Table of Contents

Getting Started
1) Unboxing Fingbox .................................................................p3
2) Downloading the Fing App ......................................................p3
3) Setting Up Your Fingbox ..........................................................p3
4) LED Lights: Meanings and Settings ..........................................p4
5) Main Tabs ..............................................................................p5

The Features
6) Protection Tools
   a. Device Inventory ...............................................................p5
   b. Device Blocking ...............................................................p6
   c. Setting Up Alerts .............................................................p6
   d. Network Vulnerability Test ................................................p9
   e. WiFi Intrusion Protection ..................................................p10

7) Performance Tools
   a. Bandwidth Analysis ..........................................................p11
   b. WiFi Performance Test ......................................................p11
   c. Internet Outage Recording ................................................p12
   d. Internet Speed Test ..........................................................p12

8) Other Tools
   a. DigitalFence™ .................................................................p13
   b. Digital Presence ...............................................................p14
   c. Recent Network Events ....................................................p15
   d. Internet Pause .................................................................p16

9) Fingbox Business Beta Only Features
   a. DNS Filtering Protection ....................................................p18
   b. Content Filtering .............................................................p19
Getting Started

Unboxing Fingbox

Fingbox components include:
- 1x Fingbox
- 1x network cable
- 1x power cable
- Power adapters: US, UK, EU, and AU (included in all Fingboxes)
- 1x instruction manual
- Fingbox packaging

Downloading the Fing App

Download the Fing app for free on iOS and Android.
- Fing for iOS is available on the App Store
- Fing for Android is available on Google Play

Creating an Account

- Launch the Fing App on your device.
- Click the cog icon in the top right-hand corner of the screen
- Click SIGN IN at the top of the page and you will be taken through an account creation screen.
- Create an account using an email address and password, Google+ or Facebook
- A confirmation email will be sent to your email address. Click the confirmation within this message to activate your account.
Alternately you can also create an account using the Fing web app

Setting Up Your Fingbox

Fingbox is very easy to set up. It’s designed to be completely plug & play.
1) Pass the cables through the hole in the blue casing
2) Plug the cables into the white casing
3) Afterward, put the white casing back inside the blue casing

4) Plug the power cable into the wall
5) Plug the Ethernet cable into your router—after a minute the lights on top of your Fingbox should turn green
6) Open the app and click on your icon in the top right-hand corner. The screen below should appear.
7) Click *Add a Fingbox* and follow the step-by-step process to configure your Fingbox.

8) Once configured the lights on top of your Fingbox should turn blue.

### Fingbox LED Legend and Meanings

<table>
<thead>
<tr>
<th>Color</th>
<th>Motion</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>White</td>
<td>Single light</td>
<td>Powering up</td>
</tr>
<tr>
<td>Green</td>
<td>Pulsing</td>
<td>Ready for activation</td>
</tr>
<tr>
<td>Blue</td>
<td>Steady/Continuous</td>
<td>Normal Operation. This is the new LED quiet mode which is enabled by default during onboarding.</td>
</tr>
<tr>
<td>Blue</td>
<td>Half-circles alternating</td>
<td>New devices detected: open Fing app (4th tab) to recognize or block them!</td>
</tr>
<tr>
<td>Blue Green</td>
<td>Spinning CW</td>
<td>Bandwidth Analysis running</td>
</tr>
<tr>
<td>Blue</td>
<td>Spinning CCW</td>
<td>Internet Speed Test (uploading)</td>
</tr>
<tr>
<td>Green</td>
<td>Spinning CW</td>
<td>Internet Speed Test (downloading)</td>
</tr>
<tr>
<td>Blue</td>
<td>Opposite lights spinning CW</td>
<td>WiFi Speed Test</td>
</tr>
<tr>
<td>Blue</td>
<td>Sides pulsing</td>
<td>DigitalFence sensing</td>
</tr>
<tr>
<td>Blue</td>
<td>Sides pulsing</td>
<td>Change received (e.g. when blocking a device)</td>
</tr>
<tr>
<td>Pink</td>
<td>Steady, dark pulse every 3s</td>
<td>Security Alert! Please open the app (4th tab) and check</td>
</tr>
<tr>
<td>Orange/Red</td>
<td>Pulsing</td>
<td>Internet unreachable for more than 5 minutes. Please check Fingbox cable and ISP modem/router</td>
</tr>
<tr>
<td>Yellow</td>
<td>Spinning CW</td>
<td>Upgrade in progress</td>
</tr>
</tbody>
</table>

