **"guest" network**, it's important to note that it is completely separate from your home network. Technically, the guest network is a dedicated subnet, with its own dedicated "internal" router interface and network address numbers. Typically a guest device cannot access devices on your home network (and this is a security best practice: you can offer your guests free Internet access without having them looking around your cameras, computers, personal files or, worse, your router!).

DMZ

If your router offers the DMZ functionality (De-Militarized Zone!), it’s good to know that devices you attach to the DMZ will be exposed to the Internet but usually cannot access the internal network. In this way, if they get compromised, the malicious attacker should remain confined to the exposed device, without an easy route to your home systems and data. Consult the router manual to know more about the DMZ configuration when available.

Port forwarding

One important role of the router is to control the traffic between the internal and the external worlds.

Typically, in a basic setup, all the internal devices can reach any destination on the Internet, but nothing from the Internet can reach an internal device (except for *answers* to communications *initiated* by an internal device such as requesting a web page). In this way, your router protects your devices from unauthorized access attempts coming from literally anywhere in the world.

Sometimes, certain internal devices may act as a server and need to be reached from the Internet in order to provide the information they generate. For example, **surveillance cameras** have a built-in video server that you can reach only when you are in the internal home network (not very useful). If you want to see the video feed from outside and the camera manufacturer doesn’t provide a cloud service, you need to expose the camera to the public Internet. To do this, your router provides the **port forwarding** service. **Game consoles** may need port forwarding for multi-player online gaming. **Skype**, **WhatsApp** and other similar communication tools may need port forwarding to allow bi-directional chats with audio and video. **BitTorrent** may need port forwarding to communicate with more peer nodes and speed up file transfer.

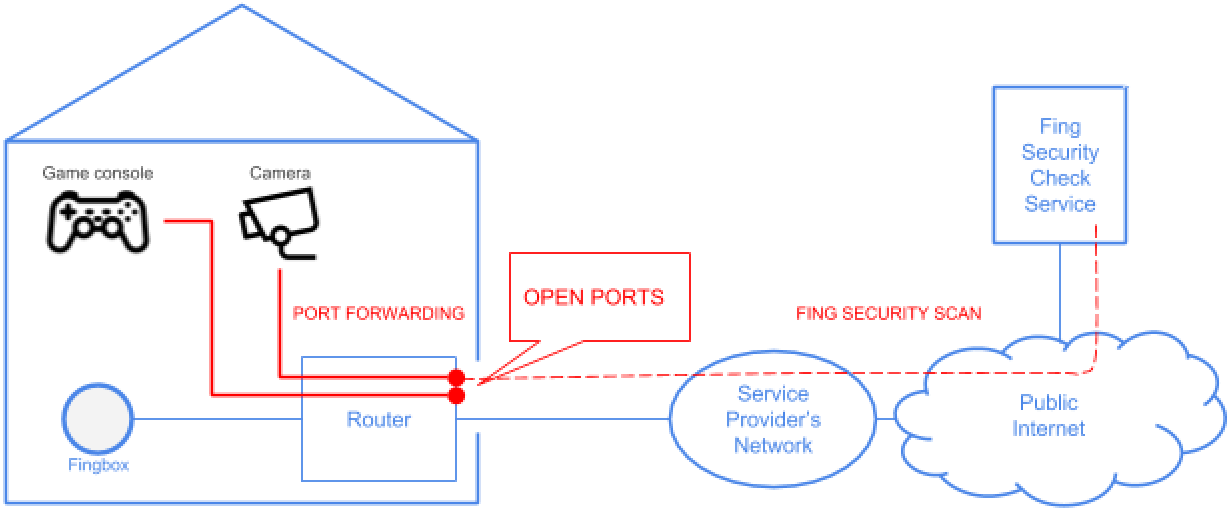
UPnP and NAT-PMP

Port forwarding can be configured manually or **automatically** whenever the applications need it. Manual configuration is typically done via the router configuration web page or mobile app. For automatic port forwarding, many routers offer services like UPnP and NAT-PMP that applications can use to open the ports they need.

Unfortunately, UPnP and NAT-PMP do not ask for any authorization to open the ports; for this reason malicious applications can use them to expose the network to the Internet, gain unauthorized access or leak information. For example, a malware may ask the UPnP router service to expose a Windows PC or a surveillance camera with a software vulnerability.

