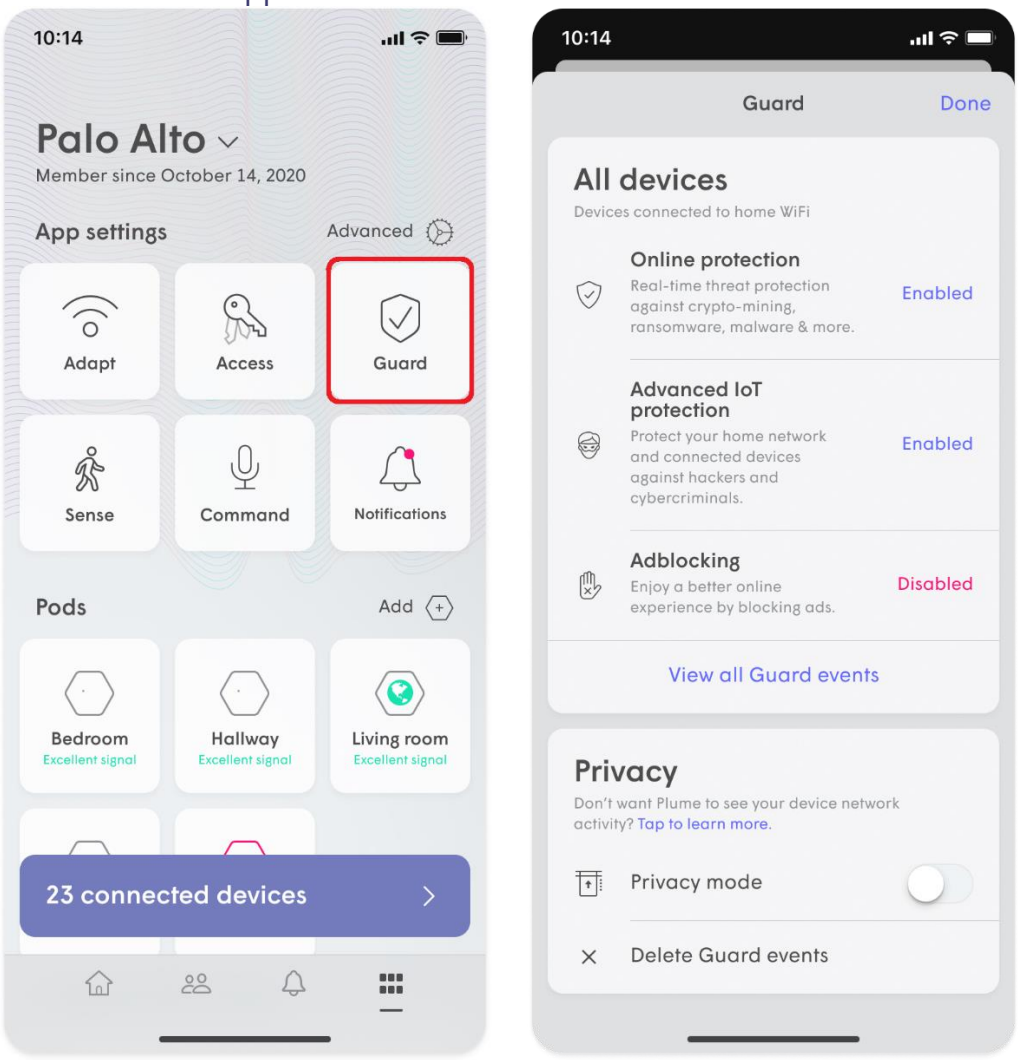
Table of Contents

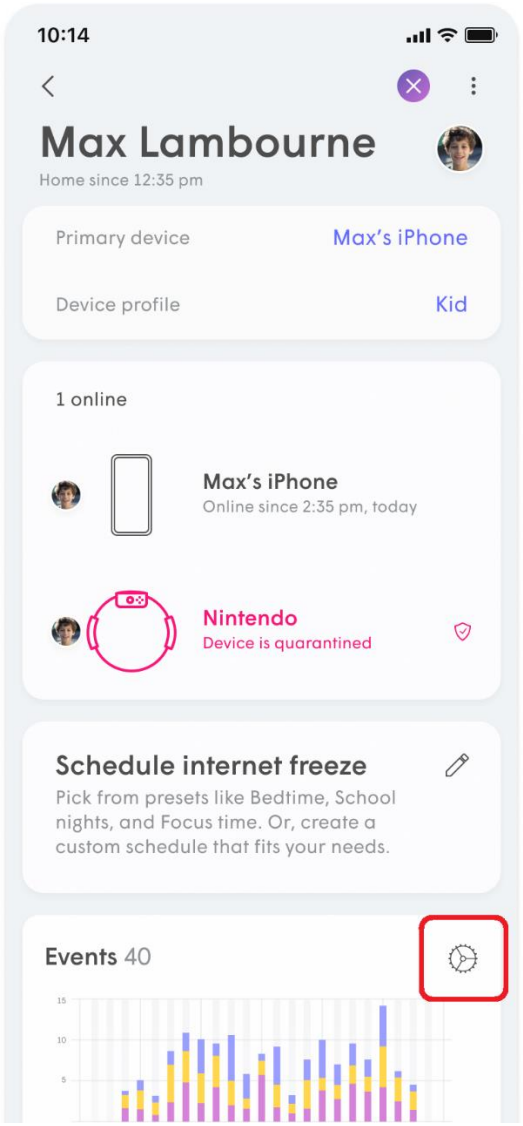
Can I set different parental controls on a person, device or location level?

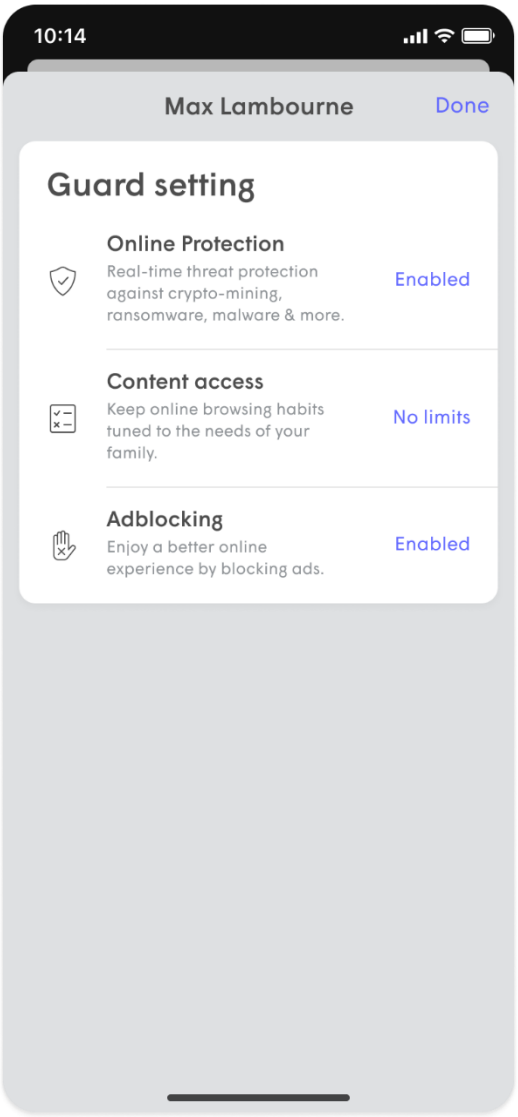
Adblocking, Online Protection, and any custom Approve / Block lists can only be configured on a location, person, or device level. Content Access (parental control) settings can be configured on a person and device level.

Location level: Applies to all devices connected to the network.

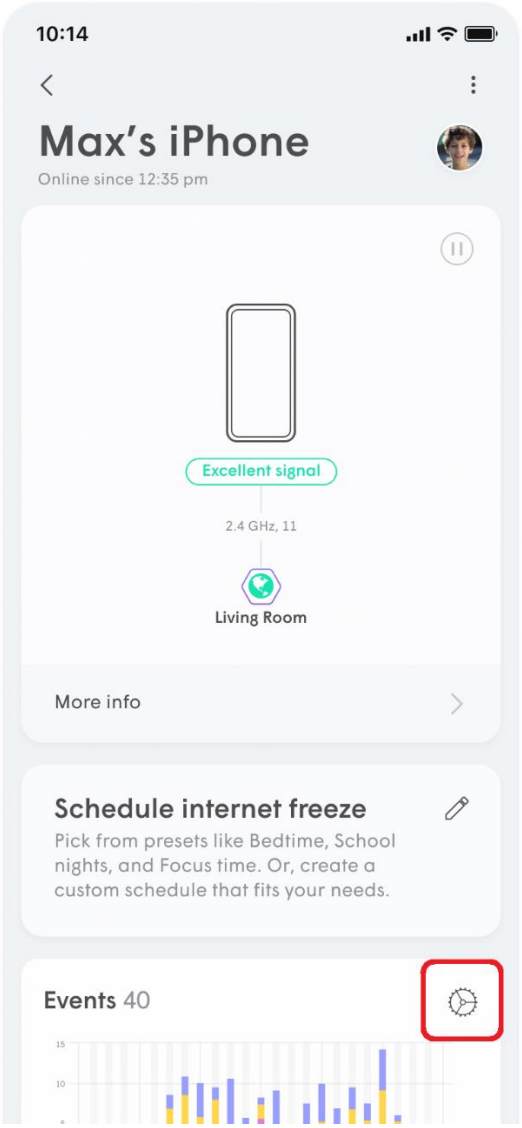


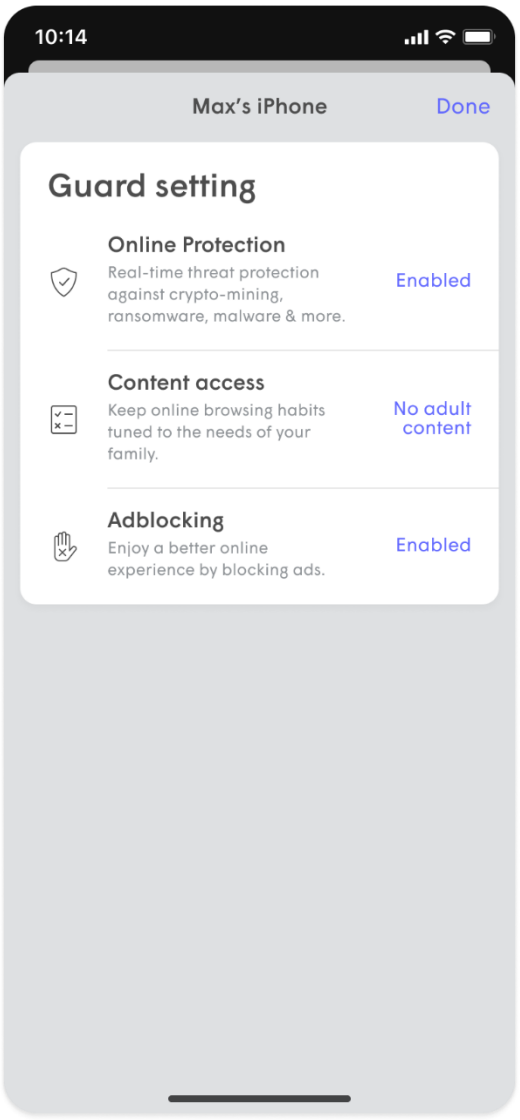
Person level: Applies to all devices assigned to a person.





Device-level: Applies only to the single device only if unassigned. If the device is assigned to a person, the Content Access rule will be applied to that person.





What happens if you have different settings configured on different levels for a device?

Priority is given to the most specific settings for a device. For example, if Online Protection is disabled on a location level and enabled for a device, the setting is turned on for the device.

Additionally, if a location has a setting enabled, any new devices and profiles added will inherit the same settings by default.
If should be noted that if a device is assigned to a person, Content Access rules will always be the same for a person and their associated devices.
For any additional questions, please contact our support staff for assistance.

Choosing your Motion Detection Devices

How are devices chosen to detect motion?

Sense uses a behind-the-scenes algorithm to pick from the **Sense device list** devices that are best suited for motion detection. Click here to learn more about Sense devices and how they are chosen.

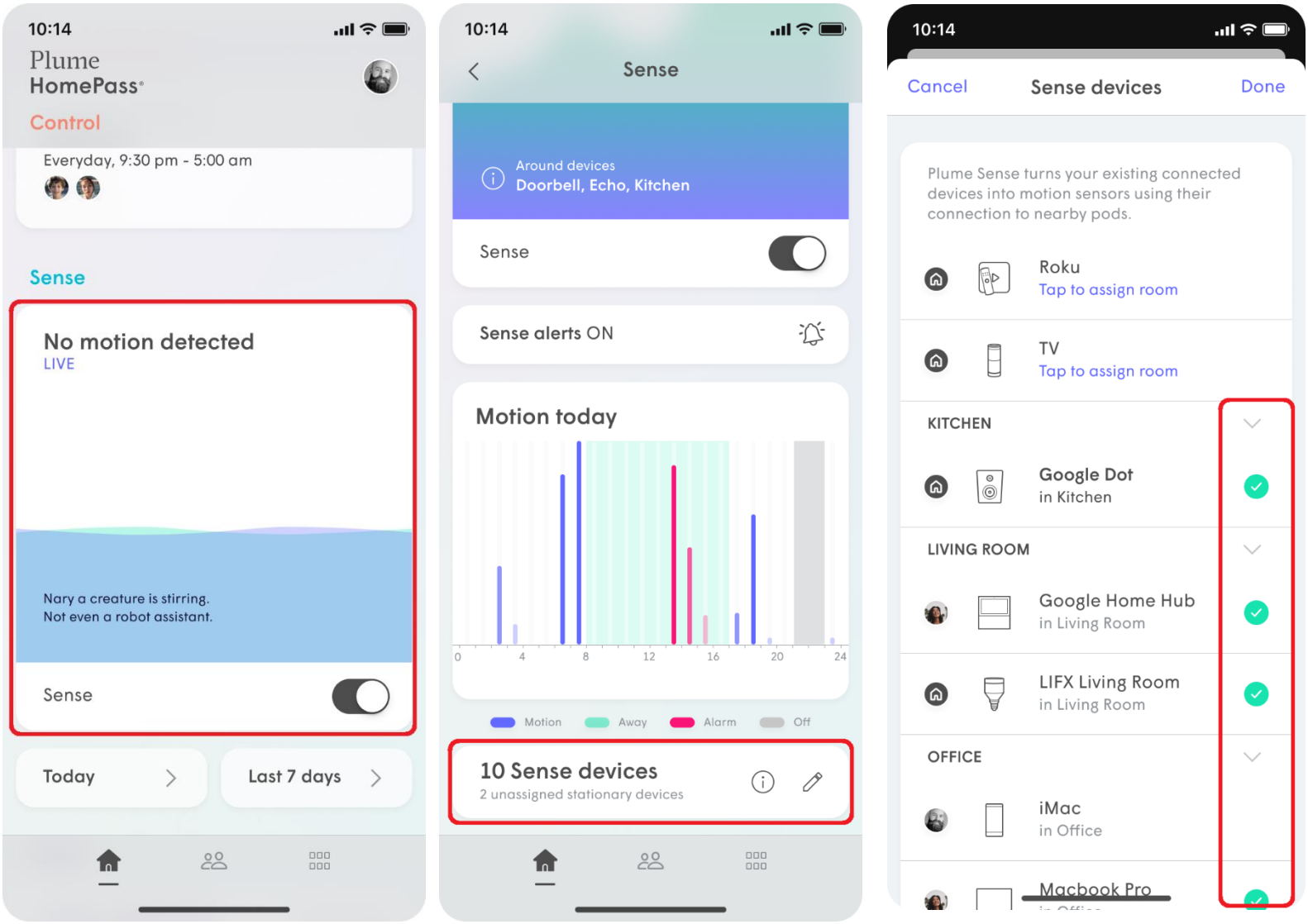
Modifying the Sense device list

The pool of available devices (Sense device list) from which the algorithm chooses is based on all Wi-Fi devices currently connected to a SuperPod, excluding mobile devices. This Sense device list can be modified by you to limit motion detection in certain areas. We recommend leaving all devices in the Sense Devices list selected for optimal performance, but if you would like to manually choose which devices can be used, the following guidelines will help you get the most coverage in your home.

- If you want to limit motion detection in certain areas of your home, deselect devices in those areas.
- Although Sense will keep most mobile devices separate, ensure you choose devices that will remain static.
- Avoid choosing devices that are battery operated or may frequently go into a low-power state. Always-on devices such as voice assistants and other smart home devices are good candidates.
- Since SuperPods are already being used to detect motion, avoid choosing devices that are either in the same room or very close to them.
- To better refine the motion sensitivity, use the Live View feature to test the motion detection in each room.

How do I access and modify the Motion Detection Devices list?

1. From the **home screen**, scroll down to the **Sense** section and tap on the **Live view**.
2. Scroll down and tap on the pencil icon next to **Sense devices.**
3. Remove the **green checkmark** next to any device you do not want to be used for motion detection or add a green checkmark next to devices you want to be used.
4. Be sure to assign rooms to your devices if you haven't already done so.

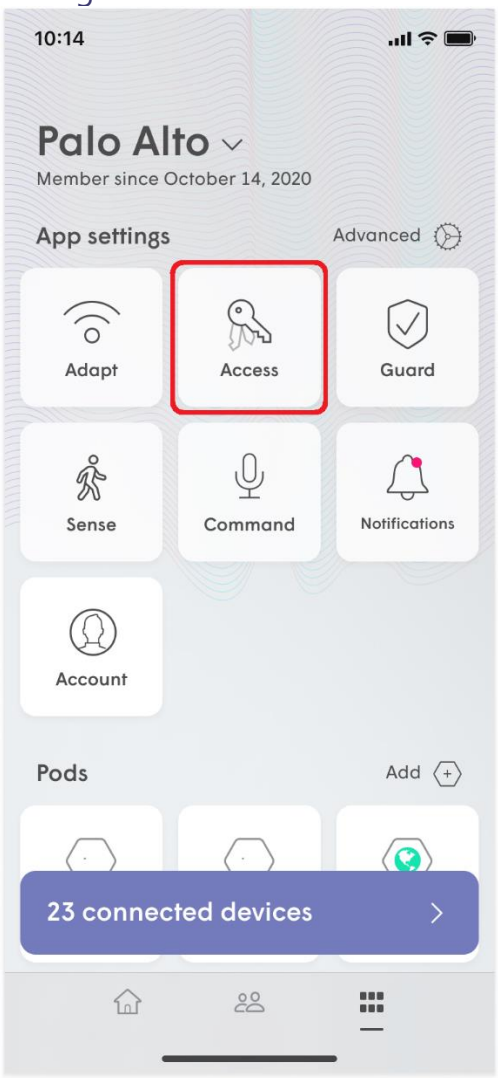


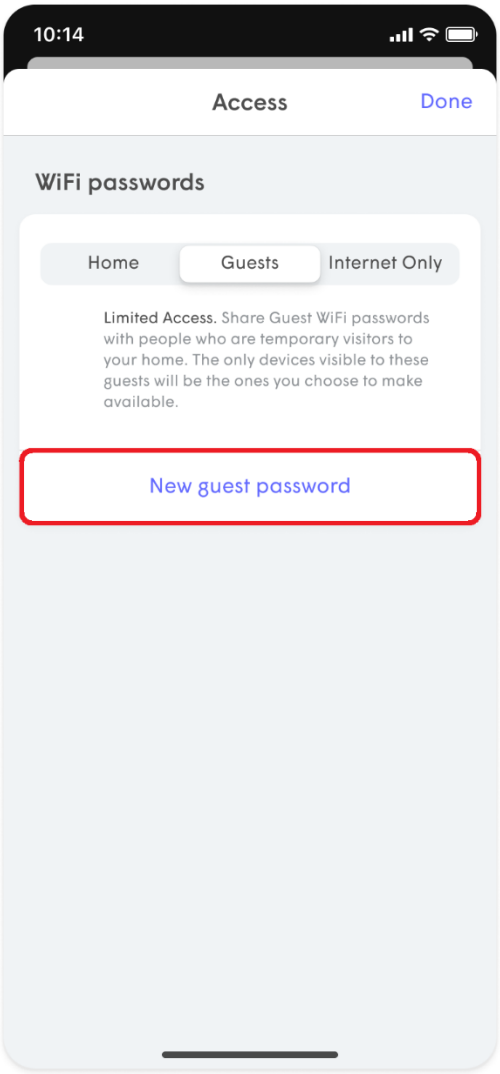
The cloud will only use the 3 most appropriate devices connected to each SuperPod from your choices.
If the device you are trying to choose is not appearing in the list, click here to find out why and how to add them to the list.

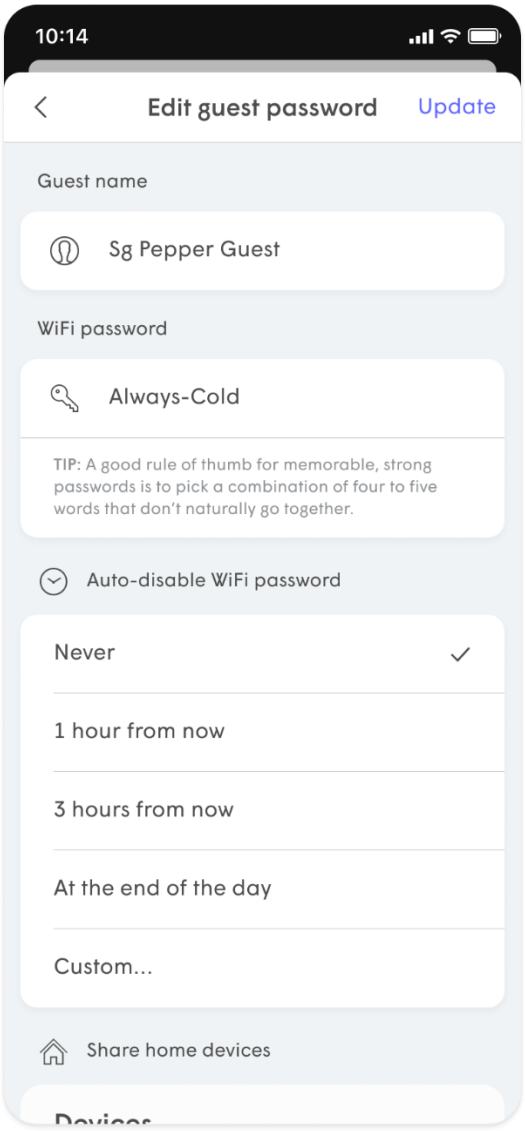
Create a new password for a Guest

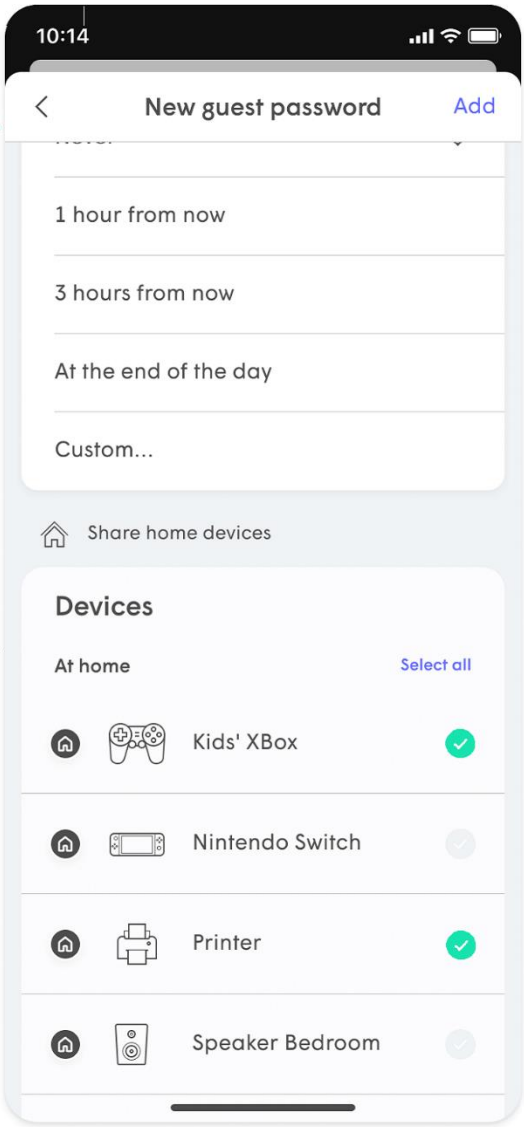
1. Open the **More** tab and click on the **Access** button.
2. While in the **Guest** settings page, tap on **New Guest Password**.
3. Enter a name* and a new password.
4. Use the drop-down arrow next to **Auto-disable Wi-Fi Password** and choose one of the options.
5. Add a checkmark next to one or more **Shared Home Devices** (printer, NAS, media player), to allow your guest access to it over the local network.
6. Tap on the **Add** to save.

*You can set up different device access permissions and Auto-disable Wi-Fi Password settings for each name under the Guest zone



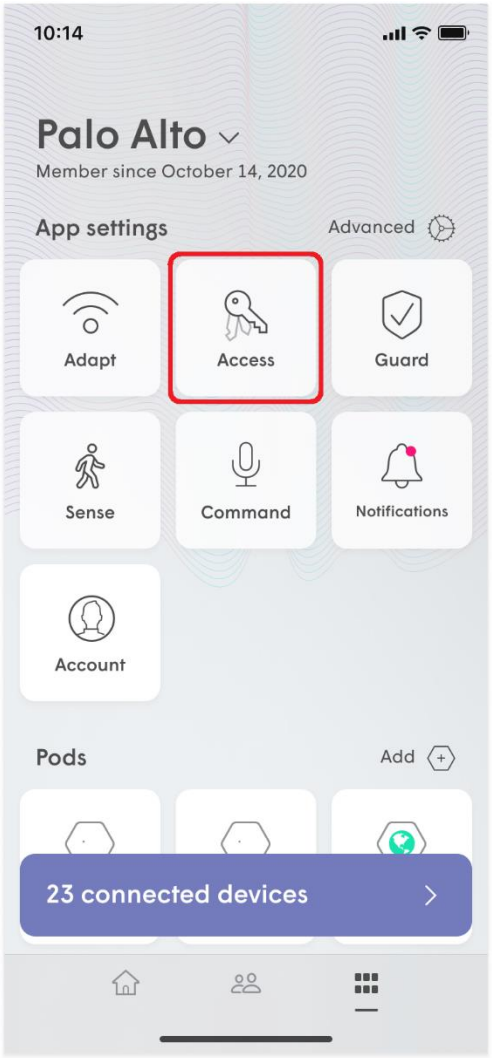


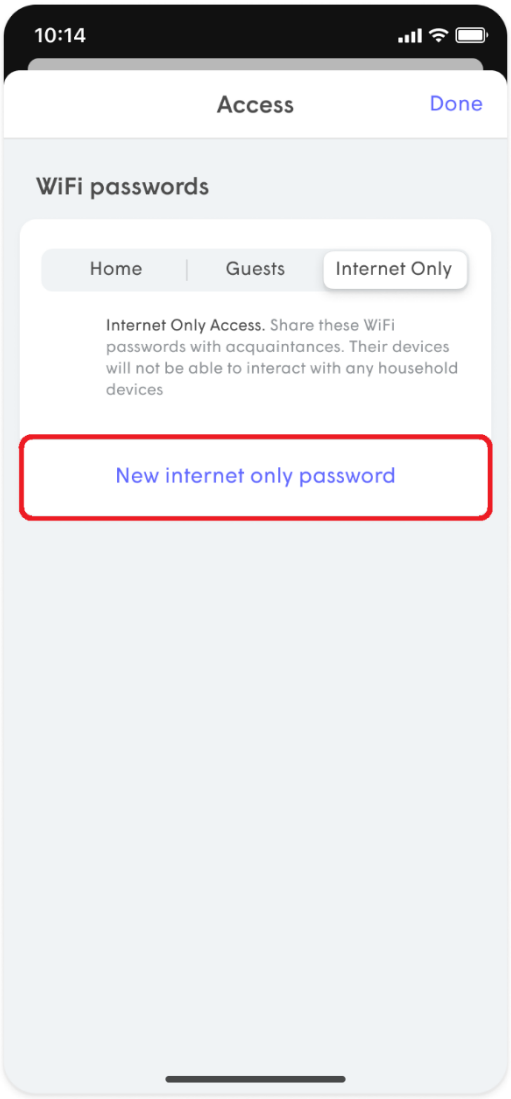

10:14
Edit guest password
Update
Guest name
Sg Pepper Guest
WiFi password
Always-Cold
TIP: A good rule of thumb for memorable, strong passwords is to pick a combination of four to five words that don't naturally go together.
Auto-disable WiFi password
Never
1 hour from now
3 hours from now
At the end of the day
Custom...
Share home devices

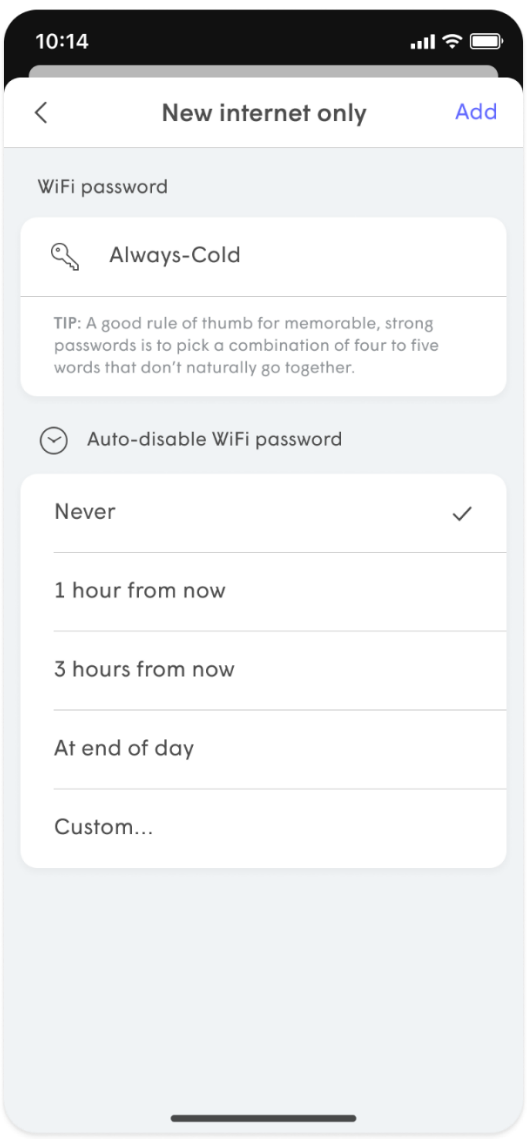

10:14
New guest password
Add
1 hour from now
3 hours from now
At the end of the day
Custom...
Share home devices
Devices
At home
Select all
Kids' XBox
Nintendo Switch
Printer
Speaker Bedroom

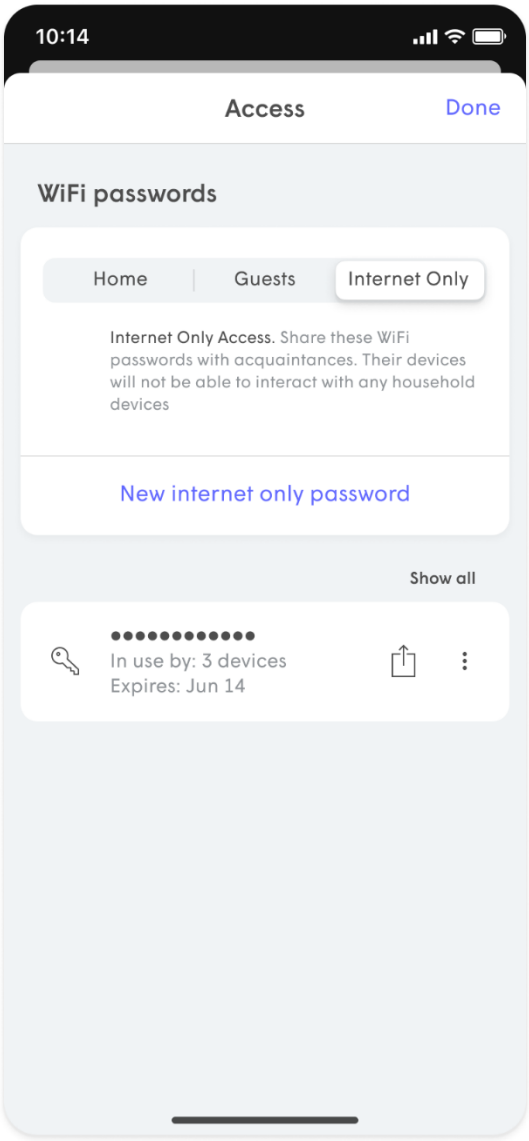
Create a new password for Internet Only

1. Open the **More** tab and click on the **Access** button.
2. While in the **Internet Only** settings page, tap on **New internet only password**.
3. Enter a new password.
4. Use the drop-down arrow next to **Auto-disable Wi-Fi Password** and choose one of the options.
5. Tap on the **Add** to save.





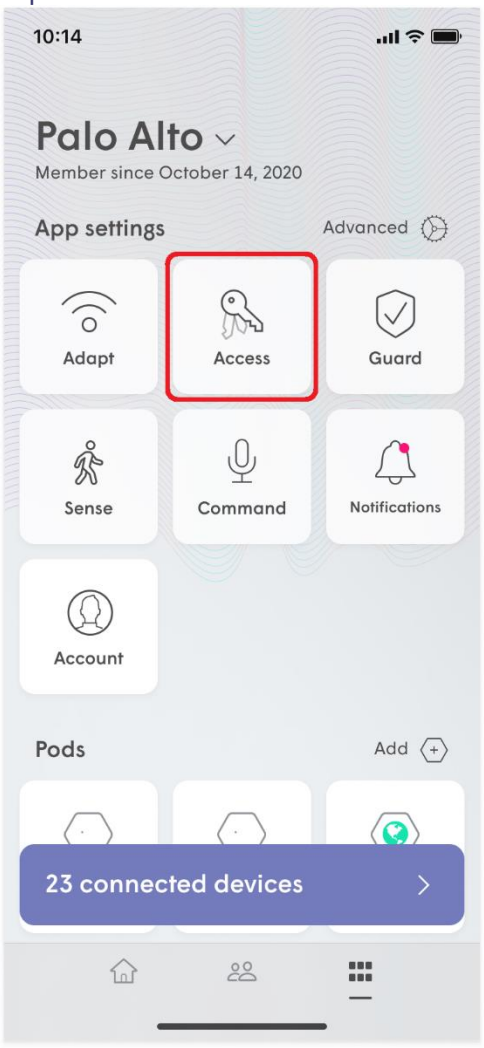

10:14
New internet only
Add
WiFi password
Always-Cold
TIP: A good rule of thumb for memorable, strong passwords is to pick a combination of four to five words that don't naturally go together.
Auto-disable WiFi password
Never
1 hour from now
3 hours from now
At end of day
Custom...

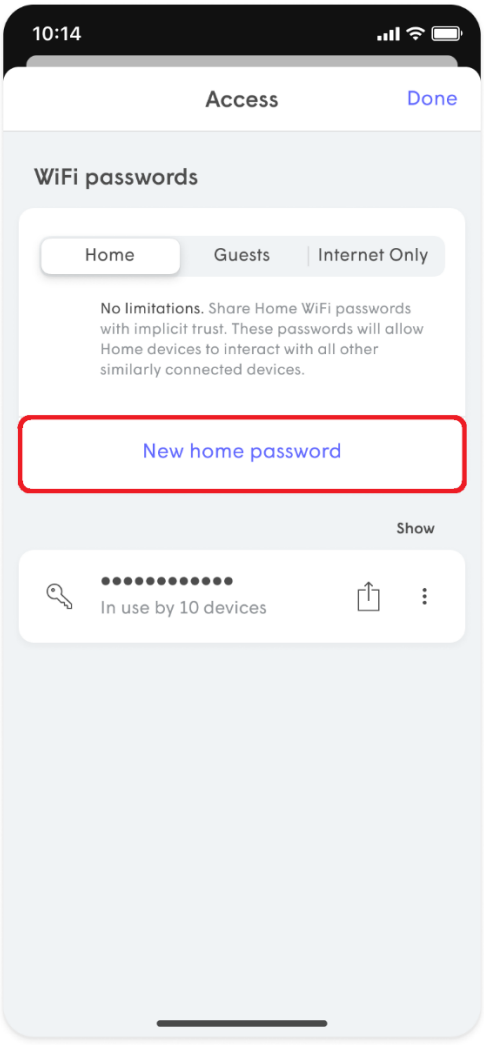

10:14
Access
Done
WiFi passwords
Home
Guests
Internet Only
Internet Only Access. Share these WiFi passwords with acquaintances. Their devices will not be able to interact with any household devices
New internet only password
Show all
••••••••••••
In use by: 3 devices
Expires: Jun 14

Create a new Wi-Fi Password for Home

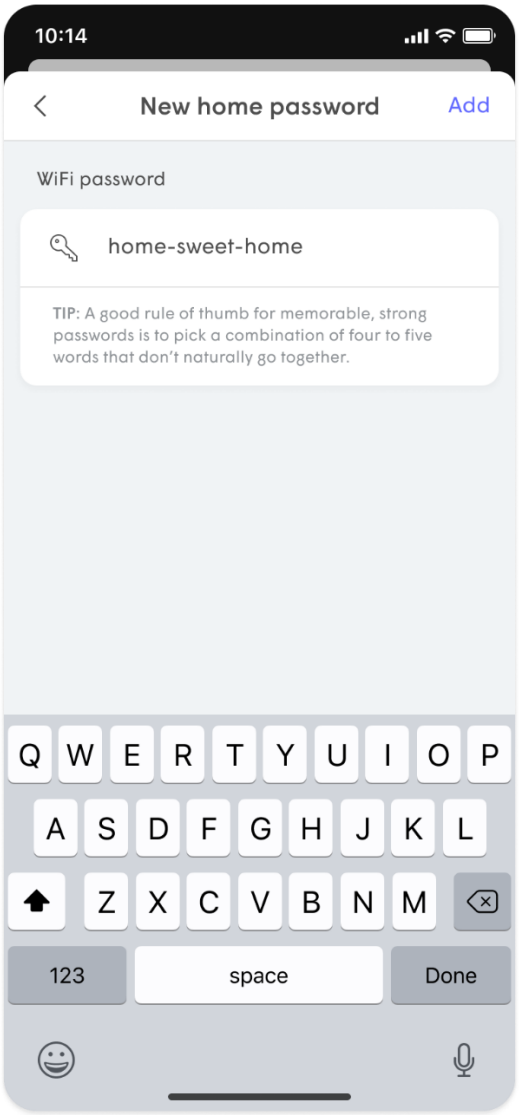
During the initial setup, the first password created is a Home zone password, although you can add more. Local network access to devices connected to your network in the Home zone can be selectively shared with devices connecting with a Guest zone password.