### Dimming or Turning Off Fingbox LEDs

Dim or turn-off Fingbox lights by opening the Fing app and:

- Clicking on your icon in the top right-hand corner
- Click Fingbox settings
- Move the slider on the *LED Brightness* setting to adjust brightness
- Use *Do Not Disturb* to keep the lights low and only brighten when attention is required
Main App Tabs

When you login to the Fing app, you'll see 3 main tabs (at the very bottom of the screen). Here's a quick snapshot of what each of the tabs does.

- **Devices**: This tab shows you your device inventory (i.e. all the devices seen by Fingbox)
- **Network**: This tab contains all the tools to protect and troubleshoot your network
- **People**: From the People tab you will access Digital Presence (who is on the network and when they came and went), The Digital Fence, Device Blocking, Internet Pause. You will also be able to access all Restricted devices and all Internet Pause schedules which are in place.

The Features – Security Tools

Devices Inventory

Visit the “Devices” tab where you’ll see all the devices which have connected to your network. Your devices will be displayed with details including:

- **Name**: The name the device has been given. For example; Violet’s MacBook.
- **Type icon**: What kind of device it is. For example, mobile, tablet, computer, TV, VoIP phone.
- **Vendor**: The maker of your device. For example, Apple.
- **Model**: The generation of the device. For example, MacBook PRO.
- **IP address**: The numeric identifier assigned to the device on this network. Usually, it’s temporary and can change over time, typically assigned by the DHCP service running on the Internet router.
- **MAC address**: This is the serial number of the device which is set when the device is made at the factory. Note that the MAC address of the device is only displayed if the model information is not available.

Device Tab Icons:

At the top of the Devices Screen, each icon represents an action that can be completed.

- **CIRCLE icon**: runs another Fing scan
- **DROP DOWN icon**: you can easily switch between networks
- **AVATAR**: access account settings
- **BURGER icon (3 lines icon)**: allows you to sort/filter your devices list

Sorting Your Device Inventory

Click on the 3 lines icon in the top right of the device list. This will bring up a pop-up menu.

From here you can select to either:

- **Search**: look for specific device in the list
• **Export:** export a list of your devices to an Excel spreadsheet  
• **Clear devices:** clear all devices so you can start from scratch with your device scanning  
• **Order By:** arrange the list by one of the various device elements  
• **Filter By:** filter the list down to just certain devices  
• **Alerts:** set up alerts on your devices so you can be notified if new devices join your network since your last scan.

**Device Blocking**

Fingbox includes a simple (yet groundbreaking!) Device Block feature which acts as a form of network security and parental control.

• **Device Block:** The Device block feature will completely block a device from both internal LAN traffic and Internet traffic. This defends your network against intruders, and it will have an On/Off functionality.

• **Internet Pause:** The Internet Pause feature gives you the ability to pause the Internet connectivity of a device temporarily but still allow connectivity to internal devices. For example; a computer could be paused from the internet but still send something to the printer. This is the perfect simple internet parental control.

• **Scheduled Pause / Parental Controls:** The Fingbox Internet Pause feature lets you schedule Internet Pausing. All of a user’s Devices – the devices which have been assigned to the person – can be paused during specific times or on specific days/times.

**Using the Device Blocking Feature**

This feature is used to permanently block a device from accessing your network.