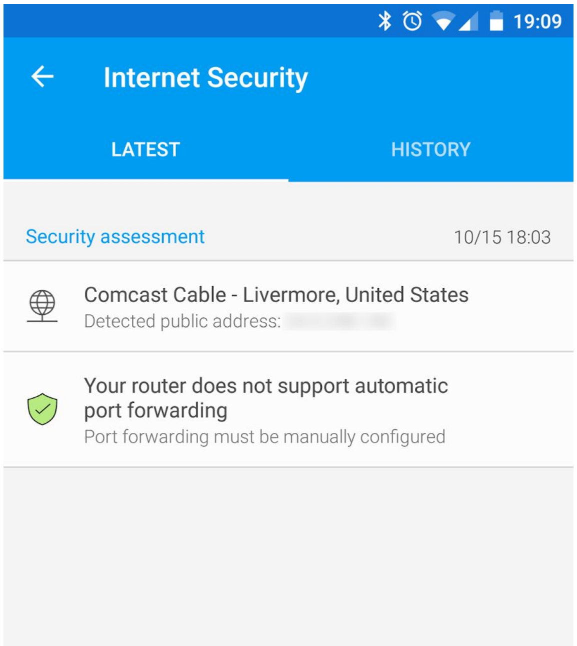
This lack of access control makes UPnP and NAT-PMP as potential security hazards. Many security-concerned users prefer to turn off these services from their router configuration.

Internet Security Check - Conceptual Diagram



Security check results

Clean check result - In the example below, you can see a "clean" check result. The check found **no open ports** and the **router doesn't allow applications to forward ports without user control**. It shows the Internet service provider, the public IP address as detected by the Fing Service and the city associated to this IP address as declared by the service provider.



Internet Security

Security assessment 10/15 18:03

Comcast Cable - Livermore, United States
Detected public address: [redacted]

Your router does not support automatic port forwarding
Port forwarding must be manually configured

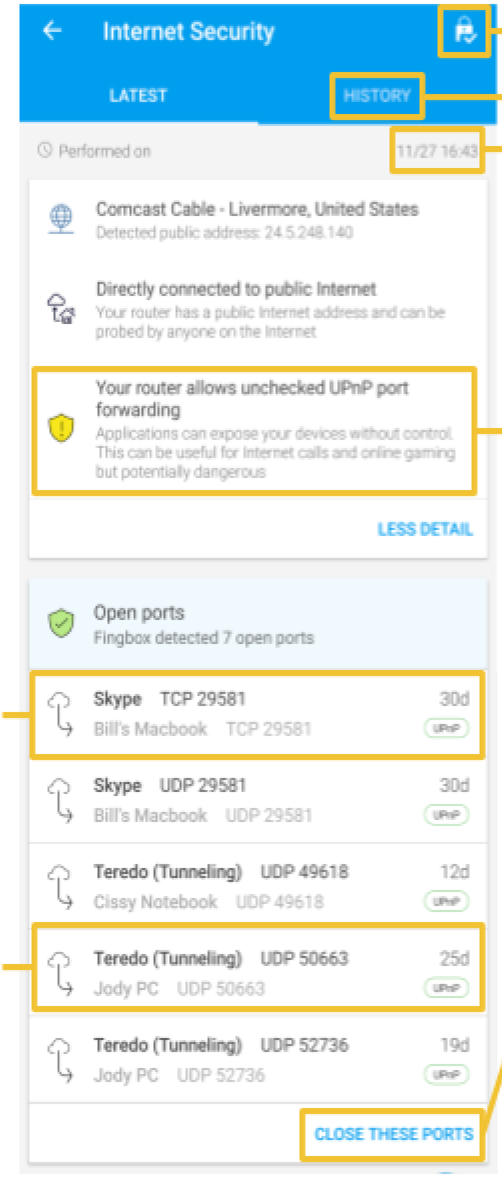
Open ports found - In the following example, the Security Check found 15 ports exposed to the public Internet. It also shows a router with a firewall that is explicitly rejecting connection attempts from the external side (green shield). You can see that this router allows applications to freely setup port forwarding without any control (yellow shield).

Scrolling down you can see the list of the open ports (left side). Wherever possible, the right side shows the internal device receiving the forwarded traffic coming from the Internet.

The Internet Security Report

Here is an example of an Internet Security report.