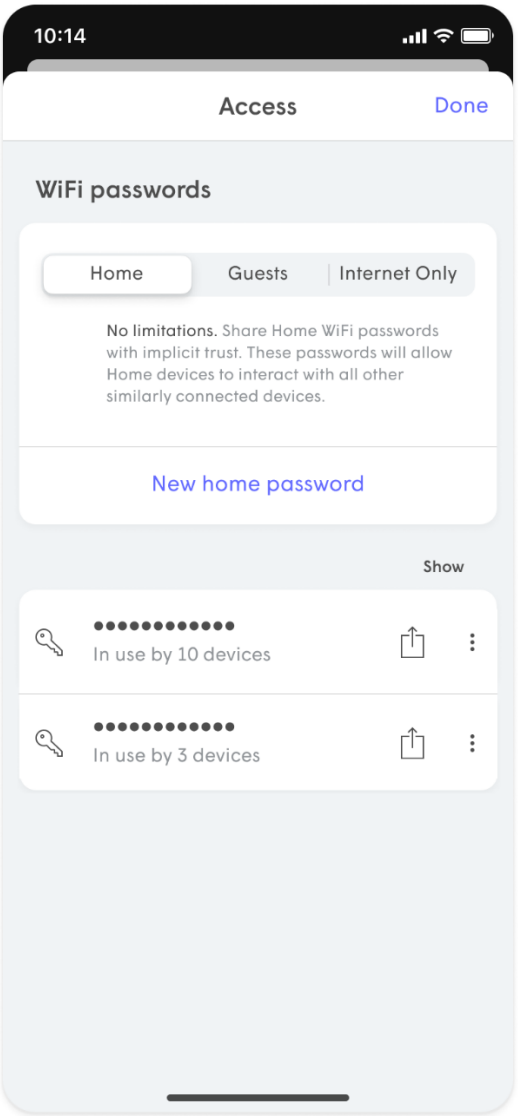
1. Open the **More** tab and click on the **Access** button.
2. While in the **Home** settings page, tap on **New home Password**.
3. Enter your new password.
4. Tap on the **Add** to save.





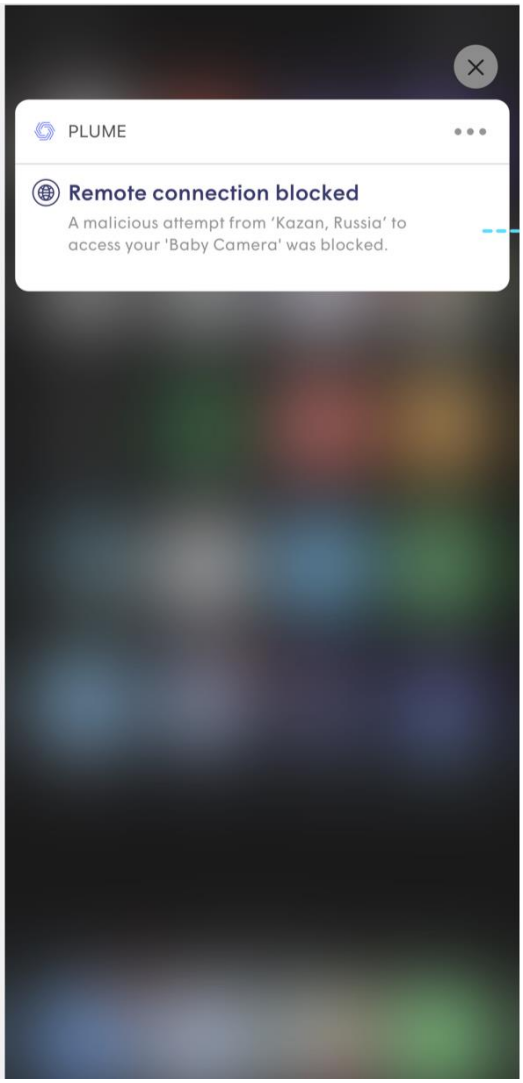
HomePass®

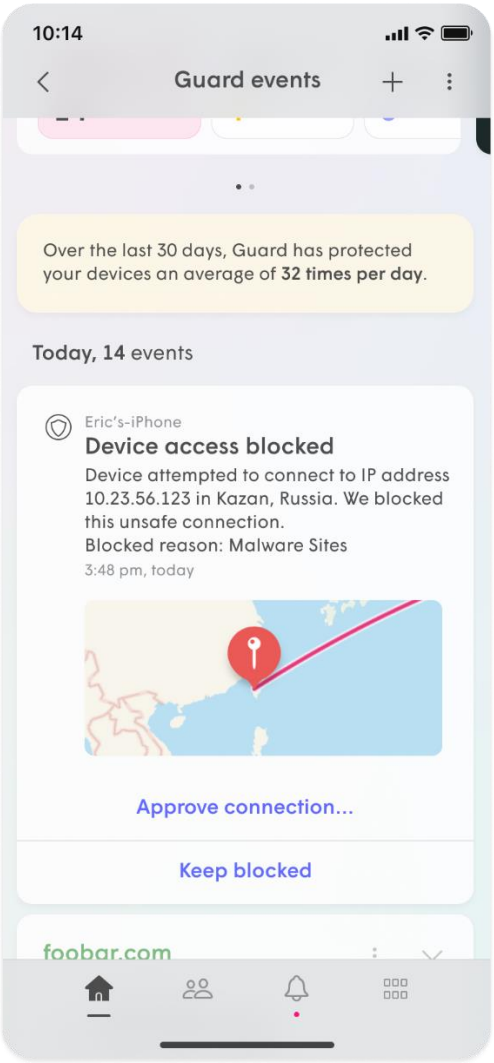

10:14
New home password
Add
WiFi password
home-sweet-home
TIP: A good rule of thumb for memorable, strong passwords is to pick a combination of four to five words that don't naturally go together.
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
space
Done


10:14
Access
Done
WiFi passwords
Home
Guests
Internet Only
No limitations. Share Home WiFi passwords with implicit trust. These passwords will allow Home devices to interact with all other similarly connected devices.
New home password
Show
In use by 10 devices
In use by 3 devices

Does Plume's Online Protection secure my network against IP based threats?

Plume's Online Protection now supports **Outbound IP Protection and Intrusion Prevention**, the latest advancement of Plume Guard features! Previously, Online Protection worked by detecting only malicious DNS based threats. By now protecting devices from connecting to malicious sites using IP addresses (**Outbound IP Protection**) and DNS based lookups, your home is now more protected than ever! Additionally, **Intrusion Prevention** automatically blocks connections from high-risk IP addresses trying to remotely connect to your devices, keeping you and your family safe from online threats.





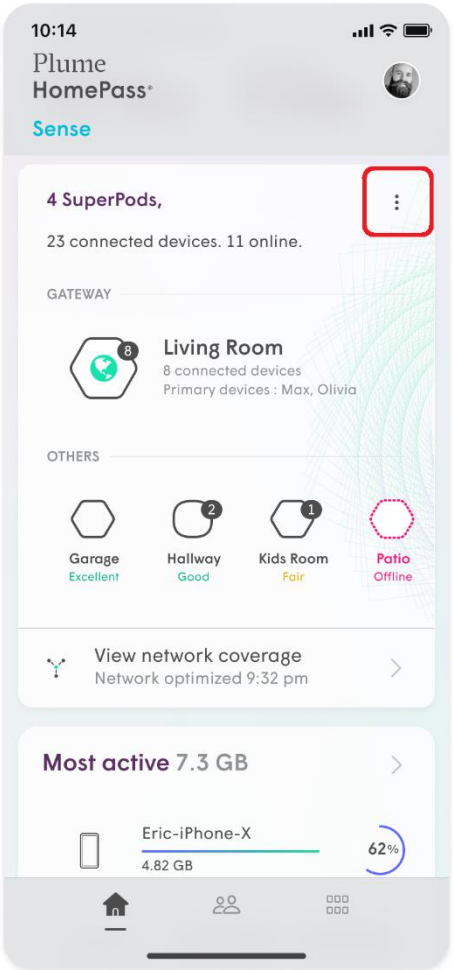
Another benefit of the IP based protection is that it enhances our Content Access feature by making it possible to manually block specific IP addresses in addition to domains.
Outbound IP Protection and Intrusion Prevention are included when turning on Online Protection if you have a SuperPod or SuperPod with WiFi 6 connected as the Gateway Pod with firmware 2.4.3 and higher.

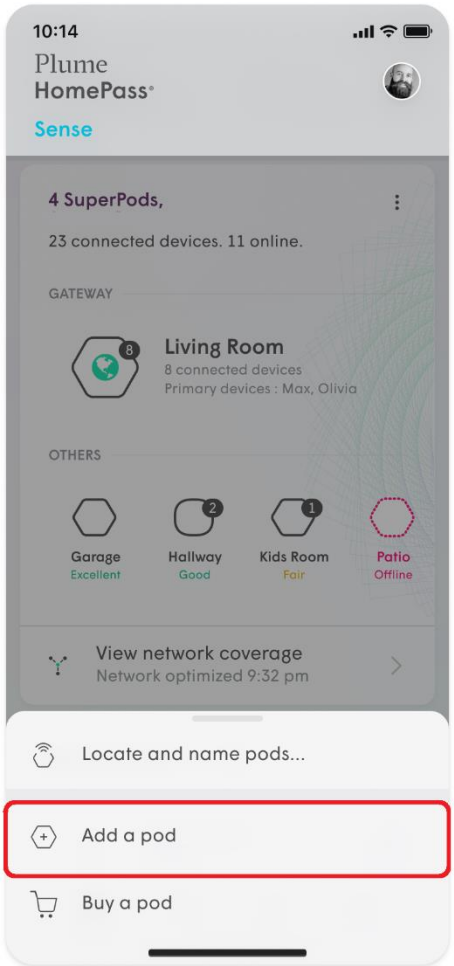
How can I add SuperPods to an existing Plume account?

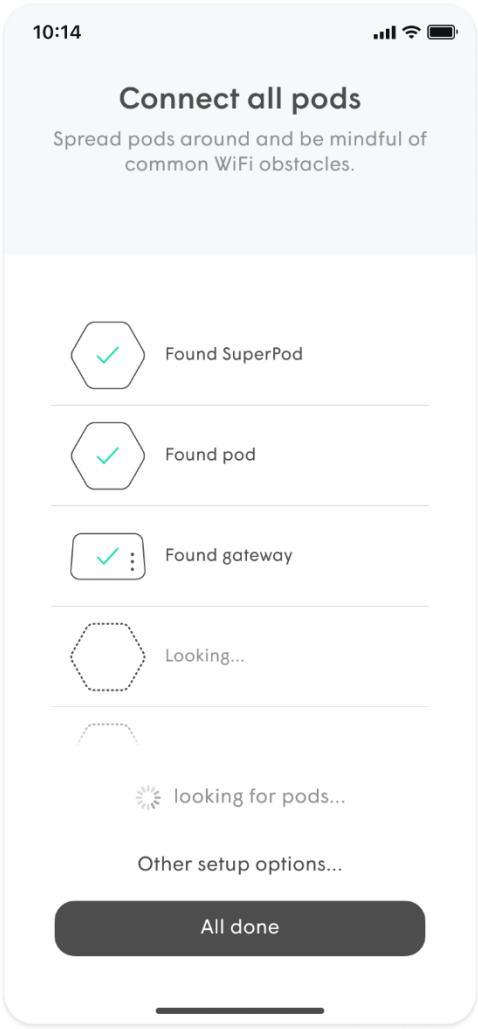
We strongly recommend that you use a SuperPod as your gateway in order to distribute the best performance across your entire home!

Adding a new pod

1. Plug in your SuperPod anywhere within your home and stay nearby.
2. On the Home page, scroll down to the **Adapt** section.
3. Tap the ⋮ to open the **Options** Menu.
4. Tap on **Add a pod**.
5. Wait until your new pod(s) is found and select **Done Adding Pods** when all additional pods have been claimed.







Upgrading or swapping your gateway pod

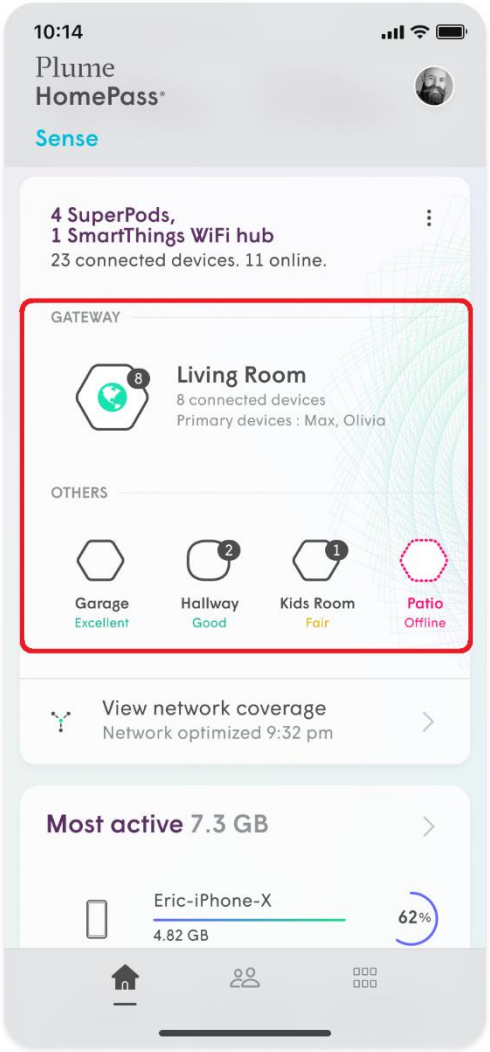
If you want to swap your existing gateway pod with another SuperPod or SuperPod with WiFi 6, continue with the following steps:

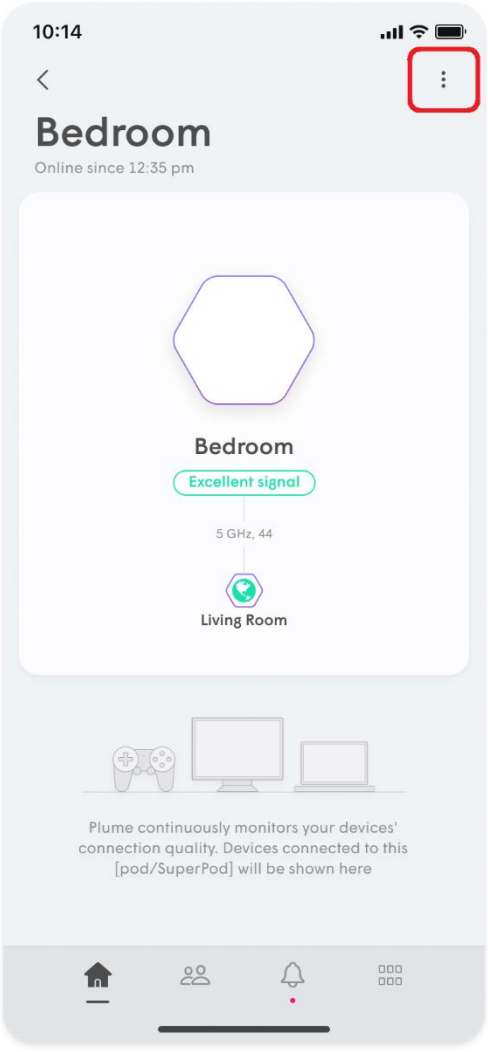
1. Unplug the current gateway pod.
2. If you have a modem, unplug it from the power outlet.
3. Connect the new SuperPod to your modem by Ethernet cable. If it a SuperPod with WiFi 6, make sure you are using the left Ethernet port.
4. Plug your new SuperPod into the power outlet. Once the SuperPod's LED starts to slowly pulse, plug your modem back into power and wait until the LED turns off.
5. You should be able to view your SuperPod and other pods in your app when the network is back online.

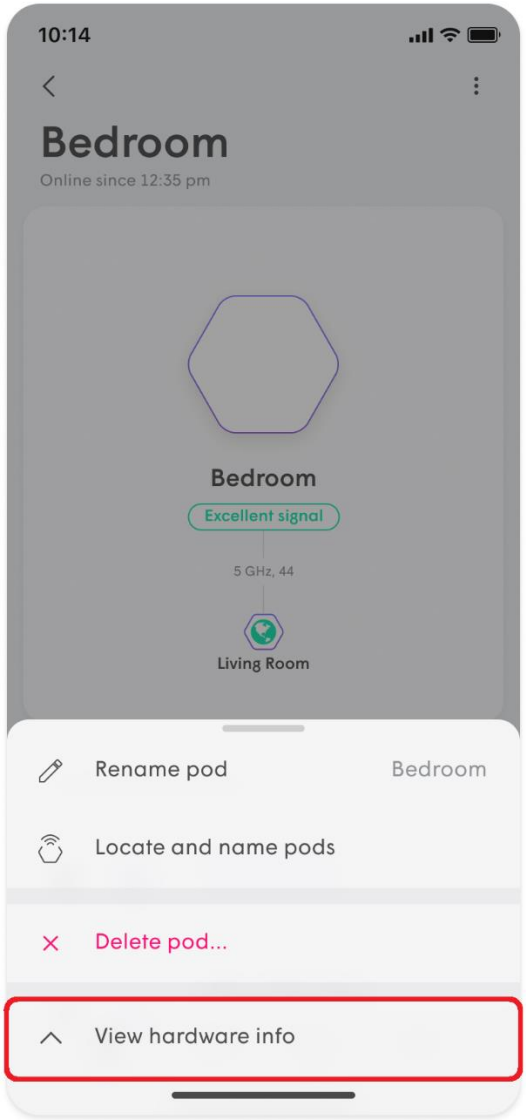
How can I check the firmware version on my pods?

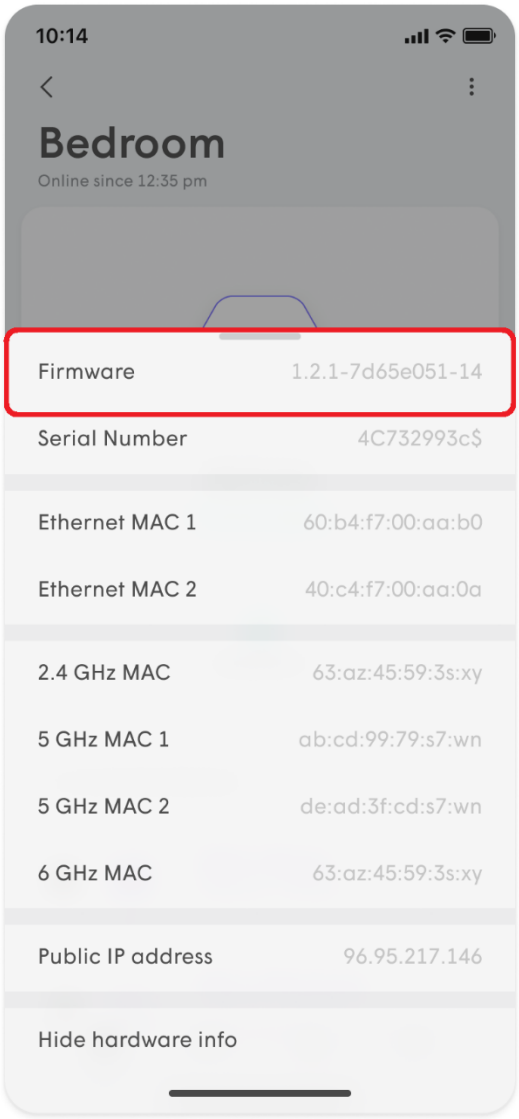
1. From the Home screen, scroll down to pod list in the **Adapt** section.
2. Tap on any pod you wish to see device information about.
3. Tap the ⋮ icon in the upper right-hand corner.
4. Tap **View Hardware Info.** Firmware version will be the first item in the list. Please visit this link for full release notes.

In addition to the firmware version, you can also view the pod's serial number, MAC address and assigned IP address.






10:14
Bedroom
Online since 12:35 pm
Bedroom
Excellent signal
5 GHz, 44
Living Room
Rename pod
Bedroom
Locate and name pods
Delete pod...
View hardware info

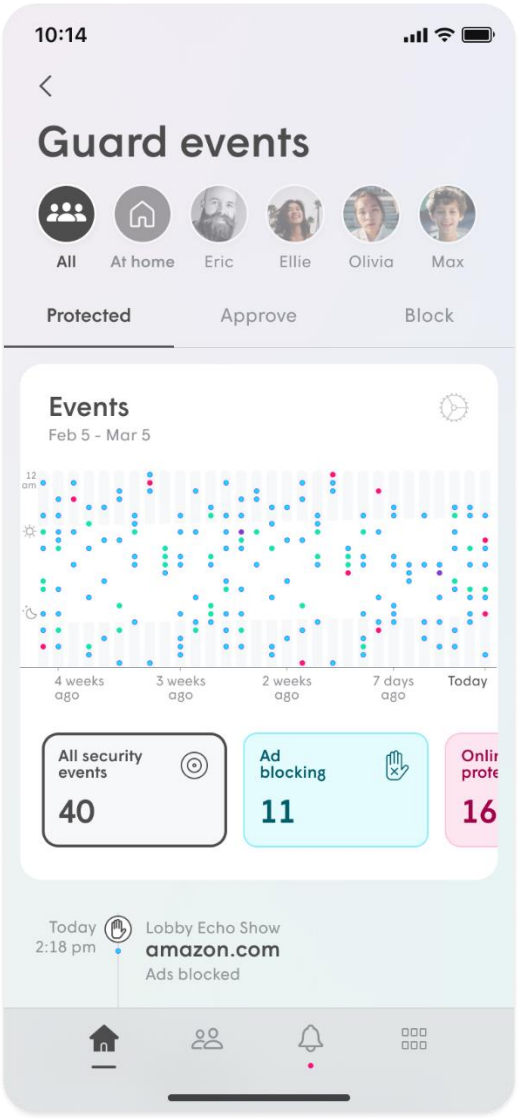

10:14
Bedroom
Online since 12:35 pm
Firmware
1.2.1-7d65e051-14
Serial Number
4C732993c$
Ethernet MAC 1
60:b4:f7:00:aa:b0
Ethernet MAC 2
40:c4:f7:00:aa:0a
2.4 GHz MAC
63:az:45:59:3s:xy
5 GHz MAC 1
ab:cd:99:79:s7:wn
5 GHz MAC 2
de:ad:3f:cd:s7:wn
6 GHz MAC
63:az:45:59:3s:xy
Public IP address
96.95.217.146
Hide hardware info

How can I delete my Plume data history?

All Plume members have the right to be forgotten. HomePass supports two different types of data deletions.

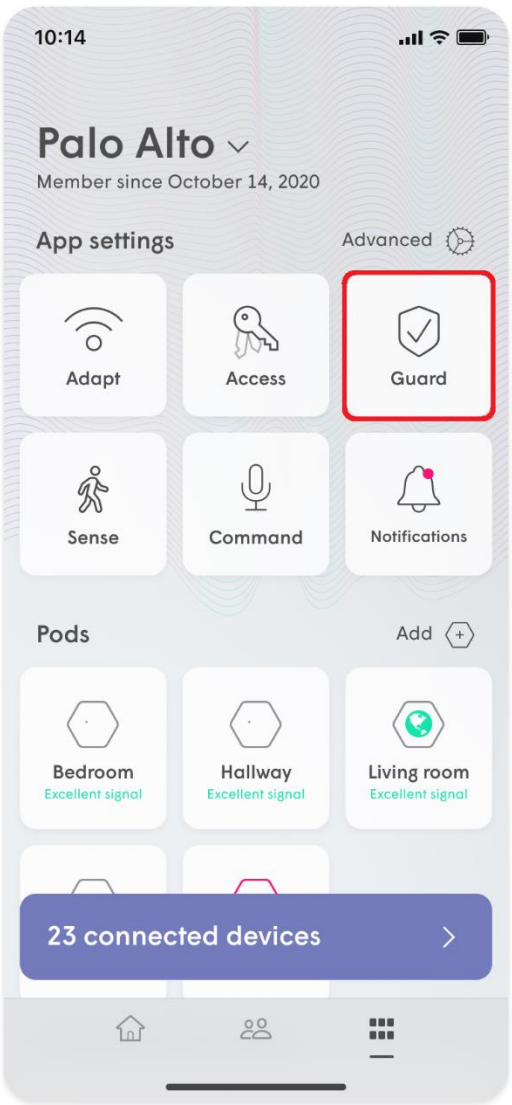
Delete security event data

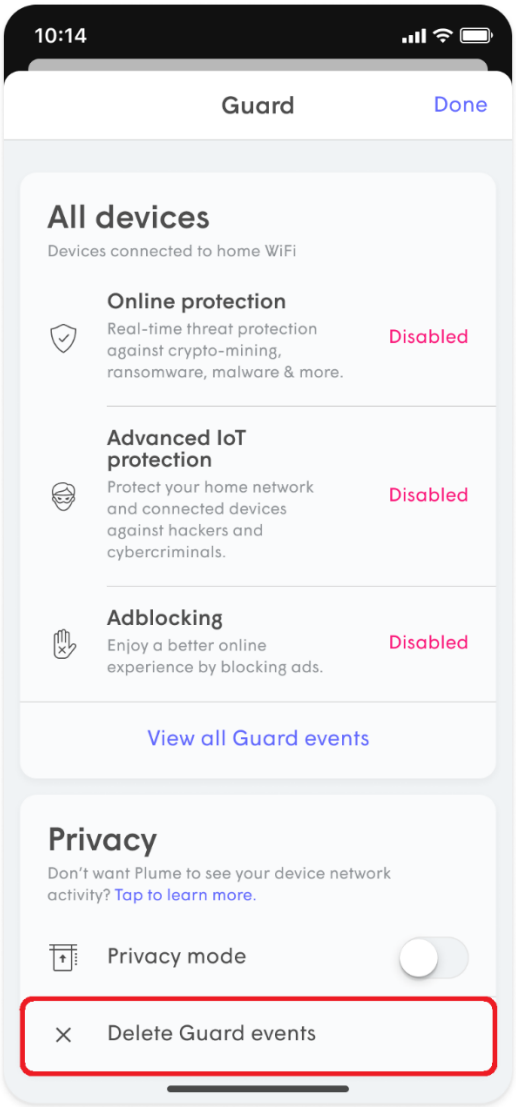
If you'd like to just remove items from your list of blocked events from either Guard or Content Access:



1. In the HomePass app, open the **More** menu.
2. Select the **Guard** option.
3. On the bottom of the Guard settings page, you will find the **Delete security events** button.
4. Simply tap the button and confirm that you would like to **clear the data.**

- Note that once deleted, this data cannot be recovered
- If you haven't disabled Guard or Content Access features, more events will continue to populate the list. Just continue to repeat this process as often as you need.



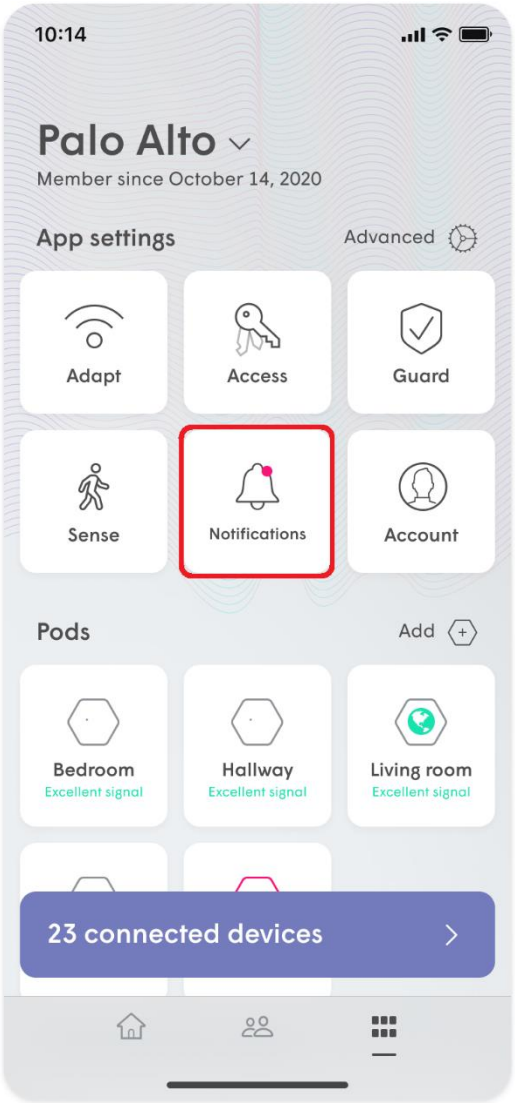


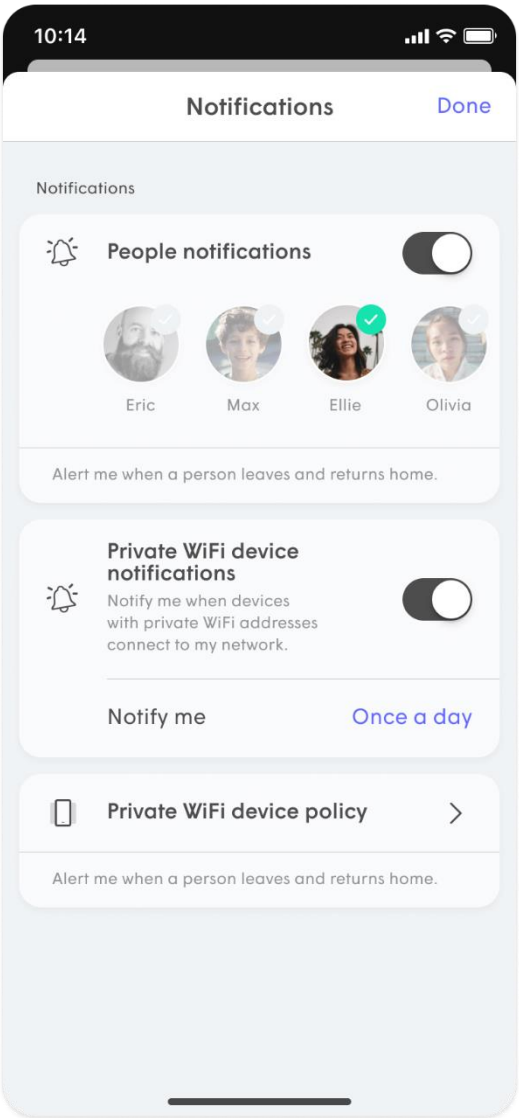
How can I tell if someone is home?

If you have assigned a primary device for everyone in your home, you can use the **People Notifications** feature to receive notifications when people return home or leave.

Enable People Notifications

1. Open the **More** menu and tap on **Notifications**.
2. Make sure **People notifications** are turned on and select the profiles for which you would like to receive alerts.





HomePass®

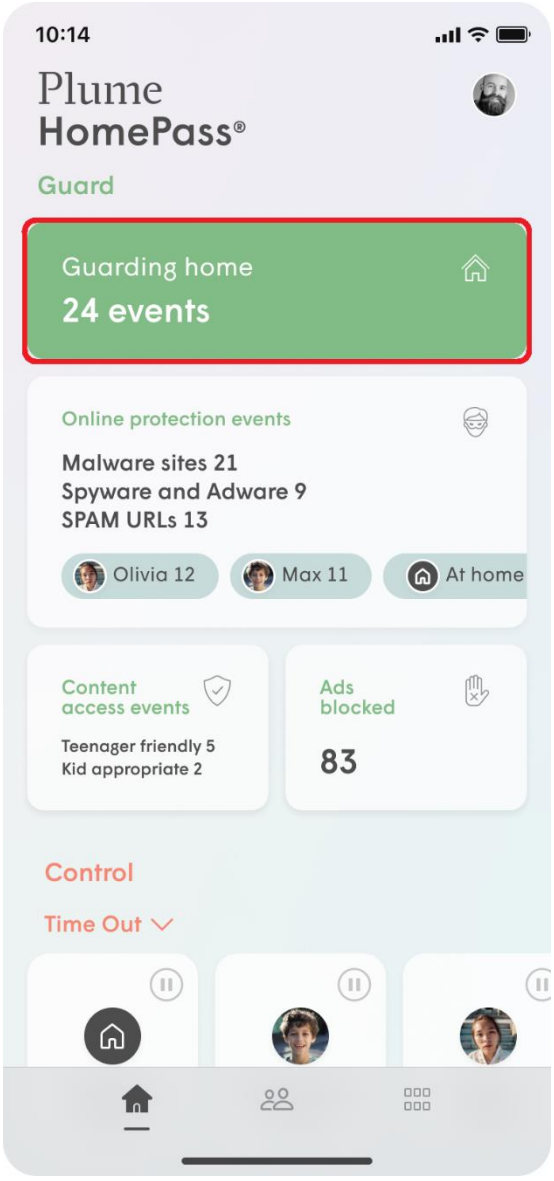
Viewing your People at Home history

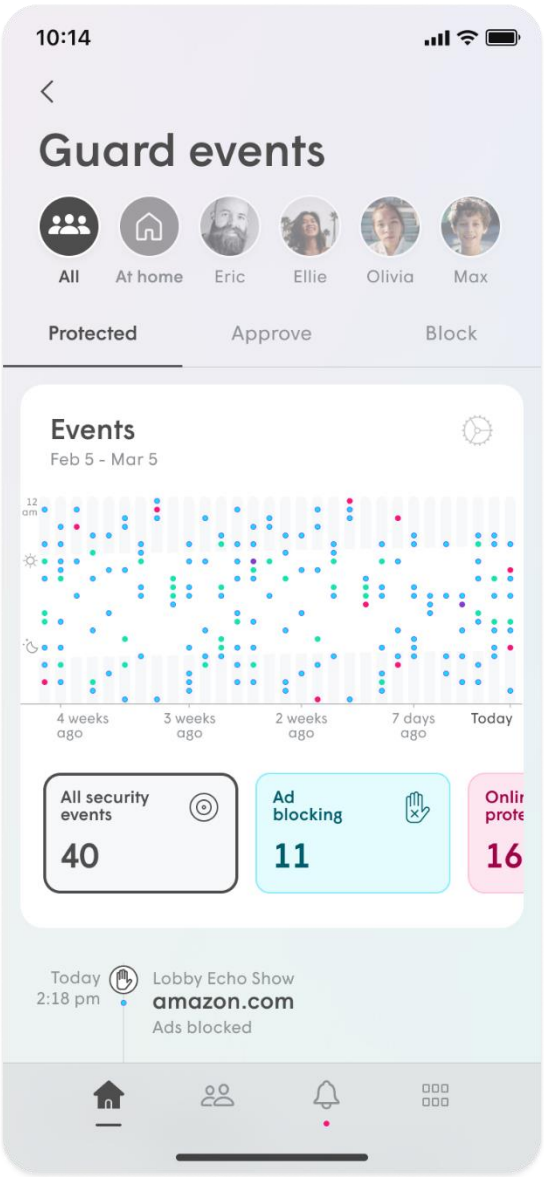
1. Open the **People Profiles** view of the HomePass App
2. If you have set up People Profiles and assigned them primary devices, the history of when they've been home will appear at the top.
3. You can use the arrows to cycle the daily event history from **Today** all the way to **6 days ago**.

Each person's status is based on when their assigned primary device connects and disconnects from the network. Because of this, it is important to assign suitable primary devices like mobile phones or Wi-Fi enabled smartwatches.
If their device disconnects because it is powered off or the Wi-Fi is turned off, it will show them as having left.
If you have **Sense Alerts** set up to be sent only when away (Smart Activation), those alerts will be sent 15 minutes after the last person with an assigned device disconnects from your network.

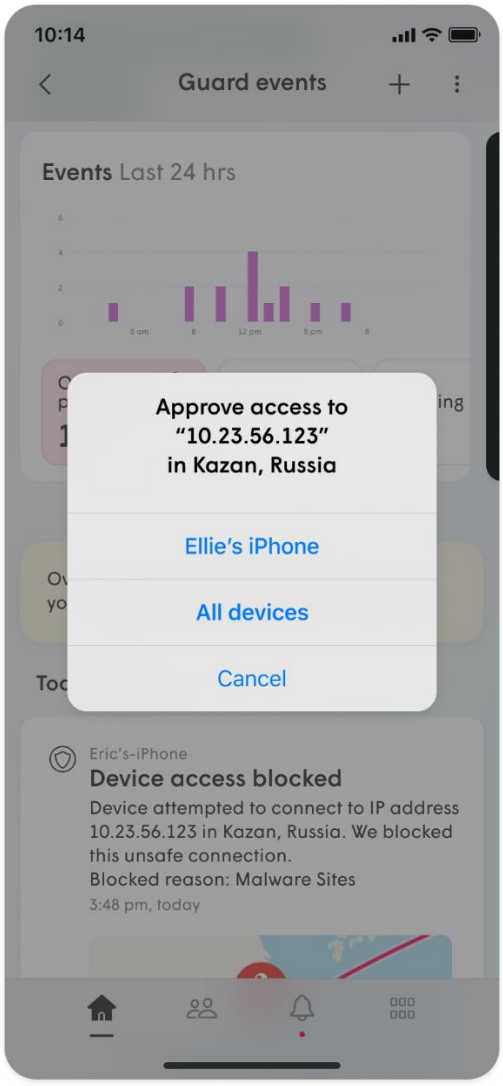
How can I tell what events have been blocked by Online Protection?

1.
    1. From the **Home** screen and tap on the **Guard events** button.
    2. The **Protected** tab will display all blocked events.
    3. You can sort the list of events shown below by type of event or by choosing a person.
    4. Simply tap on any event to add the site to the **Approved** list if you trust that it is actually safe.






10:14
Guard events
Today
2:18 pm
Lobby Echo Show
amazon.com
Ads blocked
Today
2:17 am
iPad Air
section.io
Blocked reason : Phishing and Other Frauds
Today
2:16 am
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.
East Palo Alto
Menlo Park
Palo Alto
Stanford University
Ladera

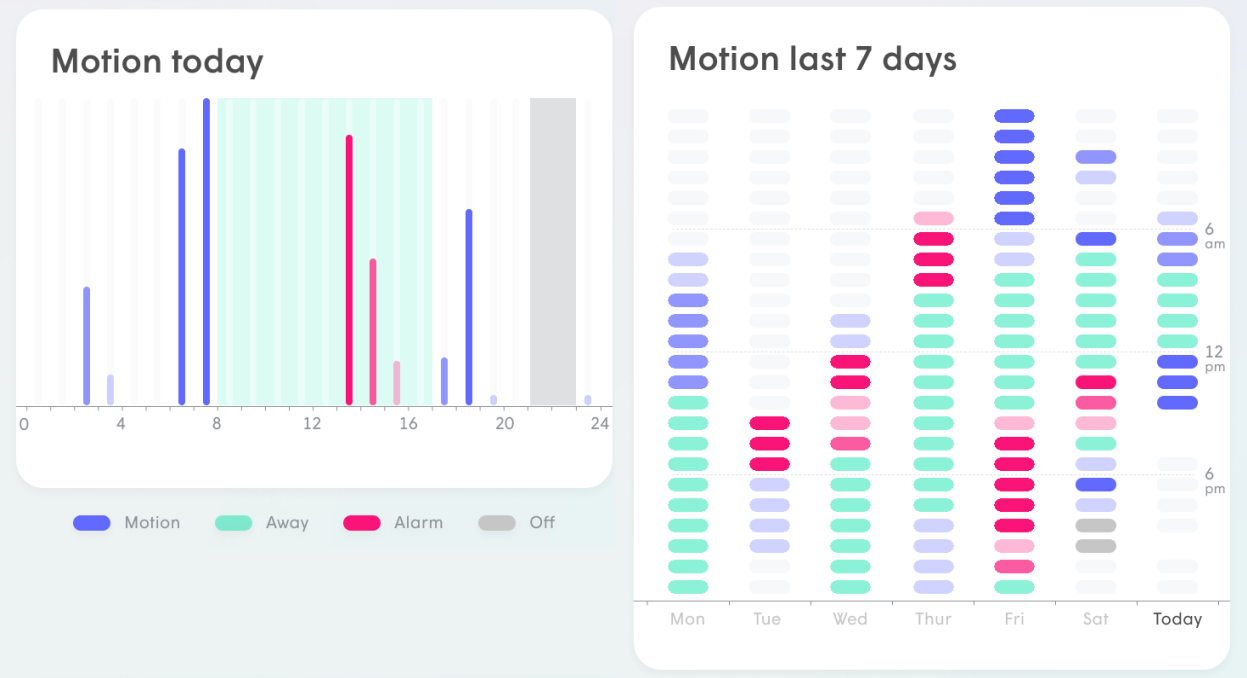

10:14
Guard events
Events Last 24 hrs
Approve access to
"10.23.56.123"
in Kazan, Russia
Ellie's iPhone
All devices
Cancel
Eric's-iPhone
Device access blocked
Device attempted to connect to IP address 10.23.56.123 in Kazan, Russia. We blocked this unsafe connection.
Blocked reason: Malware Sites
3:48 pm, today

How do I access my home's motion history?