• Navigate to the “Devices” tab from the bottom menu bar  
• Click on the device you’d like to block  
• Click on block device  
• Confirm you’d like to block the device

**Restricted Devices**

Now, you can see in real time which devices are restricted. These devices can either be blocked devices you selected manually, or paused devices you chose from the scheduled pause.

• Navigate to the “People” tab from the bottom menu bar  
• Scroll down until you reach “Blocked and Paused” - select Restricted Devices

**Setting Up Alerts**

Fingbox includes real-time alerting features for devices in and around your network. Currently, Fingbox provides real-time alerts for:
• **New Device Alerts** (new devices that have connected to your network)
• **Individual Device Status Alerts** (devices that you choose to be alerted to state changes)
• **DigitalFence** (devices that may be outside your network that you choose to be alerted to when in proximity)

Before setting up these alerts you first of all need to allow notifications either to your phone and/or your email account. Follow the steps below.

**Allowing Email Alerts**
To enable email alerts or change how you receive email alerts:

• Visit the web app: [https://app.fing.io](https://app.fing.io)
• Log in with your Fingbox credentials
• Visit “Settings”
• Choose how you would like to receive email alerts

![Email Alerts](image)

**Allowing Push Notifications**
First, on the web app, be sure that the send message option on [app.fing.io](https://app.fing.io) are turned on. This should be on by default, but if you are not receiving push notifications, double check.
Make sure the settings are:

**Send notification as:** A Message for each event

![Push Notifications](image)

After you have enabled this you then need to go to you phone settings. Follow the relevant instructions below.

**iPhone**

• On iOS, go in “My Networks” -> “Account” (icon on the right of the toolbar), so that we can ask permission for push notifications

![iPhone Settings](image)

• To adjust settings from the tab “My Networks”, tap on “Settings” in the top-left corner.
• Tap on “Privacy”
• From here you can access the global alert settings of the app where you can toggle push notifications On/Off
Android

- Go into your device settings (usually a cog icon in the applications menu).
- This may vary from device to device, but click on either APPS or Application Manager, and then Fing
- Click on Notifications and then make sure “Allow Notifications” is on.

Setting Up Your Different Types of Alerts

**New Device Alert Settings:**

- On the Devices tab, click on the 3 horizontal lines icon in the top bar.
- On the pop-up click Alerts.
- At the top of the alerts page, under ALERTS ON NEW DEVICES, you can then select ‘First seen on network’ to get alerts when new devices join your network.
- You can also select ‘At every change’ to set a default Device Status alert on new devices, meaning you will be alerted whenever they join and leave the network moving forward.
- Click SAVE to save your changes and exit the screen.

**Device Status Settings:**

- On the Devices tab, click on the 3 horizontal lines icon in the top bar
- On the pop-up click Alerts
- Under ALERTS ON KNOWN DEVICES you will see a list of your devices. Select them to set a default State Change Alert. This will let you know when the devices joins and leaves the network
- Click SAVE to save your changes and exit the screen
• To adjust the amount of time an individual device is online/offline before you are alerted, head to Devices tab of your Fingbox network
• Click on the individual device from your list that you wish to adjust the timing on.
• Use the State Change Timeout to select how long after a device has gone on or offline for you to get notified. You can also turn off and on alerts here as well.

Network Vulnerability Test

The Network Vulnerability Test automatically runs weekly but you can also perform an on-demand scan. The test is made up of two parts:
• The Remote Scan Test performs a port scan on your public Internet address (the individual numerical address visible to the public when you are online) to see which ports are open to the external world: these are the open doors in your home, and you should make sure to have only the strictly necessary ones open.
• The Internal Router Audit checks the router addresses, the NAT configuration and whether or not UPnP or NAT-PMP is activated. In the house metaphor, this would be the equivalent of checking the security measures placed inside the building in case an intruder did make it through the door.

Where Do I Find the Network Vulnerability Test Feature?
To access the Vulnerability Test you simply click on the Network tab in the bottom middle of the screen. You will find the Vulnerability Test under the Protection segment, with a summary of your latest test.

