wightfibre
because we care

For Business

Island call centres, Island staff and Island engineers.

WorkPass User Guide

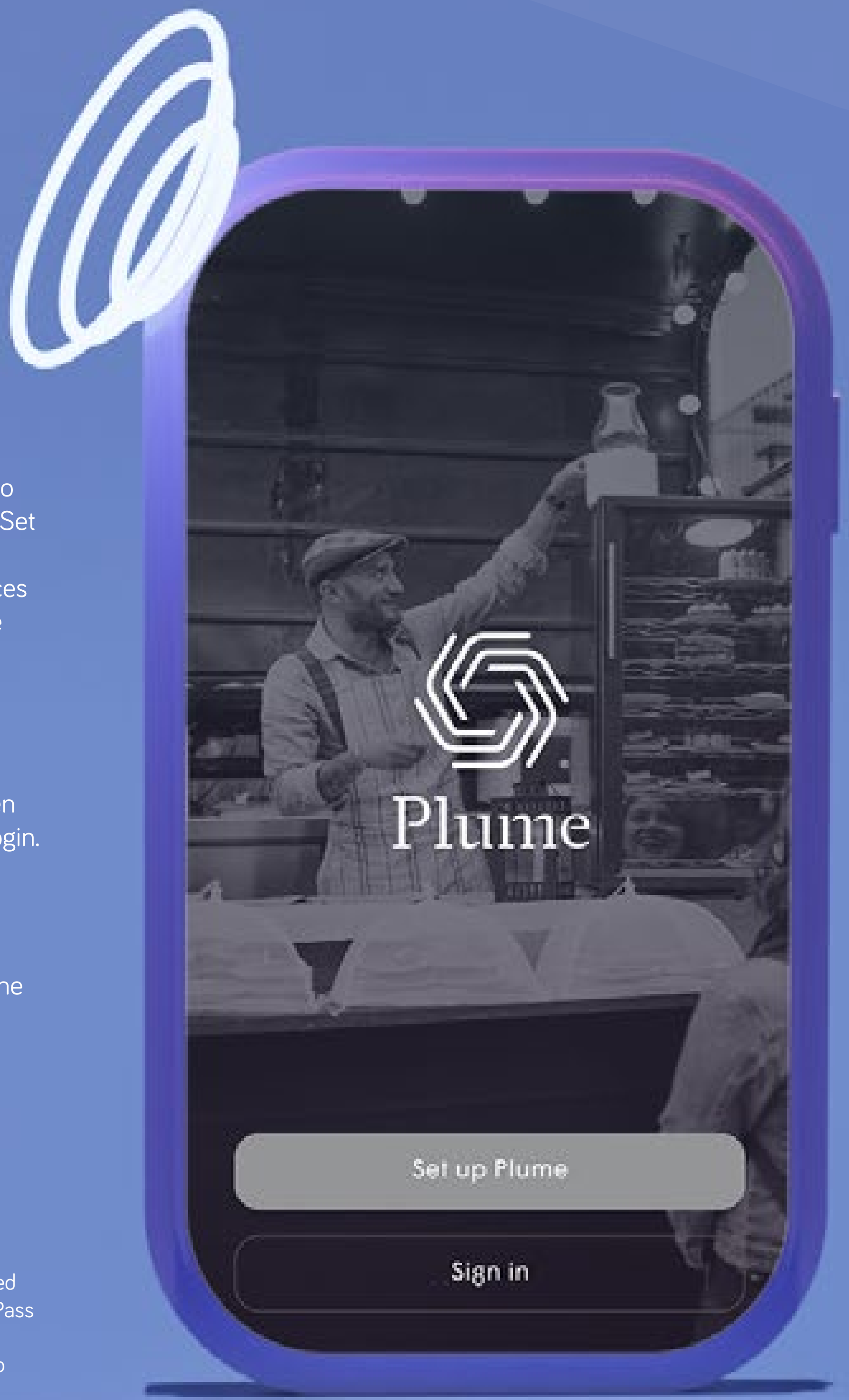
The Perfect Wi-Fi Solution for your Business

Contents

Getting Started with the WorkPass App

Download the WorkPass® by Plume app from either the Google or Apple app stores.

1. On the start screen make sure to choose "Sign in". If you choose "Set up Plume" there may be some issues that our Customer Services team will need to resolve before proceeding further.
2. Use the email address that was given to WightFibre as the account contact address, as this is the address that will have been automatically assigned as the login.
3. A magic link will be emailed to the address. Once you click the verification inside the email, the WorkPass app will progress to the next screens.



Note: If the email address has been used for another service, such as our HomePass residential product, you may need to contact our Customer Services team to resolve any login issues.

Setting Up the Wi-Fi Networks

There are 3 Wi-Fi zones.

Secure Wi-Fi zone

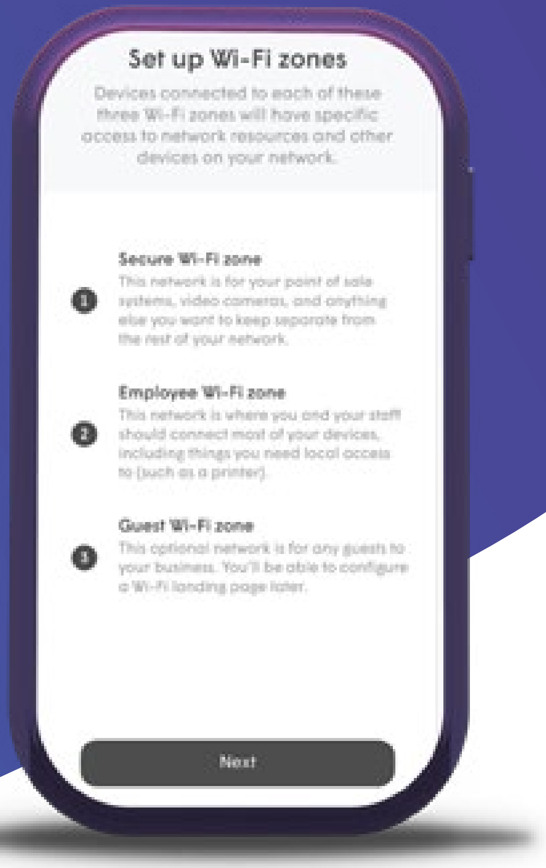
This zone is used for local devices that absolutely need to be kept separated from the rest of the network. For example, office PCs, EPOS/tills etc. Anything plugged into the ethernet on Plume will also be connected to the secure zone.

Employee Wi-Fi zone

This zone can be used for the admin and other staff to connect to the network. Local devices that will be shared will also connect to this zone. Employee devices can be given a timeout, and their primary device can be used to confirm if they're onsite or not.

Guest Wi-Fi zone

This zone is for visitors. Users accessing this zone will use a landing page to log in and will only have access to the internet.



Set up Wi-Fi zones

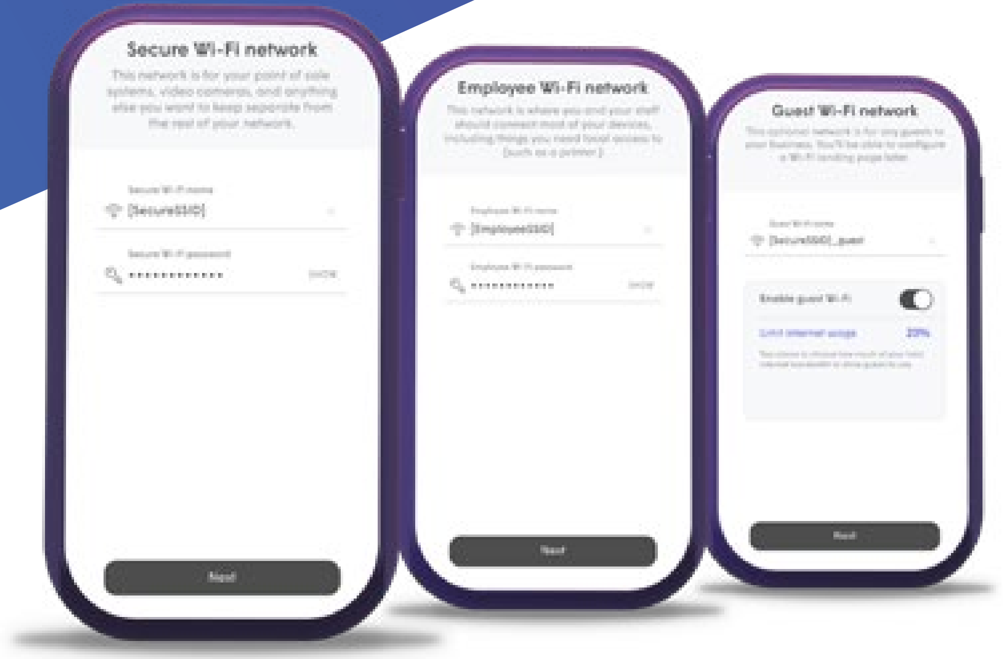
Devices connected to each of these three Wi-Fi zones will have specific access to network resources and other devices on your network.

1 Secure Wi-Fi zone
This network is for your point of sale systems, video cameras, and anything else you want to keep separate from the rest of your network.

2 Employee Wi-Fi zone
This network is where you and your staff should connect most of your devices, including things you need local access to (such as a printer).

3 Guest Wi-Fi zone
This optional network is for any guests to your business. You'll be able to configure a Wi-Fi landing page later.

Next



Secure Wi-Fi network

This network is for your point of sale systems, video cameras, and anything else you want to keep separate from the rest of your network.

Secure Wi-Fi name: [SecureSSID]

Secure Wi-Fi password: •••••••••••• SHOW

Next

Employee Wi-Fi network

This network is where you and your staff should connect most of your devices, including things you need local access to (such as a printer.)

Employee Wi-Fi name: [EmployeeSSID]

Employee Wi-Fi password: •••••••••••• SHOW

Next

Guest Wi-Fi network

This optional network is for any guests to your business. You'll be able to configure a Wi-Fi landing page later.