What is kind of motion history is displayed?

There are two available historical views:

- **Motion Today** - Each column represents an hour.
- **Motion Last 7 Days** - Each segment represents 1 hour.

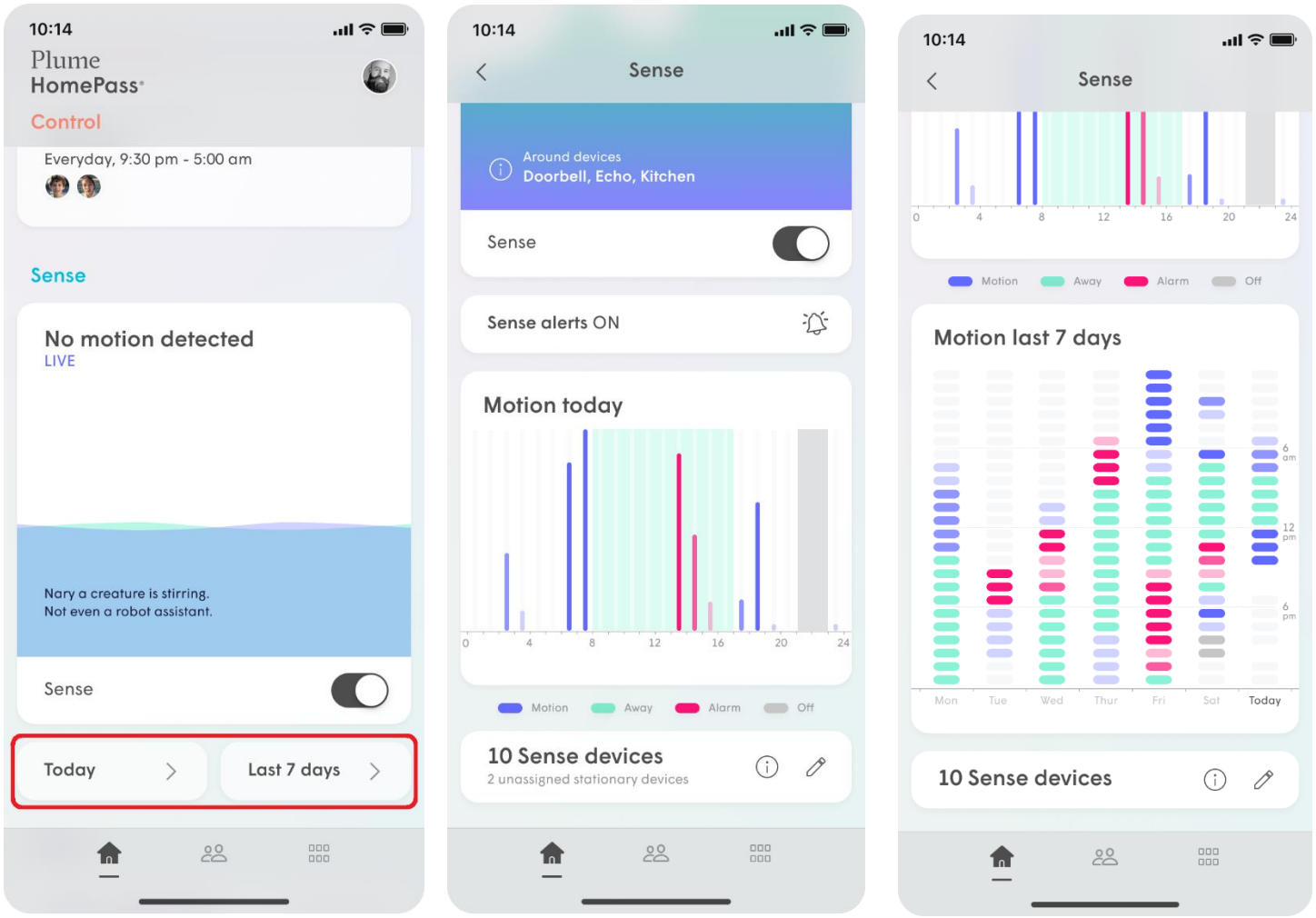


In each of the historical views, the colours in the charts represent the various states of the motion detection system.

- **Blue** - Motion was detected (System unarmed)
- **Red** - Motion was detected when people are away (System armed) and triggered a Sense Alert
- **Green** - All people are away (System armed) and no motion is present in the 7-day view. Layered in the background of the Today view.
- **Grey** - Plume Sense motion detection was turned off in the 7-day view. Layered in the background in the Today view.
- The degree of transparency represents the intensity of the motion at the time.

How do view motion detection history?

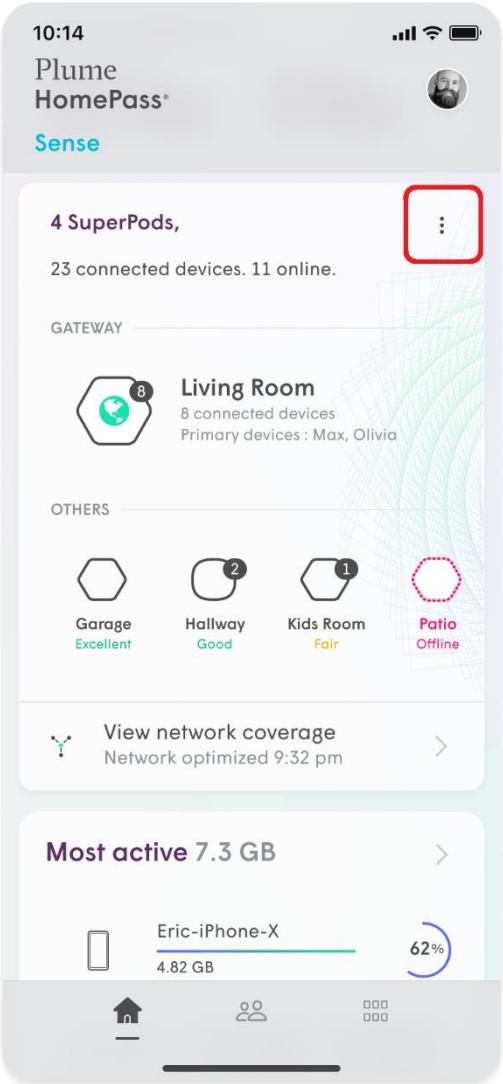
1. From the **home screen**, scroll down until you get to the **Sense** section.
2. Tap on either the **Today or Last 7 days** buttons to view that historical view.

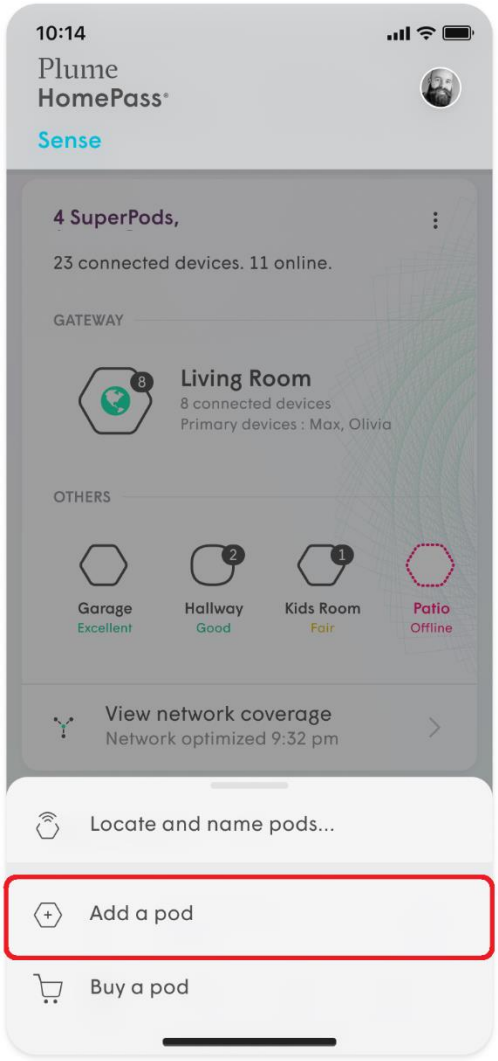


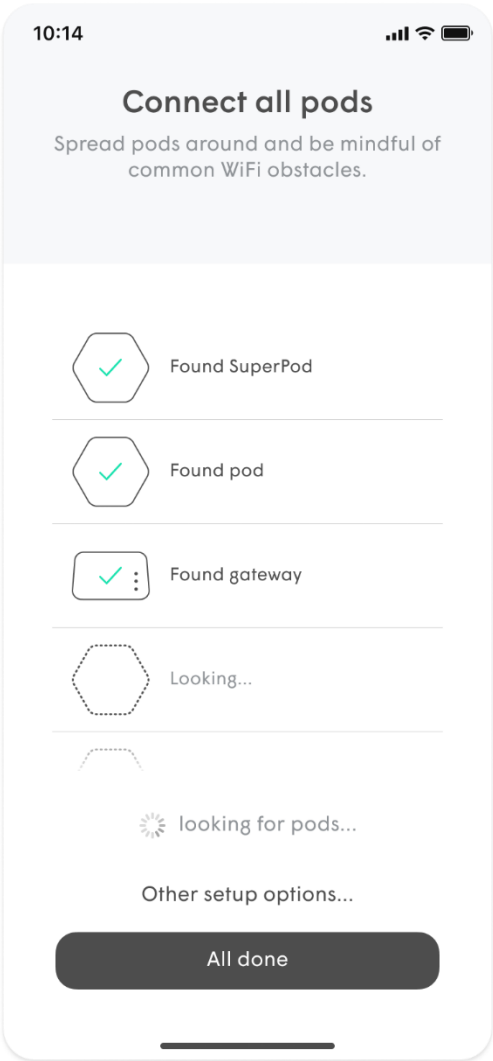
How do I add a pod to my network?

Adding additional pods is effortless!

1. From the **Home** screen, scroll down to the **Adapt** section.
2. Tap on the ⋮ icon. and choose the **Add a pod** option.
3. While the app shows that it is "looking for pods...", plug-in the new pod(s) or wait for them to connect if already they were already plugged-in.
4. When the new pod is added, tap **Done Adding Pods**.
5. You can now see the new pod added in the topology view of app.







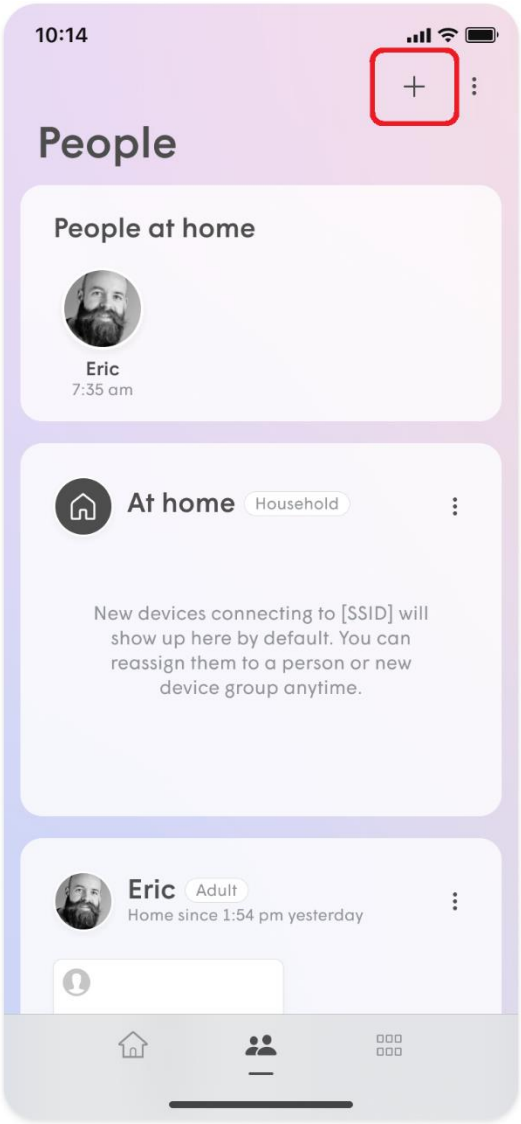
How do I add or remove a person?

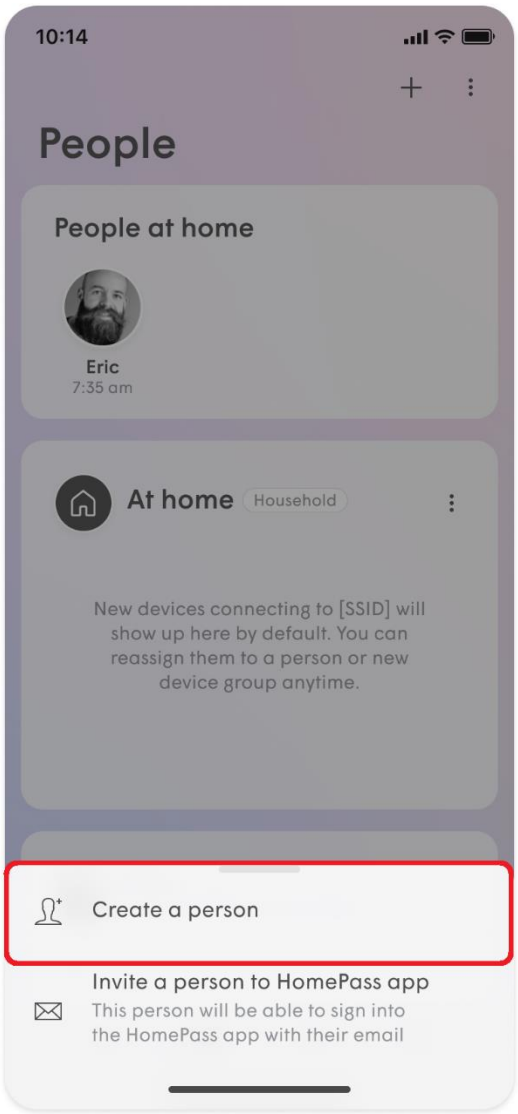
Adding people allows you to conveniently monitor and manage their Wi-Fi access.

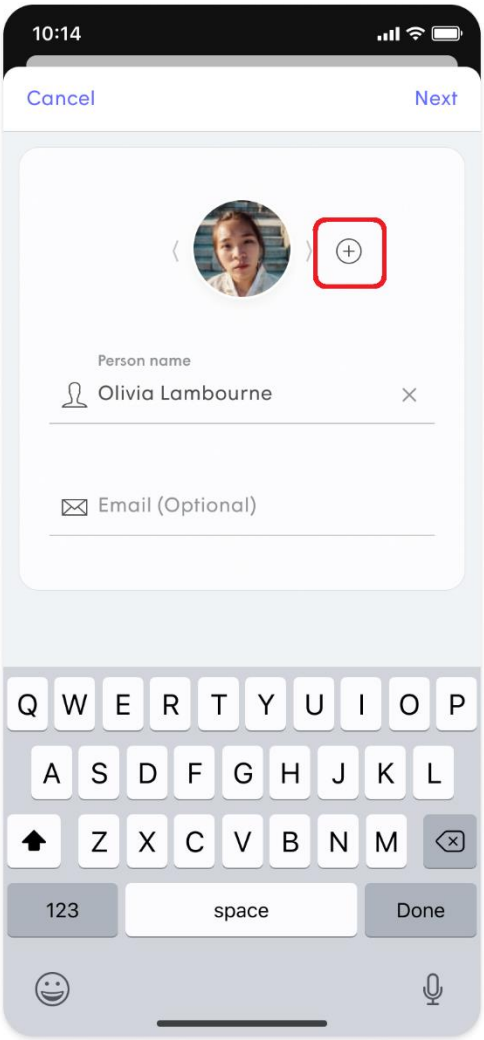
Adding a Person

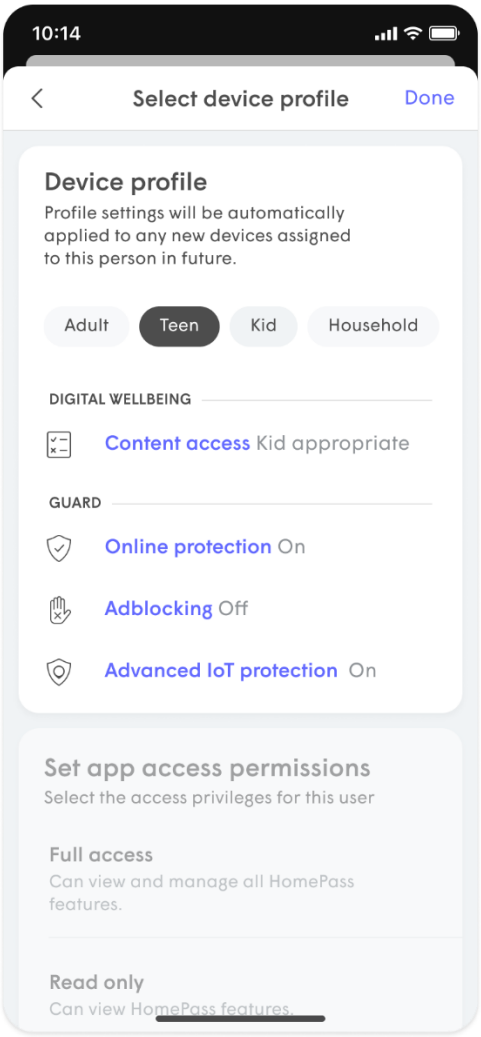
1. From the **People** screen, tap on **+** button.
2. Choose the **Create a person** option.
3. Add a photo using the **+** , enter the **Person name** and **Email** (optional) and tap on **Next**.
4. Set their Device profile information. This allows you to control **Content access** as well as their **Guard** settings for all their assigned devices while they are connected to the network.
5. Tap on **Done** and the person will be added to the list of people.
6. Use the **Tap to assign device** option under their card. The devices you select will apply the rules set in the previous step to those devices and allow you to monitor and manage the person's Internet usage.
7. Once all device have been selected and you tap on **Done**, you will be prompted to assign a Primary device, which is used to determine if they are home. Be sure to choose a device that they will always take with them.
8. Tap on **Done** once a primary device is chosen.

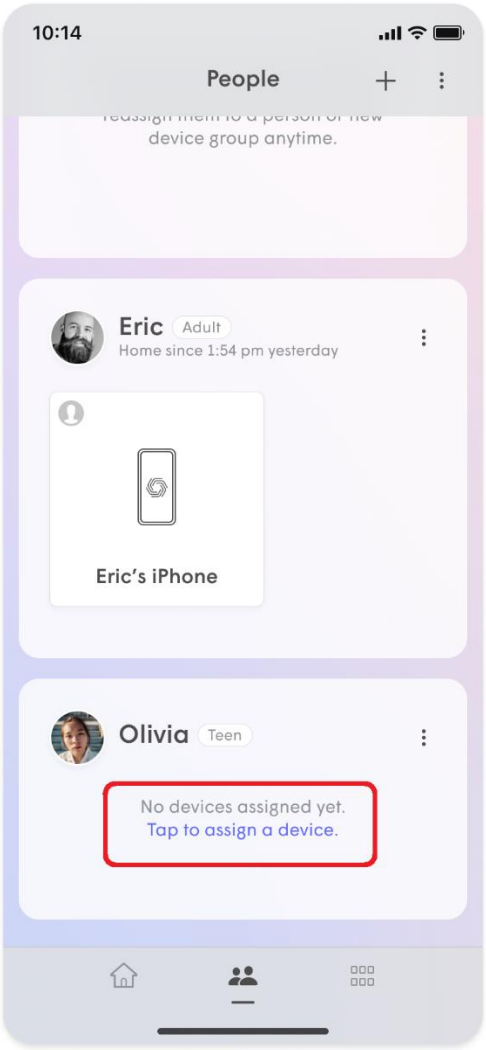
Please note that creating a person using the steps above does not give them the ability to manage the network. Click here if you want to Invite a person to help you manage the the network.

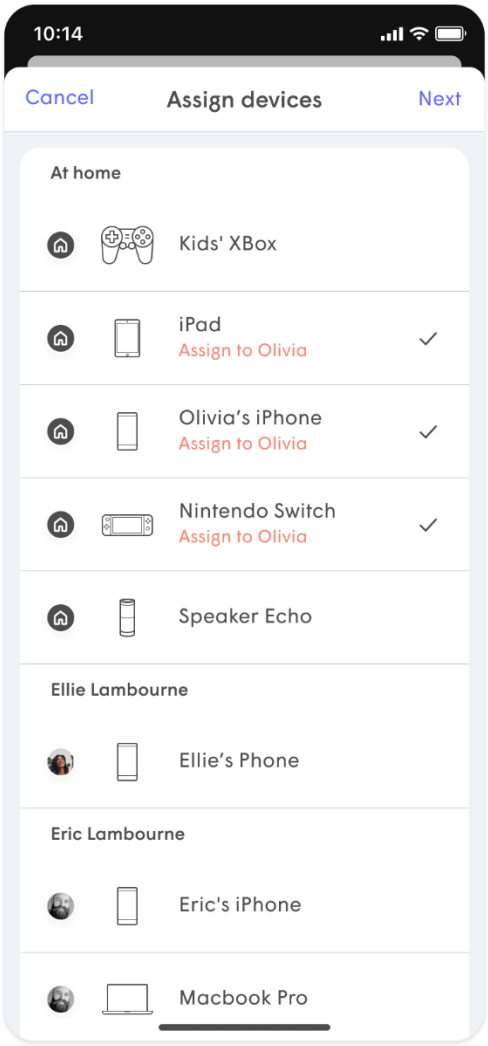

10:14
People
People at home
Eric
7:35 am
At home
Household
New devices connecting to [SSID] will show up here by default. You can reassign them to a person or new device group anytime.
Eric
Adult
Home since 1:54 pm yesterday

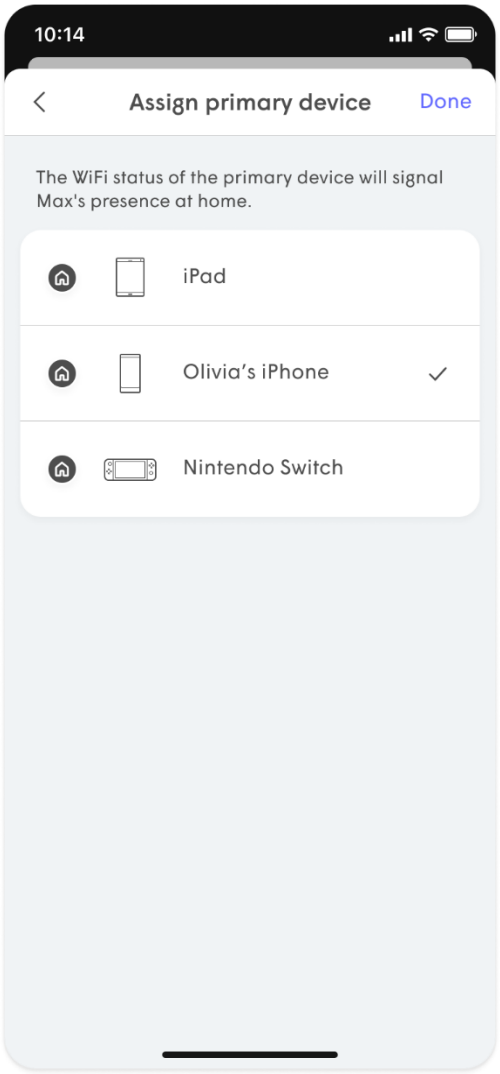

10:14
People
People at home
Eric
7:35 am
At home
Household
New devices connecting to [SSID] will show up here by default. You can reassign them to a person or new device group anytime.
Create a person
Invite a person to HomePass app
This person will be able to sign into the HomePass app with their email


10:14
Cancel
Next
Person name
Olivia Lambourne
Email (Optional)
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
space
Done


10:14
Select device profile
Done
Device profile
Profile settings will be automatically applied to any new devices assigned to this person in future.
Adult
Teen
Kid
Household
DIGITAL WELLBEING
Content access Kid appropriate
GUARD
Online protection On
Adblocking Off
Advanced IoT protection On
Set app access permissions
Select the access privileges for this user
Full access
Can view and manage all HomePass features.
Read only
Can view HomePass features.


10:14
People
device group anytime.
Eric
Adult
Home since 1:54 pm yesterday
Eric's iPhone
Olivia
Teen
No devices assigned yet.
Tap to assign a device.

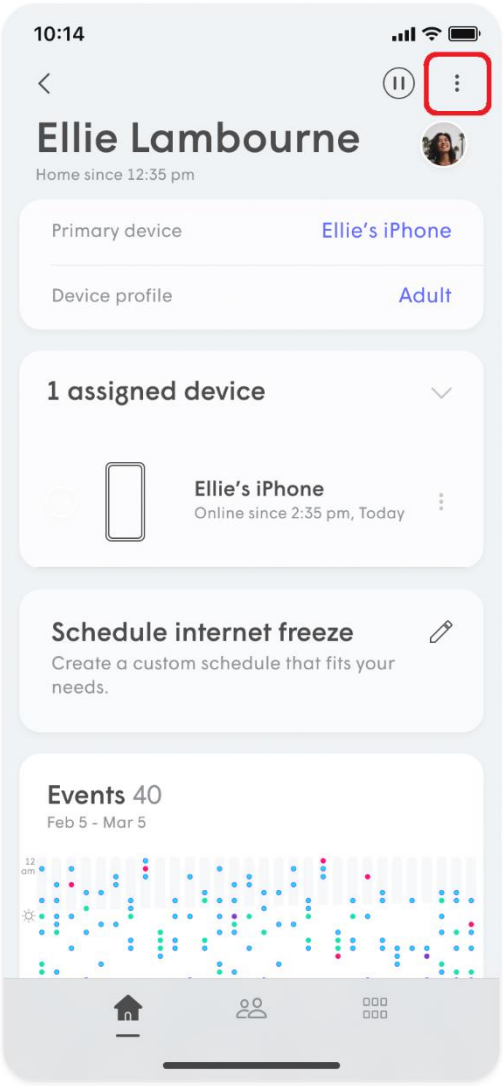

10:14
Cancel
Assign devices
Next
At home
Kids' XBox
iPad
Assign to Olivia
Olivia's iPhone
Assign to Olivia
Nintendo Switch
Assign to Olivia
Speaker Echo
Ellie Lambourne
Ellie's Phone
Eric Lambourne
Eric's iPhone
Macbook Pro

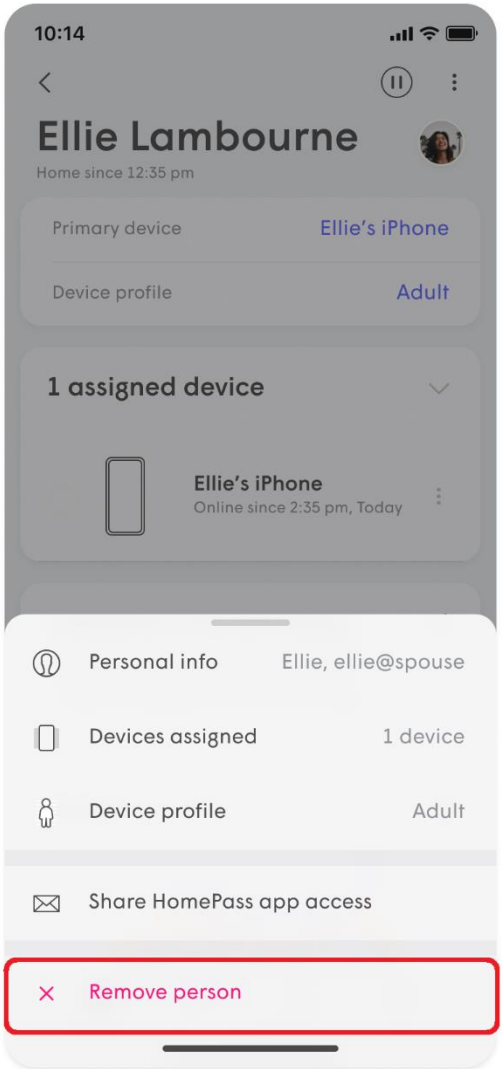


Removing a Person

1. From the person's detail screen, tap on the ⋮ on the top right-hand corner.
2. Tap on **Remove person** which will remove the profile and historical data consumption information for that person. All previously assigned devices for that person will now be unassigned.

Note: This does not disable their access to the Wi-Fi if they still have the password.


10:14
Ellie Lambourne
Home since 12:35 pm
Primary device
Ellie's iPhone
Device profile
Adult
1 assigned device
Ellie's iPhone
Online since 2:35 pm, Today
Schedule internet freeze
Create a custom schedule that fits your needs.
Events 40
Feb 5 - Mar 5

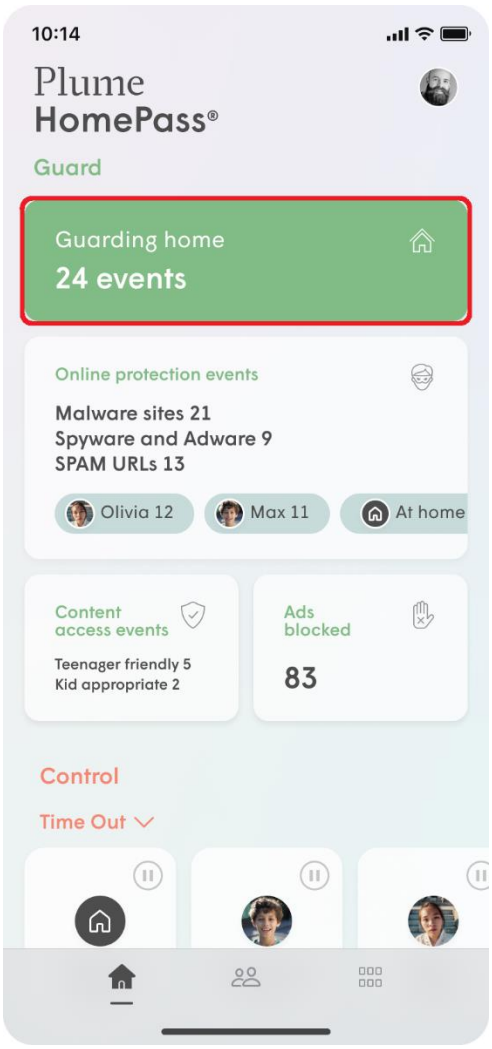

10:14
Ellie Lambourne
Home since 12:35 pm
Primary device
Ellie's iPhone
Device profile
Adult
1 assigned device
Ellie's iPhone
Online since 2:35 pm, Today
Personal info
Ellie, ellie@spouse
Devices assigned
1 device
Device profile
Adult
Share HomePass app access
Remove person

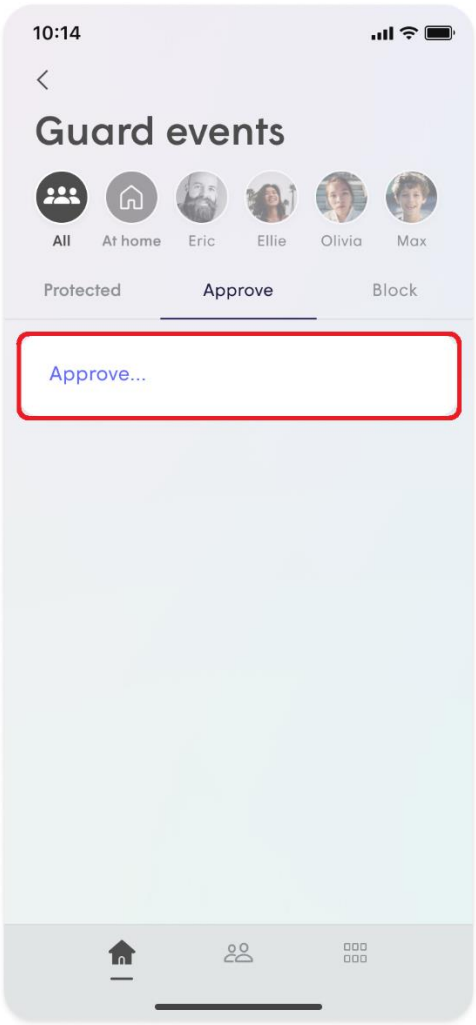
How do I approve (unblock) a website?

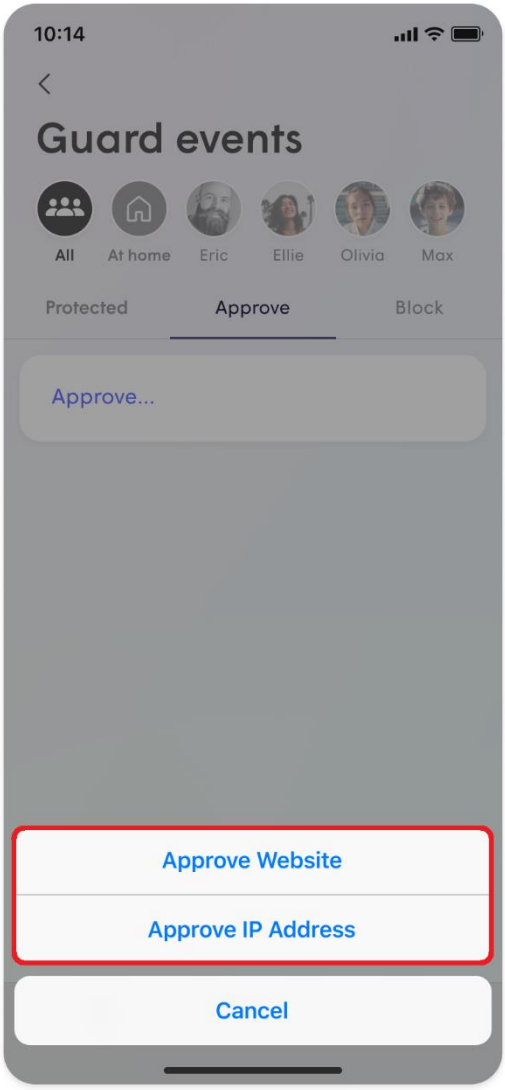
You can approve a website for a person, the entire network or a device if not assigned to a person. Up to 50 websites can be approved in total.
If you notice a website has been incorrectly blocked, please report it to support.

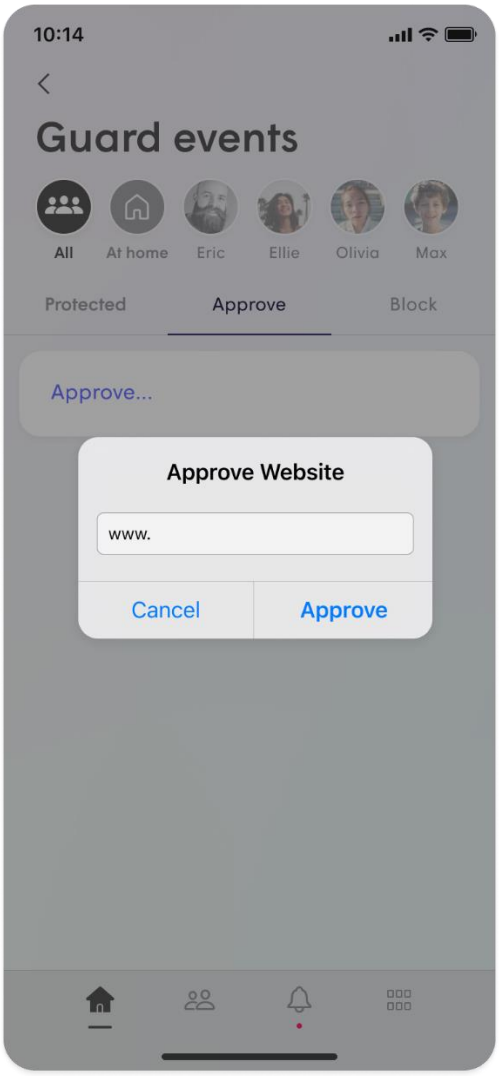
Approving Websites for Everyone

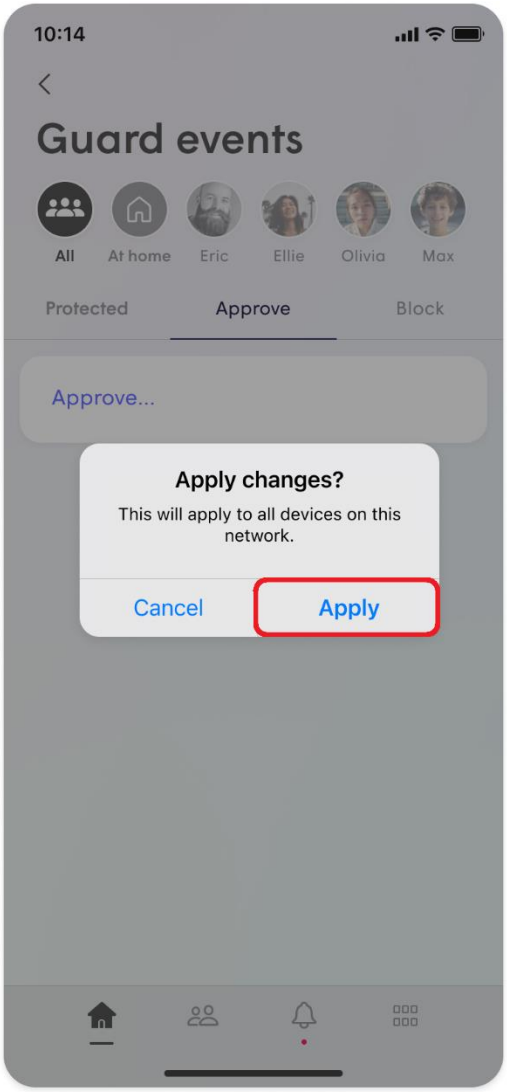
1. From the Home page, tap on the **Guard events**.
2. Go to **Approve** tab and tap on **Approve..**
3. Choosing **Approve Website** allows you to enter the URL of domain, while **Approve IP Address** allows you to enter the server IP address.
4. Enter the URL or IP address and tap on **Approve** to save. Please note that the full domain name is required. For example; make sure to write "youtube.com" instead of "youtube".
5. Tap on **Apply** to confirm the changes.
6. Additionally, you are able to view previously blocked sites under the **Protected** tab. Tap or swipe on the blocked event to start the approval flow.