To manually refresh the report, tap on the blue round button in the bottom-right corner. The full refresh and the scan of all the 65,535 ports, may take up to 10 minutes.



Performed on 11/27 16:43

Comcast Cable - Livermore, United States
Detected public address: 24.5.248.140

Directly connected to public Internet
Your router has a public Internet address and can be probed by anyone on the Internet

Your router allows unchecked UPnP port forwarding
Applications can expose your devices without control. This can be useful for Internet calls and online gaming but potentially dangerous

Open ports
Fingbox detected 7 open ports

Skype	TCP 29581	30d
Bill's Macbook	TCP 29581	UPnP
Skype	UDP 29581	30d
Bill's Macbook	UDP 29581	UPnP
Teredo (Tunneling)	UDP 49618	12d
Cissy Notebook	UDP 49618	UPnP
Teredo (Tunneling)	UDP 50663	25d
Jody PC	UDP 50663	UPnP
Teredo (Tunneling)	UDP 52736	19d
Jody PC	UDP 52736	UPnP

Manually close ports using UPnP.

See the previous reports.

Date and time of this report.

This router allows applications to open ports without any control. Most of the consumer routers come with UPnP port forwarding and it's perfectly normal. If you want to have full manual control, you can disable UPnP.

A typical port forwarding set by a video call application.

Another port forwarding, likely set by an online game using a tunneling service.

Tap here to attempt closing all the UPnP ports listed above. Some routers may not allow it: ports must be closed from the device that requested them. In this case, restart the router to clean them.

Frequent questions about Internet Security Check

The report shows old information

The Internet Security Check runs automatically every 7 days. The time of the last check is displayed in the top-right corner of the Internet Security Check screen.

You can run it immediately by tapping on the round blue button in the bottom-right corner.

The refresh and the full scan of 65,535 ports will take up to 10 minutes to complete.

The report doesn’t list all the ports I know are open

Fing Security Check scans all the 65,535 ports for TCP and UDP protocols. However, the firewall on your router, or your service provider’s firewall, may detect this as a “burst” scan attack and temporarily ban the Fing scanning server. The Fing scanner applies all the modern techniques to avoid detection (as a malicious attacker would do) but router manufacturers and service providers have smart people doing their job! Good news for your security.

I see UPnP-mapped ports pointing to devices that are no longer in my network

This may be because the applications that asked the mapping didn’t clean up or crashed before being able to do it. In most cases, these “stale” mappings can be manually cleared using Fingbox:

- tap on the **small lock icon** in the top-right corner
- select the ports you want to close
- Tap on the red lock button in the bottom-right corner
- Fingbox will attempt to close the selected ports and then re-run the security check; it may take up to 10 minutes to complete.

If the manual closure doesn’t work, try restarting your router (this is actually good news: the router doesn’t allow Fingbox to close ports requested by other devices; for these routers, only the original requester can ask to remove a port forwarding).

Security Alerts

Fingbox continuously monitors your network looking for suspicious events. Every time that something is detected, it will send you an alert and record the event in the recent events journal accessible from the Dashboard. Here is a list of events generating security alerts, the Fing team is at work to add more coverage every time that we learn of a new type of attack or security threat.

New device found (MAC address never seen before)

A new device has joined your network. You have the choice to acknowledge or block the device. It's good practice to name and assign any new device as soon as they join the network.

New or malicious Wi-Fi Access Point

A new Wi-Fi access point is using your Wi-Fi network name (SSID) but with a BSSID that has never been seen before.

If it's a new Access Point you just replaced or added to your home, **you can acknowledge** this message: open the Recent Events screen and **tap on this event**.

If you just installed Fingbox, this can happen as Fingbox learns the BSSIDs over time. If you have **multiple access points** and **multiple Wi-Fi names** on the same network, you can speed up this learning process. For each Wi-Fi network, connect your phone to Wi-Fi and run a manual scan from the Devices screen; Fingbox will notice you're in the same LAN and will add the BSSID to the list.

If you have **multiple access points** advertising the **same Wi-Fi name**, turn off Wi-Fi on your phone, go very close to an access point and turn on the Wi-Fi; usually it will connect to the closest access point. Run a manual scan and Fingbox will learn the BSSID.

If you're not in any of the above situations, then a malicious wireless access may have been installed near your network without authorization, with the intent of inducing your devices to connect and try to steal your data.