Guest Wi-Fi name: [SecureSSID]_guest

Enable guest Wi-Fi ●

Limit internet usage 20%

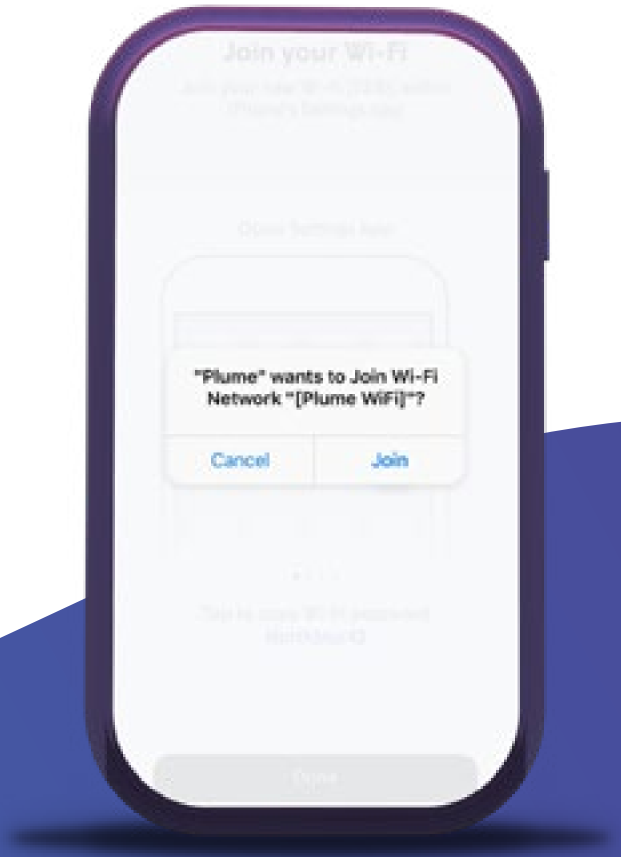
Next

A separate SSID and password will need to be created for both the Secure and Employee zones.

The Guest zone will also need its own SSID, but there is no password required. If the Guest zone is enabled, a percentage of available bandwidth can be allocated for guests.

Once all three zones have been configured, you will be prompted to join the new Wi-Fi network.

- Tapping on Join will take you out of the app and into the Wi-Fi - settings to connect to the Employee Wi-Fi zone.
- iOS users will be prompted to copy the password, while Android users will join automatically
- Once back in the WorkPass app, a Welcome Aboard message indicates that your device is now connected and the new Wi-Fi network is operational.



Join your Wi-Fi

"Plume" wants to Join Wi-Fi Network "[Plume WiFi]"?

Cancel | Join

Home Screen Summary

The home screen provides a summary of events for the past 24 hours, and is a springboard on to all the other features in the app.

Settings

Accesses location settings, including SSIDs, Pods, Shield, Support, More, Account and Advanced Settings menus.

Location

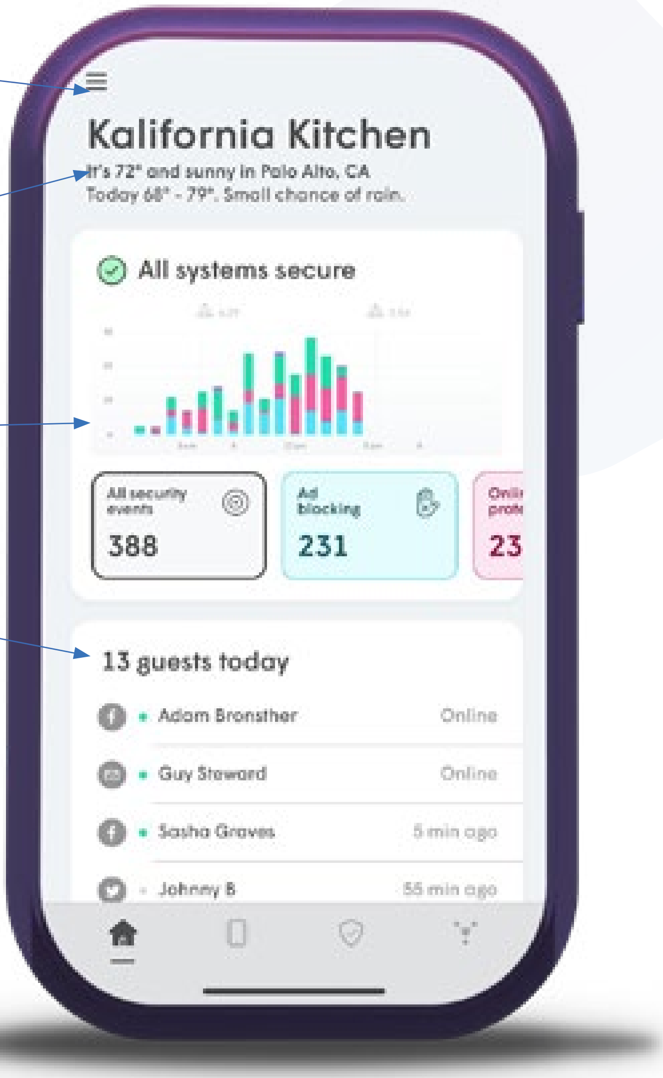
Provides location information, including weather.

Shield Overview

Contains graph of Shield security events, which can be sorted by type.

Guests

Display a list of guests that have connected to the network today.



Kalifornia Kitchen

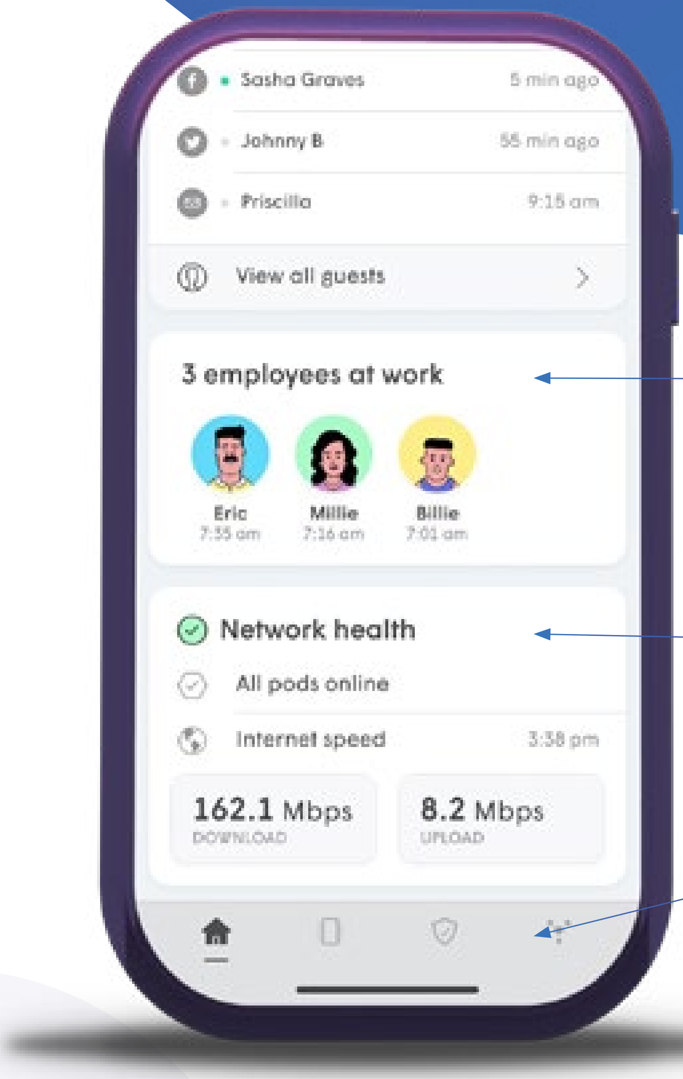
It's 72° and sunny in Palo Alto, CA
Today 68° - 79°. Small chance of rain.

All systems secure

All security events	Ad blocking	Onli prote
388	231	23

13 guests today

Adam Bronsther	Online
Guy Steward	Online
Sasha Graves	5 min ago
Johnny B	55 min ago



Sasha Graves	5 min ago
Johnny B	55 min ago
Priscilla	9:15 am

View all guests

3 employees at work

Eric	Millie	Billie
7:35 am	7:16 am	7:01 am

Network health

All pods online

Internet speed 3:38 pm

162.1 Mbps DOWNLOAD

8.2 Mbps UPLOAD

Employees

Displays employees currently at work (connected), including timestamp of when they arrived.

Network Health Overview

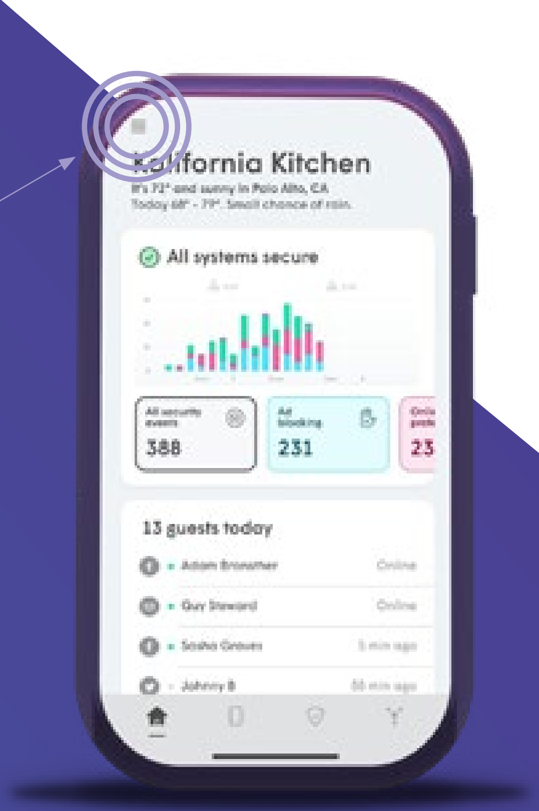
Shows current status of network (pods online) and recent speed test results.

Menu Bar

Switches between Home, Zones, Security and Network tabs.