Understanding Your Vulnerability Test
After a few minutes, you’ll get the results of your Network Vulnerability Test. With the Vulnerability Test, you can see where your router leaves you vulnerable to hacking. This allows you to make the changes required to toughen up your network security against incoming threats.

The Vulnerability Test include:

• Last Test: See when the last test was performed.
• ISP & Public IP: Your Internet Service Provider’s (ISP) information and your public IP address. This is what anyone on the public Internet sees when you connect.
• Firewall Presence: If your router has an activated firewall in it to protect against malware traveling on the network traffic.
• Open Port List: A list of detected open ports. Each row indicates how a service connects to your network so you can investigate why they are open and if they are necessary. You can also close UPnP ports directly from the app.
• On-Demand Scan: the ability to perform scans on demand.
• History: a log of all your previous scans.
• Automatic Port Forwarding: if your router has UPnP or NAT-PMP activated, allowing programs and devices to automatically open ports to the external world. This may sound nice and easy, but can be a major security hazard. Soon as a hacker gets on your network they can then use the UPnP or NAT-PMP protocol to access and control every device on your network.
• UPnP Port Closing: If you have UPnP enabled on your router you can use Fingbox to close your open ports.
Automated Network Vulnerability Tests
The weekly automated Vulnerability Tests are automatically set up when you set up your Fingbox, and so will run weekly around that same time. You cannot edit the automated schedule but you can run on-demand tests (see below). After Fingbox has run its weekly scan, if new ports are open or vulnerabilities are spotted within your router, Fingbox will alert you immediately!

Run an On-Demand Vulnerability Test
To run an on-demand Vulnerability Test you simply click on the refresh icon (curly arrow) in the top right-hand corner of the screen. This will take you through to a progress screen to show you the test is in action. This may take a little while as there are a lot of ports to check.

Closing Opened Ports via UPnP
With the Fingbox you can close ports via UPnP directly from the Vulnerability Test feature. Simply click on the CLOSE button at the top of the open ports list.

WiFi Intrusion Protection

Fingbox’s WiFi Intrusion Protection feature alerts you to attacks on your WiFi, so you can take action to protect your home.

What Attacks Can the Fingbox Wireless Intrusion Protection Feature Spot?
Fingbox tracks devices even before they get a valid network address in your network, making our Wireless Intrusion Protection feature fast to spot potential malicious behavior on your network. Fingbox will alert you to:

- New BSSID with same SSID not in discovery state
- Evil Twin/Rogue Access Point & Main in the Middle Attacks
- Deauth Attacks & WiFi Jamming
- New Gateway Not in Discovery State

What Will Happen If Fingbox Picks Up On An Attack?
Depending on your notification configurations, Fingbox will either send you a push notification and/or an email when an attack is detected.

This alert will tell you what the problem is and how best to deal with it.

For the first 24 hours after the attack is first detected you will also find an alert under the Requires Attention section on the Network tab – this section only appears if a serious network event has taken place.

After 24 hours if they are not detected again they will be automatically dismissed, but you can still access the notification by going to the Network tab and clicking on Recent Events on the top right of the Protection segment.

How Do I Enabled/Disable the WiFi Intrusion Protection Feature?
This feature is enabled by default, but if you wish to change this visit the Network tab and look for Wi-Fi Intrusion Protection under the Protection segment. By clicking on the Enabled/Disabled button on the right you can turn it off and on.
The Features – Performance Tools

Bandwidth Analysis

The Fingbox Bandwidth Analysis feature lets you discover the bandwidth consumption of selected devices. You can use this feature to discover if one of your devices is hogging a lot of bandwidth resulting in a slower internet connection.

Using the Bandwidth Analysis Feature

To use the bandwidth analysis feature, you need to choose the devices which you believe are the bandwidth hogging culprits from your list of devices.