In this case, shut down your network and change the Wi-Fi password immediately. Make sure you're using WPA2-only with AES or CCMP encryption (no WEP, no WPA, no mixed WPA/WPA2, no TKIP) and the password is 16 character long and look as random as possible (don't use pets or people's names, birth dates or anything that is connected to your personal life).

And if you can, don't give guests and visitors access to your main Wi-Fi network: use a Wi-Fi access point that is capable of creating a Guest Wi-Fi with WPA2 encryption, a separate password and network confinement.

A WiFi station is being attacked

Fingbox is detecting an abnormally high frequency of Wi-Fi de-authentication messages.

This can be due to a couple of causes:

1. One or more of your **access points are not working properly** and are continuously telling clients to disconnect. Try restarting your access points and see if the alerts stop coming.

2. Your network is getting a real **Denial of Service (DoS) attack** with a flood of de-authentication messages. These messages are telling your devices to immediately disconnect from the Wi-Fi access point. Because of this attack, your network performance becomes very unstable and slowed down. Unfortunately, the Wi-Fi standard makes networks vulnerable to this attack and there is not much to do.

Evil Twin attack

Fingbox detected a Wi-Fi “Evil Twin”: a malicious Wi-Fi access point acting as a “clone” of another legitimate access point but on a different radio channel. It has been installed near your network without explicit authorization. Attackers intent may be of inducing your devices to connect to it and then intercept your data.

Default gateway has changed (different MAC address for network gateway)

Fingbox noticed that the MAC address of the default gateway has changed. Because the default gateway (i.e. the router) is a critical connectivity element, this is an important check.

If you installed a new router, just acknowledge this alert.

If you didn't change your default gateway, then check immediately all the connections to see if there is any “alien” equipment attached to any part of your network.

This may be a man-in-the-middle attack, where a computer is acting like a default gateway, intercepting your traffic before sending it to the Internet via the legitimate router.

New open ports found (Only if the port was not seen open in the previous 2 months)

The Internet Security Check scanned the external side of your router and found an open port that was not seen open for the last 60 days.

Please check your router and NAT configuration for port forwarding: review the port forwarding rules and remove the unneeded ones.

If UPnP or NAT-PMP are enabled on your router, devices and applications can automatically bypass the firewall to allow incoming connections without additional control or authorization.

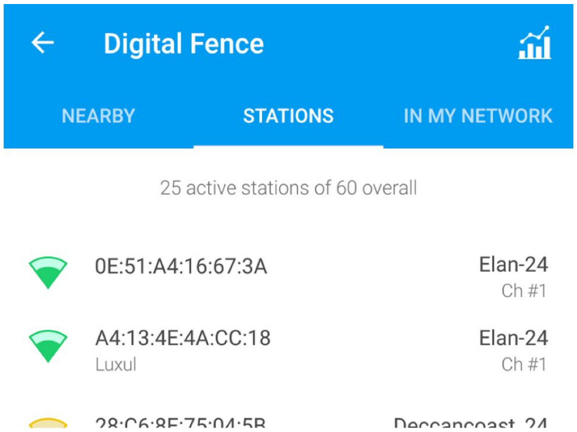
For more details and to see the full list of open ports, open the 'Internet Security' section in the Fing app.

A Wi-Fi station is being attacked

A very common way to start an attack via Wi-Fi is by forcing the client devices to detach from the current “legitimate” access point and reconnect to a “rogue” one. This is a very common attack, usually performed in coffee shops, hotels and public places (if you often use such public WiFi services without Wi-Fi encryption, we suggest you activate a high quality VPN service like ProtonVPN or similar, before turning on the Wi-Fi). This attack is also popular in office places where the Wi-Fi password is one and shared among all users (versus Wi-Fi authentication with personal credentials).

After the deauthentication attack, clients typically reconnect to the access point with the stronger signal. For this reason, the rogue access point “shines” in the radio spectrum.

Immediately after receiving the Fingbox alert, open the Fing app, go to the **DigitalFence** screen and tap on **STATIONS**. At the top of the list you should see your access points plus another one claiming the same Wi-Fi network name (SSID). In the example below, the first access point is the rogue one, claiming the same SSID.