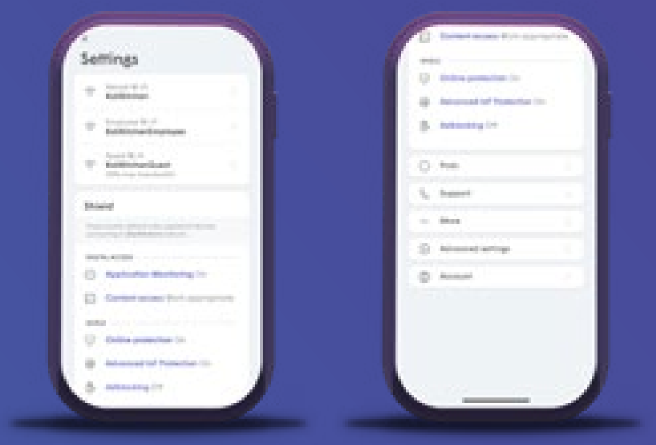
Settings Menu

The settings menu allows configuration of some network settings, and configuration of the Guest Portal. Settings can be accessed from the Home tab using ☰

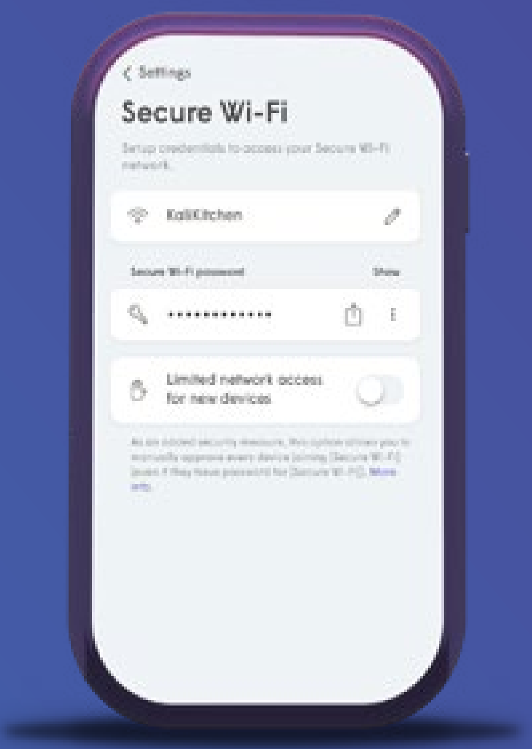


Kalifornia Kitchen
It's 72° and sunny in Palo Alto, CA
Today 68° - 79°. Small chance of rain.
All systems secure
All security events 388
Ad blocking 231
Online people 23
13 guests today
Adam Bronother Online
Guy Steward Online
Sasha Groves 5 min ago
Johnny B 35 min ago

Manage Wi-Fi passwords by tapping the corresponding zone SSID in the settings screen.



Settings
Shield



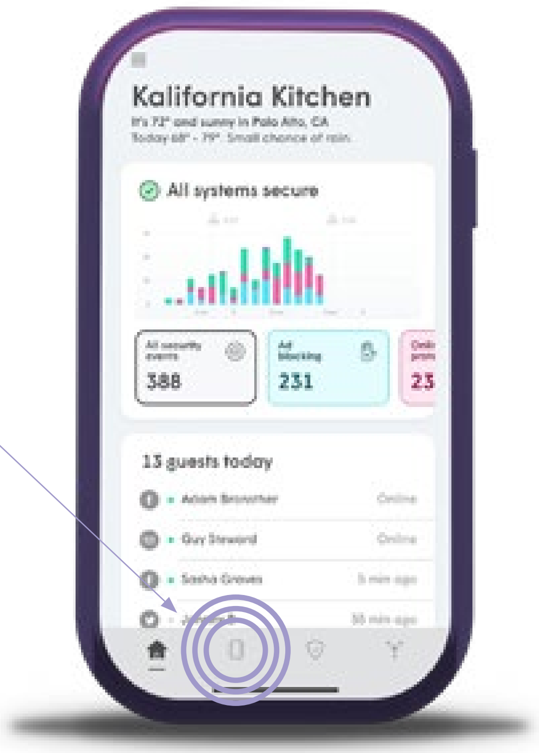
Settings
Secure Wi-Fi
Setup credentials to access your Secure Wi-Fi network.
KaliKitchen
Secure Wi-Fi password Show
••••••••••••
Limited network access for new devices
As an added security measure, this option allows you to manually approve every device joining Secure Wi-Fi (even if they have password for Secure Wi-Fi). More info.

- Edit the SSID name, or change and share the password.
- When sharing a password, the recipient will receive a time-limited link that opens a webpage containing the SSID and their password.
- You can also limit network access for new devices. This allows you to approve every device joining the Secure or Employee zones, even if they have the password.
- All ethernet devices are connected to the Secure Zone.

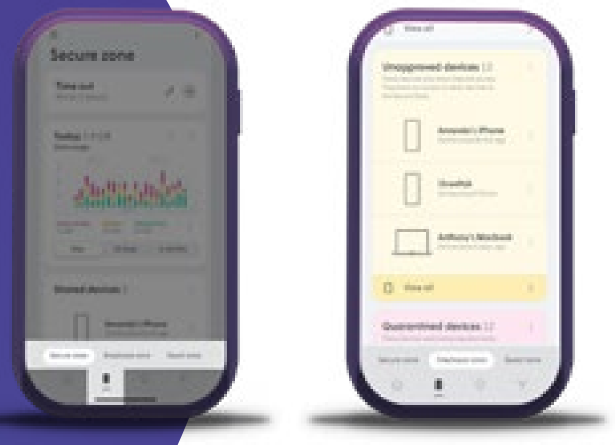
Approving Access for New Devices

Manually approving new devices for local access is handled through the **Zones** tab.

- The **Zones** tab further organises all devices based in the three available zones:
- Secure Zone
- Employee Zone
- Guest Zone
- Tap on the Secure zone or **Employee Zone** for the devices you wish to manage and scroll down to **Unapproved Devices**.

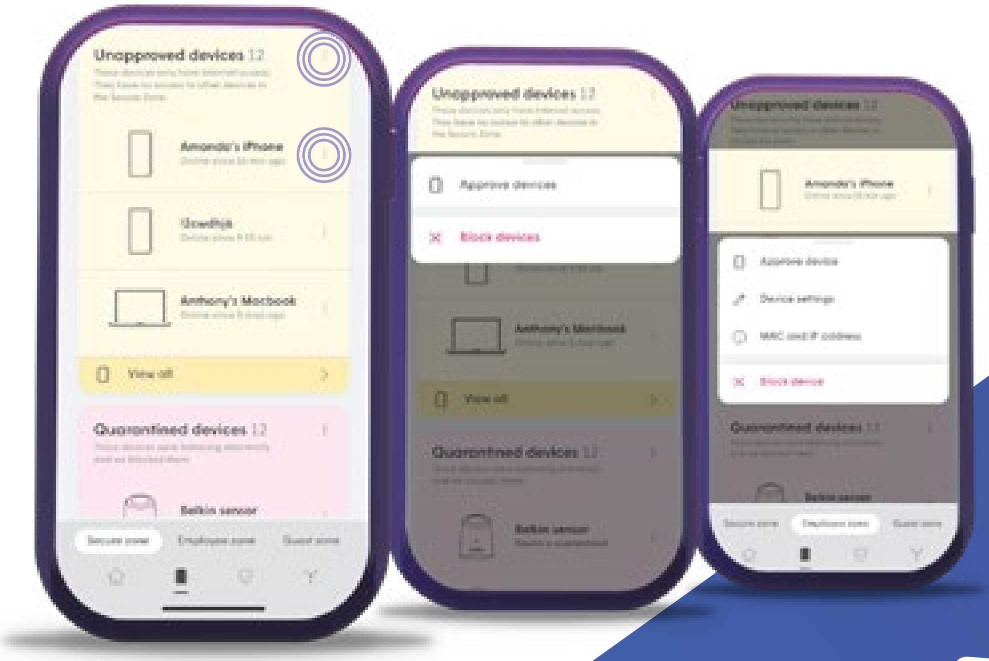


Kalifornia Kitchen
It's 72° and sunny in Palo Alto, CA
Today 68° - 79°. Small chance of rain.
All systems secure
All security events 388
Ad blocking 231
Online people 23
13 guests today
Adam Bronother Online
Guy Steward Online
Sasha Groves 5 min ago



Secure zone
Unapproved devices 12
View all
Quarantined devices 12

- Tap the options icon to the right of Unapproved devices to approve the devices all at once, or use the **options** icon next to the specific device to approve just that device.
- Tapping **Approve device(s)** removes the device(s) from Blocked list and allows for local access based on the current zone.



Unapproved devices 12
Amanda's iPhone
OnePlus
Anthony's Macbook
View all
Quarantined devices 12
Belkin sensor
Secure zone Employee zone Guest zone
Approve devices
Block devices
Approve device
Device settings
MAC and IP address
Block device

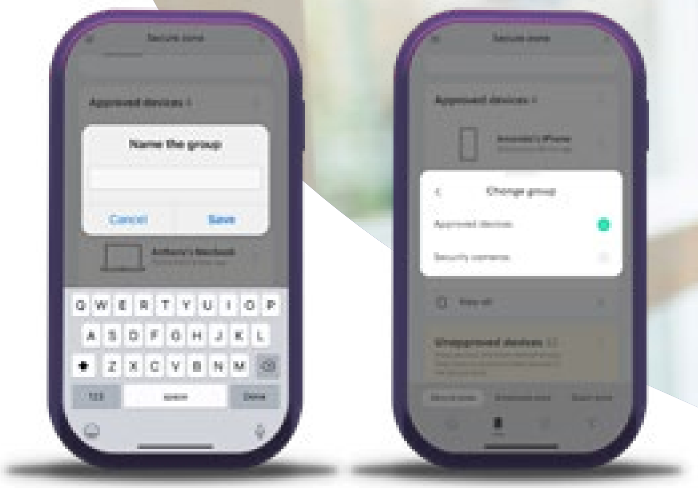
Once approved, the devices will be shown in the **Approved devices** list of the zone.

Approved devices options include **Change group**, **New group**, and **Block Access**.

Device Groups

Creating device groups makes it easier to share a set of devices in the Secure zone with employees. Device Groups are for organisation purposes only and do not block a device from accessing another within the same zone.