- Click on your “Networks” tab
- Scroll down to the “Performance” section, and select “Bandwidth Analysis”
- Select the devices you believe are the culprits by clicking on them
- Press on the “Play” icon located at the top right corner of the screen, the bandwidth analysis will launch
- Click on the “drop down arrow” to change the analysis between download speed, upload speed, download size and upload size
- If you want to see previous bandwidth history, select on the history tab.

WiFi Performance Test

Fingbox’s Wi-Fi Performance Test is an interactive tool which allows you to find the best spots for WiFi connectivity around your home or office.

Fingbox’s Wi-Fi Performance Test also shows you the streaming quality you can achieve in different locations: SD, HD and 4K.

Use the feature by moving around your home or office and see the speed change up or down based on how good your connection is in any corner of the building. By performing the test next to the router, you can also tell if your router is failing to deliver the speed that was promised by the manufacturer.

Where Do I Find the Wi-Fi Performance Test?

To access the Wi-Fi Performance Test click on the Network tab in the bottom middle of the screen. Under the Performance section, you will see the Wi-Fi Performance Test, with a summary of the results of your latest test.

How to Use the Wi-Fi Performance Test

When you open the Wi-Fi Performance Test it will show you the latest test you performed. To perform a new test:

- Click the “Refresh” icon in the top right-hand corner of the screen
- Now have fun and move around your home or office. As you move you’ll see the Wi-Fi speed change up or down to reflect the quality of your connection in each spot in your home.
- On the lower part of the screen under Streaming Quality, you will see SD, HD or 4K. If these appear in green it indicates your Wi-Fi is able to support these streaming qualities of various media types.
How To Access Your Wi-Fi Performance Log
To access your Wi-Fi Performance Log simply click on History in the top bar. Here you will be able to see all your previous Wi-Fi Performance Tests.

Internet Outage Recording
Fingbox now records internet outages on your network. To see any Internet Outages Recorded on your Network:
• Tap on the Network tab and scroll down to “Requires Attention”
• This will lead to the network event log which will show any Internet Outages
This feature lets you visualize Internet Service Provider (ISP) performance over time.

Internet Speed Test
The Internet Speed Test is designed to give you visibility over the quality of the Internet your Internet Service Provider (ISP) is delivering.

Where to Find the Internet Speed Test
To access the Internet Speed test click on the Network tab in the middle at the bottom. Scroll down to the Performance section and there you will see the Internet Speed test, with a summary of your last test.

What are the Features of the Internet Speed Test?

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 them schedule you will need to do the following:
• On the Internet Speed Dashboard, click 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.
• You can run up to 6 automatic tests a day
• Once you have selected the hours click Ok
• The Performance Graph in the Internet Speed Dashboard will show you the results of your scheduled Internet Speed tests over the past week
• It will also show you your average Internet Speed for the past week
How to Check Where My ISP Ranks

- On the Internet Speed Dashboard, click on Scoreboard
- Here you will see a list of how your own network (FYI, your SSID only visible to you), and your ISP’s average, compares to others in your city
- Click Country at the top to see how your ISP compares on a national level
- You can also click on any of the ISPs to see further statistics about that provider

How to Export Your Internet Speed Test Results from Fingbox

The email reports allows you to export all the data on your Internet performance for the current or last month. This allows you to have something in hand if you would like to report a problem to your ISP.

To receive an email report click on the arrow/paper plane icon in the top right hand corner – this will bring up the option to be sent an email report. You will then receive a breakdown of how your Internet performed over the last month, including daily, weekly and average download, upload, latency and Internet outage results.

The Features – Other Tools

DigitalFence™

What Does the Fingbox DigitalFence do?

The Fingbox DigitalFence is designed to give you visibility over all the WiFi-enabled devices within 15 meters of your Fingbox, even if they are not connected to your network. This feature acts as both an extra security and troubleshooting feature for your network, as well as an additional form of Digital Presence.