25 active stations of 60 overall

0E:51:A4:16:67:3A — Elan-24 Ch #1

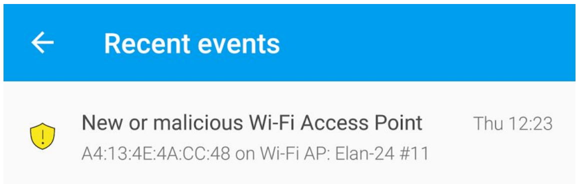
A4:13:4E:4A:CC:18 Luxul — Elan-24 Ch #1

28:C6:8E:75:04:5B — Deccancoast-24

New or malicious Wi-Fi Access Point

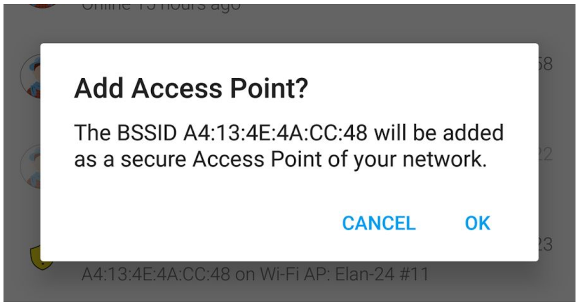
When a **new access point** appears on the network, Fingbox will log this event as a **potential risk** (yellow shield).

An attacker may add an access point to induce client devices to connect and intercept their traffic looking for access credentials or valuable information (typical Man-in-the-middle approach). This technique also allows the attacker to serve fake web pages inducing people to enter their credentials voluntarily (this approach is called phishing).



New or malicious Wi-Fi Access Point — Thu 12:23
A4:13:4E:4A:CC:48 on Wi-Fi AP: Elan-24 #11

If you added this access point, tap on the event and acknowledge by tapping OK.

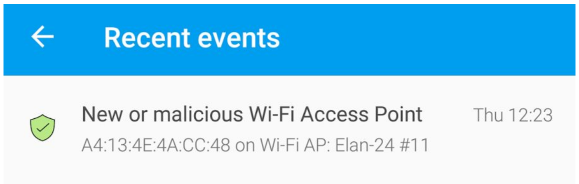


Add Access Point?

The BSSID A4:13:4E:4A:CC:48 will be added as a secure Access Point of your network.

A4:13:4E:4A:CC:48 on Wi-Fi AP: Elan-24 #11

Fingbox will confirm and mark the event as SAFE (green shield).

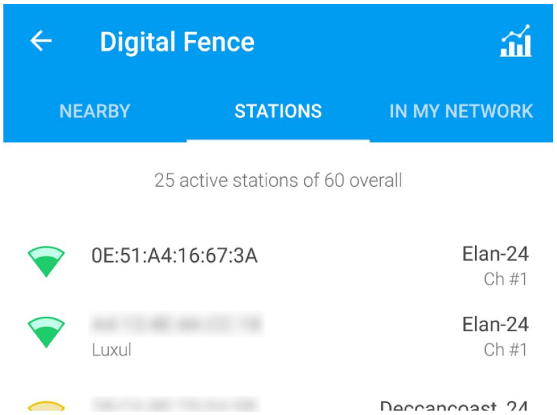


Recent events

New or malicious Wi-Fi Access Point — Thu 12:23

A4:13:4E:4A:CC:48 on Wi-Fi AP: Elan-24 #11

If you didn't add this access point, you can open the Fing app, go to the **DigitalFence** screen and tap on **STATIONS**. Stations are sorted by signal strength; at the top of the list you should see your access points plus another one claiming the same Wi-Fi network name (SSID). In the example below, the first access point is the rogue one, claiming the same SSID "Elan-24".



Digital Fence

25 active stations of 60 overall

0E:51:A4:16:67:3A — Elan-24, Ch #1

[redacted] Luxul — Elan-24, Ch #1

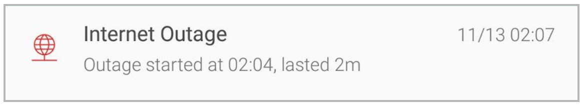
[redacted] — Deccancoast_24

If you're reasonably sure that this is a Wi-Fi attack and this is a rogue access point, you may decide to shut off your network (at least turn off the router and the internal servers) and look around for the radio signal transmitted by the rogue access point. If it is within your premises, you can use a Wi-Fi radio scanner to look where the signal is at the maximum level (it means you're physically close to the access point antenna). However, consider that sophisticated attackers may use high-power directional antennas from nearby positions outside your house or office.