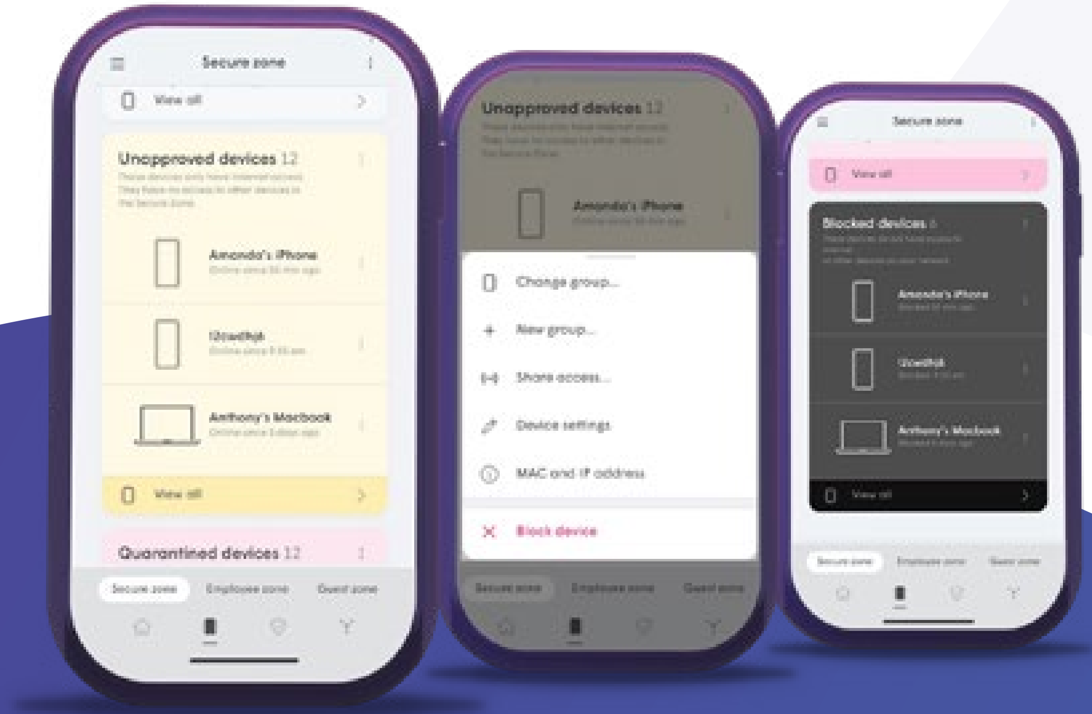
- Choose New group from the Approved devices option to create the group. This can also be done from the options at the top-right of the Secure zone page,
- Once the group is created, use the Change group option to add the individual device to the new group.

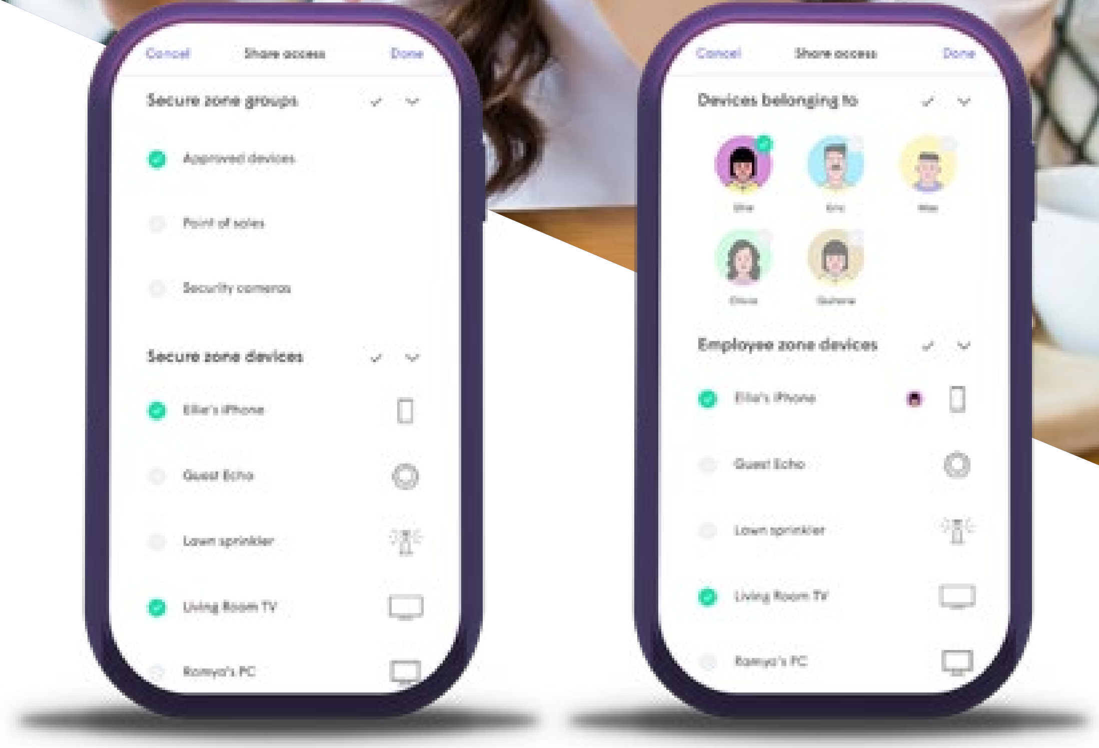


Blocking Devices

If a device in the Secure Wi-FI or Employee Wi-Fi zone is not recognized, the admin can manually use the Block Device option to prevent it from having Internet AND local access.

Once blocked, the devices will be shown in the **Blocked devices** list of the zone. The blocked devices can still be approved if the admin changes their mind.





Sharing Devices

Devices in the Secure Wi-FI zone can be shared with devices from the Employee Wi-Fi zone to allow local network traffic to access the shared resource.

If a device is not setup to be shared, the device is inaccessible through the local network.

A Group of devices or individual devices from the Secure Wi-FI zone can be shared.

Note: Ethernet connected devices are always added to the Secure zone and can therefore be shared.

Advanced Router Settings

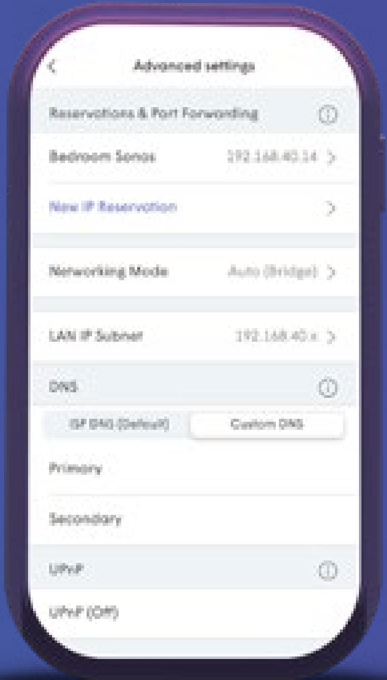
Advanced settings are only available if the first SuperPod is in router mode. If another device has been supplied that is performing router functions, then these options will not be available and will be greyed out.

- Open Settings screen by tapping ☰
- Router settings are found in the **Advanced Settings**

If you set the Networking mode to Router, when you already have a device running router mode. You may have issues such as Double NAT. If you switch mode settings, this will not be effective until the SuperPods are rebooted.

The following settings that can be changed (when in Router mode):

- Custom DNS. A primary and secondary DNS can be configured instead of the DNS provided by WightFibre. Changing these settings will not impact any of the advanced features, such as Shield.
- UPnP on/off. This allows devices like games consoles and media centres to connect to other devices or servers on the internet.



Advanced settings

Reservations & Port Forwarding

Bedroom Sonos 192.168.40.14

New IP Reservation

Networking Mode Auto (Bridge)

LAN IP Subnet 192.168.40.x

DNS

ISP DNS (Default) | Custom DNS

Primary

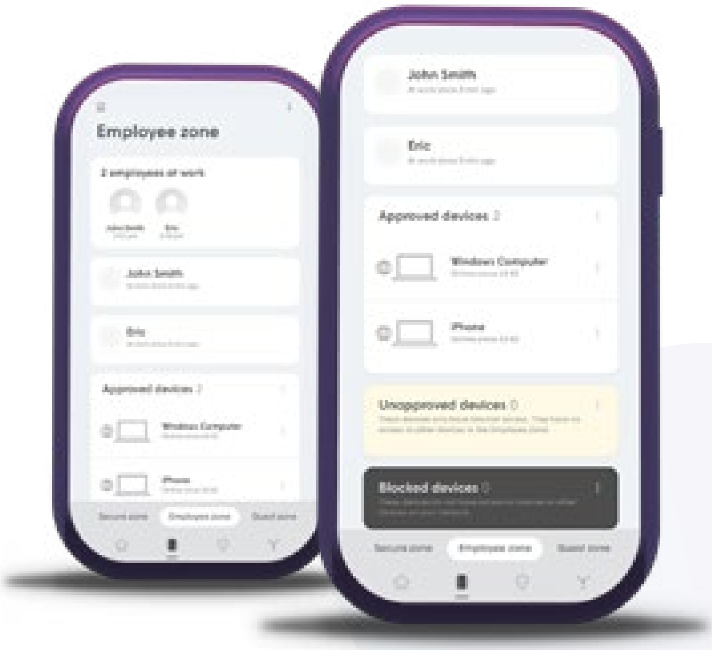
Secondary

UPnP

UPnP (Off)

- Lan IP Subnet for the Secure and Employee network zones. You can choose from:
  - 10.0.0.x
  - 172.16.0.x
  - 192.168.1.x
  - Or enter a specific range to use
- IP Reservations. You can reserve a specific IP address against any device that has connected to the network, or manually add an IP for one that has not yet connected but you will need to know the MAC for any unconnected devices.
- Port Fowarding can be set for any devices that has an IP address that has been reserved. All you need to do is specify the Port Name, and the External port and the Internal port and the protocol (TCP&UDP, TCP, UDP)

Managing Employees



The Employee zone is managed through the devices menu.