- **Security**: people often forget that the physical security of your network is as important as the cybersecurity. Physical access to your router, or the majority of IoT devices in your home, can open easy opportunities for hacking those devices. The DigitalFence allows you to see what devices have come near your Fingbox and set alerts to watch them.
- **Troubleshooting**: have a device that the Internet isn’t working on? The DigitalFence will allow you to see if that device’s WiFi antenna is still working, as well as which SSID and channel it is connected to.
- **Digital Presence**: With the DigitalFence you can look at what is near your Fingbox in real-time and at historical logs of each device that has been in range between set times. You can also select devices to watch and receive alerts when they move in and out of range.

What are the DigitalFence™ Features?

![DigitalFence Features Diagram](image-url)
How to Watch A Device and Set Up Alerts
So, you’ve seen a device that you want to keep an eye on? Well, it could not be more simple!

• Once you have found the device within the DigitalFence, click on the device.
• This will bring up the Device Details Page – from here you will also see a log of that device’s history.
• Click on Watch Device.
• This will bring up a pop-up that gives you the option to name that device, i.e. The Postman.
• Click ‘Watch’ and this will automatically set up the alerts that will tell you when that device moves in and out of range of your Fingbox.
• The alerts will arrive in the same format you have set up for other alerts on your Fingbox (either push notifications, email, or both).
• Once you have selected to watch a device it will then appear in your network Devices List.
• Note: a watched device appearing in your Devices List does not mean it is now connected to your network. It appears here for your convenience so you no longer have to search for it in the DigitalFence. It will say ‘In range’ under it and have a green eye symbol next to it which indicates it is in range of your Fingbox rather than connected to your network.

Digital Presence

Fingbox’s Digital Presence feature enables you to monitor the presence of the people in your home or office. Using this feature, you can set up user profiles and assign devices to your users.

Where Can I Find the Digital Presence Feature?
The Digital Presence feature can be found under the People tab in the bottom right-hand corner of the screen. On the Digital Presence home screen you can see the following things:

Users: See who is currently online and easily access their user details by clicking on their icon

Online Users: The ring is dark grey and the picture is not faded. The number underneath indicates how long they have been on the network

Offline Users: The ring is light grey and the picture faded. The number underneath indicates how long since they were last online

Summary Graph: A summary of the users presence on the current day

Setting Up A New User On The Digital Presence Feature
Setting up a new user on the Digital Presence feature is very easy. Scroll to the right on the user carousel at the top of the Digital Presence page until you see a circle with a cross in it. Under this icon, it should say Add New User – click on this icon.

From here you can add:

• A name for the user
• A photo or icon
• A category they fall under – these categories will be different depending on if you have set up your Fingbox in a home or office environment
• Select the devices on the network that belong to that user
• **IMPORTANT STEP BEFORE YOU SAVE** – for the Digital Presence feature to accurately show when someone is in and out of the home/office, you must set up the PRESCENE device for that user. Please see below.

**What is a PRESENCE Device and How Do I Step It Up?**

A PRESENCE Device in the Digital Presence feature is the device that most mirrors that person’s presence in the home.

A mobile phone, for example, will tend to be on that person 24/7, i.e. when they leave the house so does the phone. This device’s presence on the network therefore accurately represents when that person is in the home. An Xbox, on the other hand, is likely to stay in the home regardless of whether that person is in or not – this device does not mirror its owner’s presence in and out of the home as it may sit connected whilst the owner is away.

So when selecting a PRESENCE Device the question you need to ask yourself is ‘does this device’s presence on the network mirror it’s owner’s presence in the home/office?’

We recommend using a mobile phone as a PRESENCE Device, but you may find a tablet or smartwatch represents that person better.

To select the PRESENCE Device, click on the user in the user carousel and then select Devices in the pop-up. Find the device you wish to turn into the PRESENCE device and click the CHANGE button on the right-hand side of the device. This will then give you the option to state that it always travels with that user. You will then see the CHANGE become PRESENCE.

You can currently only select one device as the Personal Device. Click Save in the top right-hand corner to save your new user.