Internet Outage

Fingbox and the Fing Service monitor the availability of your Internet connection.

Every interruption of the Internet connection is registered in the Recent Events section together with the time and duration of the interruption.



Internet Outage 11/13 02:07
Outage started at 02:04, lasted 2m

The Fing Service is able to detect Internet Outages even if the Fingbox is disconnected and unreachable.

DigitalFence

Every **device with a Wi-Fi radio** periodically sends messages to explore the nearby space, looking for known networks. Fingbox has a **built-in Wi-Fi antenna** that “senses” all the Wi-Fi devices in a range of about 30 meters (100 feet). This feature allows to map the surroundings in terms of other Wi-Fi access points (or stations) as well as client devices that are not connected to the local network (such as neighbors or people and vehicles just passing by your house).

DigitalFence maintains three lists of detected devices:

Nearby - devices that are active but are not connected to the local network managed by Fingbox.

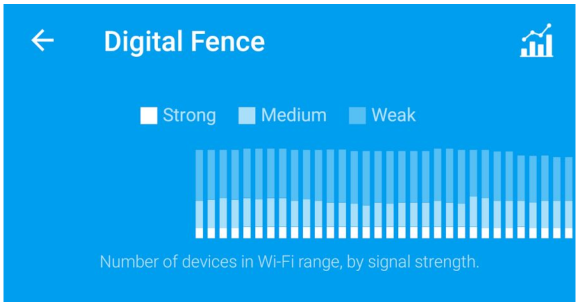
In my network - devices that are active and are connected to the Wi-Fi of the local network managed by Fingbox.

Stations - Wi-Fi access points in the vicinity, sorted by signal strength.

Nearby devices are usually described with **less accuracy** than devices connected to the local network. This is because they are not accessible to Fingbox device scanner and there are less information to recognize device type, brand and model.

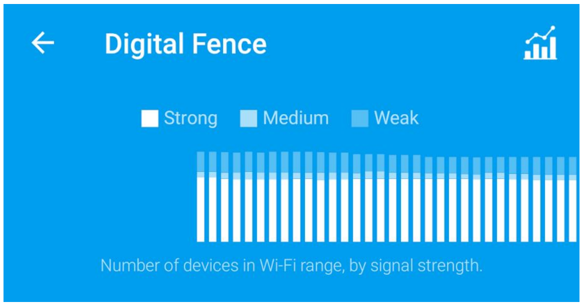
Device density by distance

You can have a rough idea of whether the majority of wireless devices is nearby or far away from the Fingbox Wi-Fi sensor. Tap on the chart icon in the top-right corner to see a bar chart of the device number grouped by signal strength. Signal strength (strong, medium, weak) is a good indication of how far the device is from the Fingbox. The chart adds a new bar every 5 seconds.



Number of devices in Wi-Fi range, by signal strength.

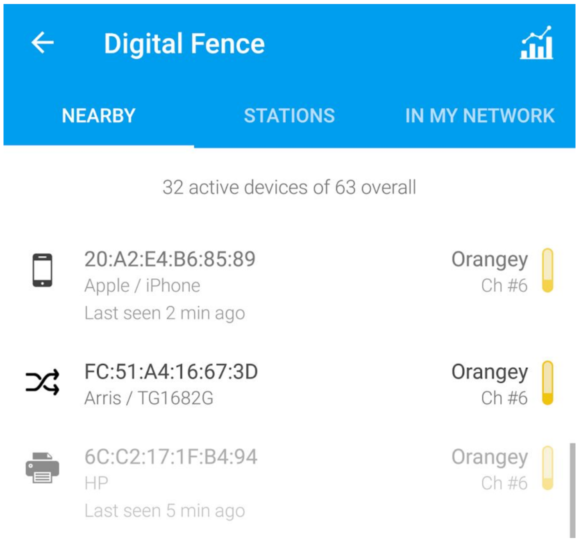
Typical home - Majority of the devices “outside” the fence (white portion of each bar)



High-density office - Majority of the devices “inside” the fence (white portion of each bar)

Monitoring off-network devices

With DigitalFence you can **“watch” Wi-Fi devices** even when they are not connected to your network. In this way you can detect the presence of a device **without giving away the Wi-Fi password**. You can also get **alerts when they come in the vicinity** of your house (aha! a digital fence!).