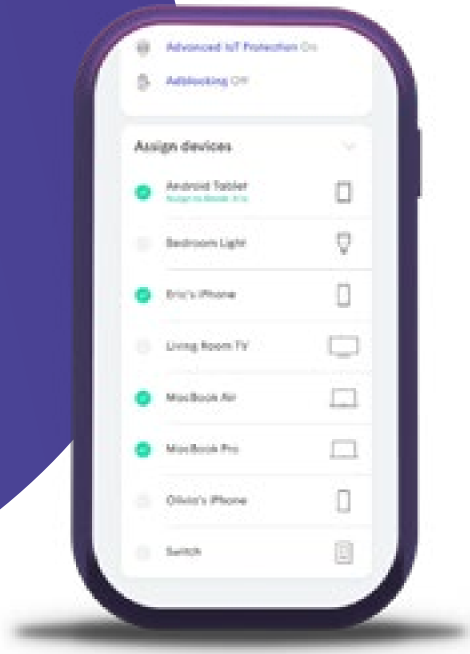
All devices connecting to the network using the Employee SSID will appear in the Employees zone. This provides the admin an overview of employee activity including:

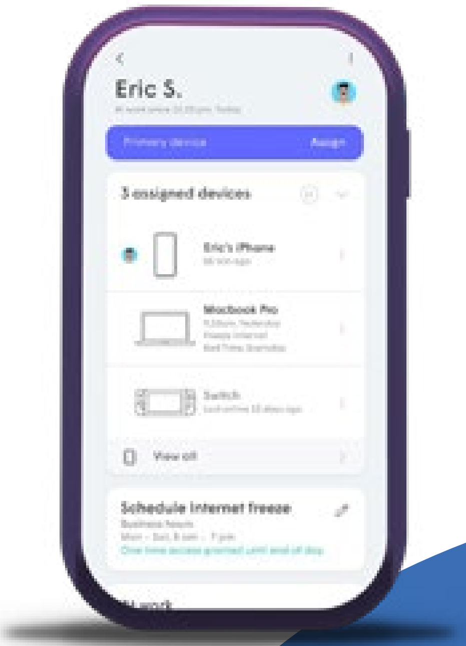
- Who is currently at work
- Data about the devices being used

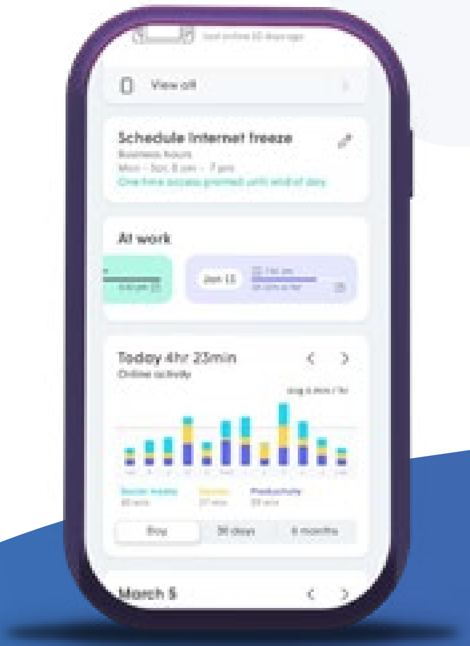
The admin can also put Employee devices in a Time out.

Adding Employees

1. To add an employee, tap the options on the top right.
2. Enter the employee's name.
3. Assign devices to the employee. Additional devices can be assigned later from the device's options. Note: assigning a device from the unapproved, or blocked list to an employee automatically approves the devices.
4. Once saved, the primary device can be assigned to the employee. This is used to track when the employee is at work, their mobile phone is typically best for this.







Employee Avatar

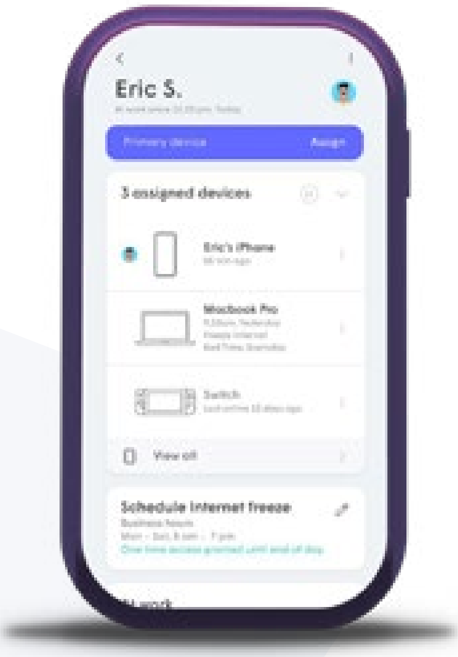
One of 16 generic avatars will be assigned automatically. By swiping right on the avatar, a further 80 avatars are available to choose from. Tapping on the + symbol next to the avatar will allow a picture to be taken, or you can choose a photo from the devices gallery.

Employee Options

Further devices can be assigned to the employee in the "Assign devices" card.

Secure zone devices can also be shared with the employee, along with setting online protection and adblocking.

Internet Freeze schedule can also be applied to the employee's devices.



Eric S.

Primary device Assign

3 assigned devices

Eric's iPhone

Macbook Pro

Switch

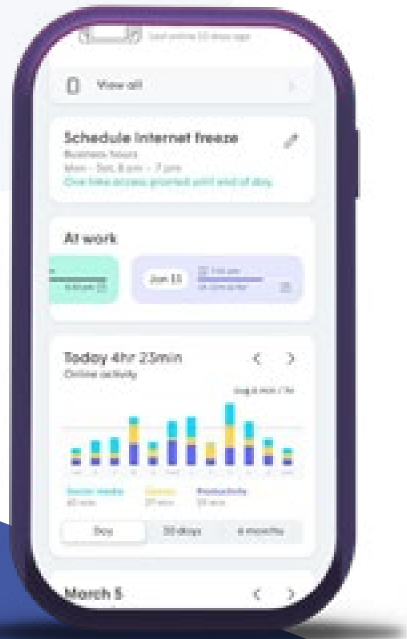
View all

Schedule Internet freeze

Business hours

Mon - Sat, 8 am - 7 pm

One time access granted until end of day



View all

Schedule Internet freeze

Business hours

Mon - Sat, 8 am - 7 pm

One time access granted until end of day

At work

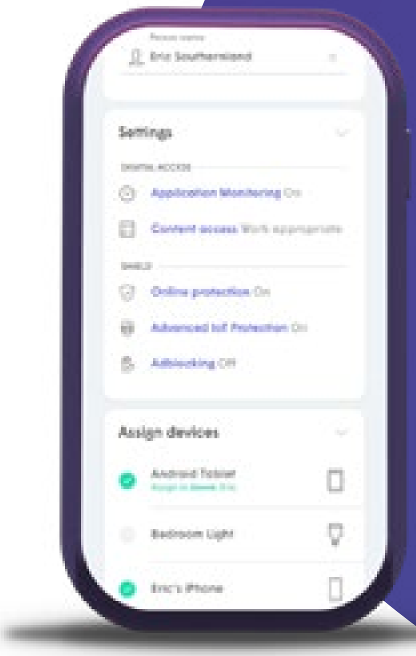
Jun 11

Today 4hr 23min

Online activity

Day 30 days 6 months

March 5



Eric Southernland

Settings

Application Monitoring On

Content access Work appropriate

Online protection On

Advanced IoT Protection On

Adblocking Off

Assign devices

Android Tablet

Bedroom Light

Eric's iPhone

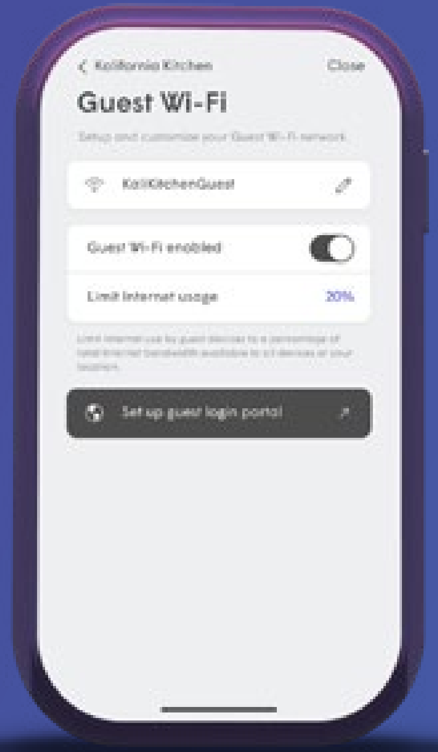
Guest Portal

If the guest network was not enabled during the initial setup, it can be created afterwards from the settings screens.

The SSID can be changed and once enabled, Limit Internet usage can be used to limit guest bandwidth to a specific percentage.

Guests use a captive portal instead of a Wi-Fi password.

You must Set up guest login portal before your visitors can use the Wi-Fi.



Kalifornia Kitchen Close

Guest Wi-Fi

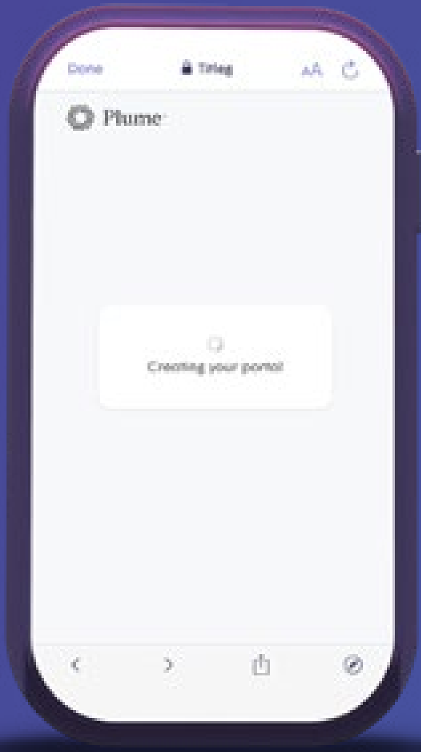
Setup and customize your Guest Wi-Fi network

KaliKitchenGuest

Guest Wi-Fi enabled

Limit Internet usage 20%

Set up guest login portal



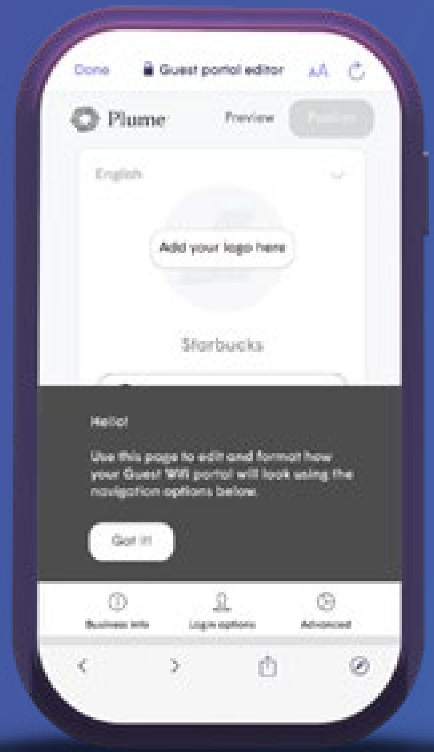
Done Titleg AA

Plume

Creating your portal

Enter your business details by tapping the Business Info button. Includes Business Name, Footer Text, Logo and Terms and Conditions.