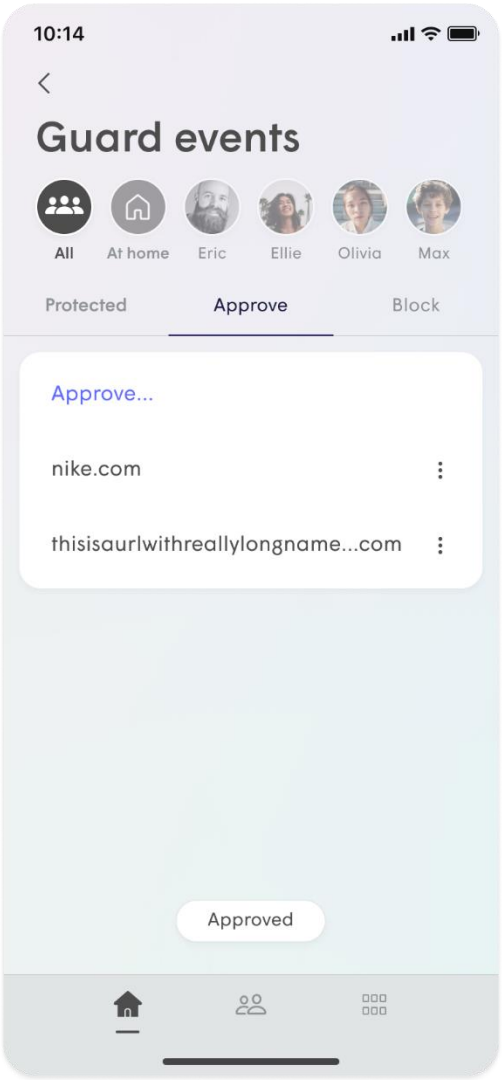

10:14
Plume
HomePass®
Guard
Guarding home
24 events
Online protection events
Malware sites 21
Spyware and Adware 9
SPAM URLs 13
Olivia 12
Max 11
At home
Content access events
Teenager friendly 5
Kid appropriate 2
Ads blocked
83
Control
Time Out


10:14
Guard events
All
At home
Eric
Ellie
Olivia
Max
Protected
Approve
Block
Approve...


10:14
Guard events
All
At home
Eric
Ellie
Olivia
Max
Protected
Approve
Block
Approve...
Approve Website
Approve IP Address
Cancel

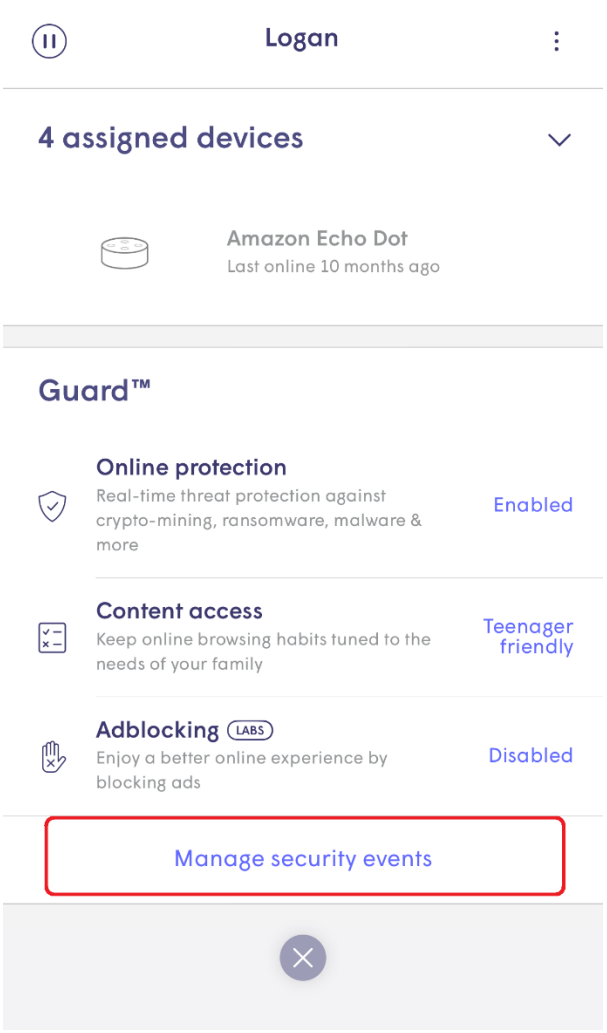

10:14
Guard events
All
At home
Eric
Ellie
Olivia
Max
Protected
Approve
Block
Approve...
Approve Website
www.
Cancel
Approve

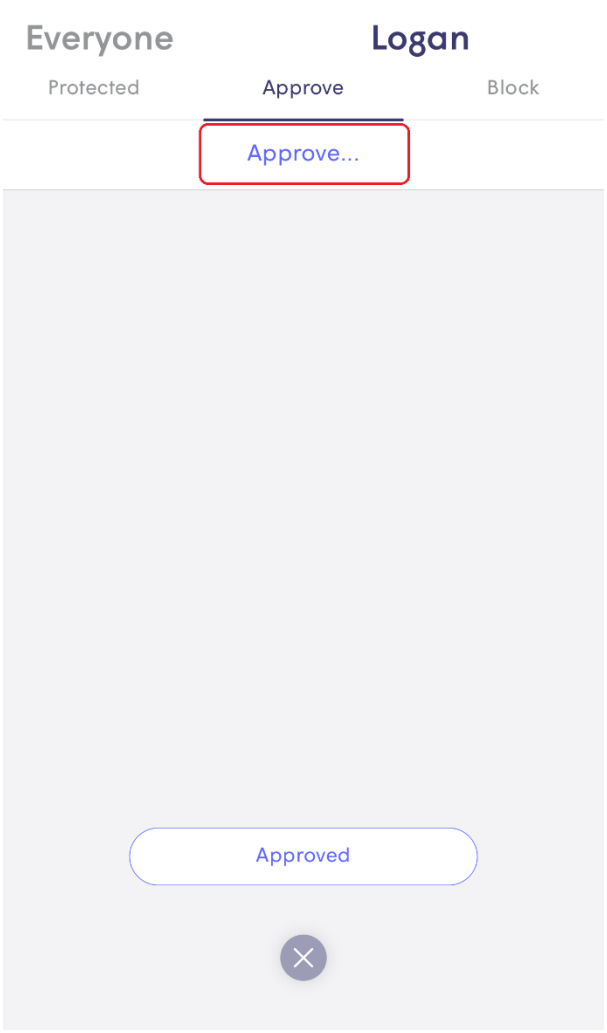


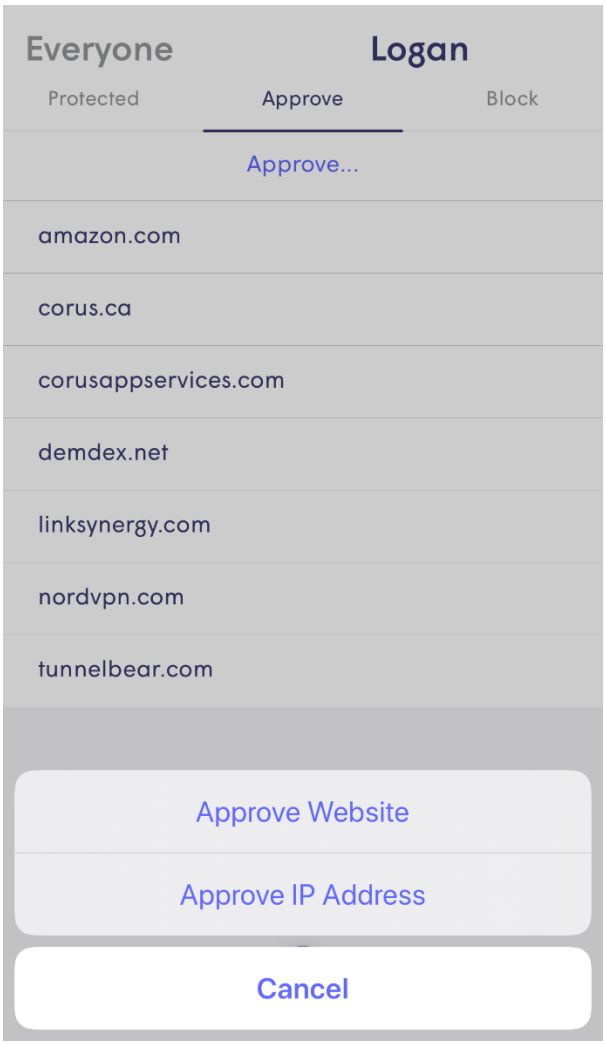


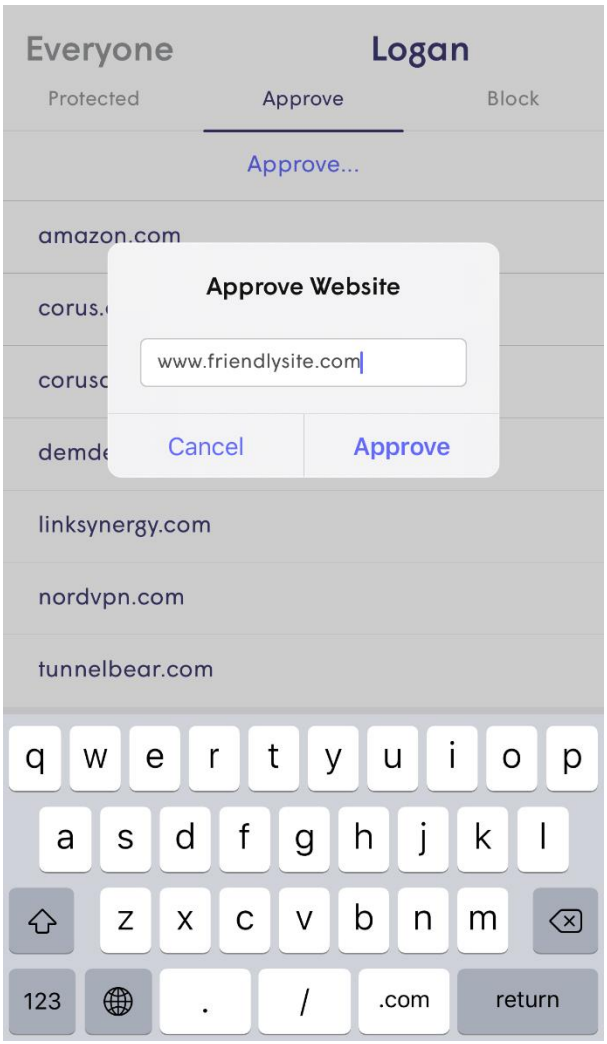
Approve websites at a person or device level

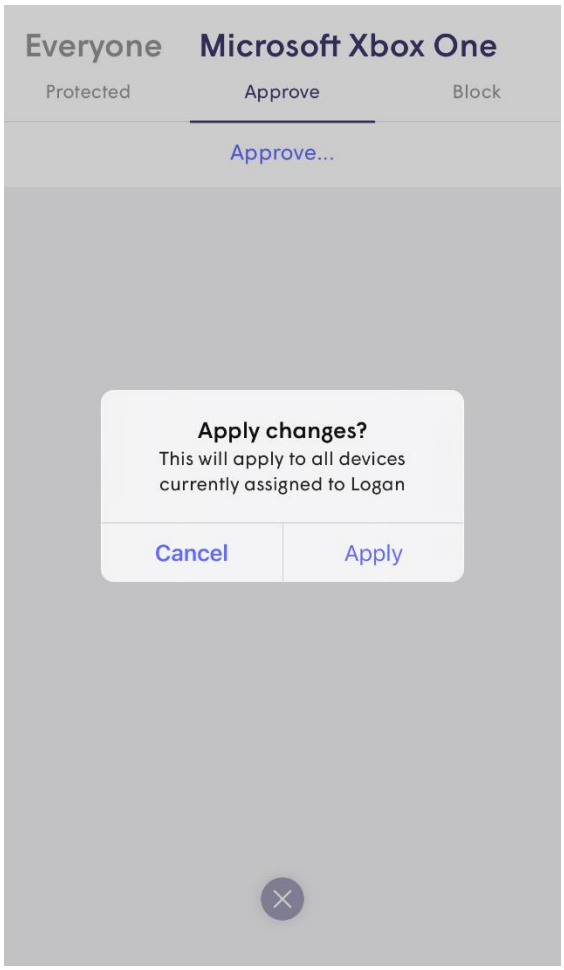
1. Navigate to the desired person or device
2. Tap on **Manage security events** at the bottom of the page
3. Tap on **Approve**
4. Choosing **Approve Website** allows you to enter the URL of domain, while **Approve IP Address** allows you to enter the server IP address.
5. Based on your previous choice, enter the URL or IP address and tap the checkmark to save. The full domain name is required for websites. For example; make sure to write "youtube.com" instead of "youtube".
6. Tap on **Approve** to confirm your choice.
7. If you are approving the site for a device that has been assigned to a person, the rule will also apply to the person. Likewise, approving a site for the person automatically applies that rule to all of their assigned devices. If the device is not assigned, the rule will only apply to the device.

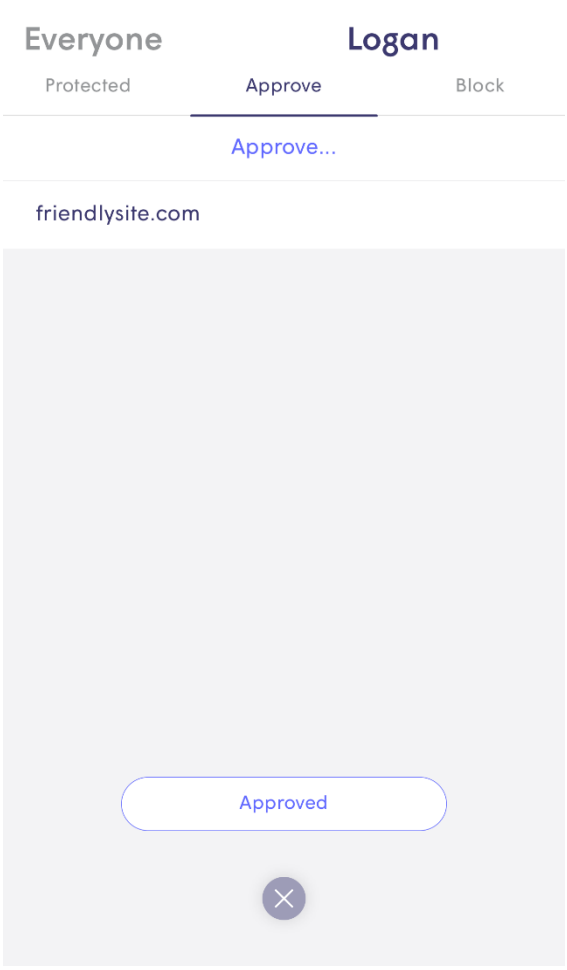

Logan
4 assigned devices
Amazon Echo Dot
Last online 10 months ago
Guard™
Online protection
Real-time threat protection against crypto-mining, ransomware, malware & more
Enabled
Content access
Keep online browsing habits tuned to the needs of your family
Teenager friendly
Adblocking
LABS
Enjoy a better online experience by blocking ads
Disabled
Manage security events


Everyone
Logan
Protected
Approve
Block
Approve...
Approved

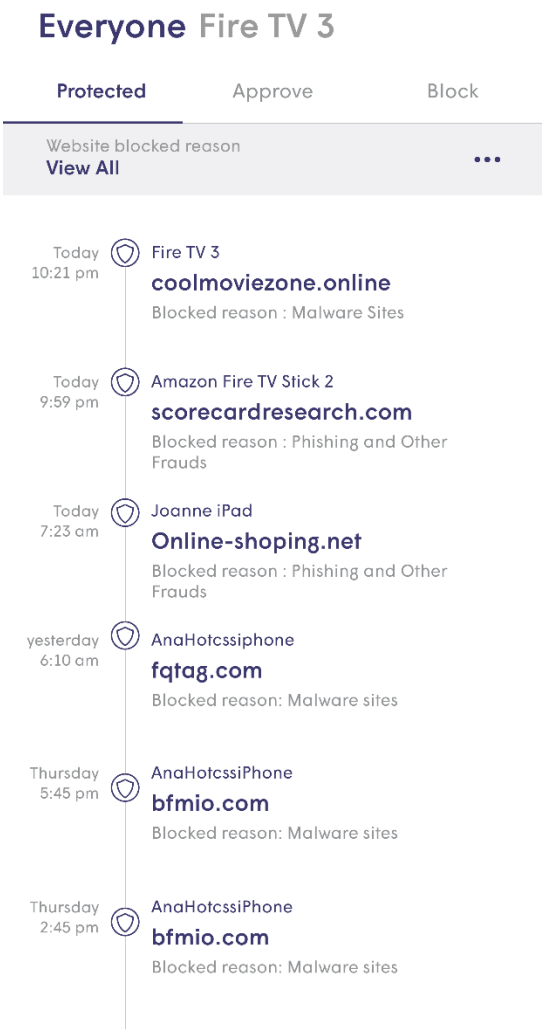

Everyone
Logan
Protected
Approve
Block
Approve...
amazon.com
corus.ca
corusappservices.com
demdex.net
linksynergy.com
nordvpn.com
tunnelbear.com
Approve Website
Approve IP Address
Cancel


Everyone
Logan
Protected
Approve
Block
Approve...
Approve Website
www.friendlysite.com
Cancel
Approve
linksynergy.com
nordvpn.com
tunnelbear.com
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
.
/
.com
return

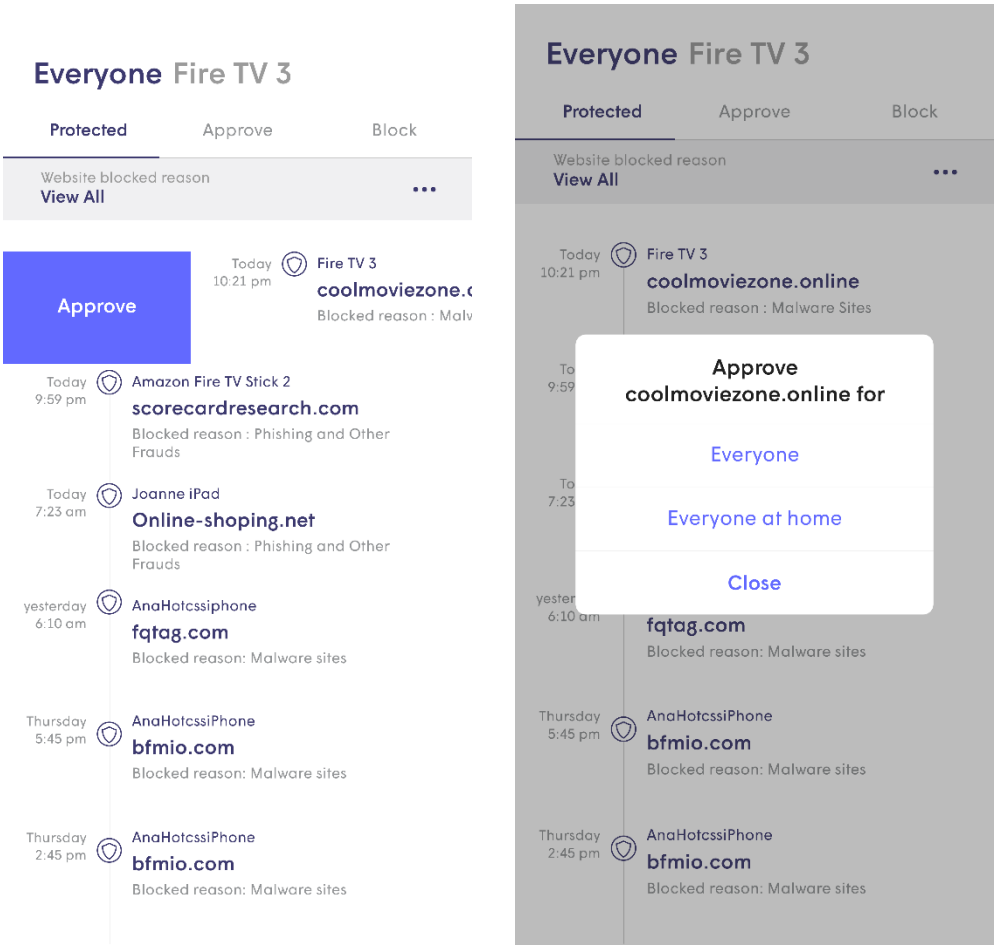

Everyone
Microsoft Xbox One
Protected
Approve
Block
Approve...
Apply changes?
This will apply to all devices currently assigned to Logan
Cancel
Apply


Everyone
Logan
Protected
Approve
Block
Approve...
friendlysite.com
Approved

You can also unblock a website from **Protected** list.



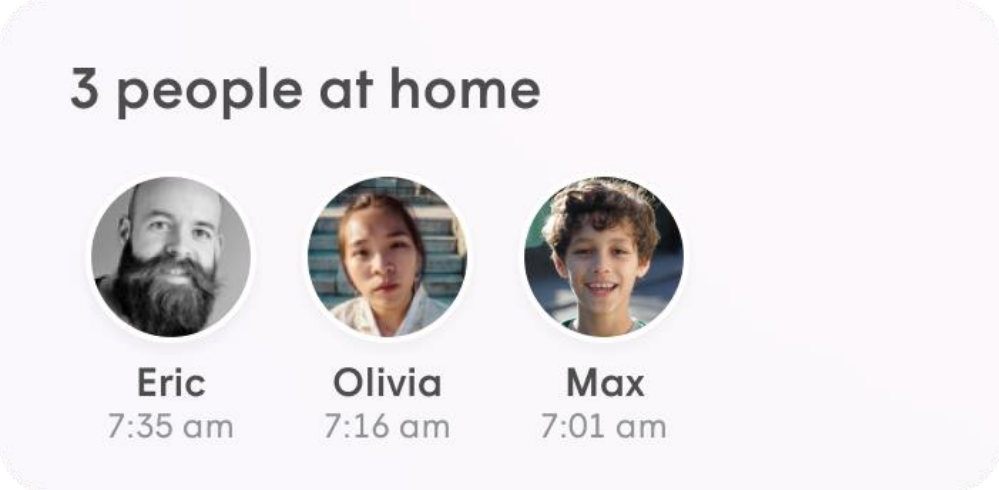
Simply swipe or tap to add a site to your **Approved** list



Confirm that the site is now Approved

How do I assign a Primary Device to someone?

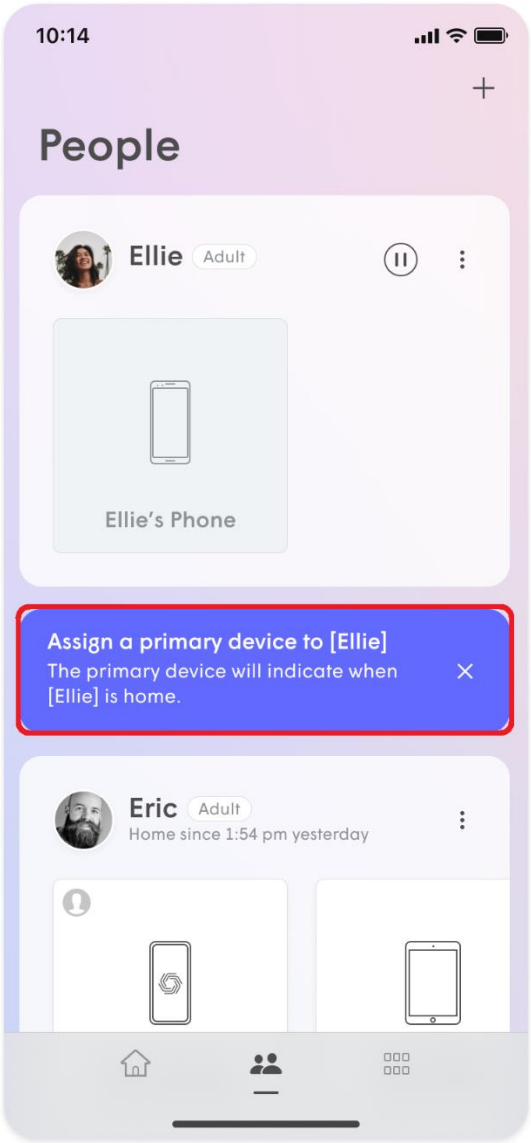
Each person can have a primary device assigned to their profile. That primary device's connections and disconnections from the network determines if they show up as being at home, which is also important for managing Sense alerts.

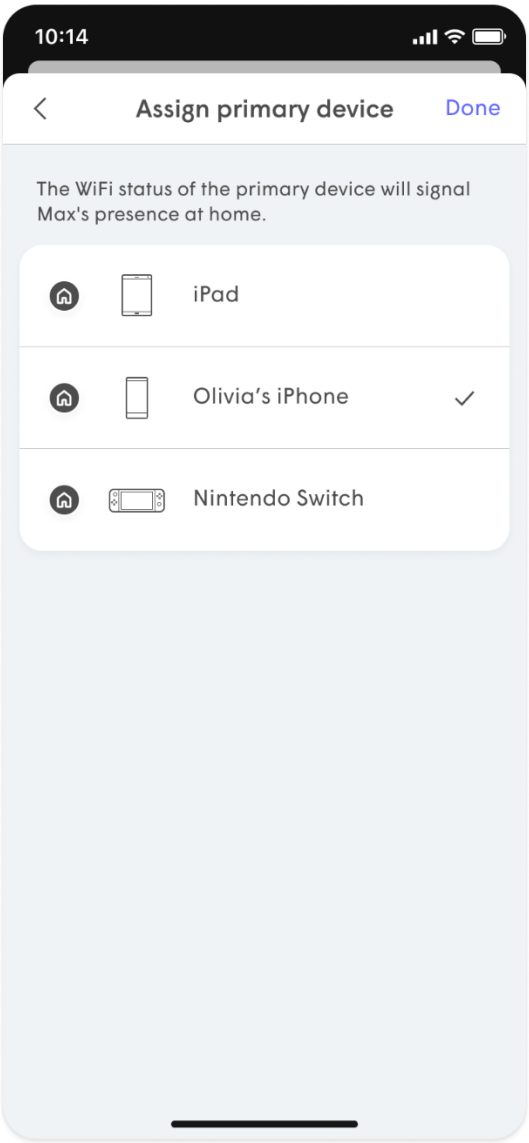


You should always choose a device they are not likely to leave home without and that will always stay powered. Smartwatches that connect to Wi-Fi or mobile phones are ideal.

Assigning a primary device to a person

1. Tap on the **people icon** and choose a person. Ensure the device in question is already assigned to that person.
2. If a primary device has not been set, the **Assign primary device notification** will be shown. Tap on the notification.
3. Choose a primary device and tap on **Done** to save.


10:14
People
Ellie
Adult
Ellie's Phone
Assign a primary device to [Ellie]
The primary device will indicate when [Ellie] is home.
Eric
Adult
Home since 1:54 pm yesterday

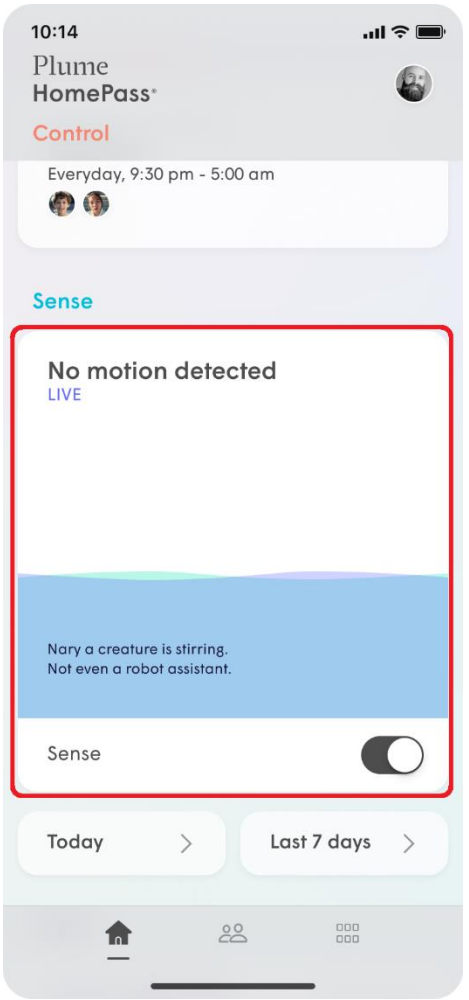

10:14
Assign primary device
Done
The WiFi status of the primary device will signal Max's presence at home.
iPad
Olivia's iPhone
Nintendo Switch

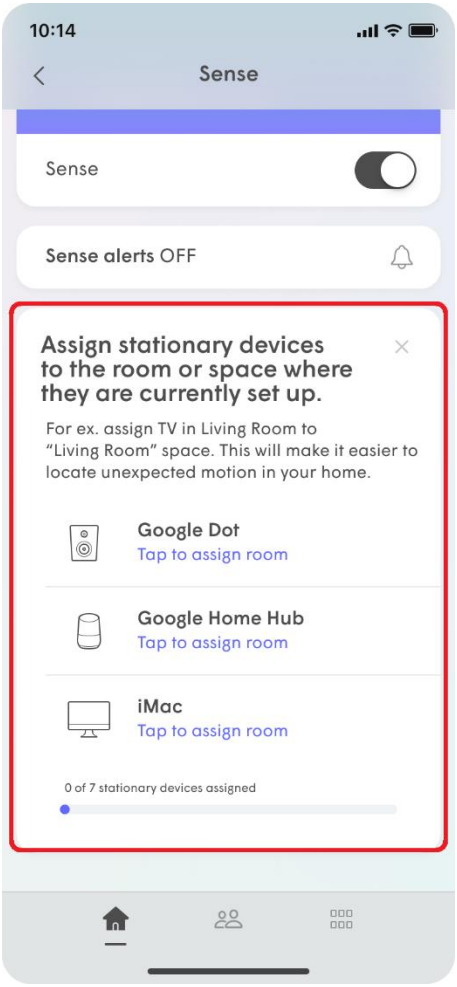
How do I create rooms?

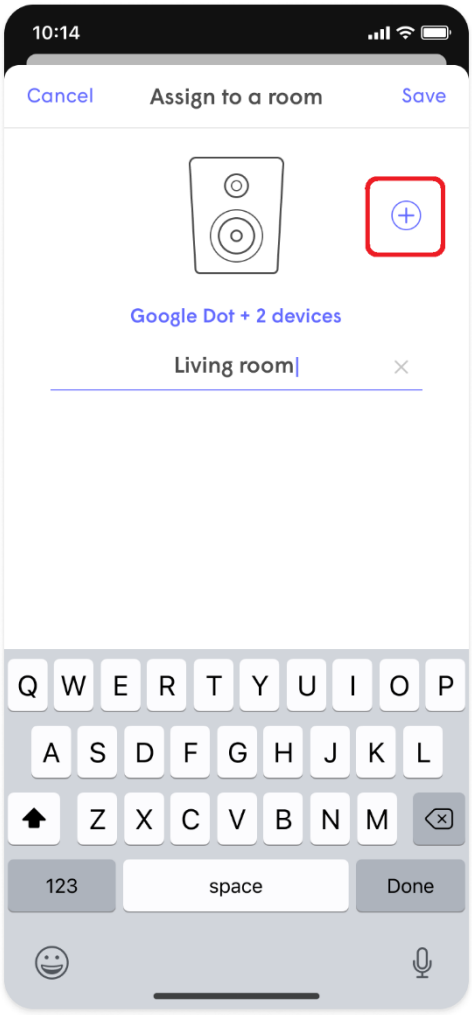
The HomePass App allows you to group your devices into rooms to improve motion detection accuracy. For example, if your living room has a smart TV, smart speaker, and voice assistant, motion detection on any of these devices can be localized to your living room!

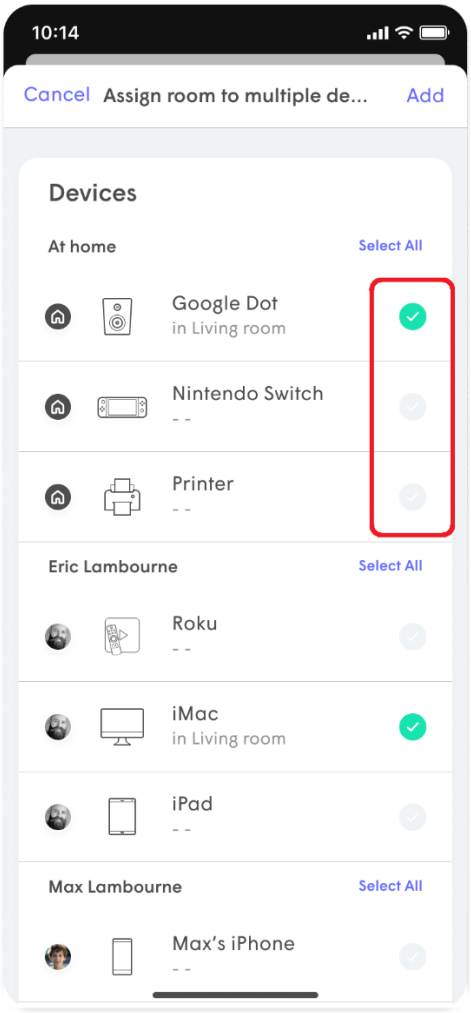
Creating rooms

1. From the home screen, enable **Sense.** Once Sense is enabled, a list of eligible devices will begin to populate and you will be prompted to assign devices to a room.
2. Tap on one of the devices in the unassigned device list.
3. Enter the name of the room for this device and tap on **Save**.
4. If there is more than one device in that room, tap on the **+** icon.
5. From the device list, add a **green checkmark** next to all the devices in that room and tap on **Add**.
6. From the unassigned device list, tap on another device and repeat the previous three steps until all devices have been assigned a room.






10:14
Cancel
Assign to a room
Save
Google Dot + 2 devices
Living room
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
space
Done

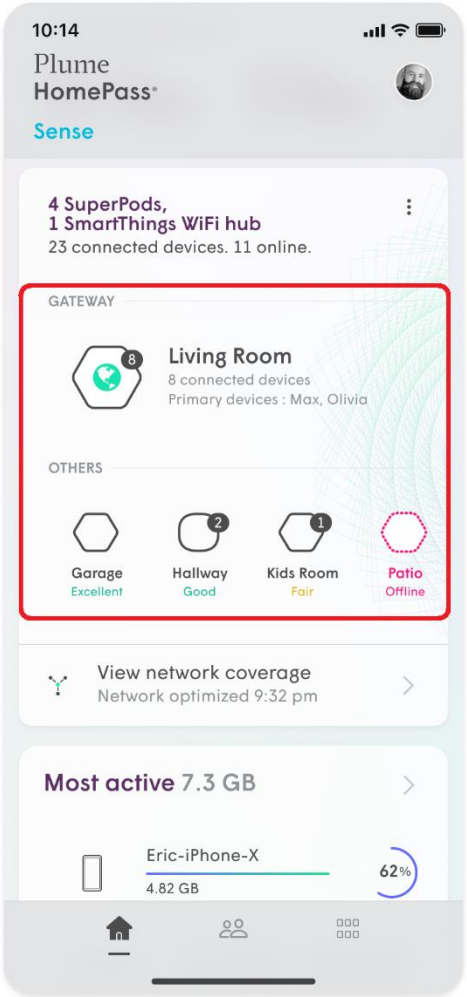

10:14
Cancel
Assign room to multiple de...
Add
Devices
At home
Select All
Google Dot
in Living room
Nintendo Switch
- -
Printer
- -
Eric Lambourne
Select All
Roku
- -
iMac
in Living room
iPad
- -
Max Lambourne
Select All
Max's iPhone
- -

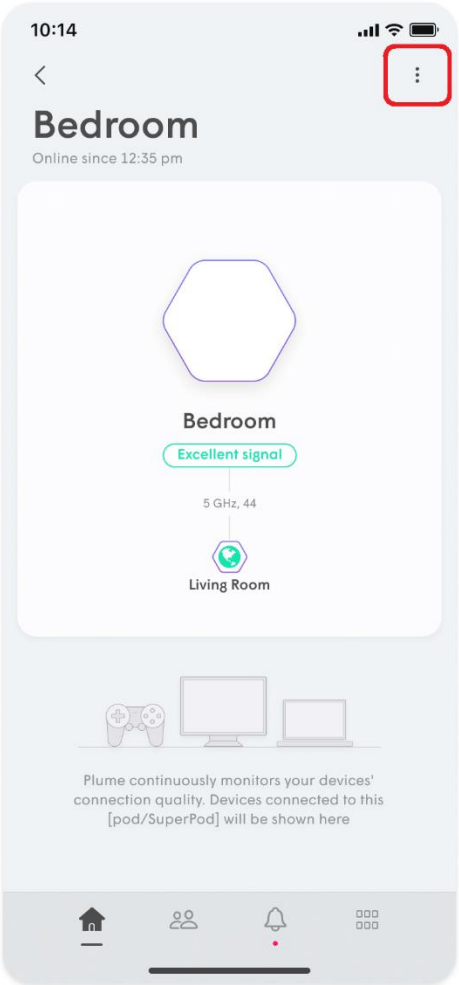
How do I delete a pod?

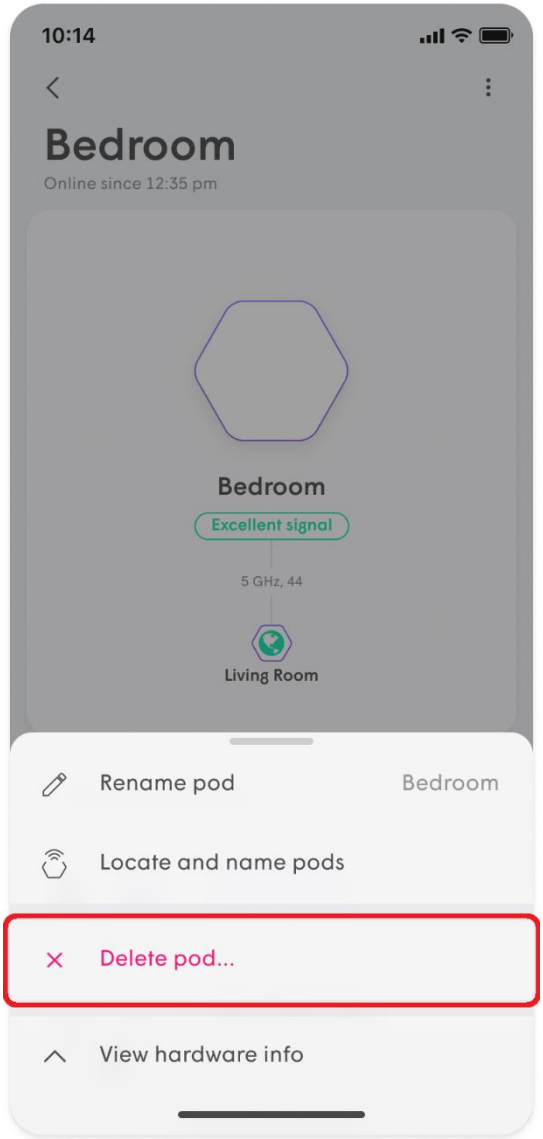
Deleting a pod from your account will completely disassociate this pod from your account. You will be able to add the pod back to your account or add it to another Plume account after deleting the pod.