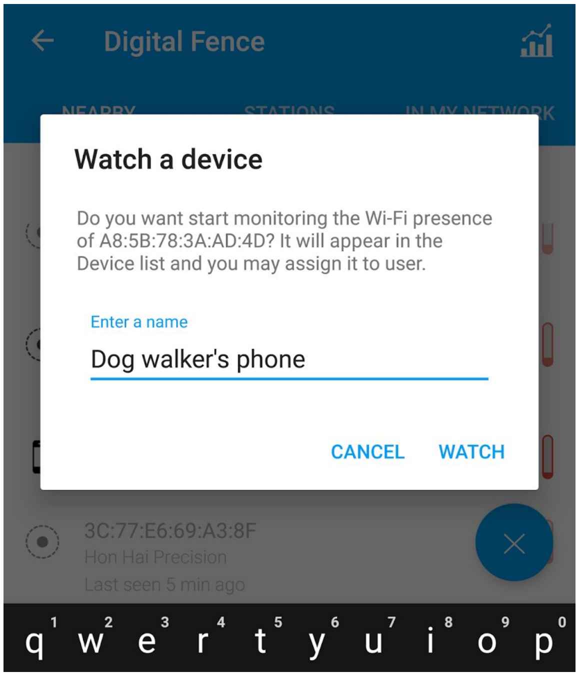
32 active devices of 63 overall

20:A2:E4:B6:85:89
Apple / iPhone
Last seen 2 min ago
Orangey
Ch #6

FC:51:A4:16:67:3D
Arris / TG1682G
Orangey
Ch #6

6C:C2:17:1F:B4:94
HP
Last seen 5 min ago
Orangey
Ch #6

For example, if you have dog walkers coming regularly to your house, you may want to be warned if they come at unusual times. You can open DigitalFence (NEARBY section), tap on the element representing the dog walker's phone and add it to the watchlist, with an appropriate name.



Digital Fence

NEARBY STATIONS IN MY NETWORK

Watch a device

Do you want start monitoring the Wi-Fi presence of A8:5B:78:3A:AD:4D? It will appear in the Device list and you may assign it to user.

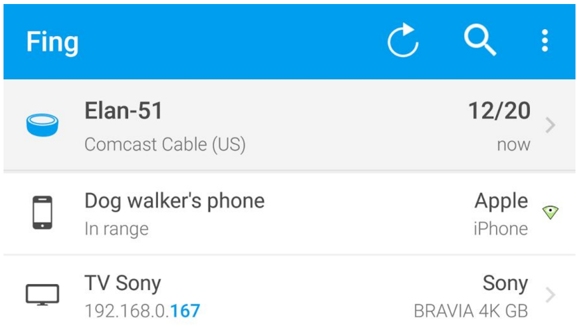
Enter a name

Dog walker's phone

CANCEL WATCH

3C:77:E6:69:A3:8F
Hon Hai Precision
Last seen 5 min ago

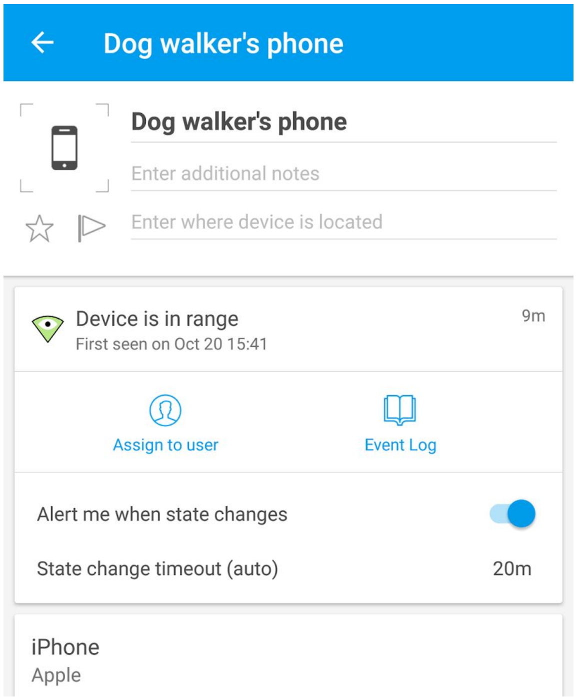
When the dog walker's phone is nearby, it will be displayed in the main Device List as "in range". The small green triangle to the right means that the device is not connected to your network, it's just nearby.