Please note, the default Terms and Conditions explain to the guest how their information is used. Should you add your own Terms and Conditions, it is best to add your own above the existing ones.



Done Guest portal editor AA

Plume Preview

English

Add your logo here

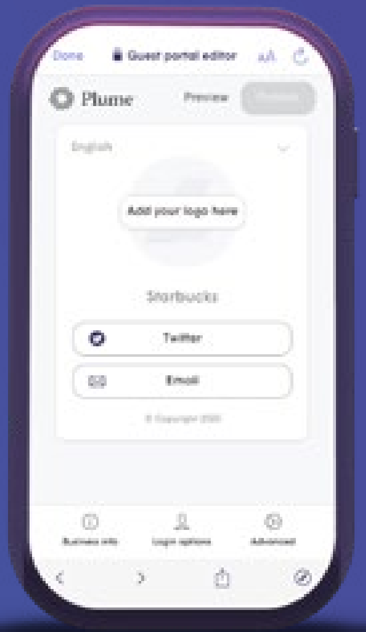
Starbucks

Hello!

Use this page to edit and format how your Guest Wifi portal will look using the navigation options below.

Got it!

Business info Login options Advanced



Done Guest portal editor

Plume Preview

English

Add your logo here

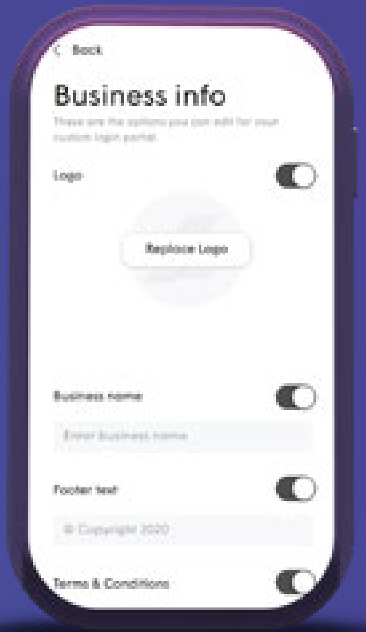
Starbucks

Twitter

Email

© Copyright 2020

Business info Login options Advanced



‹ Back

Business info

These are the options you can edit for your custom login portal.

Logo

Replace Logo

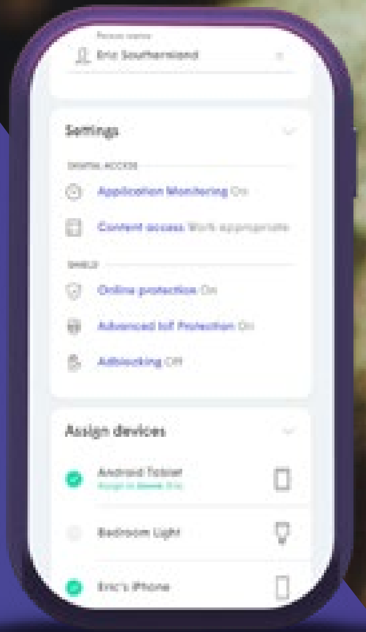
Business name

Enter business name

Footer text

© Copyright 2020

Terms & Conditions



Person name

Eric Southernland

Settings

DIGITAL ACCESS

Application Monitoring On

Content access Work appropriate

SHIELD

Online protection On

Advanced IoT Protection On

Adblocking Off

Assign devices

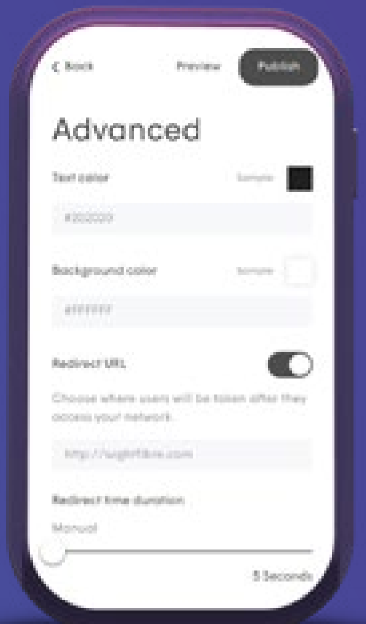
Android Tablet

Assign to Eric

Bedroom Light

Eric's iPhone

If you have a business website or facebook page, the logo can be imported by entering the website address or facebook page URL.



‹ Back Preview Publish

Advanced

Text color Sample

#202020

Background color Sample

#FFFFFF

Redirect URL

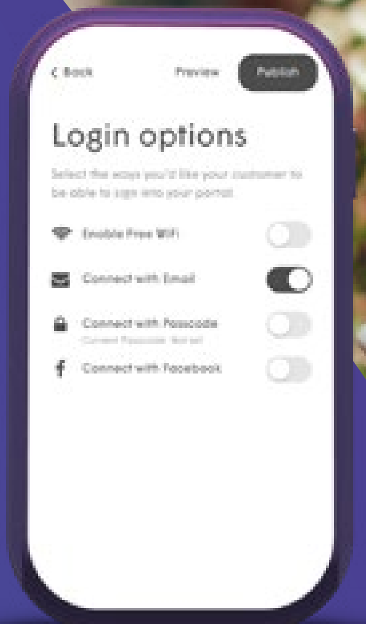
Choose where users will be taken after they access your network.

http://wightfibre.com

Redirect time duration

Manual

5 Seconds



‹ Back Preview Publish

Login options

Select the ways you'd like your customer to be able to sign into your portal

Enable Free WiFi

Connect with Email

Connect with Passcode

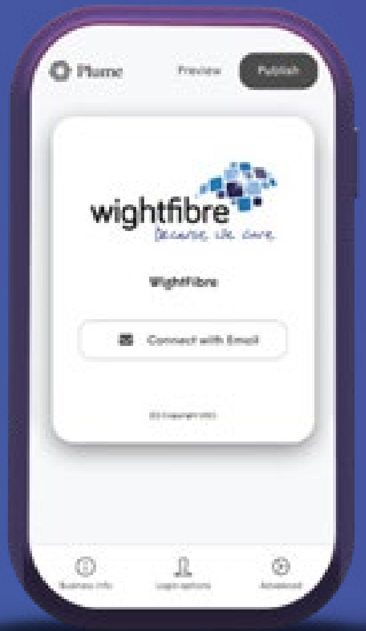
Current Passcode: Not set

Connect with Facebook

Login options allows the user to choose how the guest can sign into the portal and get internet access.

Advanced provides basic format options for the portal: **Text color** and **Background color**.

The **Redirect url** is the page the guest is redirected to once they have successfully logged in. This can be set to business' homepage, facebook page, etc. The **Redirect time duration** customizes how long that redirect takes.



Plume Preview Publish

wightfibre

because we care

Wightfibre

Connect with Email

© Copyright 2021

Business info Login options Advanced

The portal can be **Previewed** and if everything looks okay, it can then be **Published**.

Guest Zone Overview

From the Guest zone in the Device menu, you can view a whole host of metrics about how their guest are using the internet access:

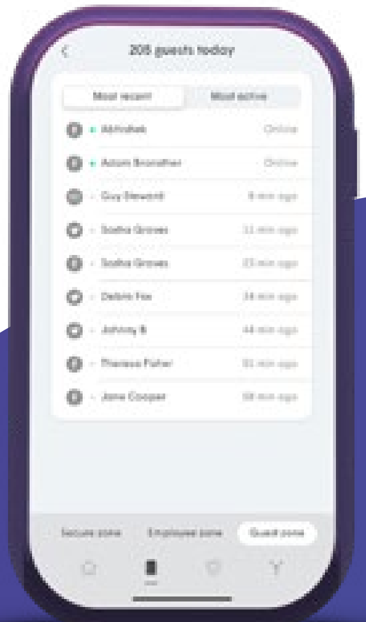
- Guest totals, including new and repeat customers.
- Session information including Average session length, Average Data usage.
- Device types and popularity.

The device MAC address is used to recognize a device. If the random MAC feature is used, common on many new phones, the same device will show again.

The Guests metrics can be broken down even further to display the Most recent or Most Active guests.

Additional information for these highlighted guests also include how many recent visits they've had and how much data they have used so far.

These metrics can be used by the business owner to make adjustments to improve their business, such as focus their social media presence or adjust scheduling.