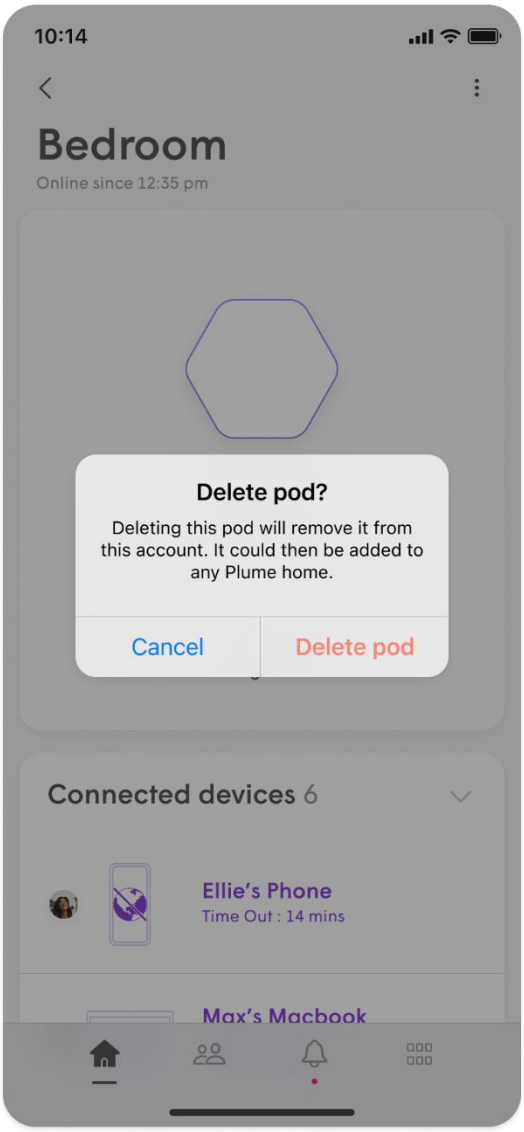
Deleting a pod

1. From the **Home** screen, scroll down to the **Adapt** section.
2. Select the pod you would like to delete.
3. Tap on the ⋮ on the top-right of the pod detail screen.
4. Select **Delete this Pod...** and then **Delete Pod** to confirm.

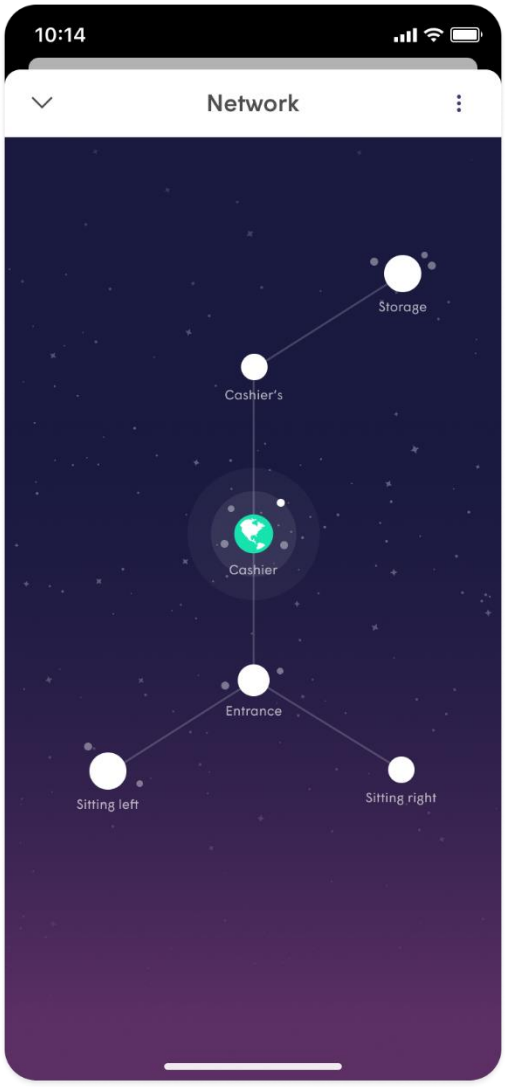


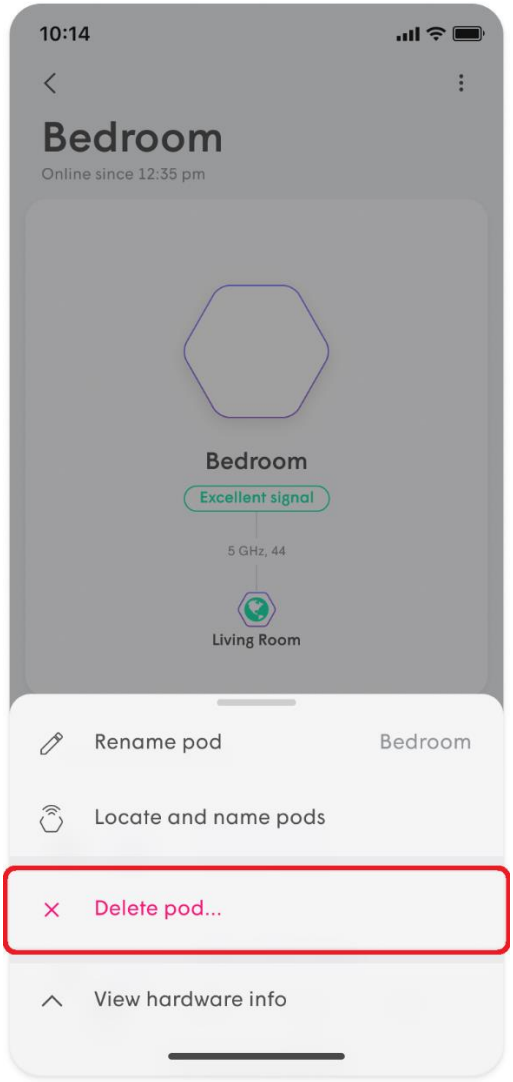



10:14
Bedroom
Online since 12:35 pm
Bedroom
Excellent signal
5 GHz, 44
Living Room
Rename pod
Bedroom
Locate and name pods
Delete pod...
View hardware info


10:14
Bedroom
Online since 12:35 pm
Delete pod?
Deleting this pod will remove it from this account. It could then be added to any Plume home.
Cancel
Delete pod
Connected devices 6
Ellie's Phone
Time Out : 14 mins
Max's Macbook

You can also go directly to the individual pod's menu by clicking it from the topology view.



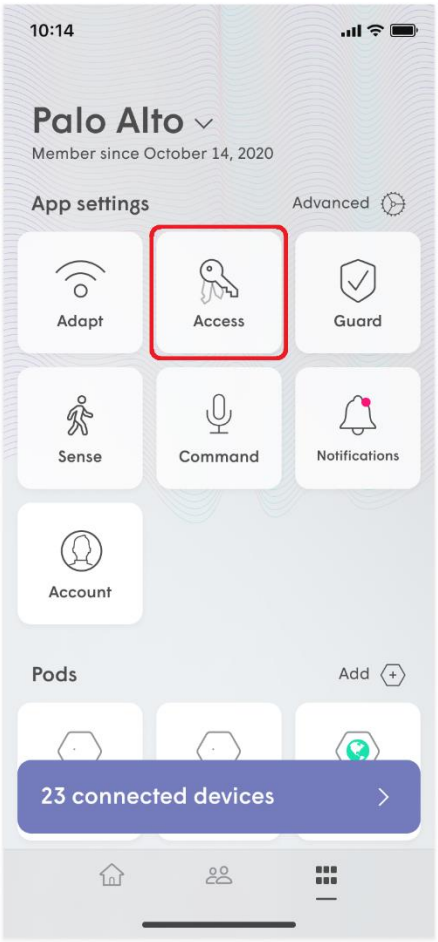


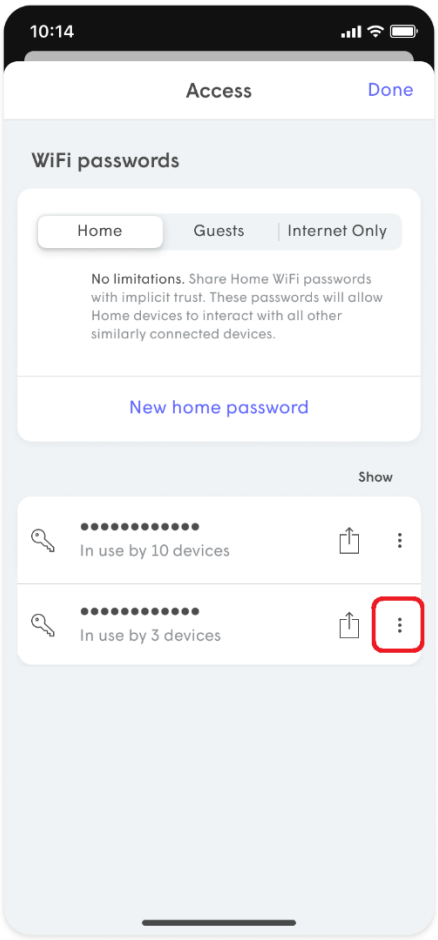
How do I disable or change a Wi-Fi password?

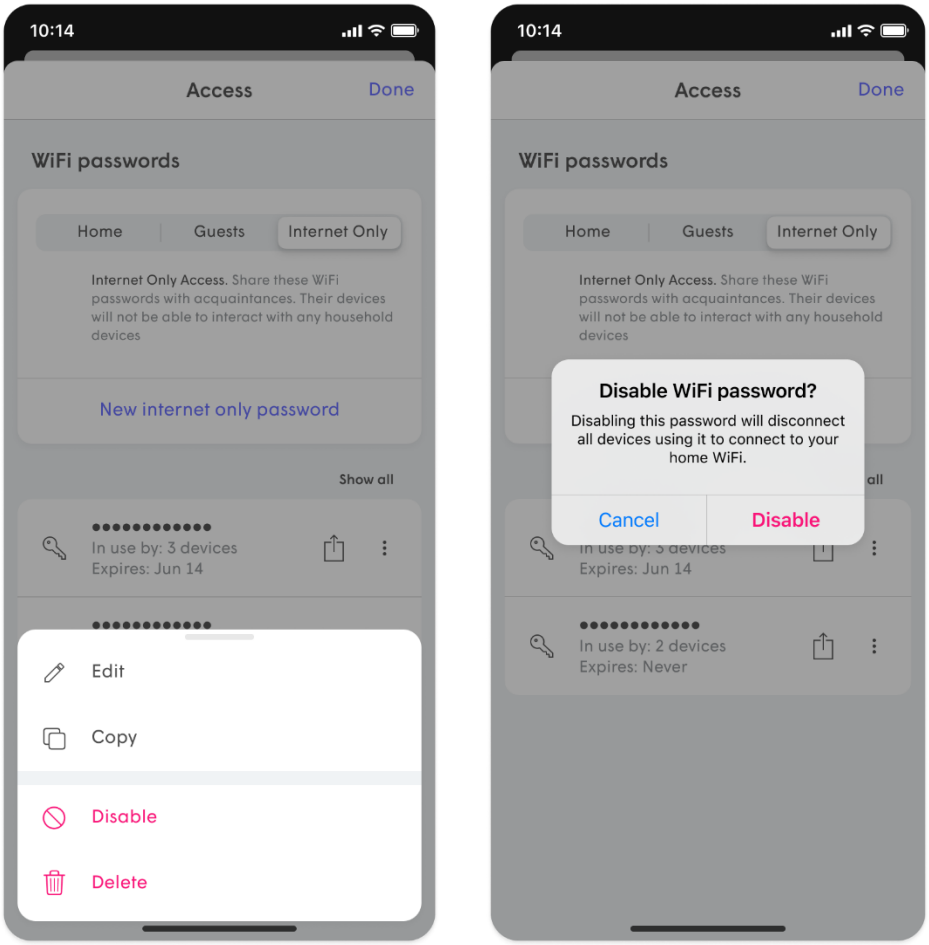
You can easily edit, delete, or temporarily disable a password by using the HomePass app. You can also edit the access level of any user with guest access.
To suspend or control access on a device level, use the Device Freeze feature.

Editing Wi-Fi passwords

1. From the More menu, tap on the **Access** option.
2. Tap on **Home**, **Guests**, or **Internet Only** to access that zone's page.
3. Tap the ••• next to the password you want to modify.
4. Choose **Edit**, **Disable**, or **Delete**.
5. In the case of Disable or Delete, confirm your selection. If you editing a password, go ahead make make your changes.


10:14
Palo Alto
Member since October 14, 2020
App settings
Advanced
Adapt
Access
Guard
Sense
Command
Notifications
Account
Pods
Add
23 connected devices


10:14
Access
Done
WiFi passwords
Home
Guests
Internet Only
No limitations. Share Home WiFi passwords with implicit trust. These passwords will allow Home devices to interact with all other similarly connected devices.
New home password
Show
In use by 10 devices
In use by 3 devices

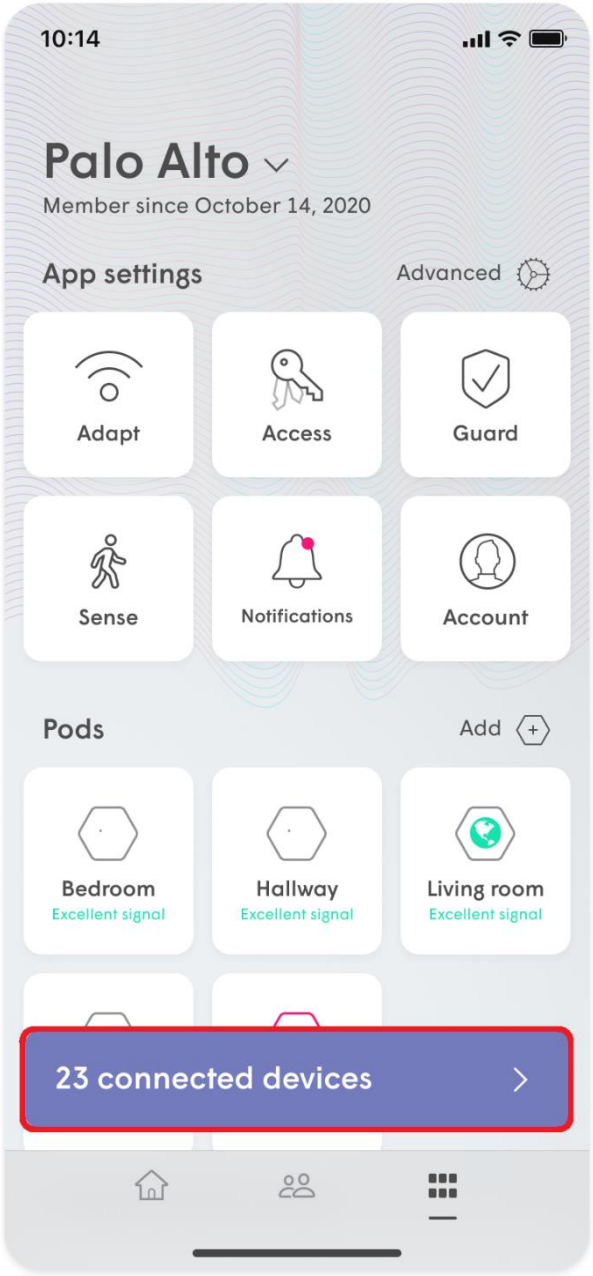

10:14
Access
Done
WiFi passwords
Home
Guests
Internet Only
Internet Only Access. Share these WiFi passwords with acquaintances. Their devices will not be able to interact with any household devices
New internet only password
Show all
••••••••••••
In use by: 3 devices
Expires: Jun 14
Edit
Copy
Disable
Delete
10:14
Access
Done
WiFi passwords
Home
Guests
Internet Only
Internet Only Access. Share these WiFi passwords with acquaintances. Their devices will not be able to interact with any household devices
Disable WiFi password?
Disabling this password will disconnect all devices using it to connect to your home WiFi.
Cancel
Disable
Expires: Jun 14
••••••••••••
In use by: 2 devices
Expires: Never

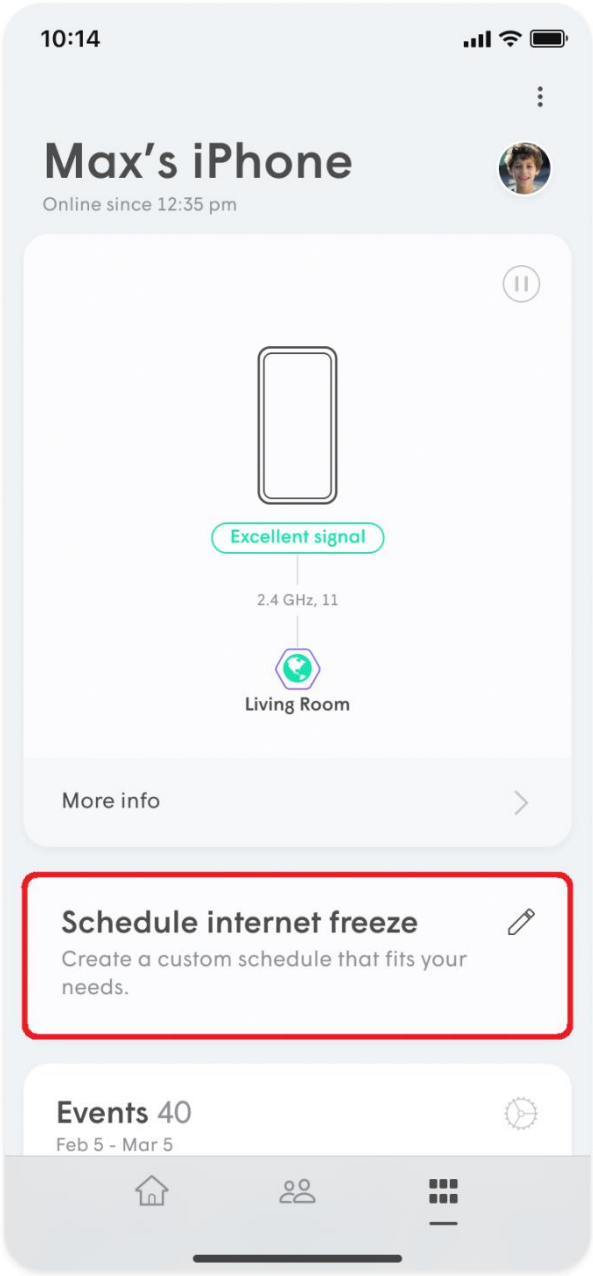
How do I schedule an Internet Freeze for a device or person?

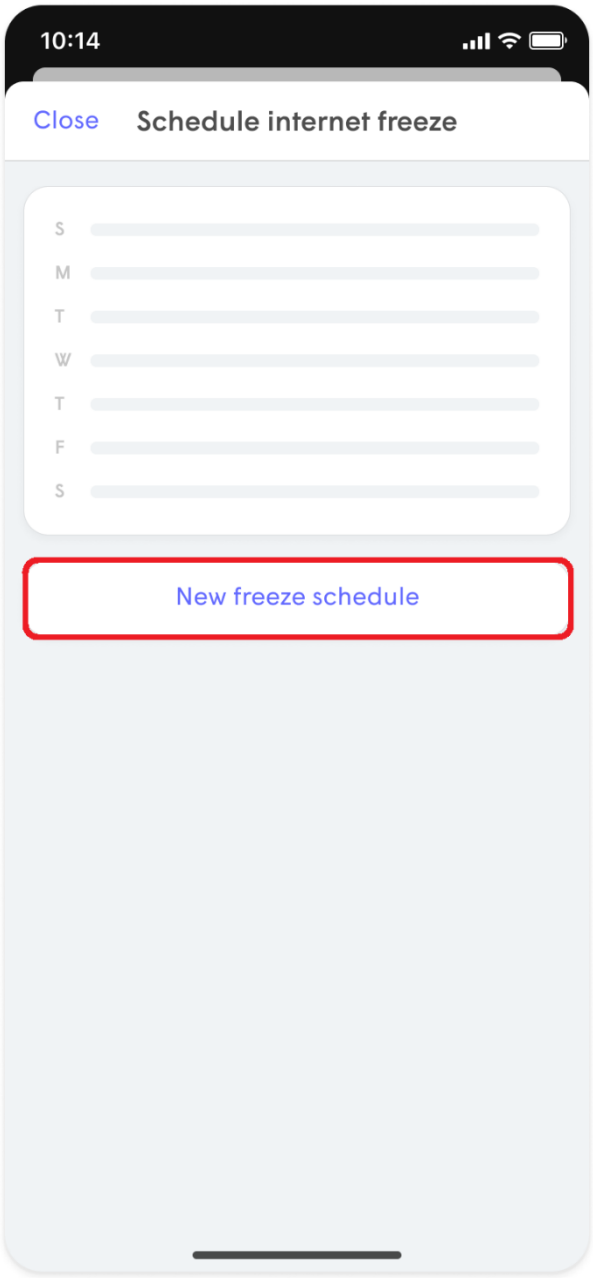
Internet Freeze allows you to easily manage how much time is spent on the internet by a device or person by using a Freeze schedule or as needed.

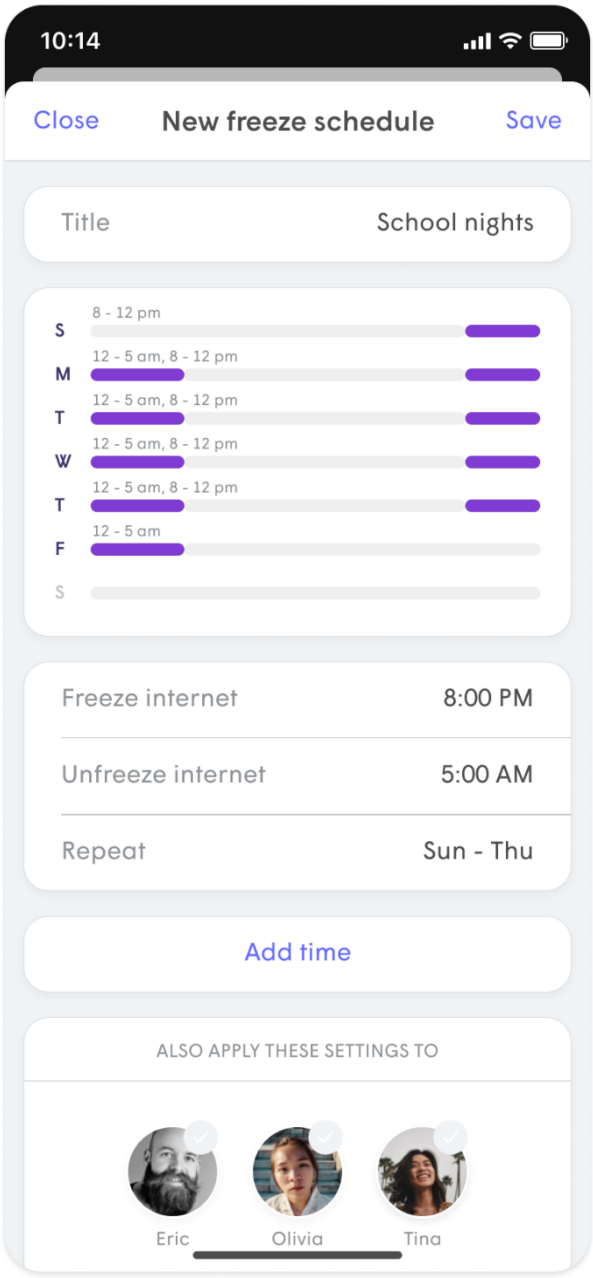
Schedule or Turn on Internet Freeze for a device

1. Select the device in the app to access the device details page.
2. Tap on **Schedule Internet Freeze.**
3. Type in a name for this Freeze schedule.
4. Tap on a day and enter the **Freeze internet** (start) time and **Unfreeze internet** (end) times.
5. Choose the **Repeat** option if this schedule will be the same on multiple days or tap on another day to set different Freeze and Unfreeze times for that day.
6. Choose a person if this Freeze schedule will be used for all of their devices.
7. Tap on **Save** once your schedule is complete.


10:14
Palo Alto
Member since October 14, 2020
App settings
Advanced
Adapt
Access
Guard
Sense
Notifications
Account
Pods
Add
Bedroom
Excellent signal
Hallway
Excellent signal
Living room
Excellent signal
23 connected devices

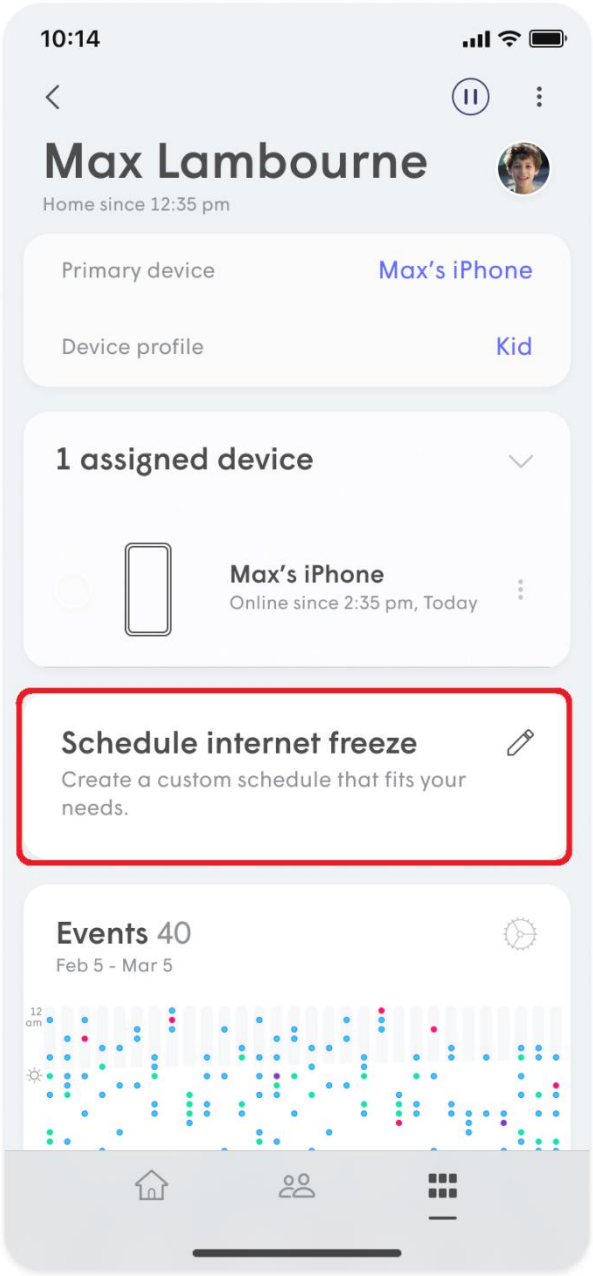

10:14
Max's iPhone
Online since 12:35 pm
Excellent signal
2.4 GHz, 11
Living Room
More info
Schedule internet freeze
Create a custom schedule that fits your needs.
Events 40
Feb 5 - Mar 5

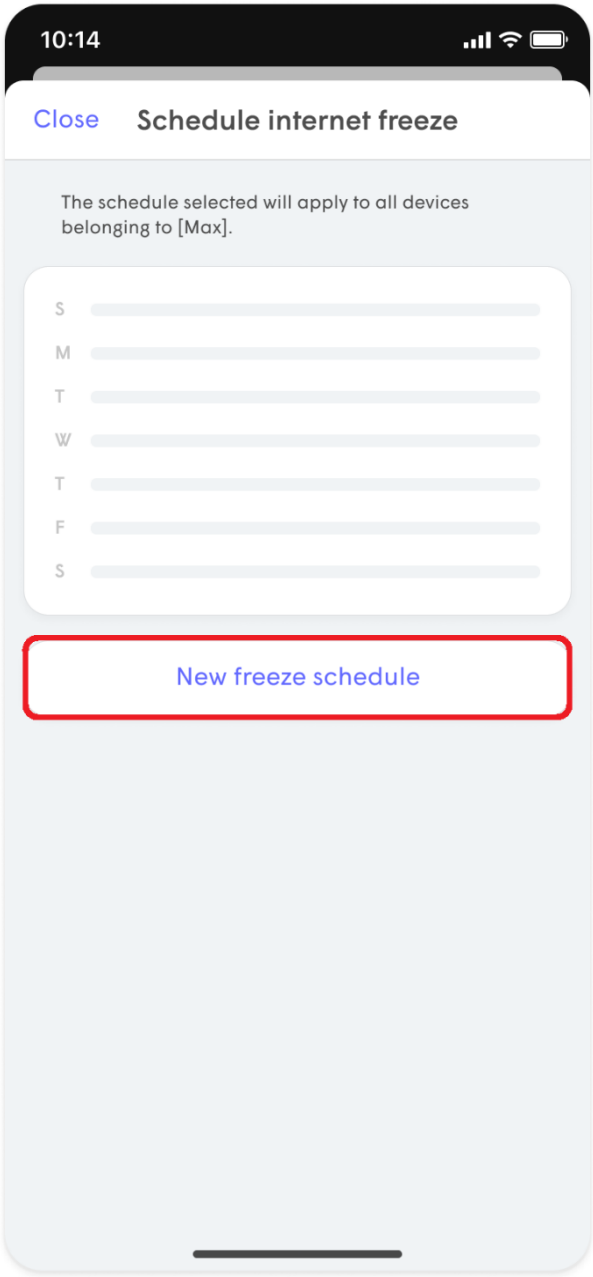


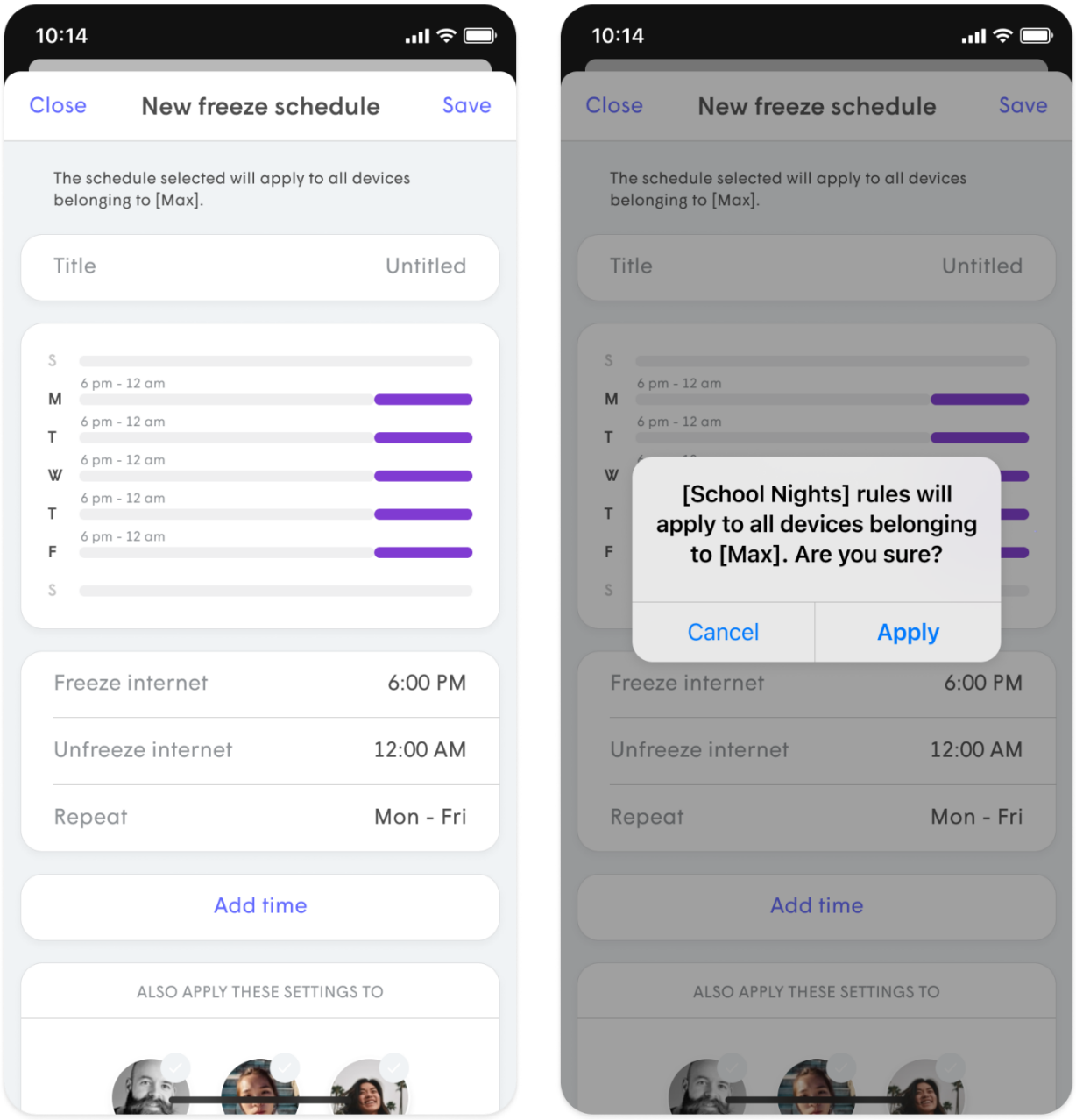


Schedule or Turn on Internet Freeze

1. Select the person from the **People** page.
2. Tap on **Schedule Internet Freeze.**
3. Type in a name for this Freeze schedule.
4. Tap on a day and enter the **Freeze internet** (start) time and **Unfreeze internet** (end) times.
5. Choose the **Repeat** option if this schedule will be the same on multiple days or tap on another day to set different Freeze and Unfreeze times for that day.
6. Tap on **Save** once your schedule is complete and **Apply** to confirm.

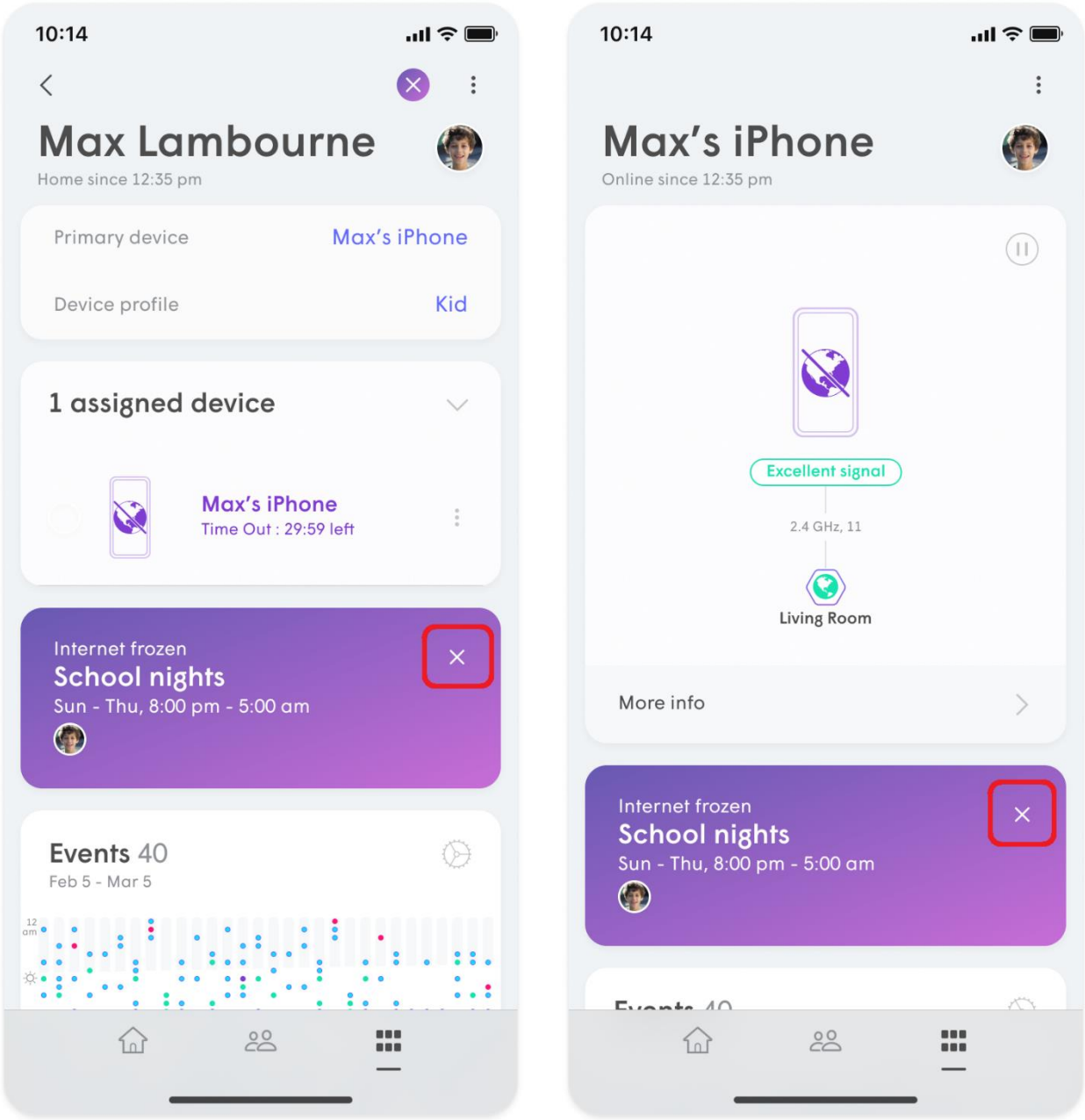

10:14
Max Lambourne
Home since 12:35 pm
Primary device
Max's iPhone
Device profile
Kid
1 assigned device
Max's iPhone
Online since 2:35 pm, Today
Schedule internet freeze
Create a custom schedule that fits your needs.
Events 40
Feb 5 - Mar 5
12 am


10:14
Close
Schedule internet freeze
The schedule selected will apply to all devices belonging to [Max].
S
M
T
W
T
F
S
New freeze schedule



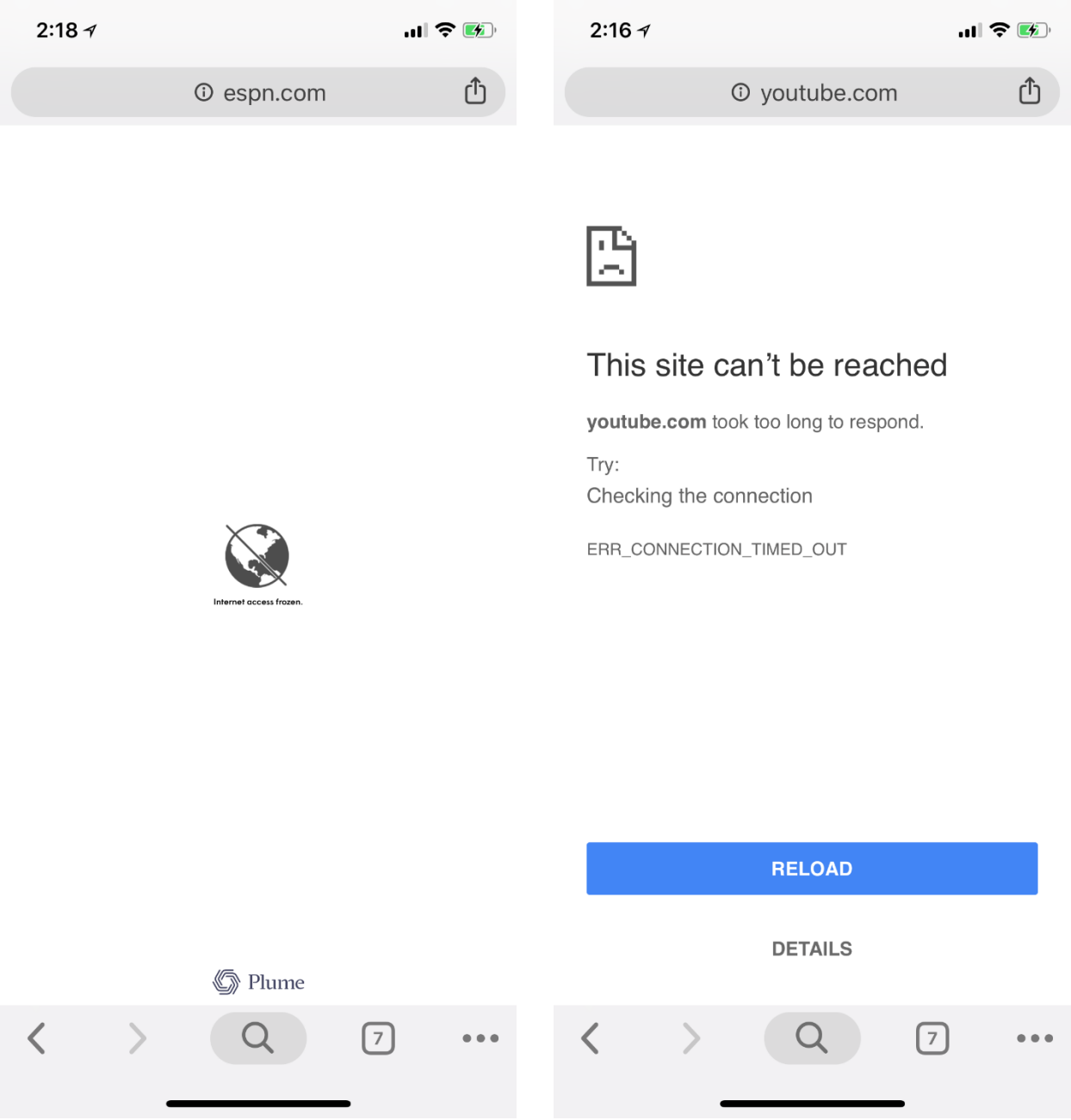
Interrupt Internet Freeze

You will be able to interrupt the internet freeze by either choosing **Unfreeze Until End of Day** or **Clear Internet Freeze** to reset the freeze internet schedule**.**



What will the user see when frozen?