Fing

Elan-51 Comcast Cable (US)	12/20 now
Dog walker's phone In range	Apple iPhone
TV Sony 192.168.0.167	Sony BRAVIA 4K GB

If you want to receive alerts every time this device gets “in range” you can simply tap on it and set the usual setting “Alert me when state changes”.



Dog walker's phone

Dog walker's phone

Enter additional notes

Enter where device is located

Device is in range 9m
First seen on Oct 20 15:41

Alert me when state changes ●

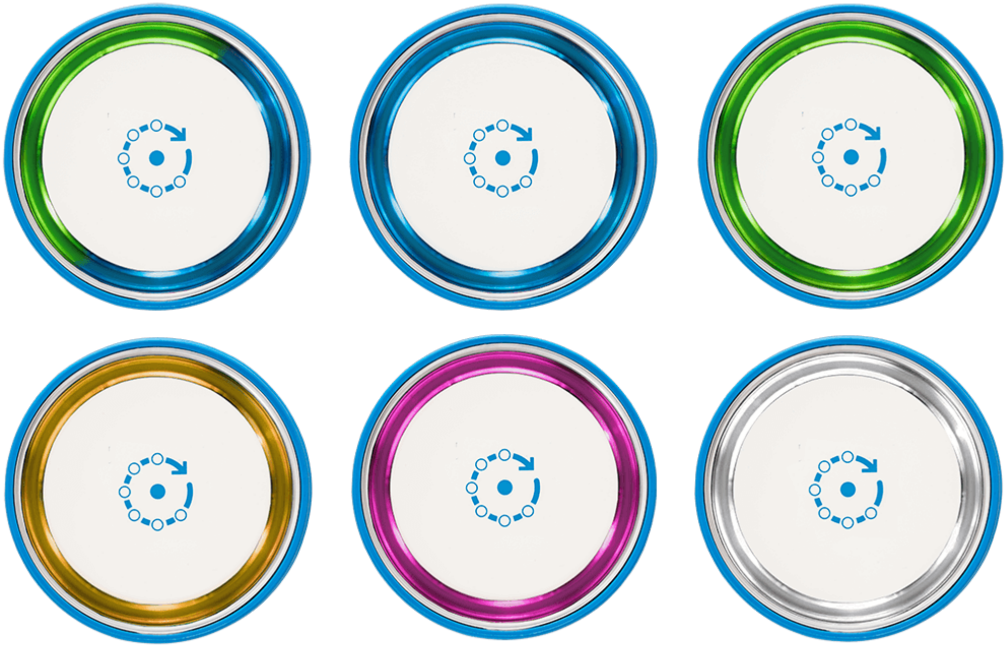
State change timeout (auto) 20m

iPhone
Apple

Top circle lights

The top circle of Fingbox is made of six multicolor lights dancing in patterns to express the current condition of Fingbox.

If you want to dim the brightness, please read the section about Fingbox Settings.



COLOR	MOTION	MEANING
White	Single light, steady	Fingbox is powering up
Green	Full circle, pulsing	Ready for activation
Green	Spinning clockwise	Internet Speed Test - Downloading
Blue	Steady, dark pulse every 3 seconds	Normal condition
Blue	Half-circles, alternating	New device detected! Open the Fing app and check the Fingbox screen to acknowledge or block the new device.
Blue Green	Spinning clockwise	Bandwidth Analysis is running
Blue	Spinning counter-clockwise	Internet Speed Test - Uploading

Blue	Opposite lights spinning clockwise	Wi-Fi Performance Test running
Blue	Sides pulsing	DigitalFence sensing
Blue	Sides pulsing	Configuration change received
Pink	Steady, dark pulse every 3 seconds	Security alert! Open the Fing app and check the Fingbox screen and the Event Journal
Orange-Red	Pulsing	Internet unreachable for more than 5 minutes. Check cables and router/modem. Try to power off->on Fingbox and router.
Yellow	Spinning clockwise	Fingbox is updating its firmware

Thank you!

Thank you for your time and your attention. We’re honored to have you as our customer and user. For questions about this guide and to report errors, please write an email to support@fing.io

The Fing Team