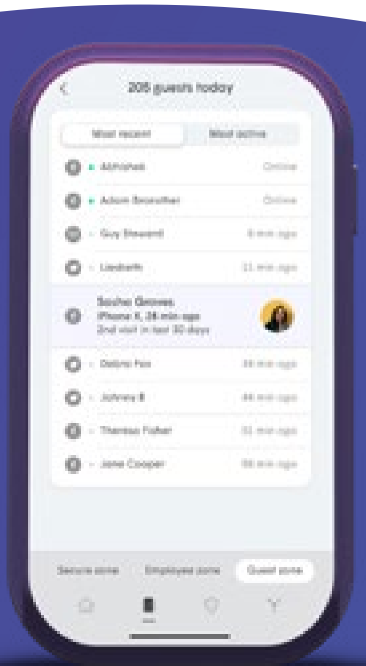


205 guests today

Most recent | Most active

Abhishek	Online
Adam Bronather	Online
Guy Steward	8 min ago
Sasha Groves	11 min ago
Sasha Groves	23 min ago
Debra Fox	34 min ago
Johnny B	44 min ago
Theresa Fisher	51 min ago
Jane Cooper	58 min ago

Secure zone | Employee zone | Guest zone

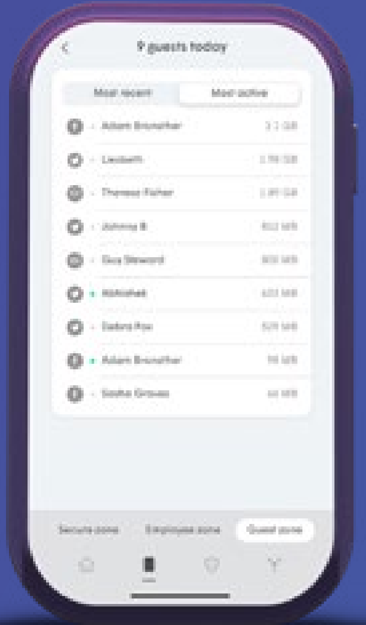


205 guests today

Most recent | Most active

Abhishek	Online
Adam Bronather	Online
Guy Steward	8 min ago
Liesbeth	11 min ago
Sasha Groves iPhone X, 28 min ago 2nd visit in last 30 days	
Debra Fox	33 min ago
Johnny B	44 min ago
Theresa Fisher	51 min ago
Jane Cooper	58 min ago

Secure zone | Employee zone | Guest zone



9 guests today

Most recent | Most active

Adam Bronather	3.2 GB
Liesbeth	1.78 GB
Theresa Fisher	1.49 GB
Johnny B	812 MB
Guy Steward	800 MB
Abhishek	423 MB
Debra Fox	329 MB
Adam Bronather	98 MB
Sasha Groves	44 MB

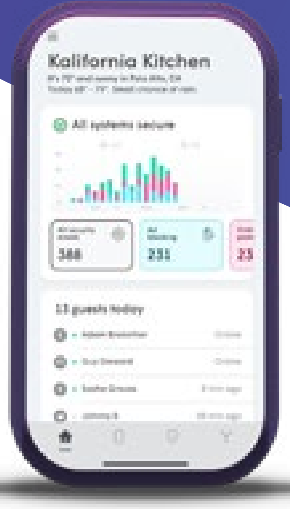
Secure zone | Employee zone | Guest zone

Shield

In the Home screen, an overview of security events is provided.

Network-wide settings are modified and displayed in the **Settings** menu. Employee level settings can also be accessed from each employee's respective page

The Shield tab provides more detail on all security events and provides additional options such as the ability to Approve (Whitelist) or Block (Blacklist sites). Shield settings and events can be easily sorted by all, employee, and event type.

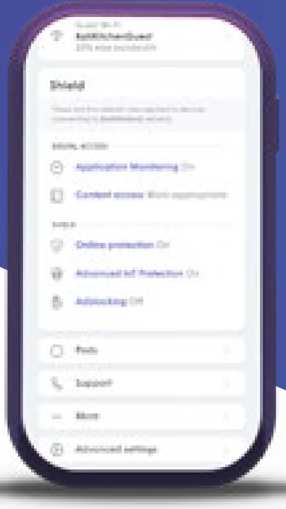


Kalifornia Kitchen

All systems secure

388 | 231 | 23

13 guests today



Shield

Application Monitoring On

Content access Work appropriate

Online protection On

Advanced IoT Protection On

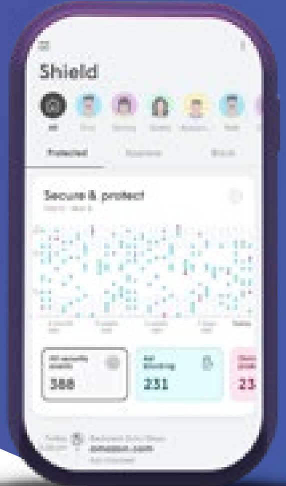
Adblocking Off

Pods

Support

More

Advanced settings



Shield

Secure & protect

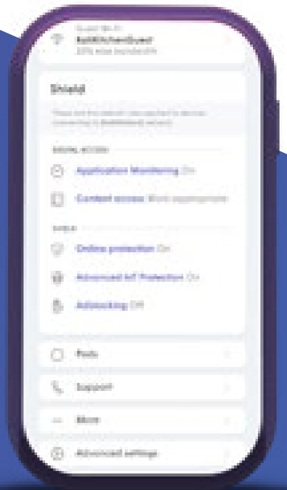
388 | 231 | 23

Online Protection

Online protection uses a constantly updating database of websites known to contain:

- Malware and Botnets
- Phishing and fraud
- Spyware and Adware,
- Spam URLs
- Keyloggers and monitoring
- Proxy avoidance and Anonymisers.

Online Protection can be set at the network, device, or employee level.



Shield

Application Monitoring On

Content access Work appropriate

Online protection On

Advanced IoT Protection On

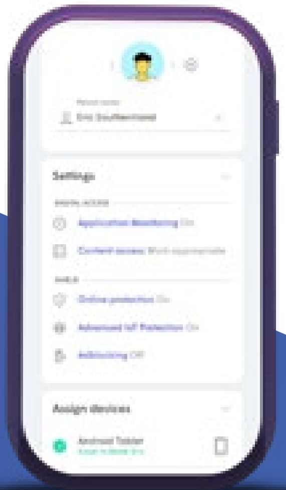
Adblocking Off

Pods

Support

More

Advanced settings



Settings

Application Monitoring On

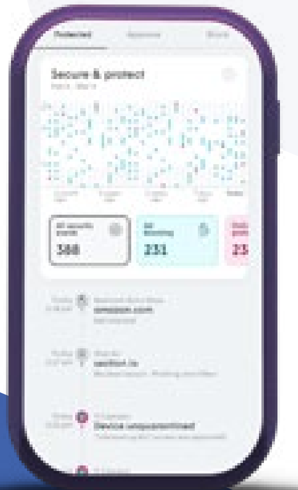
Content access Work appropriate

Online protection On

Advanced IoT Protection On

Adblocking Off

Assign devices



Secure & protect

388 | 231 | 23

amazon.com

Device unquarantined

Outbound IP Protection and Intrusion Prevention

In addition to protecting the network based on DNS lookups, Online Protection also protects devices from connecting to harmful IP addresses and blocks both incoming (Intrusion Protection) and outbound (Outbound Protection) device connections to known harmful IP addresses.

Outbound IP Protection and Intrusion Prevention is enabled by turning on Online Protection.

Specific events can be tapped to manually approve access to the site by the device.

The list on the Shield tab contains 30 days of data, tapping on the graphic will highlight the number of events during that day.

You can also filter by the type of event and by person.

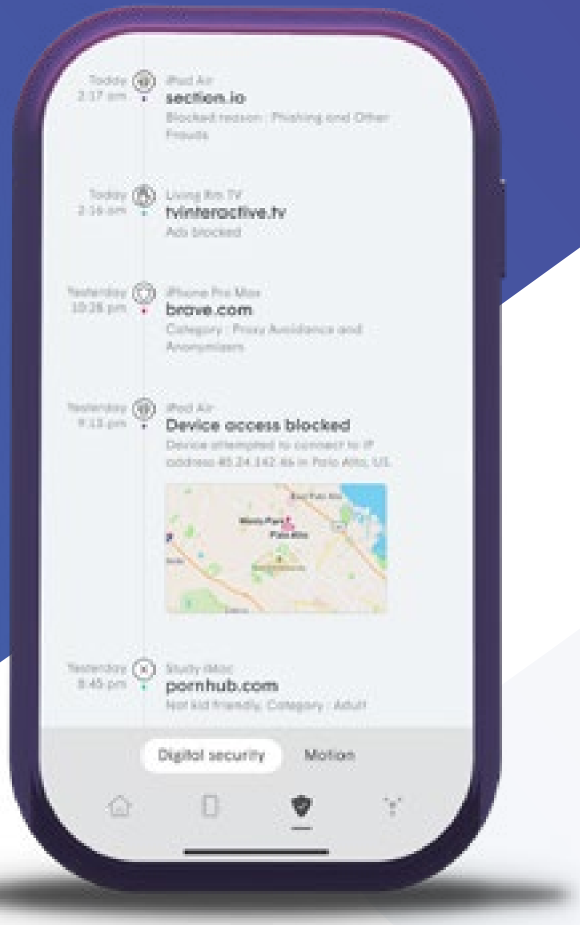
A brief description under each event provides more information on why it was blocked, and which device was trying to access it.

Tapping an event in the list gives you the option of unblocking that domain.

Depending on the level it was blocked at, you are given the option to unblock it for the person, device or everyone.

Anything unblocked for a device will automatically unblock it from the person and vice-versa.

Up to 20 entries in total can be manually whitelisted.



Today 2:17 pm iPad Air
section.io
Blocked reason : Phishing and Other Frauds

Today 2:16 pm Living Rm TV
tvinteractive.tv
Ads blocked

Yesterday 10:28 pm iPhone Pro Max
brave.com
Category : Proxy Avoidance and Anonymizers

Yesterday 9:13 pm iPad Air
Device access blocked
Device attempted to connect to IP address 45.24.142.46 in Palo Alto, US

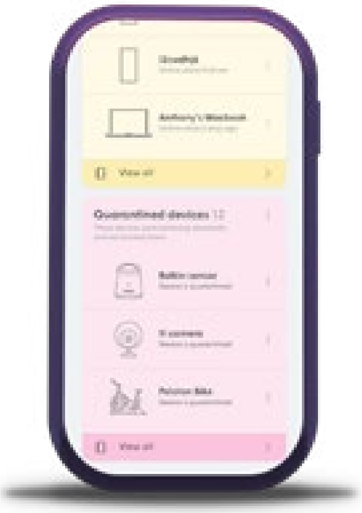
Yesterday 8:45 pm Study iMac
pornhub.com
Not kid friendly. Category : Adult

Advanced IoT™ Protection

Advanced IoT™ protection studies device behavior.

The cloud knows which domains supported smart home devices are supposed to regularly access. If a supported device tries to access a previously unknown domain, it is immediately quarantined and a notification is sent.

While in quarantine the device will maintain internet connectivity, but will not have local access so it cannot infect other local network devices.