**Editing or Deleting a User**

To edit a user simply click on their image in the User Carousel. This will bring up a pop-up. Click on Devices and that will take you through to their details screen. Here you to make amendments, including a Delete button in the top right-hand corner of the screen.

**Setting Up Digital Presence Alerts**

You can set up alerts so that you receive a notification when a user’s device comes on or goes offline. This can be handy for things such as knowing if your child has made it home safe whilst you are away from home. Visit the Alerts section to see how.

**Digital Presence Log**

And if that wasn’t all enough, the Digital Presence feature also provides you with a log of the activity of your users moving in and out of your network.

To access the log click go to the People tab at the bottom of the screen and then click on Digital Presence. Fingbox provides a historical overview of all the events that happened on your network.

**Recent Events Logs**

Using the Recent Events feature

• From the Network dashboard, navigate to “Recent Events” on either Protection or Performance
• You’ll get a full log of all the Recent Events which have happened on your network
• Click on any event to see the details of the event
**Internet Pause**

**What is the Fingbox Internet Pause feature?**
The Fingbox Internet Pause feature acts in a similar way to the Fingbox Device Block feature, allowing you to block the Internet from reaching a device or a user. However, instead of cutting off access to the entire network, Internet Pause still allows those devices to communicate with other devices on your network, i.e. you can pause a laptop’s access to the Internet, but it can still send documents to the printer.

There are 3 ways to pause the Internet with Fingbox:

1) **On-Demand Device Pause:** this feature lets you pause the Internet to a single device at the click of a button. You can select a set amount of time to pause it, or unpausing it when you wish.

2) **On-Demand User Pause:** if you have set up the Digital Presence feature, this tool will allow you to block all the devices belonging to one user at the click of a button.

3) **Scheduled User Pause:** if you have set up the Digital Presence feature, this tool will allow you to set up an Internet schedule for your users, with automatic blocking at selected times and days.

**How to Use the On-Demand Device Internet Pause**
Pausing the Internet to a single device is very easy!

**Pausing**
- Go to the **Devices** tab (bottom left of the screen)
- Find the device you wish to block and click on it – this will bring up the Device Details screen
- About halfway down the screen you will see a pause icon with **Pause Internet** underneath it – press this icon
- A pop-up will appear with a selection of time lengths in which you could pause the Internet
- Select your timeframe
- The borders of the Device Details screen will go red to indicate it is blocked

**Unpausing**
If you wish to unpausing the device sooner than the allotted amount of time simply return to the Device Details screen and click the same icon you used to pause it. It will now instead say **Resume Internet**. The borders will return to blue to indicate it is unblocked.

**How to Use the On-Demand User Internet Pause**

**Pausing**
To pause by user:
- Go to the **People** tab (bottom right-hand corner)
- Click on the user you wish to pause
- A pop-up with a big pause button with **Pause Internet** underneath it will appear – click the pause button
- Time length options will come up – select the timeframe you wish to block the user for
• The pause button and the circle around the user’s icon will turn red to indicate that the user’s devices are blocked.

Unpausing
If you wish to unpausethes user sooner than the allotted amount of time simply click on the user again and click Resume Internet. The red will disappear to indicate it is unblocked.

How to Use the Scheduled Internet Pause Feature
The Scheduled Internet Pause tool allows you to set times when your user’s devices will not have access to the Internet, i.e. bedtime. The feature comes with schedule templates that you can customize, but you can also set up your own.

Setting Up, Editing and Deleting an Internet Schedule
1. Go to the People tab (bottom right-hand corner), scroll to the bottom and click on Schedule Pause.
2. Click on the + Sign in the top right-hand corner and choose from the pop-up the type of schedule that you’d like to make.
3. Select the days of the week and times you’d like to set the schedule for and choose the user. For example; schedule Internet Pause Monday–Friday from 3 – 5 PM during homework time. Click Save.
4. From the Schedule Pause section of Fingbox, you can easily see all the schedules that you have active and edit or delete them if necessary.
The Features – Fingbox Business Beta Only

These features are currently only available to our beta testers of Fingbox Business.