When a device is frozen, it will not be able to access content. How that is displayed depends on the content you are trying to access. If you try to load an HTTP site, you will be redirected to the captive portal screen. However, if it is an HTTPS site, the page will simply timeout or say it cannot be reached.



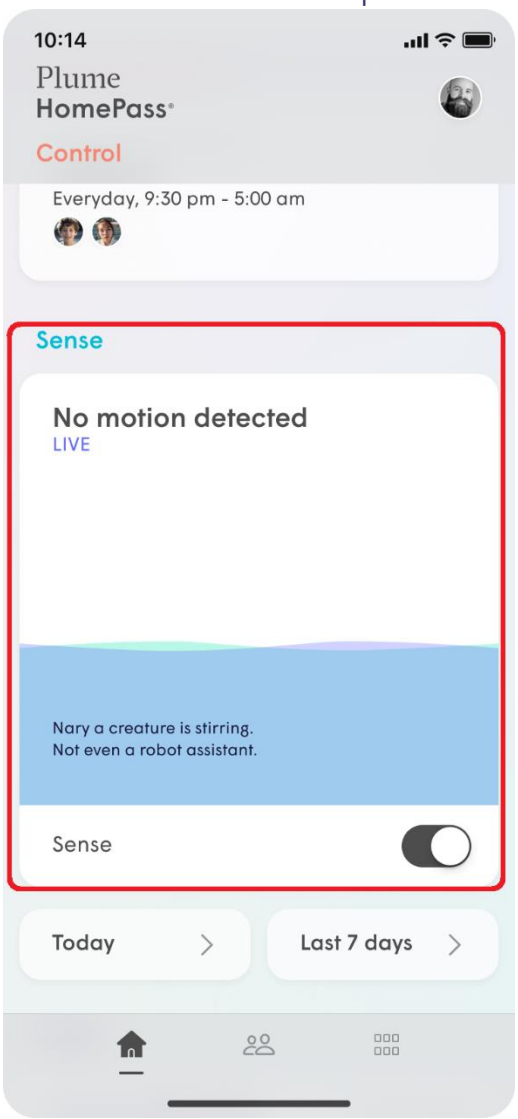
Plume also gives you the ability to pause internet access on a device or person instantly through the Time Out feature.

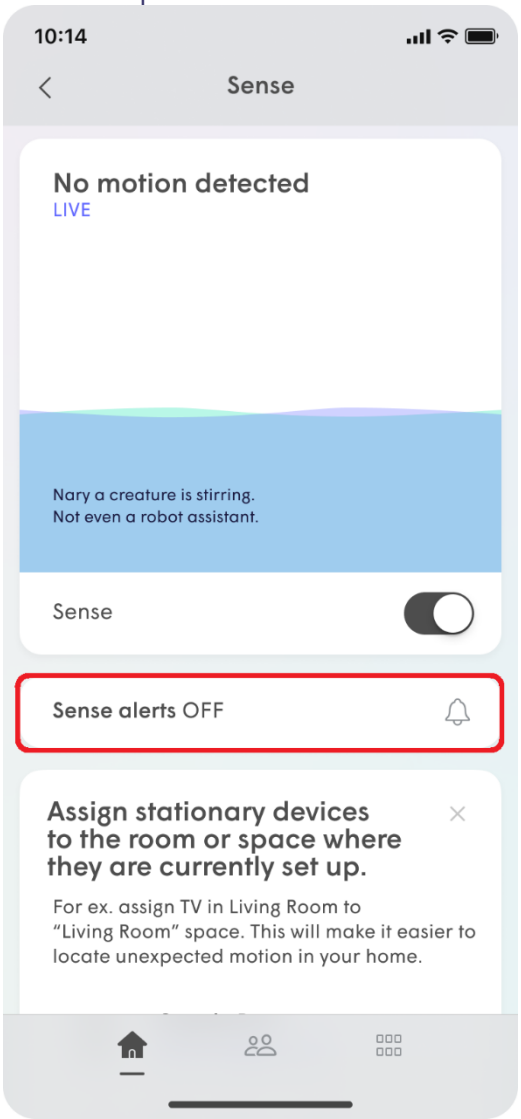
How do I set up motion alert notifications?

When Sense Alerts is enabled, push notifications will be sent to your device whenever the system detects motion. You can enable these notifications to send at all times or only while nobody is at home using the Smart Activation feature.
You need to assign a Primary device to everyone to ensure Sense can properly determine if everyone has left and also enable the People notifications.

Enable Notifications

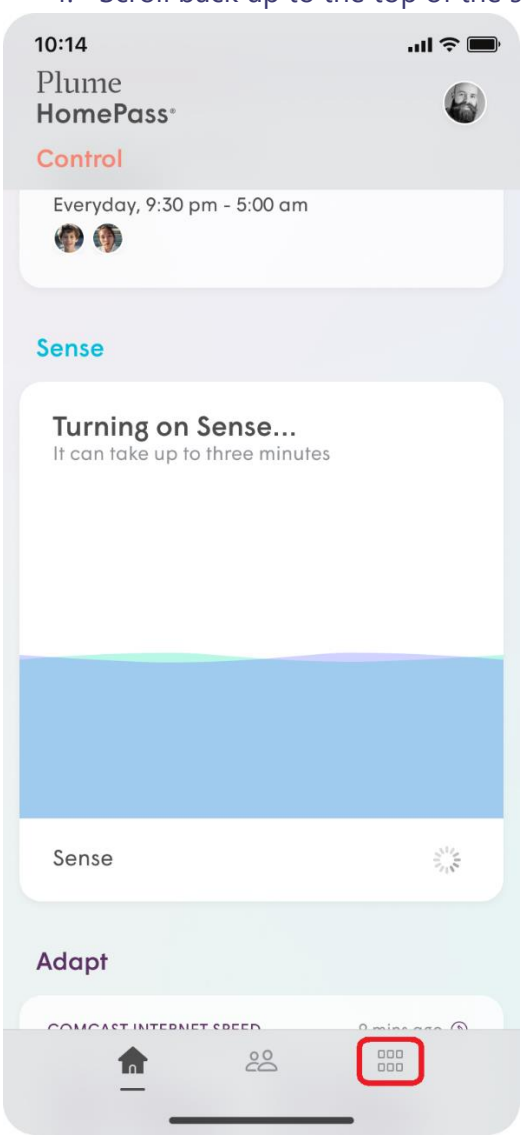
1. Scroll down to the **Sense** section on the H**ome Screen and** tap on it.
2. Scroll down to the option **Sense Alerts** and tap on the **Bell** to enable the notifications.

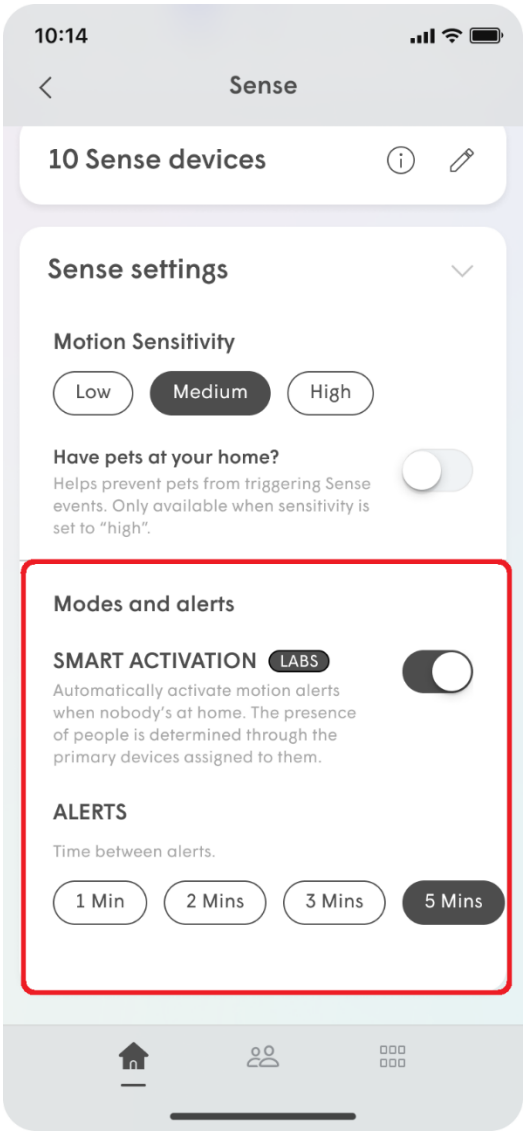




For Notifications Settings:

1. Tap on the **Main Menu** at the bottom of the screen and then tap on **Sense**.
2. Under **Modes and Alerts**, slide the **Smart Activation** toggle to the right if you do not wish to receive alerts while you are home.
3. Under the **Alerts** section, you can set the minimum **Time between alerts** to either **1 Mins**, **2 Mins, 3 Mins,** or **5 Mins**. This prevents you from getting too many notifications if a motion alert gets triggered immediately after another one.
4. Scroll back up to the top of the screen to turn **Sense alerts** from **ON** to **OFF**.





When are Sense Alert push notifications triggered?

Sense alerts will only be triggered if:

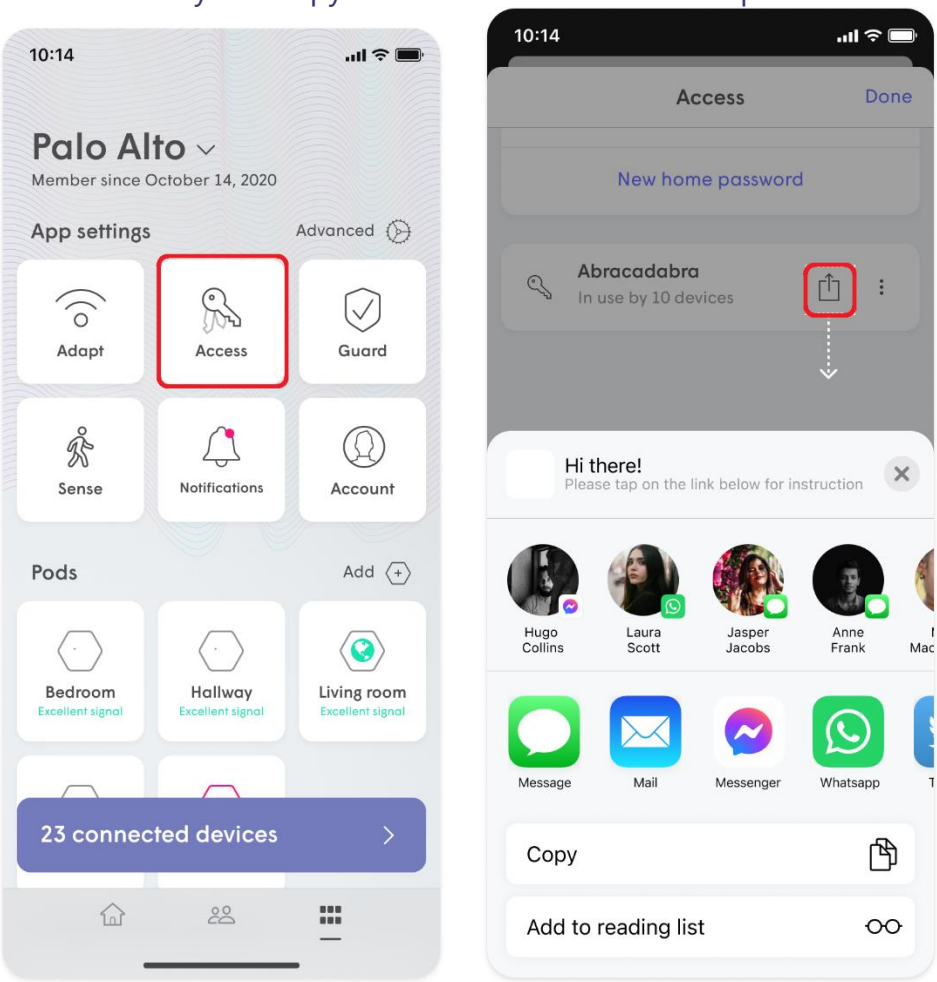
- Sense motion detection is enabled.
- Sense Alerts are enabled.
- If the Smart Activation of alerts has been enabled, everyone has left your home. (all assigned primary devices have been disconnected for 15 minutes or more)

- The motion being detected occurs for at least 2 seconds (5 seconds if pet mode is enabled), within an approximate 10'-13' radius from a motion detection device or SuperPod.
- The minimum time interval since the last alert has been met.

Click here if your Sense Alert push notifications are not behaving as expected.

How do I share network passwords?

1. Tap on the menu icon on the App home screen.
2. Tap the **Access** option to view the Network Name and Passwords.
3. Tap on **Home**, **Guests** or **Internet Only** to access that zone's settings page.
4. Next to the password, you want to share, tap on the **Share** icon.
5. Choose the method you want to use to share the password (SMS, email, Airdrop) and send it.
6. The recipient will receive a link. Clicking on it will take them to a web page from which they can copy the Network name and the password.



How do I switch from one Wi-Fi network to another in my app?

Using one login, you can manage multiple locations (networks). Follow the instructions below to switch between your locations.

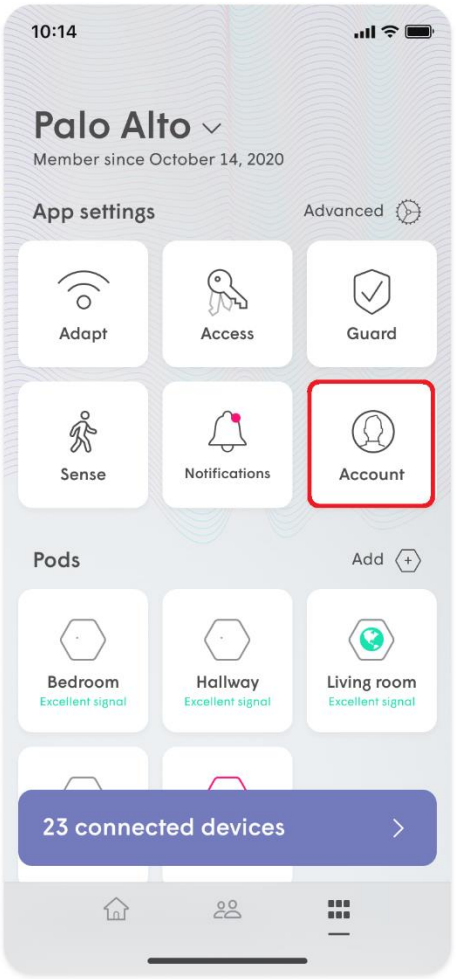
Note: Each network requires a separate membership.

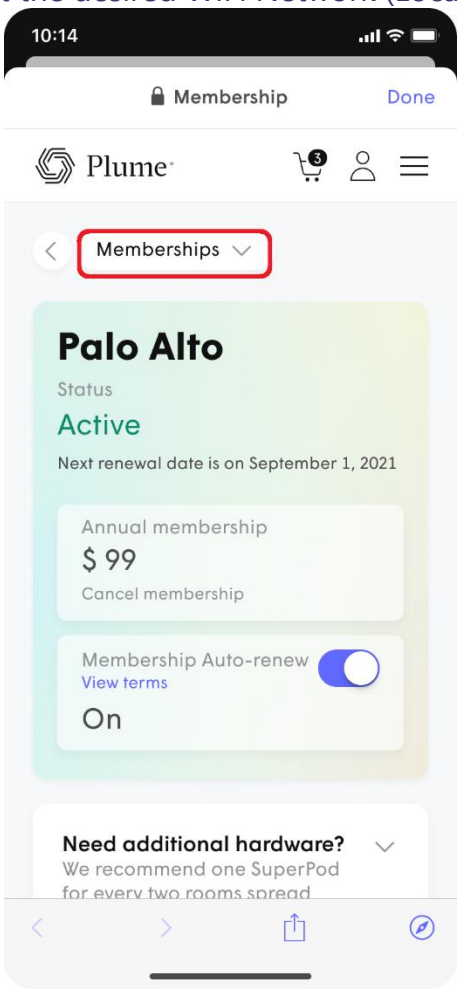
1. From the home screen, tap on your current location at the top of the page

2. Choose your desired location from the drop-down

Alternatively, you can also switch from the Account menu

1. From the home screen, tap on the ▫▫▫ button
2. Tap on **Account**
3. Tap on the **Memberships** dropdown.
4. Under Switch Location select the desired WiFi Network (Location)

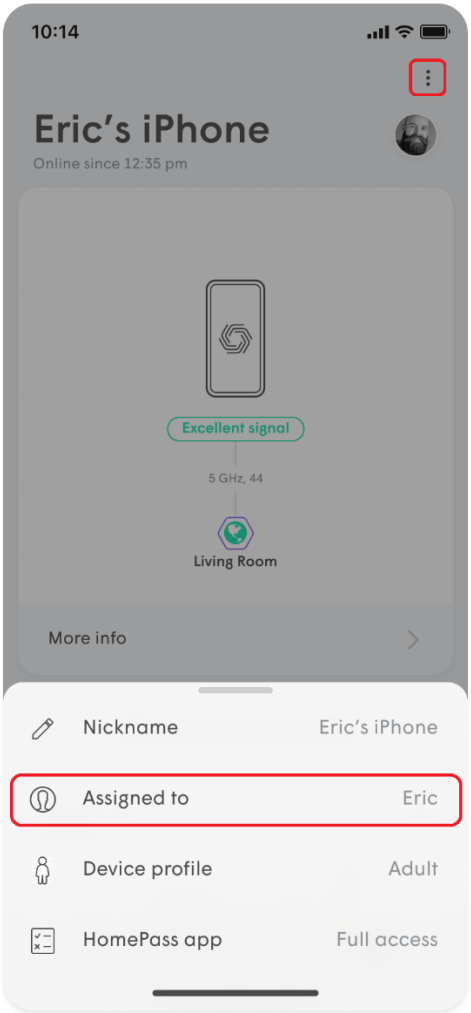


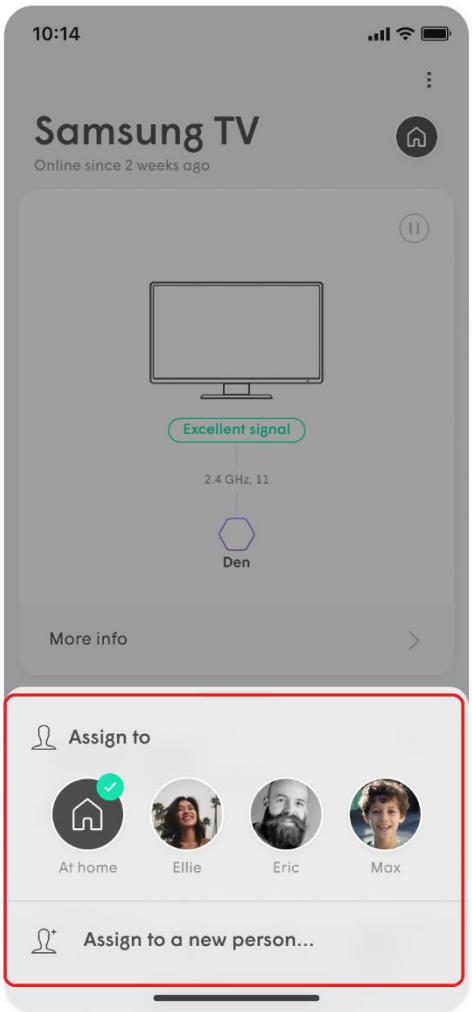


How do I transfer a device from one person to another?

If you accidentally assign a device to the wrong person, you can simply reassign it to another person's profile (or create a new profile).

1. Navigate to the incorrectly assigned device.
2. Tap on the ⋮ on the upper right-hand corner to view the device menu and select **Assign Device to...**
3. Select the appropriate profile to move the device to. You can also add a new person profile to your app at the same time!
4. Your device will now appear under the new profile!
5. Please note that any rules (Adblocking, Content Access, or Online Protection) will be reset to match the new profile.

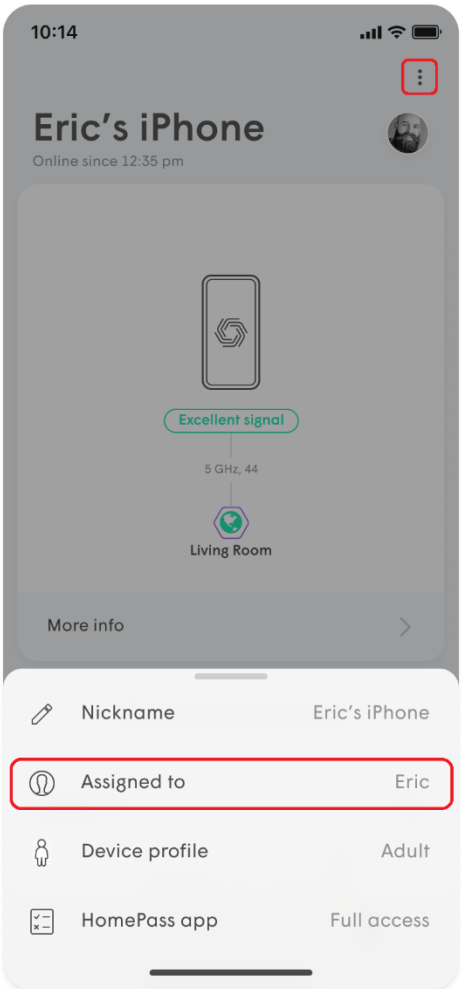


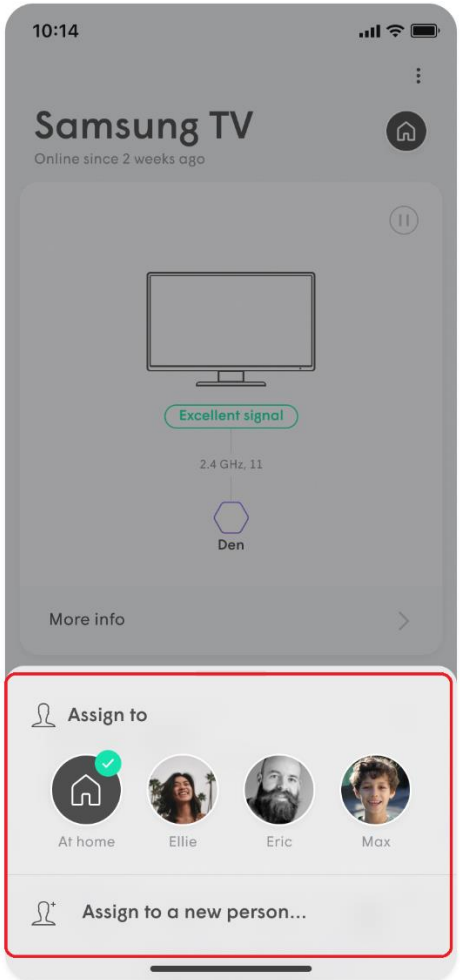


How do I transfer a device from one person to another?

If you accidentally assign a device to the wrong person, you can simply reassign it to another person's profile (or create a new profile).

1. Navigate to the incorrectly assigned device.
2. Tap on the ⋮ on the upper right-hand corner to view the device menu and select **Assign Device to...**
3. Select the appropriate profile to move the device to. You can also add a new person profile to your app at the same time!
4. Your device will now appear under the new profile!
5. Please note that any rules (Adblocking, Content Access, or Online Protection) will be reset to match the new profile.





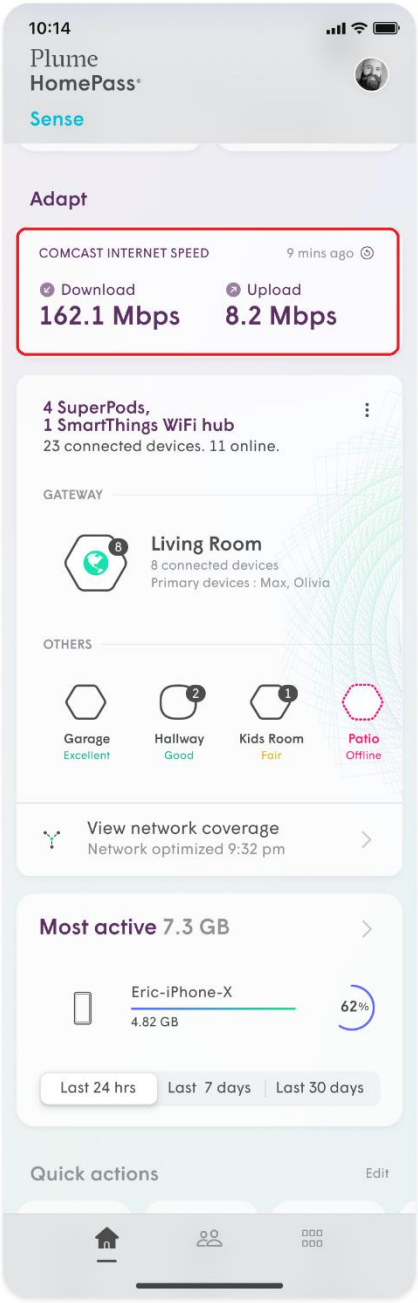
How do I view my network speeds?

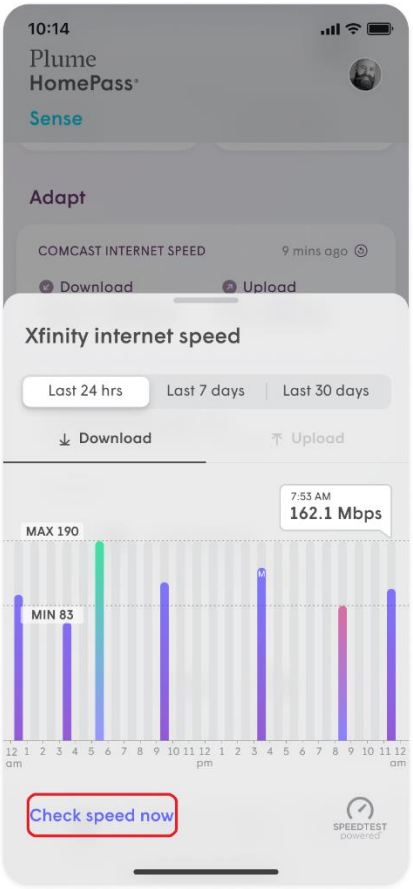
ISP Speed Test

Want to verify that you're receiving your internet plan's advertised speeds? Plume Auto-runs an ISP Speed Test off of your Gateway pod every 6 hours as long as your network is idle, in order to provide you with an up-to-date number. You can also choose to run the ISP Speed Test anytime via the HomePass app on iOS and Android, even when you are not connected to your network.

To run the ISP Speed Test:

1. Scroll to the **Adapt** section on the home page of the App.
2. The latest result of the Internet Speed test will be shown, by tapping on it the Speed Test History will come up.
3. Tap on **Check Speed Now**. This will trigger a speed test off of your gateway pod and provide you with the latest results.
4. You can turn off the **Auto-run ISP Speed Test** using the toggle switch.





ISP Speed Test limits

The limit for SuperPods and PowerPods is 1 GBps. The built-in ISP Speed Test is limited to around 200Mbps for the original Plume Pods, regardless of the actual throughput that your pods are delivering. If you have a connection faster than this and have a Pod as the gateway, you can use the Device Speed Test feature when your mobile is connected to the Gateway Pod, to get a better idea of the Speed coming into you

Gateway Pod. If you have a PC or Mac, you can download the stand-alone OOKLA speed test App to run speed tests while connected to the Gateway Pod.

Why are there missing Speed Tests?

The most likely reason there would be a gap in the ISP Speed Test history is that your network was busy at the time the automatic test was scheduled. By default Plume runs an ISP Speed Test every 6 hours. If your network is busy at the scheduled time, that test will be skipped.

The Automatic ISP Speed Test will not run if your network is offline or if the speed test servers are temporarily unresponsive. If this is the case, please check your connection and try running the test again at a later time.

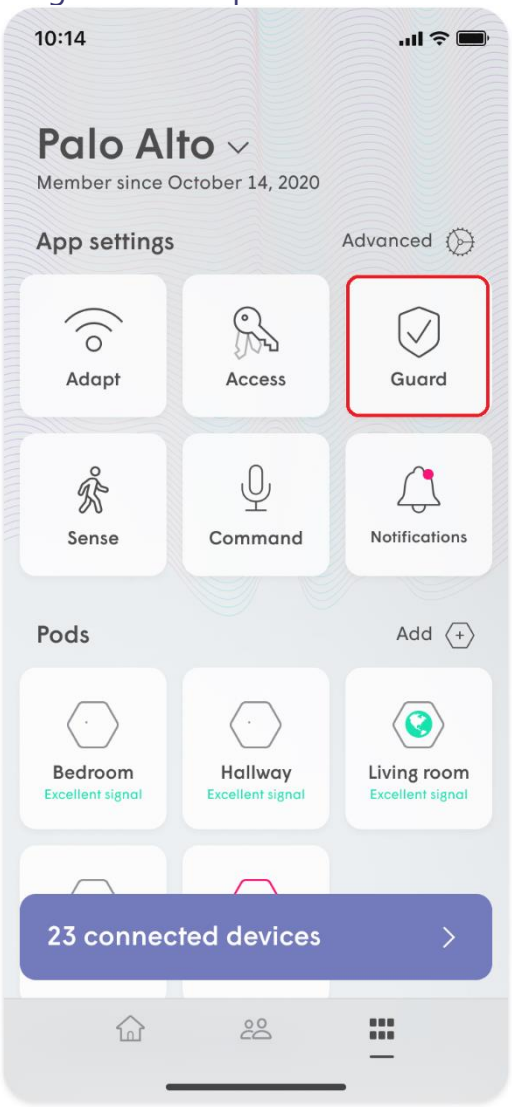
Notes

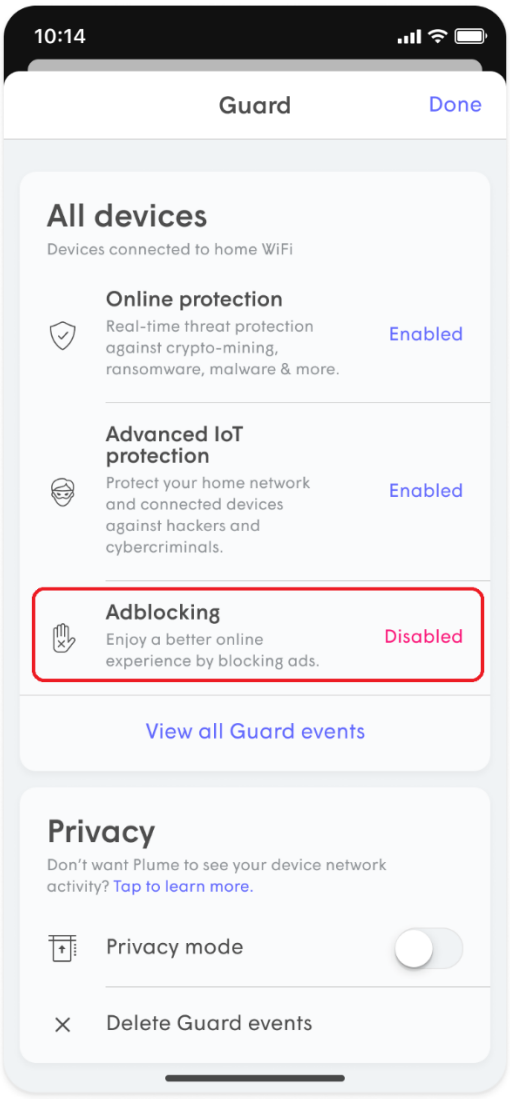
Running a speed test may affect the performance of other connected devices, which is why they do not automatically run when the network is busy.

ISP Speed Tests only test the connection at the Gateway pod. Use the Device Speed Test feature to check the Wi-Fi performance on the other pods in the network.

How does Adblocking work?

Adblocking will help you block web and video advertisements as well as requests to known ad servers. You can enable this for either a device, person profile, or everyone. When you enable Adblocking for a person, this setting will be applied to all the devices assigned to that person.





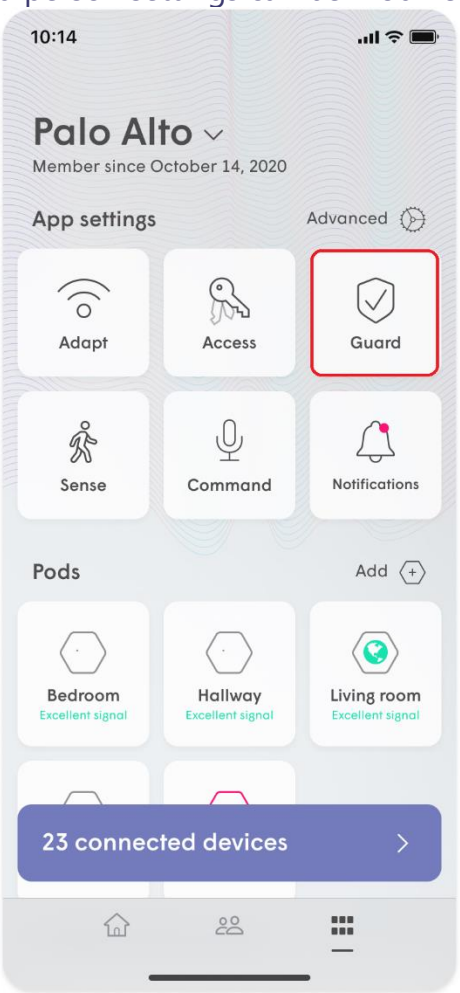
HomePass®

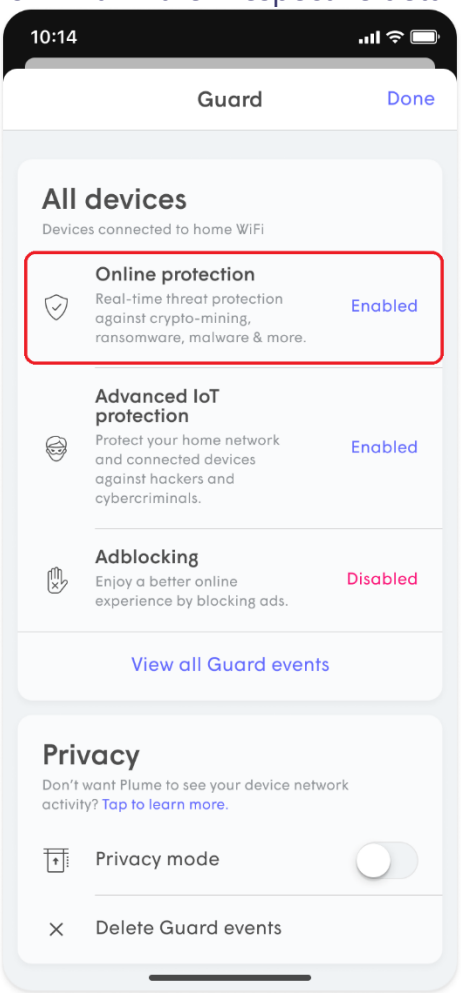
How does Online Protection work?

Enabling the Online Protection feature will protect your devices from malware sites, botnets, spyware, spam, phishing, keyloggers, monitoring, proxy avoidance, anonymizer and other harmful attacks on your network.

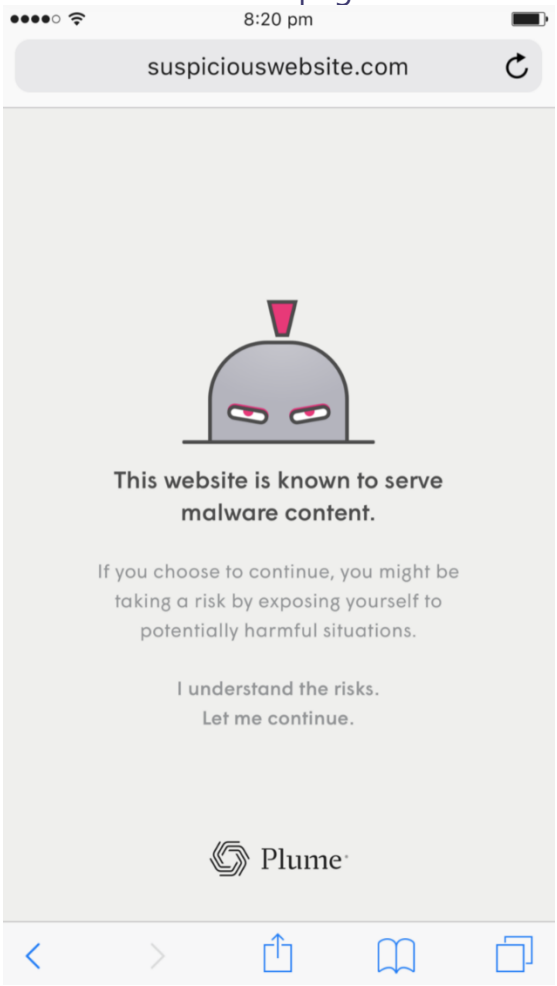
How do I turn on Online Protection?

The feature is enabled on all devices by default, but can be customized on the device or person level for an individualized experience. When this is enabled for a person, the Online Protection will automatically be turned on across all the devices assigned to that person.
Online Protection is controlled at the Network level in the **Guard** menu, while device and person settings can be modified from within their respective detail screens.