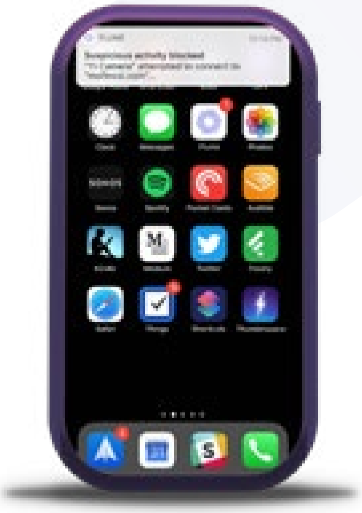
Anthony's Macbook

Quarantined devices 12

Belkin sensor

Yi camera

Peloton Bike



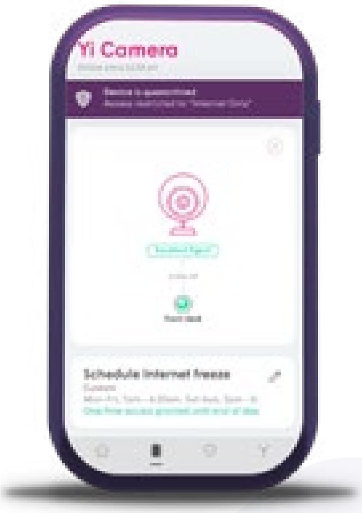
Suspicious activity blocked

Once the device is blocked, a message will appear below it, indicating that it has been restricted to only Internet access.

Tapping on the device brings up further details on why it was blocked, including the URL it was trying to access. A link in the description allows the users to search the web for more information from the manufacturer.

You can **unquarantine** the device for 1 hour so it can be tested.

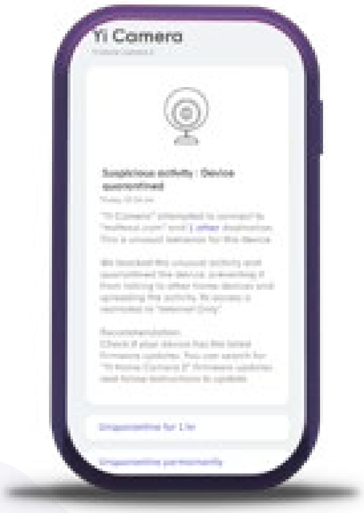
If the event is due to a recent firmware or feature update on the device that now requires access to a previously unknown domain, the device can be **unquarantined permanently**.



Yi Camera

Schedule Internet freeze

Custom



Yi Camera

Suspicious activity : Device quarantined

Recommendation:

Adblocking

Enabled at the network, person, or device level.

Adblocking blocks known advertising servers, although the websites themselves will continue to be displayed without certain ads.

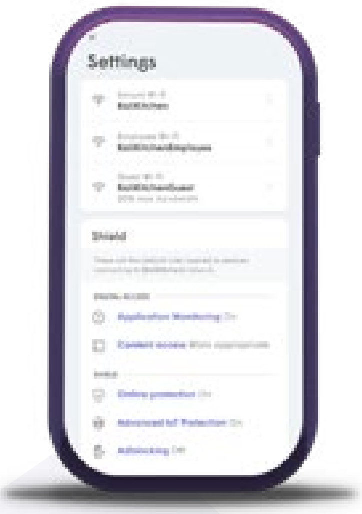
Content Access

Content Access rules can be set at the network level.

Content Access uses a database of known domains to restrict what types of websites can be accessed by the person or device based the following levels:

No Restrictions (default) - No restriction on content other than what is being applied by Shield

Work Appropriate – Content that can add potential liability to the business is blocked.



Settings

Shield

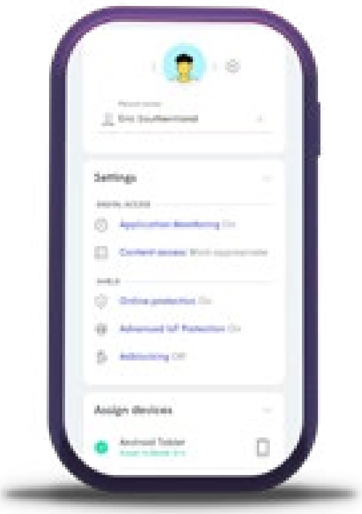
Application Monitoring

Content access

Online protection

Advanced IoT Protection

Adblocking



Settings

Application Monitoring

Content access

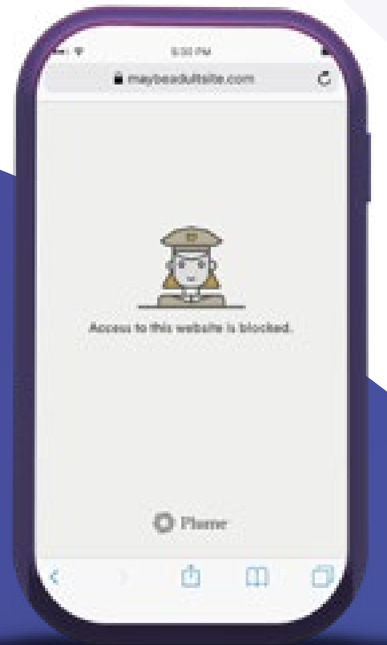
Online protection

Advanced IoT Protection

Adblocking

Assign devices

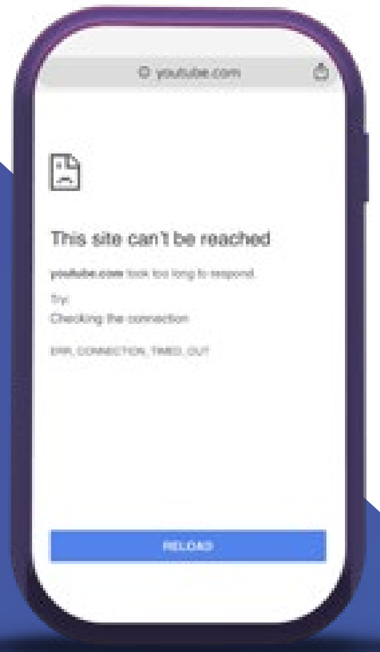
Android Tablet



maybeadultsite.com

Access to this website is blocked.

Plume



youtube.com

This site can't be reached

youtube.com took too long to respond.

Try:

Checking the connection

ERR_CONNECTION_TIMED_OUT

RELOAD

When attempting to access an HTTP site that is blocked by the Content Access feature, a page with the Plume logo and an "Access to this site is blocked" message will be displayed by the browser.

When accessing a blocked HTTPS website, the browser's default "This site can't be reached" or "Connection Timed Out" message will be displayed.

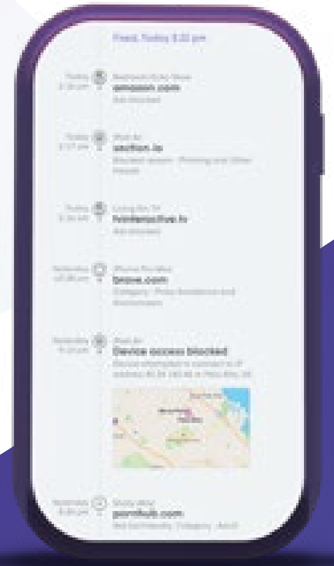
Manually Approving/Blocking Content

You can approve domains or IP Addresses that have been blocked by Content Access, Online Protection or Adblocking. Or you can block them if they have not been automatically blocked.

Up to 20 entries in total can be manually approved, and 20 manually blocked. These can be applied at the network, person or device level.

Device level settings supersede person and network level settings.

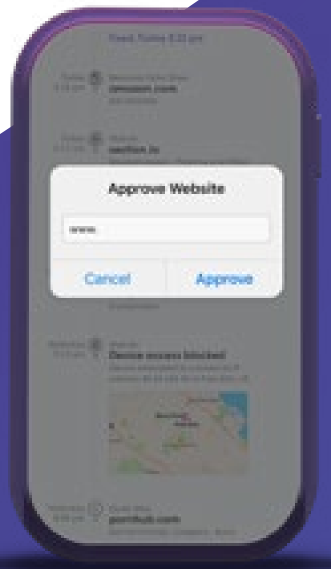
Tapping on a **security** event in the person, device or Shield pages, lets you manually approve a blocked site from the **Protected** list or enter in a specific domain or IP address in the **Approve** list. Or alternatively, lets you manually block a specific domain or IP address.



amazon.com

Device access blocked

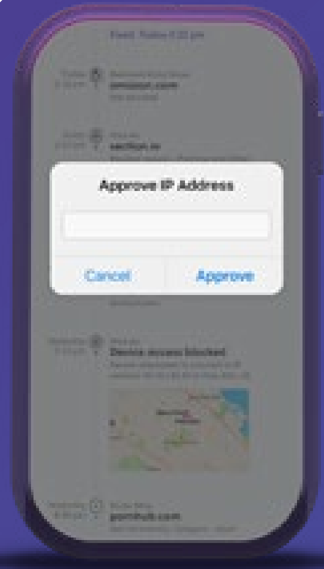
pornhub.com



Approve Website

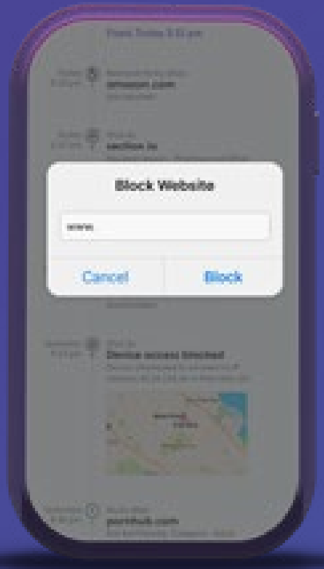
www.

Cancel   Approve



Approve IP Address

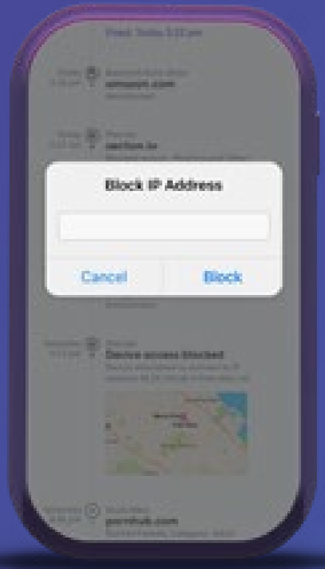
Cancel   Approve



Block Website

www.

Cancel   Block



Block IP Address

Cancel   Block

Note: IP Addresses can only be approved or blocked if Outbound IP Protection and Intrusion Prevention has been enabled.

wightfibre®

because we care

01983 300 000

www.wightfibre.com