DNS Filtering – Threat Protection

The Fingbox DNS filtering Threat Protection feature protects users and their devices from malware, phishing, BotNets and ransomware. With the DNS filtering capability of Fingbox, you can be assured that those on your network can browse the Internet safely and securely.

How is DNS Filtering done?
To allow Fingbox to advertise the correct DNS service to devices on your network, it will need to become the DHCP server, allocating IP addresses to all devices that present themselves on your network.

Once this is active, all traffic to and from the Internet passes through Fingbox which automatically scans the traffic to determine whether the policies are met and the data/content delivered. All this is done in real-time.

Access and restrictions are configured through a whitelist and blacklist, managed through the Fingbox app.

Enabling Fingbox DNS Filtering

Before enabling the DNS filter on Fingbox, you should first disable the DHCP service on your router. It is recommended that any devices configured with static IP addresses are recorded prior to disabling DHCP on your router.

To configure Fingbox as the DHCP server, go to ‘Enable Cyber Security’ under the Network tab, and click 'Automatic Setup'.

Then click ‘Go Ahead’. 
Fingbox will now enable DHCP services automatically. During this configuration step, your Fingbox will assign itself a static IP address and complete a reboot so all settings are effective.

Once the configuration is complete, you can click the button to ‘Enable DNS Filtering’ under the **Network** tab.

Should any other DCHP server be detected by Fingbox after this process, a warning will be shown in the Fing app.

If you are having difficulties with this step please contact us on support@fing.io.

**Managing Your Threat Protection & Disabling DNS Filtering**
To access your Threat Protection feature simply visit the **Network** tab. Under the Protection segment, you will see ‘Threats Blocked’.

If you click on this you will see a summary of the threats that have been blocked by the DNS filtering. To edit your filters, click on **Edit** in the top right hand of the summary screen and it will take you through to the settings screen.

Here you can easily Disable/Enable threat protection, and white or blacklist certain websites. Here you can also completely disable DNS Filtering by clicking on the top right-hand corner **DISABLE** button.

**Content Filtering**

With the content filtering capability of Fingbox, you can be assured that those on your network can browse the Internet safely and securely. When enabled on Fingbox, content filtering can protect users from inappropriate, offensive or undesirable content rather than blocking the domain.
How is Content Filtering done?
To allow Fingbox to advertise the correct DNS service to devices on your network, it will need to become the DHCP server, allocating IP addresses to all devices that present themselves on your network. Once this is active, all traffic to and from the Internet passes through Fingbox which automatically scans the traffic to determine whether the policies are met and the data/content delivered. All this is done in real-time.

Access and restrictions are configured through a whitelist and blacklist, managed through the Fingbox app. For ease of configuration, domains are allocated to categories – for example, all gambling websites are under one category so they all become blocked as a group of sites. You can also provide specific exceptions to the categories where required – for example, you may block social media but then whitelist one specific site from this category to allow access to it.

Enabling DNS Filtering for Content Management
Visit the DNS Filtering section of this guide to see how to enable this.

Managing Your Content Filtering
Fingbox, presents information in the Fing app to allow the user to manage the filtering rules. Visit the People tab and you will find a Content Filtering section.

Here you can easily Block Advertisements and Enforce Safe Search to different levels. You can also manage when websites are filtered by clicking on Sites Analyzed.

Once you have clicked on Sites Analyzed you will see a summary of the websites that have been blocked. Statistics are shown to highlight the top allowed and top blocked sites.

By selecting specific domains, you can review the categories they are associated with. From here, you can also whitelist (allow) or blacklist (block) the domain.

To edit your filtering click on Edit in the top right-hand corner.

All categories are displayed with a description of their purpose to help you determine whether the category should be allowed or blocked. To block them simply click the ‘Disabled’ button next to them and this will change to ‘Enabled’. Make sure to Save your changes!
Any further questions please contact support@fing.io