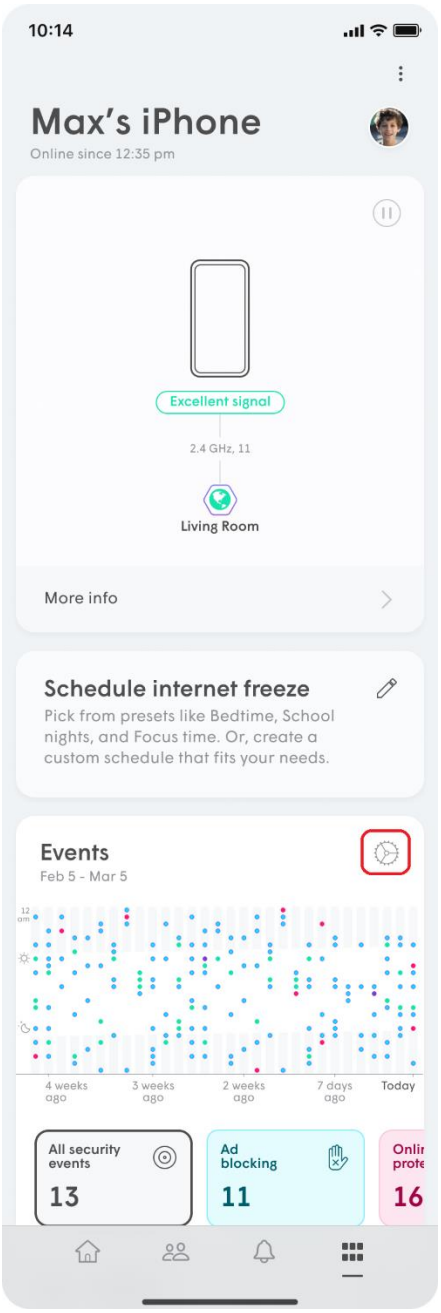
Content is restricted by our security feature whenever you see the “Access to this website is blocked” message displayed in the browser window.
Note: This only appears for HTTP sites; HTTPS sites prevent this and display the browser's default "can't be reached" message. HTTPS connections cannot be redirected to the HTTP blocked page because it would break the secure trusted SSL connection.

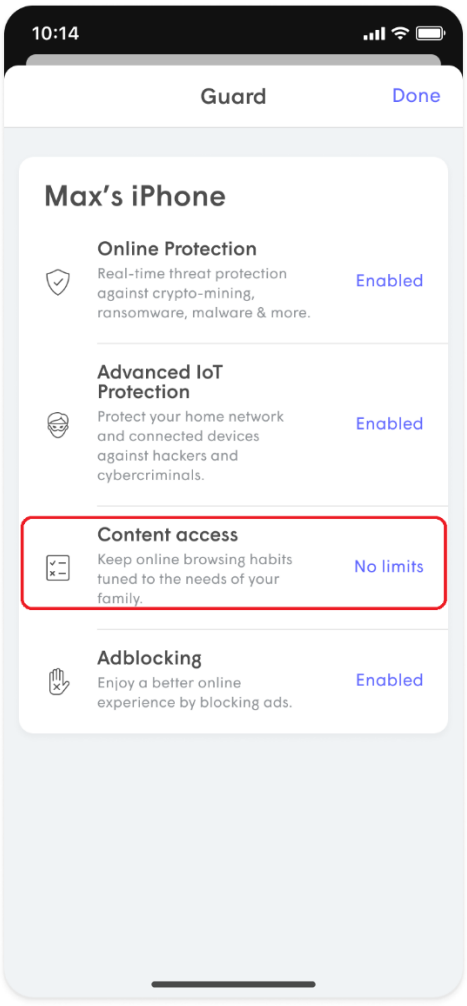


How does Plume's content access work?

Plume's content access feature will allow you to restrict content for a device or person. We have identified the most common content filtering categories that you can use when personalizing your online experience.
When setting up content filtering for a person or device, you can enable any of the four content filtering categories:

1. **No limits:** You can access all types of content.
2. **Kids appropriate**: Content that is tagged as NOT appropriate for kids will be filtered and inaccessible.
3. **Teenager friendly**: Content that is tagged as NOT appropriate for teens will be filtered and inaccessible.
4. **No adult content**: All content tagged as adult content will not be accessible.

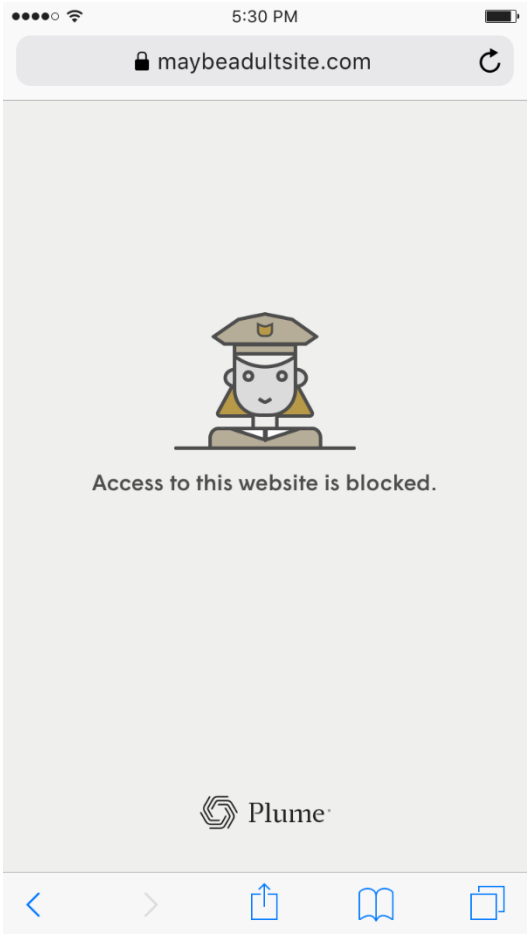


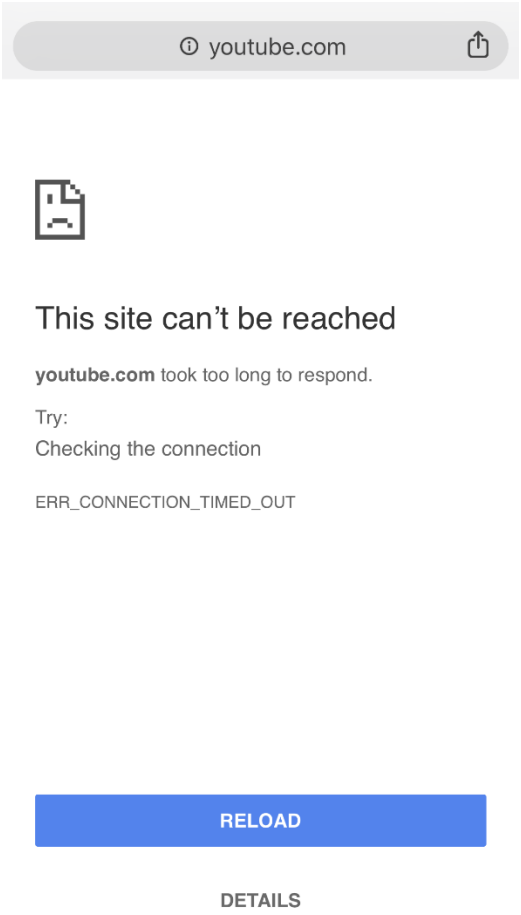


Please note that all devices associated with a person will inherit the content access settings assigned to that corresponding person. Likewise, applying content access restrictions to a device assigned to a person will apply the same settings to that person. However, if the device is unassigned, the rule will only apply to the device.
Content access will not work if Privacy Mode has been enabled or if the device is using a Private/Random MAC Address.

What is seen by the end-user when their content is blocked?

Content that was restricted by our security feature whenever you see the “Access to this website is blocked” message displayed in their browser window.
Note: This only appears for HTTP sites; HTTPS sites prevent this and display the browser's default "can't be reached" message. HTTPS connections cannot be redirected to the HTTP blocked page because it would break the secure trusted SSL connection.

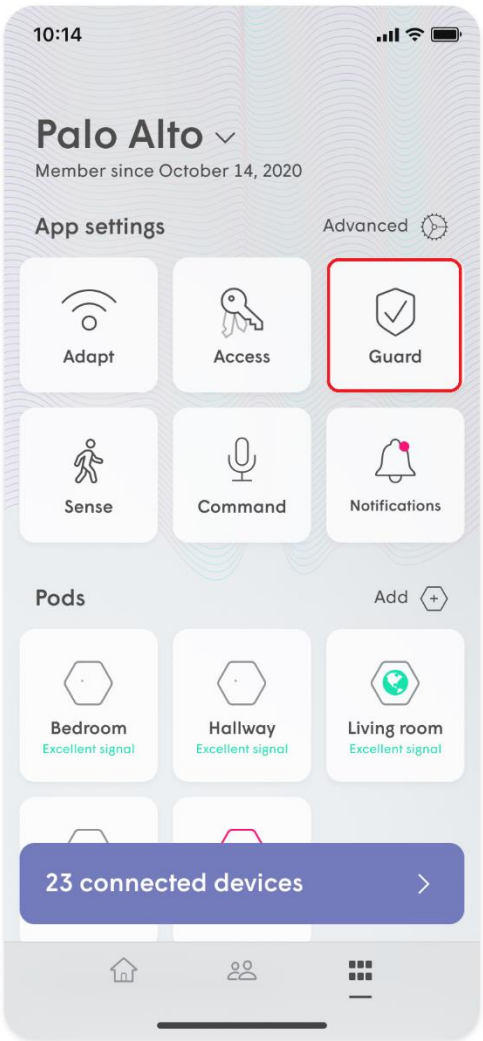


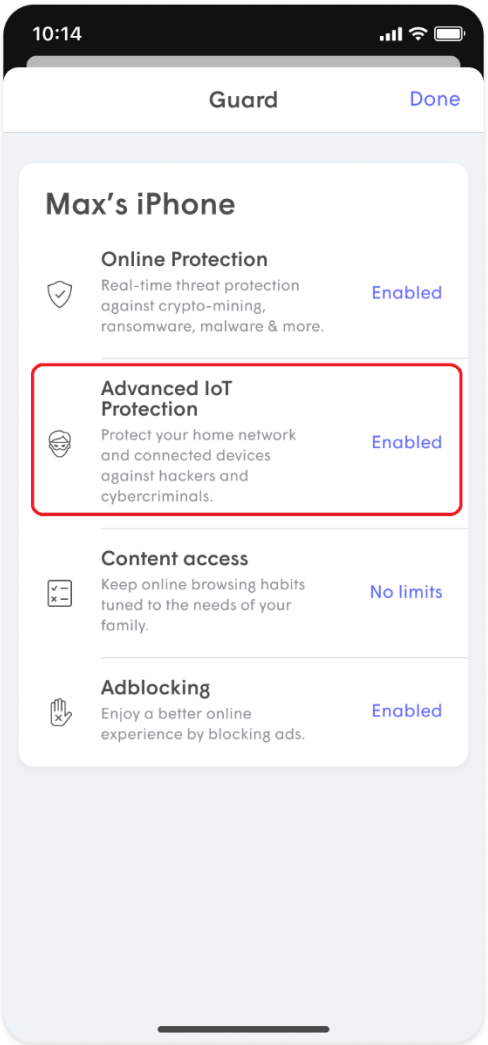


How is Advanced IoT Protection different from Online Protection?

Advanced IoT Protection (AIP) is a security advancement found in Plume Guard. Prior to its release, Online Protection protected all your connected home devices from going to sites known to host malware, spam, or phishing attacks. AIP provides protection from new, unknown attacks that are currently not part of any known threat intelligence database. It can detect unusual patterns in your IoT device's activity that indicates the device may be infected.

Advanced IoT Protection can be enabled via the **Guard** tab from within the main menu.





How to adjust motion sensitivity?

Motion sensitivity may need to be adjusted for the following reasons:

- Improve motion detection sensitivity, particularly if you have only a few SuperPods and/or Wi-Fi connected devices
- There are obstructions that are making it difficult for your SuperPods and devices to detect motion in some areas.
- You are getting too many false motion alerts because of your pets or robotic vacuums.

What are the sensitivity options?

- **Low** (less sensitive to motion intensity)
- **Medium** (default)
- **High** (more sensitive to motion intensity)

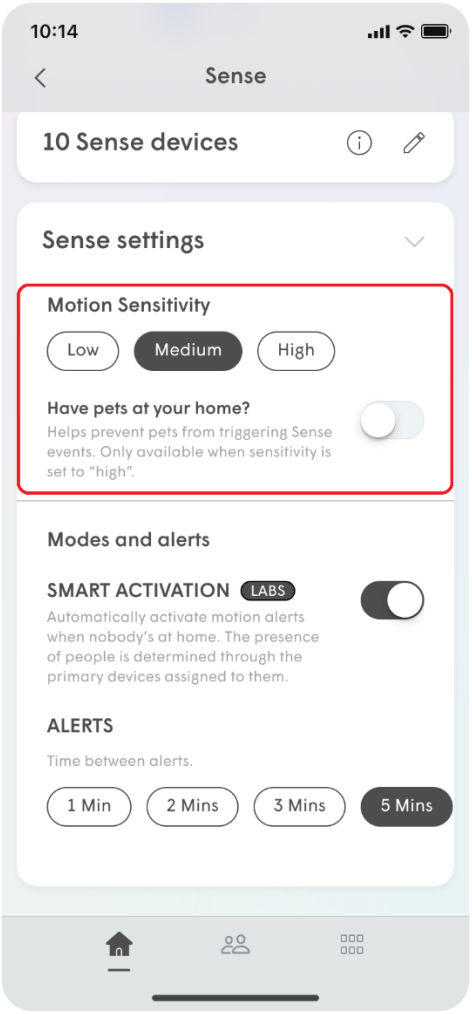
If you choose **High** sensitivity, you can also choose the **Have Pets at home** option to help filter out their movement in your home. This increases the duration of movement needed to trigger an alert from 2 seconds to 5 seconds.
After choosing your sensitivity setting, use the Live View and test the results in all the areas you want to detect motion in.

How do I change motion sensitivity?

iOS

1. Scroll down on the HOme page and Tap on the **Sense.**
2. Scroll down to the bottom of the page and open **Sense Settings**.
3. Choose your **Motion Sensitivity** option and toggle the Pet mode (optional)

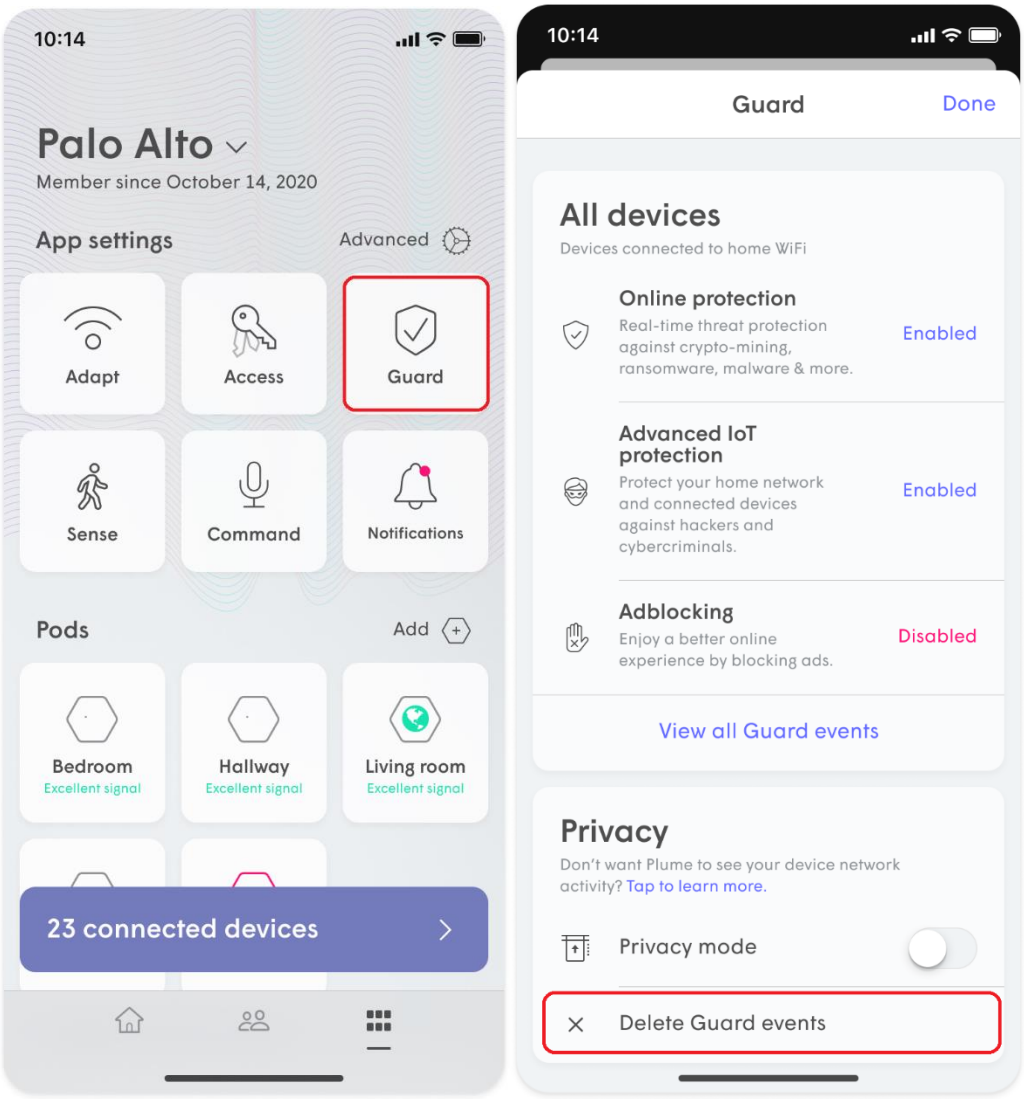

10:14
Sense
Motion detected near
Living Room, Kitchen
LIVE
Doorbell
Living room
Echo
Kitchen
Kitchen
Sense
Sense alerts OFF
Motion today
24
4
8
12
16
20
24
Motion
Away
Alarm
Off
Motion last 7 days
6
12
6
6
12
18
Mon
Tue
Wed
Thur
Fri
Sat
Today
10 Sense devices
2 unassigned stationary devices
Sense settings


10:14
Sense
10 Sense devices
Sense settings
Motion Sensitivity
Low
Medium
High
Have pets at your home?
Helps prevent pets from triggering Sense events. Only available when sensitivity is set to "high".
Modes and alerts
SMART ACTIVATION
LABS
Automatically activate motion alerts when nobody's at home. The presence of people is determined through the primary devices assigned to them.
ALERTS
Time between alerts.
1 Min
2 Mins
3 Mins
5 Mins

How to delete blocked security events?

The HomePass app allows you to delete any past blocked events, similar to clearing your browser history.

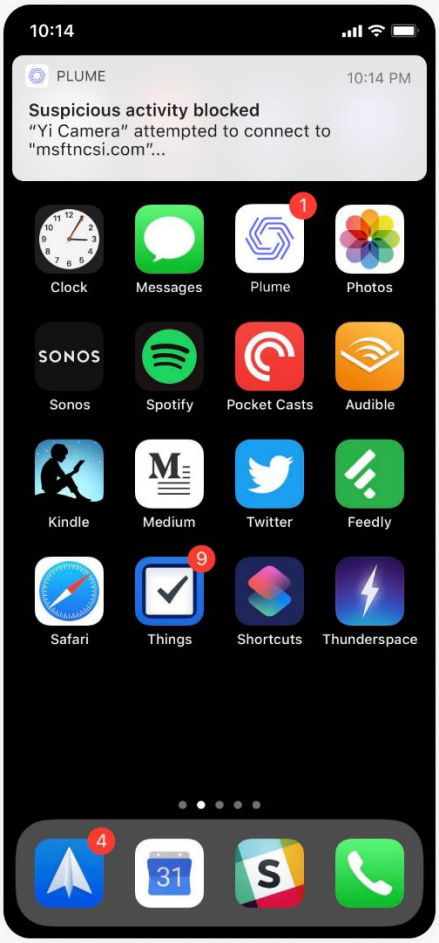
1. If you'd like to delete your past security events, open the main menu and select the **Guard** option.
2. On the bottom of the screen, you will find the **Delete security events** button.
3. Simply tap the button and confirm that you would like to **Clear data**.
    - Note that once deleted, this data cannot be recovered

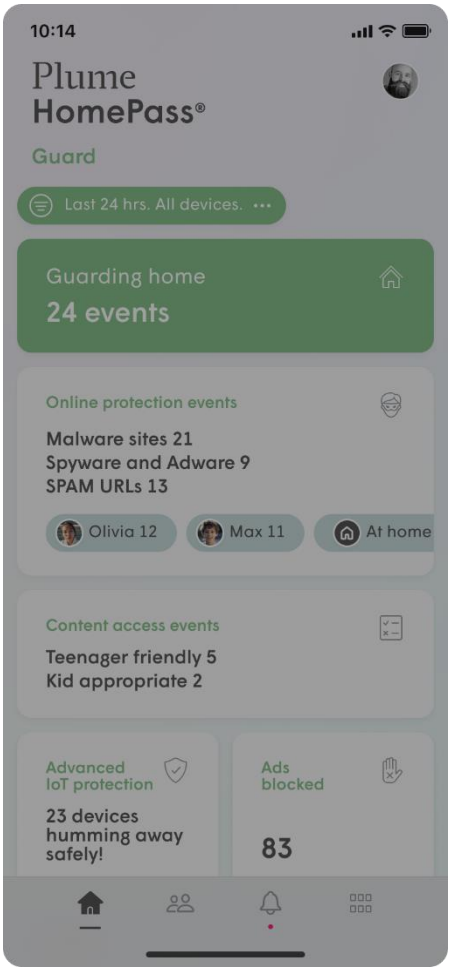


HomePass®

I see Advanced IoT Protection blocked an event. Now what do I do?

If there is a **suspicious activity blocked** event, you probably received a push notification warning you that a smart home device went to a website which is considered unusual compared to its normal behavior. There is no required action on your end other than enjoying the peace of mind that Plume is protecting you and your family!

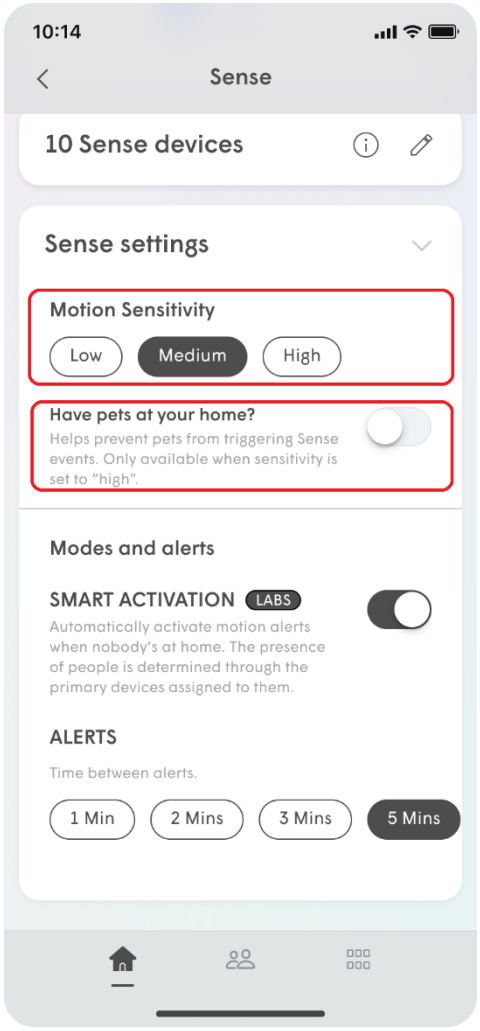




To learn more about the blocked activity, see How can I tell what events have been blocked by Online Protection? and What if Advanced IoT Protection blocks a site that is actually safe?

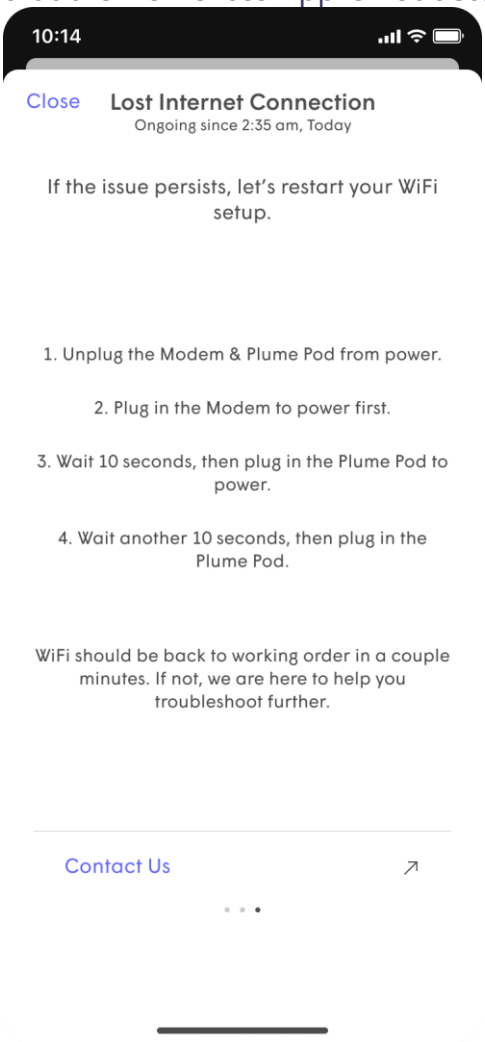
Motion is being detected but I'm not receiving an alert.

If you are in away mode and not receiving an alert when motion is detected, this is due to there not being enough motion to trigger an alert. You can try adjusting your Motion sensitivity settings to High to receive alerts when lower thresholds of motion are detected.



Notification "Lost Internet Connection". How do I get past this?

If the "Still looking for Internet connection to Plume pod..." screen pops up, it means that the HomePass App is not detecting an Internet signal on your gateway pod.



Here are the most common reasons for this issue:

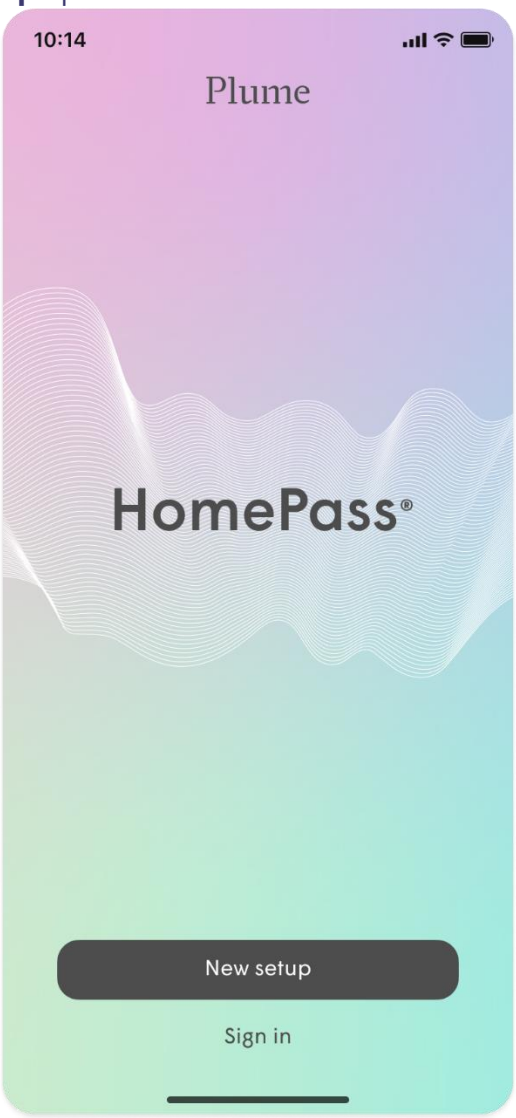
1. No Internet is provided through your modem or router.
    - Power cycle your modem. If you have recently rebooted your modem or router, re-establishing the Internet connection can take a while.
    - If your gateway pod is connected to another router or switch, verify that it's properly setup by reviewing our recommended setup here. To confirm Internet availability, try to connect the pod directly to the modem.
2. Pod is not receiving any power.
    - Try to plug in the pod to another outlet. The LED should turn on.

3. Pod does not power ON and is defective.
    - Try another pod so you can continue with the setup. Contact Plume Support to help diagnose your issue and facilitate the replacement of your defective pod.
4. Bluetooth on your device is OFF.
    - Be sure to turn ON Bluetooth on your device. The Bluetooth option is often found in the Settings section of your device.

The notification will automatically disappear once it detects your gateway pod, so you can continue with your setup.

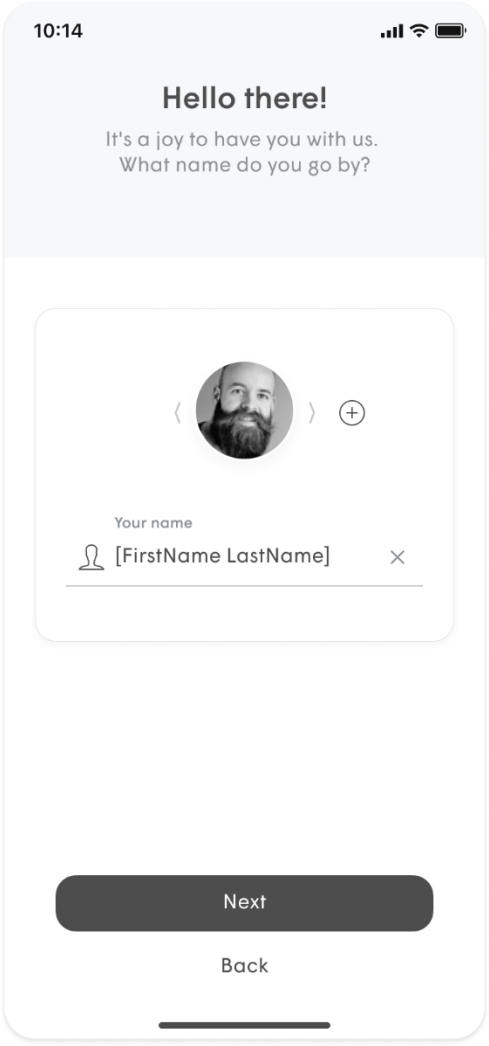
Plume Installation - App Steps

1. Launch the HomePass app and choose the **New Set-Up** option.



2. The app will prompt you to enter your name and email. This will be for your new Plume account.

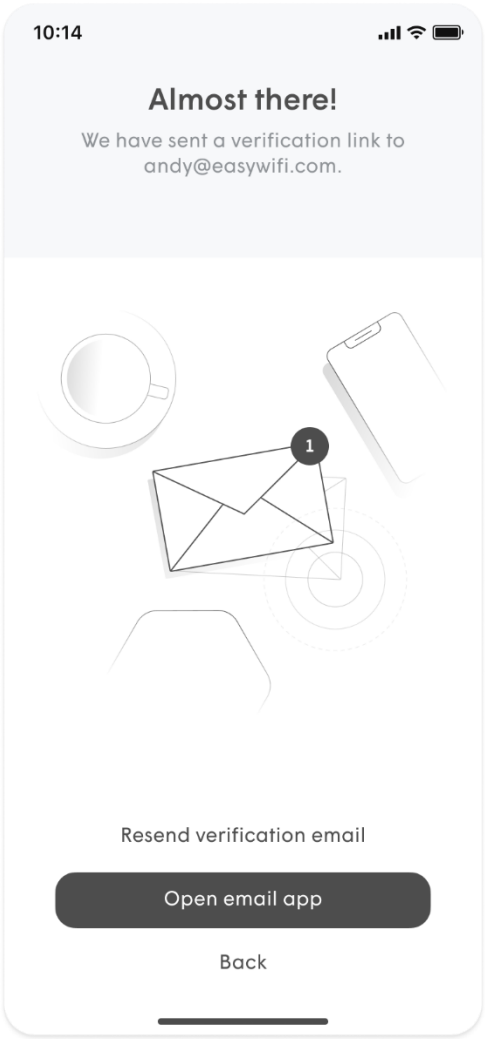
3. Choose your Plume account password, which must be at least 8 characters

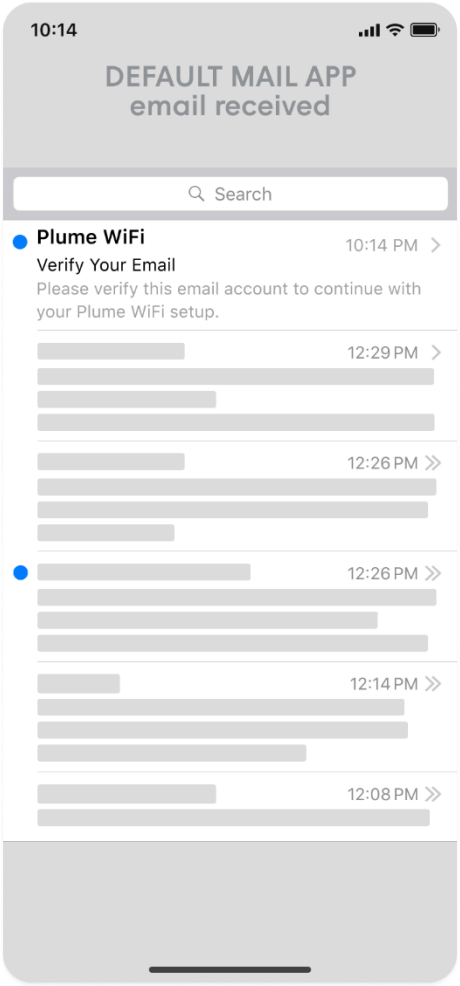


long.

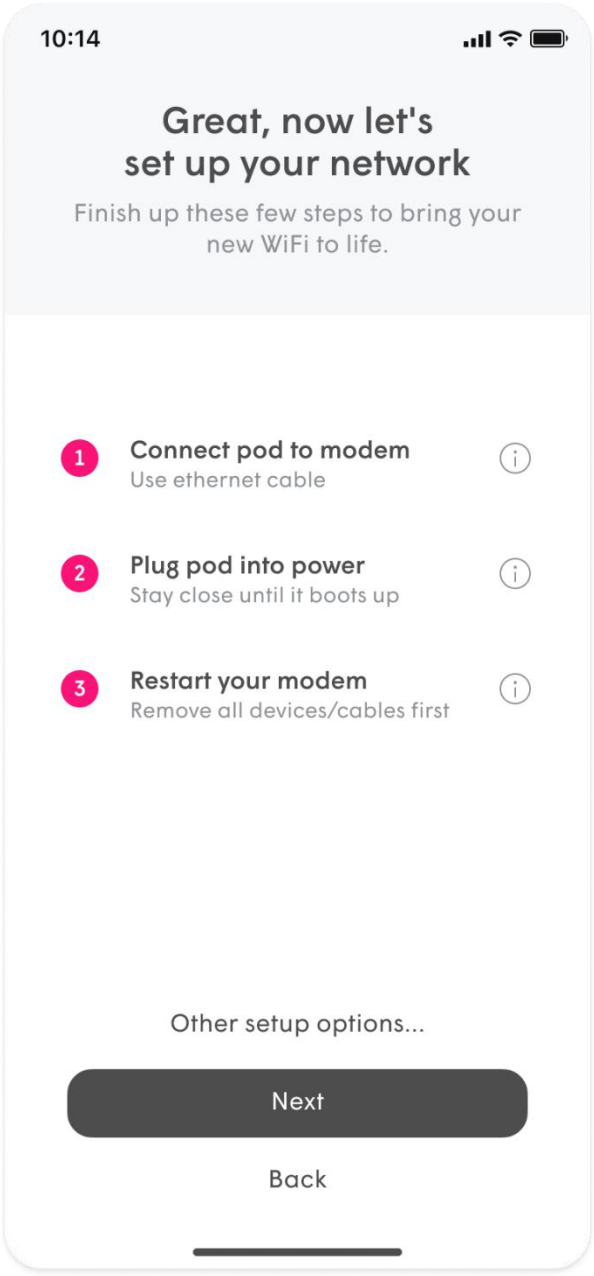
4. An email will be sent to you. Click on the **Verify Email** link within that email to continue the setup process.

5.


10:14
Almost there!
We have sent a verification link to andy@easywifi.com.
1
Resend verification email
Open email app
Back


10:14
DEFAULT MAIL APP
email received
Search
Plume WiFi
10:14 PM
Verify Your Email
Please verify this email account to continue with your Plume WiFi setup.
12:29 PM
12:26 PM
12:26 PM
12:14 PM
12:08 PM

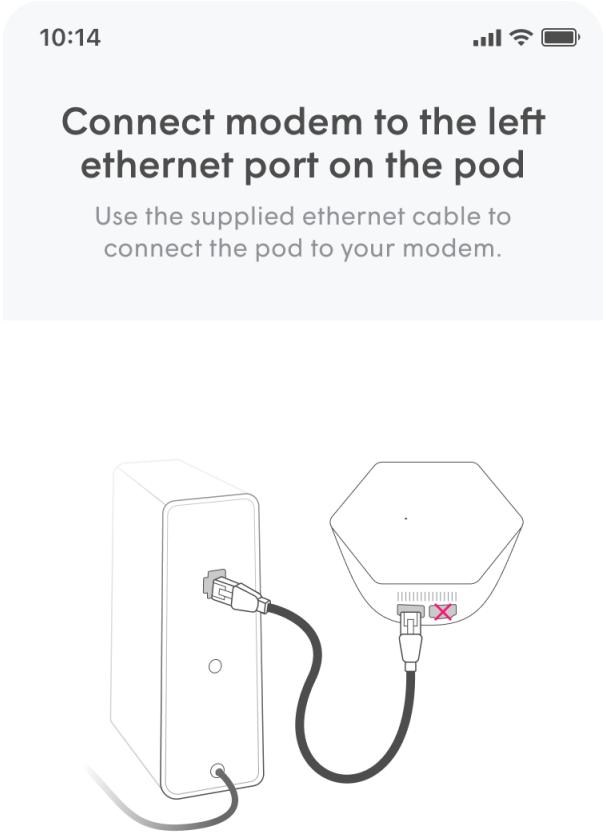
6. You'll be presented with the overall steps to get your first pod connected. This will become the Gateway pod of your Plume network. The info buttons will bring up



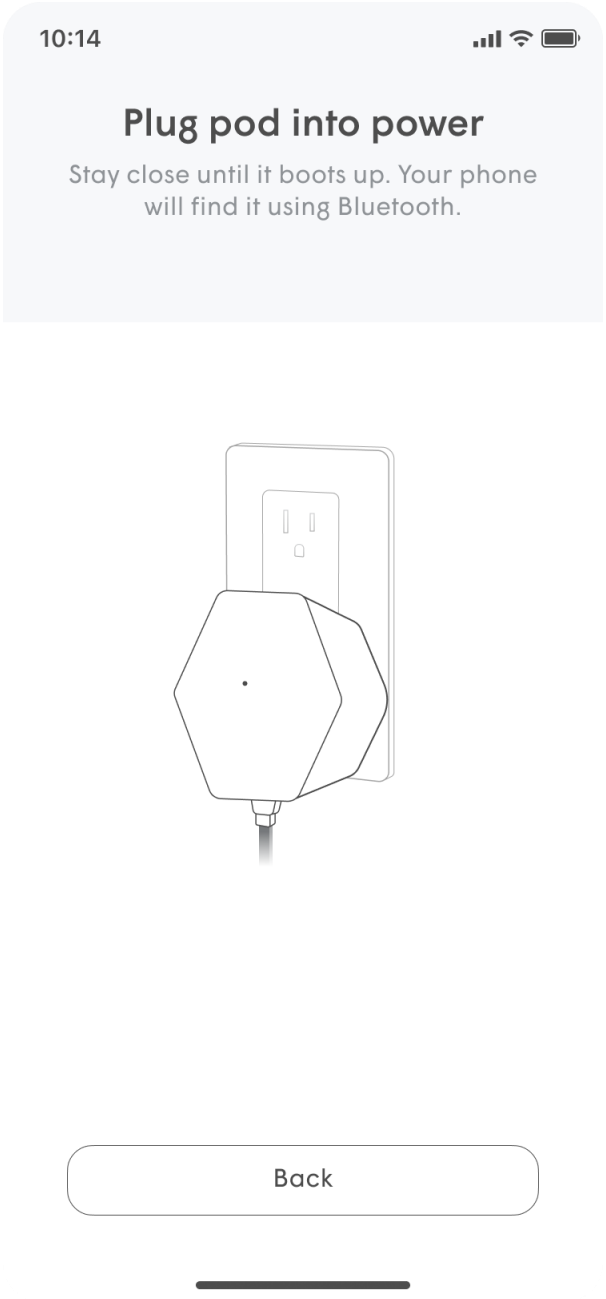
additional details for each step.

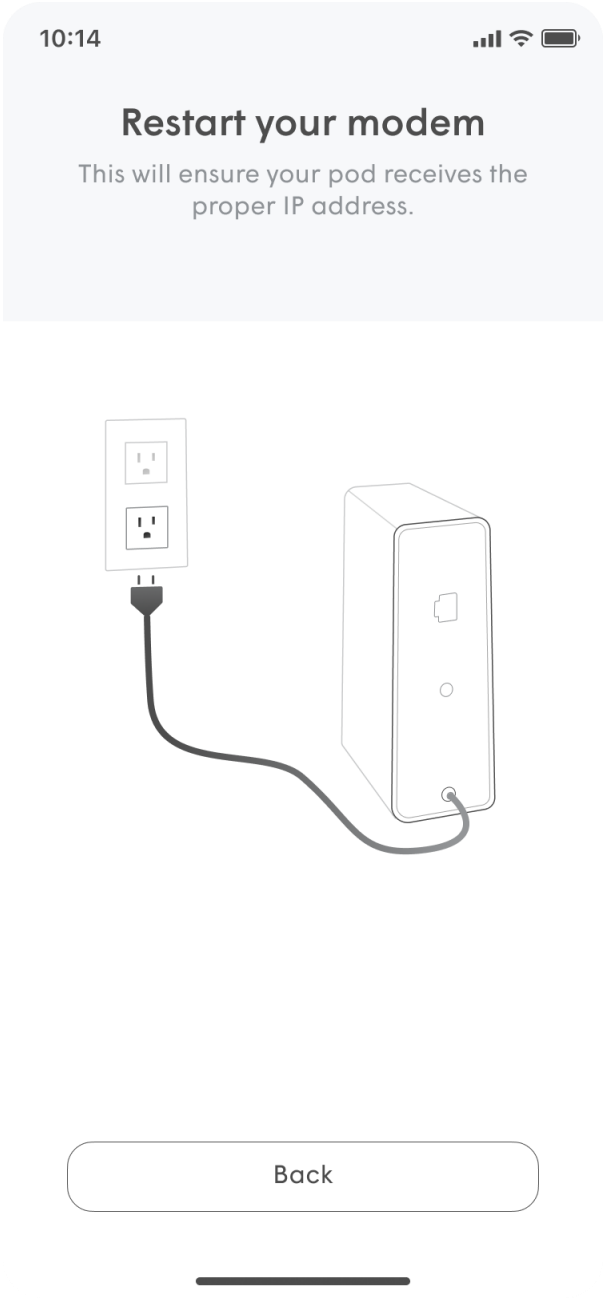
- Connect a pod by Ethernet to your modem. If you have an existing router, ONT for Fiber or other type of network configuration, use the **Advanced setup** link to get more information on how to connect the pod to the

network.



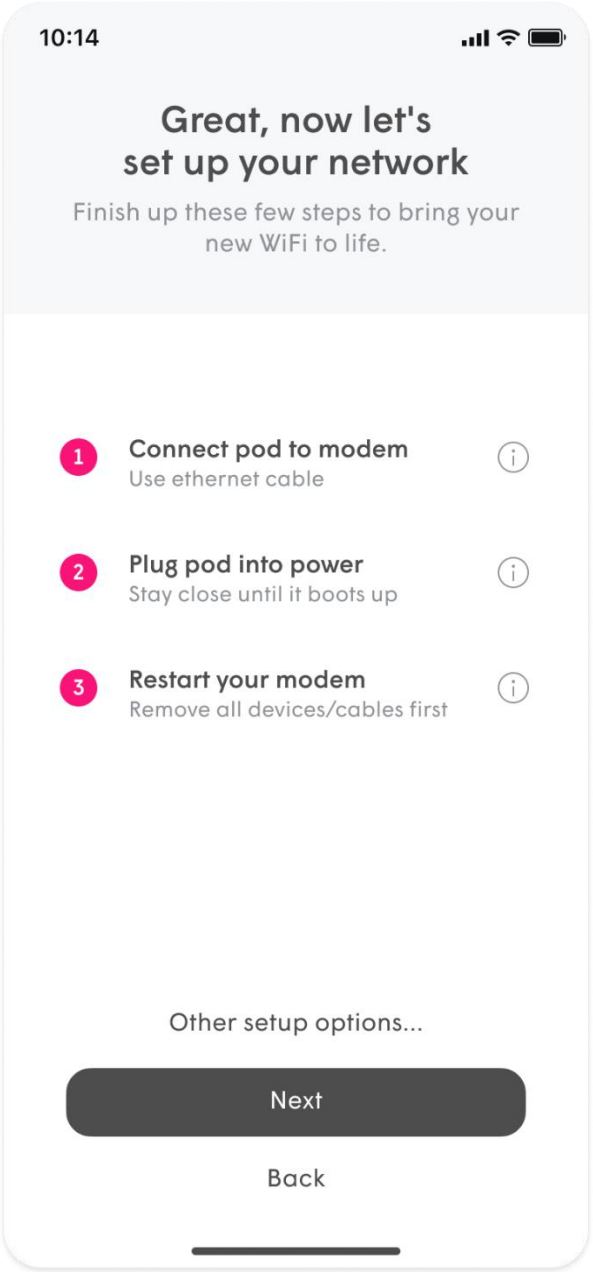
- Plug the pod into power. Restart your modem. The modem should also be left unplugged from power for a minimum of 30 seconds until the next step. If you are using your existing router, modem/router combo or ONT a restart is not necessary.


10:14
Plug pod into power
Stay close until it boots up. Your phone will find it using Bluetooth.
Back

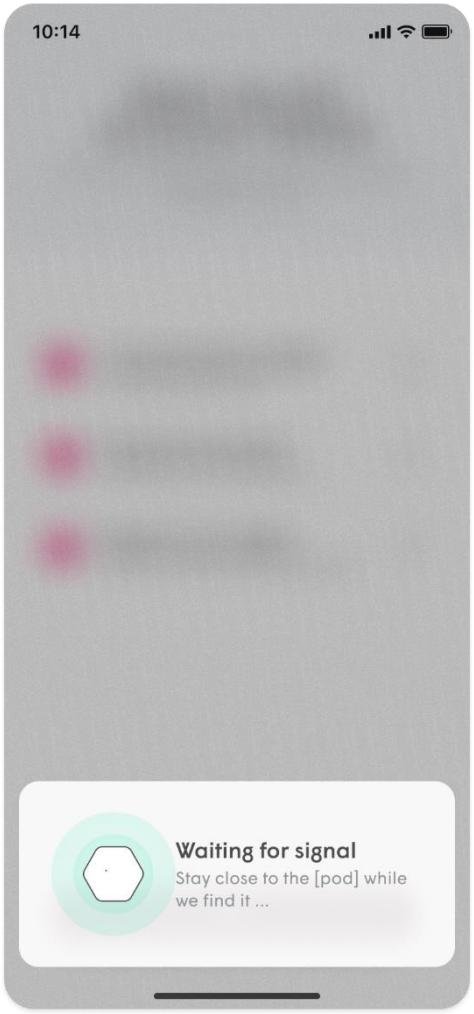


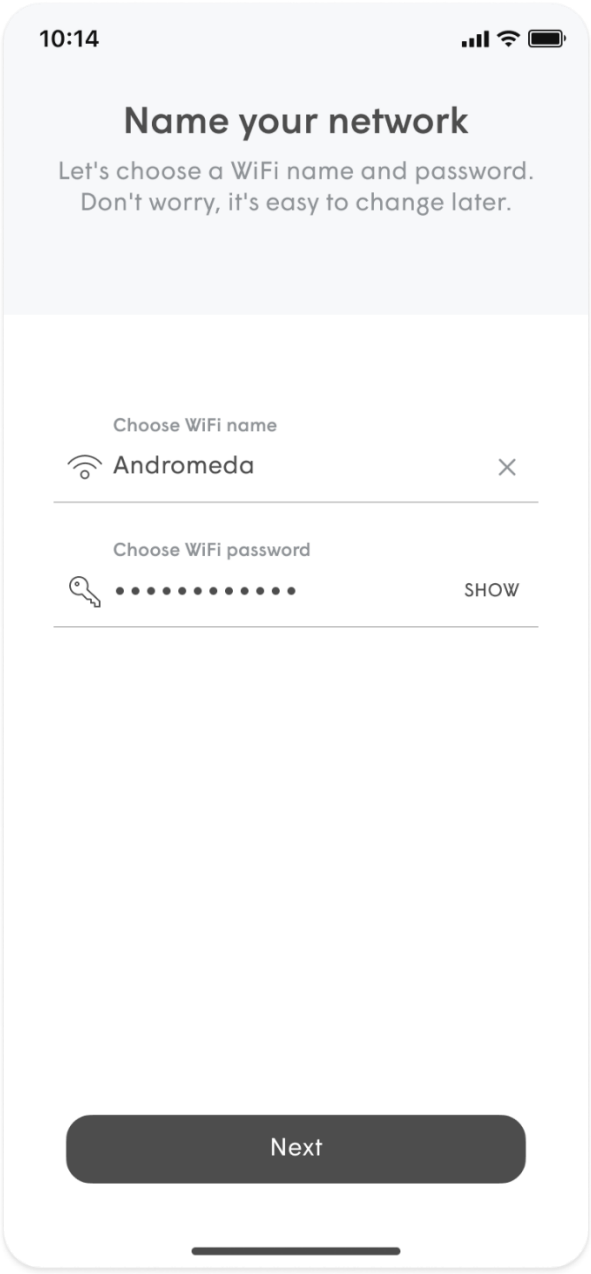
7. Once you have completed the steps to connect you Gateway pod, tap on **Next** to move on to setting up your

SSID.

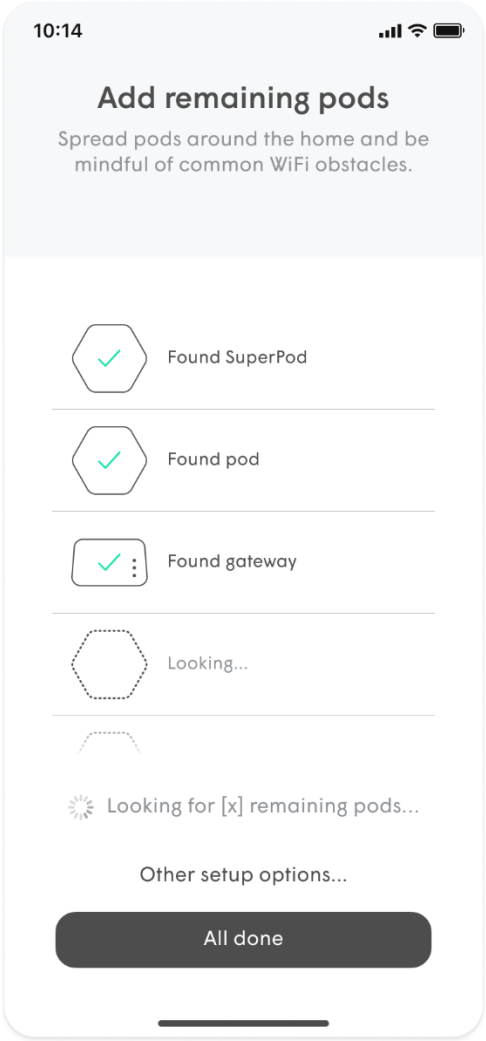


8. The LED will continue to slowly pulse until the pod connects to the Plume cloud. Once connected, the LED will turn off and the app will prompt you to input your new Wi-Fi name (SSID) and Password.
    - To simplify setup, you can use your previous Network Name (SSID) and password. This will allow all your client devices to easily switch to the Plume network once the old Wi-Fi has been turned off, without needing to update the credentials on every single Wi-Fi client.
    - Alternatively, this could be an opportunity to setup a completely new Wi-Fi network name and/or password. This would help ensure that the new Wi-Fi network starts off as secure as possible.

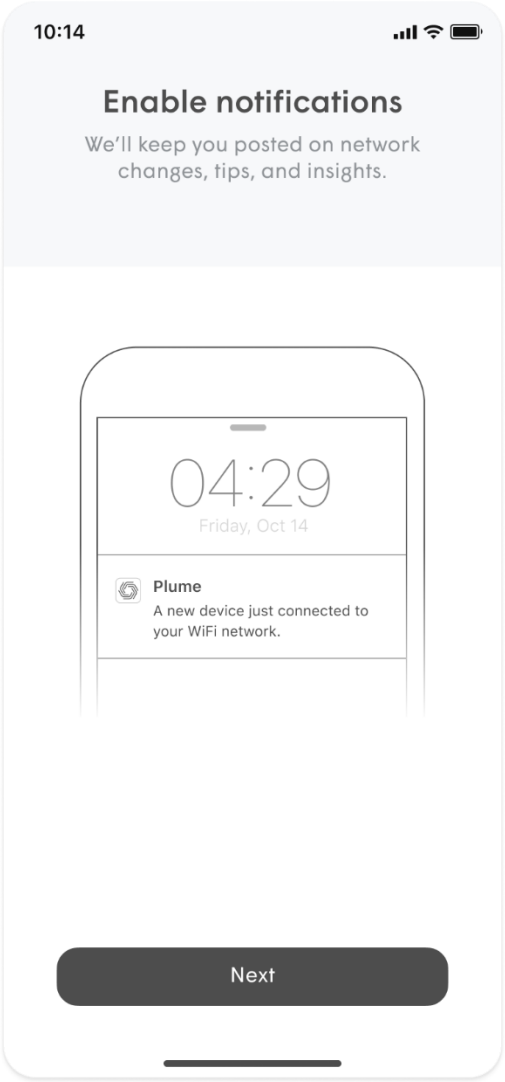

10:14
Waiting for signal
Stay close to the [pod] while we find it ...



9. If you have more than one pod, start plugging them in now. Stay close to each pod until it is found. As each one connects to the network and cloud, a green check mark will appear and the LED will turn off. Tap on **Completed** once all pods have been added.

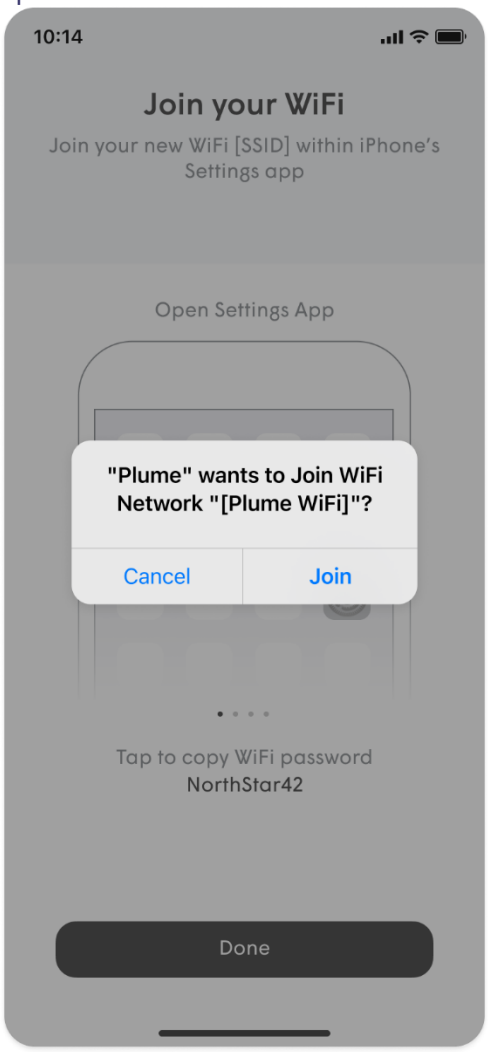

10:14
Add remaining pods
Spread pods around the home and be mindful of common WiFi obstacles.
Found SuperPod
Found pod
Found gateway
Looking...
Looking for [x] remaining pods...
Other setup options...
All done

10. Be sure to **Enable notifications**. This will help you be aware of your home network activity.

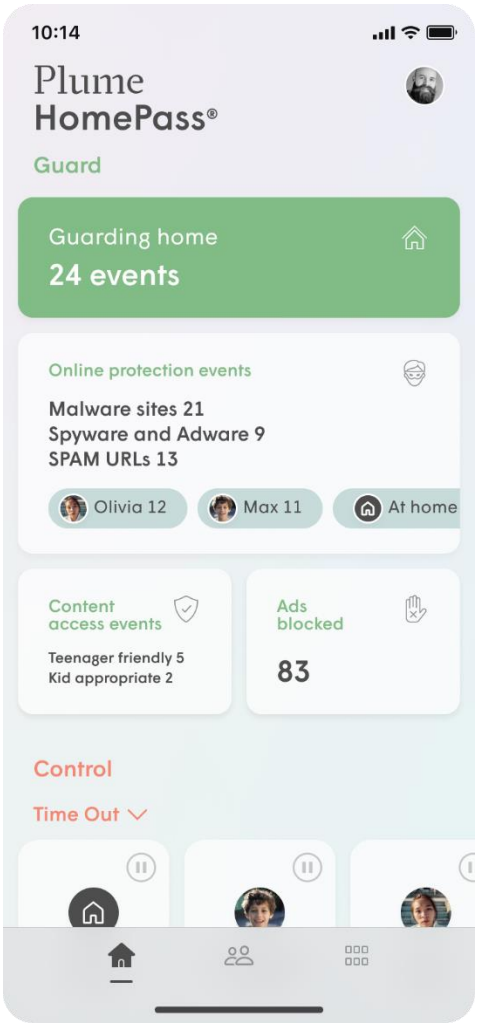


11. The HomePass app will prompt you to join the new Wi-Fi network with your mobile.
    - Tapping on **Join** will take you out of the HomePass app and into the **Wi-Fi settings** so you can join.
    - Once back in the HomePass app, a **Welcome Aboard** message indicates that the device is now connected and the new Wi-Fi network is

operational.



12. Finally, after you have joined the network, you'll be taken to the home screen.



13. As an optional step, pods can be named for easier identification later.
    - Tapping **Snooze**, will skip this step.
    - To name the pods, bring the device close to each pod that is to be named. Bluetooth is used to identify the closest pod.
    - Choose from the list of default names or enter a custom name for each pod.
14. Over the next 24 hours, your new Plume Wi-Fi network will optimize to create the best performance for your connected devices.

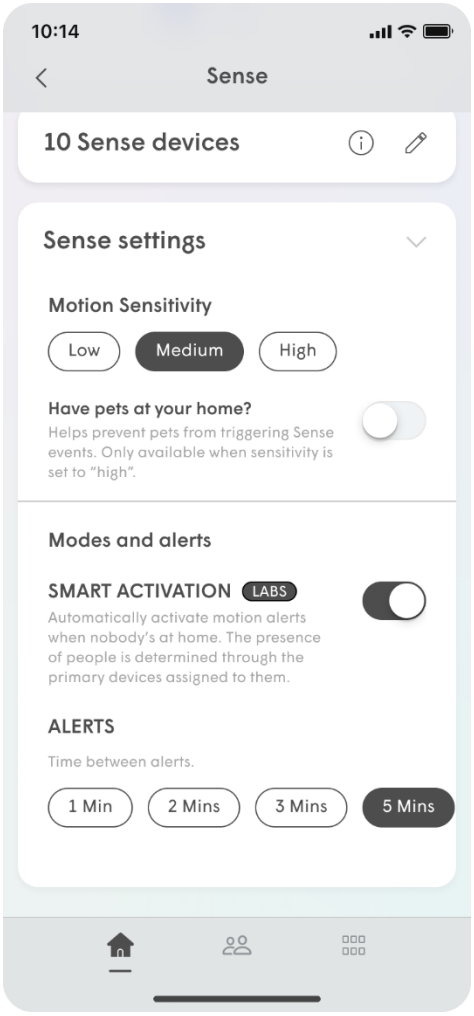
Sense Alert Notification Issues

There is motion in my home, why am I not receiving notifications?

These are the most common reasons for not receiving Sense Alerts when motion should be present:

1. Push notifications may have been disabled on your device.
    - iOS - Enable push notifications
    - Android - Enable Push notifications
2. The motion being detected is not enough to trigger a Sense Alert.
    - Alerts are triggered only if the motion event lasts at least 2 seconds (5 seconds with pet mode enabled) and within approximately 3-4 metres of a SuperPod or Sense enabled device.
3. The sensitivity is set too low for the amount of motion present.
4. Sense Alerts have been turned off.
5. Unless Smart Activation is disabled, notifications will not be sent if you and your other family members are

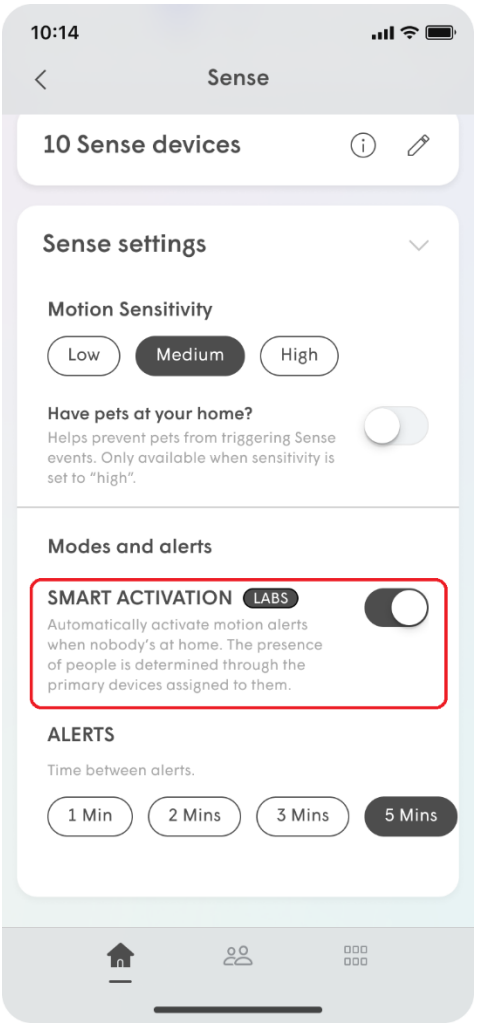
home.



6. When Smart Activation has been enabled for Sense Alerts, all Primary devices assigned to people must have disconnected from the network for at least 15 minutes. This also means that if someone leaves their primary device at home, alerts will not go out.
7. Depending on your notification interval settings, not enough time has elapsed since your last alert.

Why am I still receiving motion notifications while I'm home?

Other than Smart Activation for Sense alerts not being enabled, the most common reason you may still be getting Sense alerts while home is that Primary devices have not been assigned to people or People profiles have not been created.
Your Home / Away status is based on when all assigned primary devices have disconnected from the network. If you have not assigned any primary devices to people, your current status will always be away and notifications will always go out if there is motion.



It is also possible that if all Primary devices chosen are disconnected from the network when they go to sleep (laptops, tablets, portable game consoles) or are powered off, your status will be set to away.

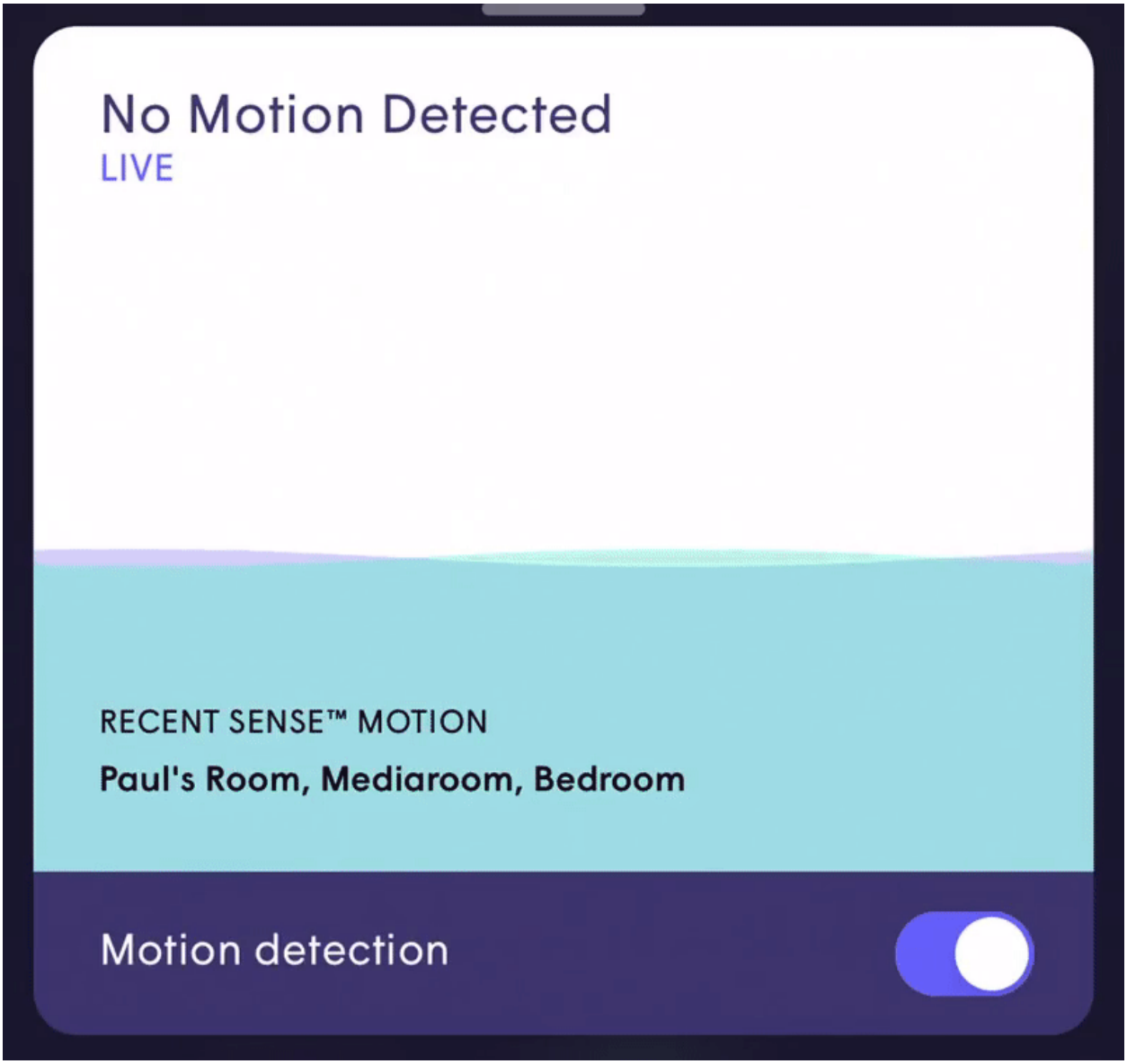
Why am I receiving notifications when no one is home?

The most common reasons for receiving false motion alerts when no one is in your home are:

1. The motion sensitivity may be set too high or pet mode is not enabled.
    - If you have pets try enabling pet mode, or try turning down the sensitivity to medium or low.
2. If you more than one location, alerts are sent for all locations under your Plume account.
    - Switch your app to the other location and check the Motion Today graph to see if the events displayed in that location correspond to the alert you have received.

Sense Live View

Live View allows you to see both the location and intensity of the detected motion in real-time.



In the Live View display, the overall intensity and duration of the motion are represented by the background wave.

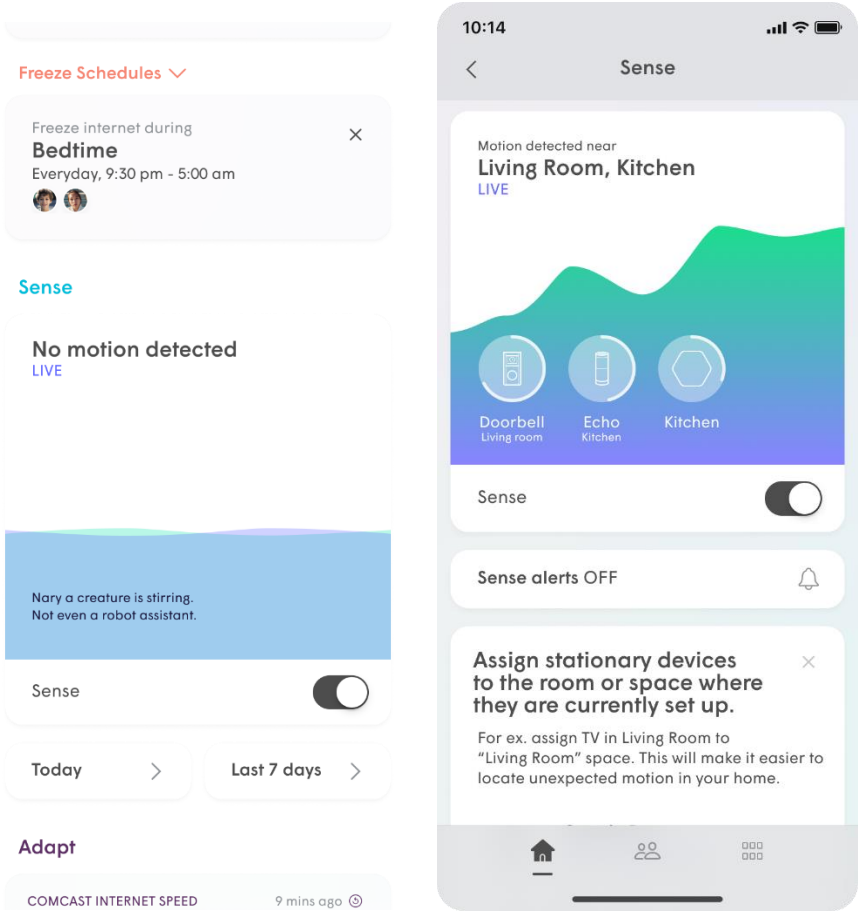
The devices detecting the motion are displayed to provide an approximate location of where the motion is being detected. Along with the motion intensity being detected by each device, this can be used to get an idea of where someone is moving.

Be sure to assign rooms to your devices to better pinpoint where motion is happening.

Accessing the Live View

1. From the **home screen**, Scroll to the **Sense** section.

2. The **Live View** will be available on the home screen. If you want to see more details tap on the Sense section.



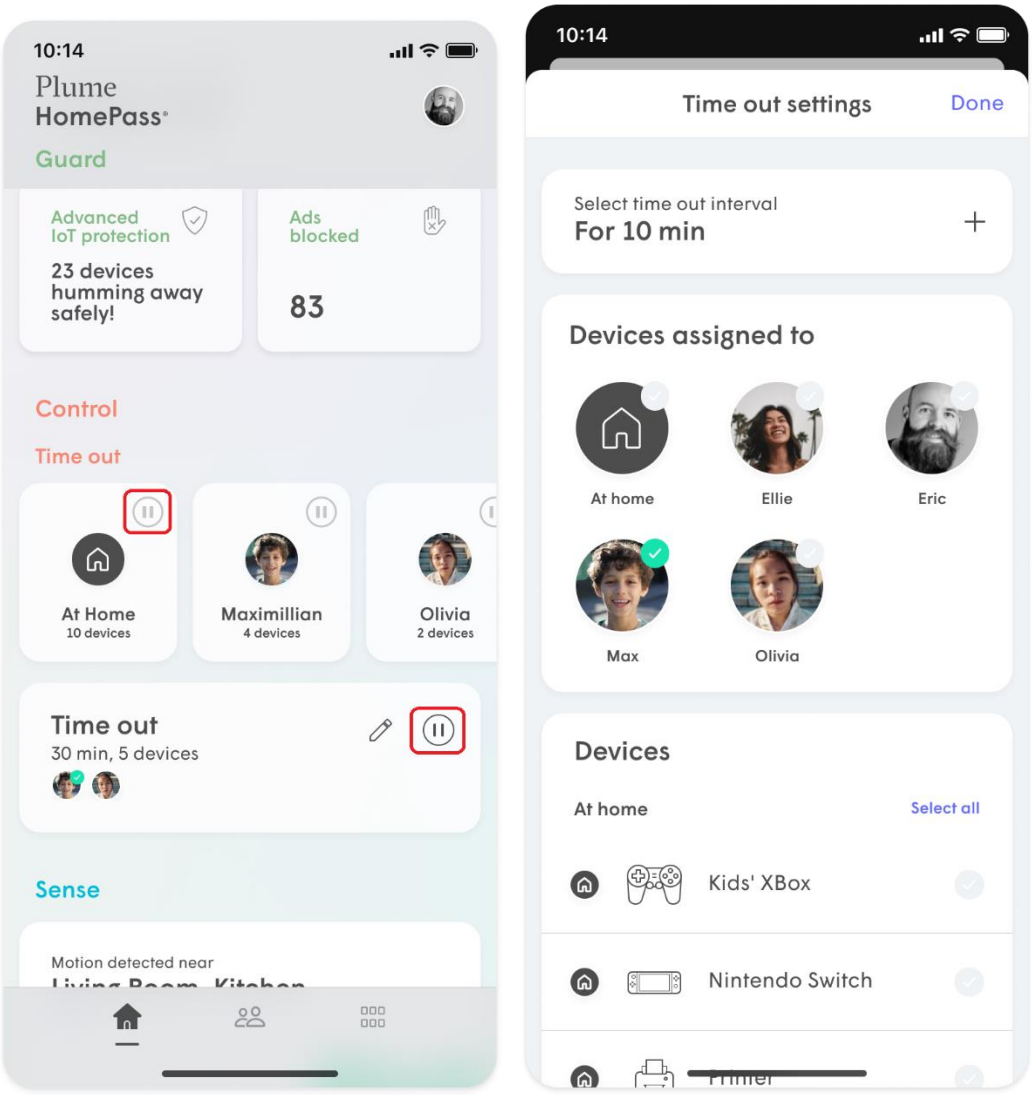
0

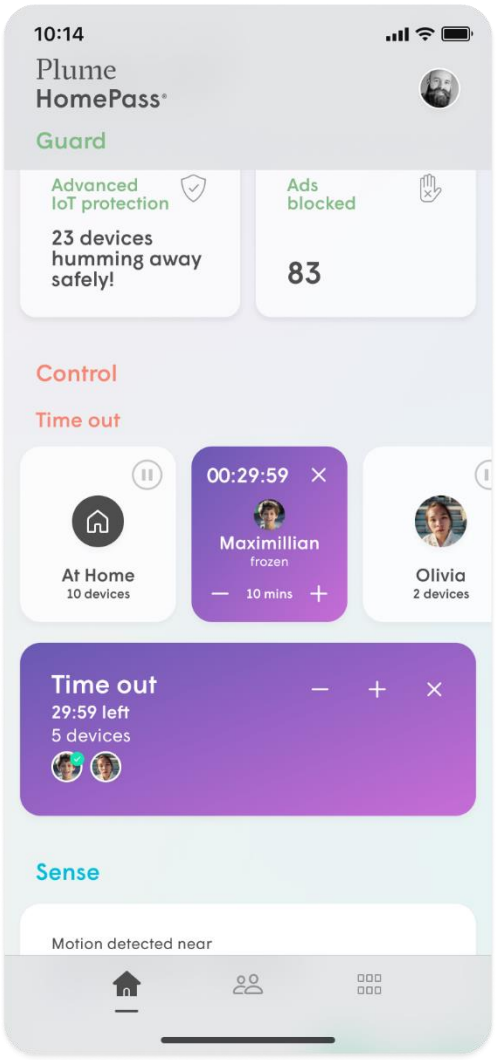
Set a global or custom Internet Time Out

Plume gives you the ability to briefly freeze or pause internet access globally for all people or for all devices instantly through the Time Out feature. If you want to set a scheduled Internet break, consider our Device Freeze feature.

Setting a custom Time Out / Global Time Out (All people)

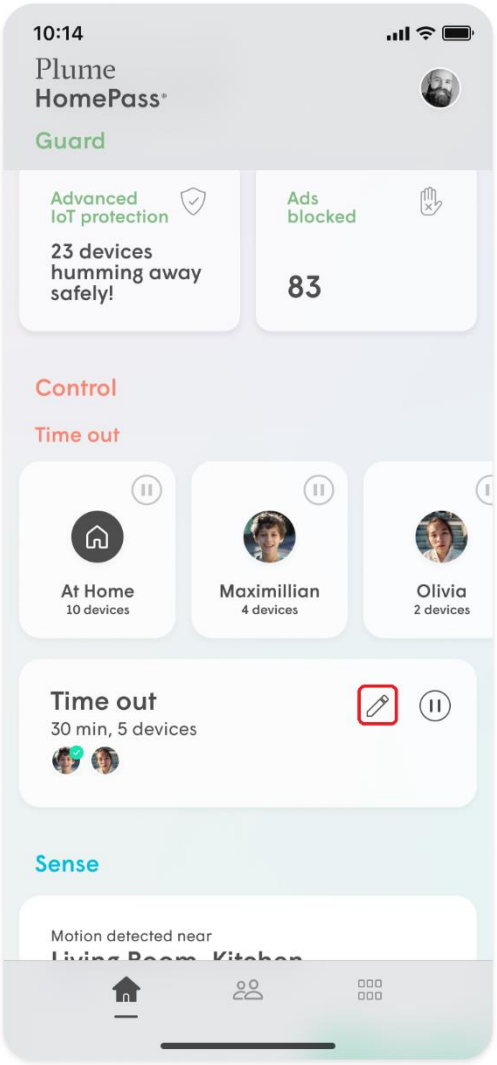
1. From the **home screen**, scroll to the Control Section and find the option **Time Out** menu.
2. Tap on the **pencil icon** to edit who will be put in a Time Out and the length of the Time Out.
3. Use the **+ or** - to modify the Time Out period in 10-minute increments.
4. Under **Devices belonging to**, tap on the people individually or you can use the **black checkmark** to select everyone.
5. Tap on **Done** to return to the previous screen.
6. Tap on the **pause icon** to activate the Time Out. All devices assigned to the people selected will now have Internet access blocked. The Time Out timer will count down until expiry.
7. Use the **+**, **-** or **x** to modify the duration or cancel the Time Out.

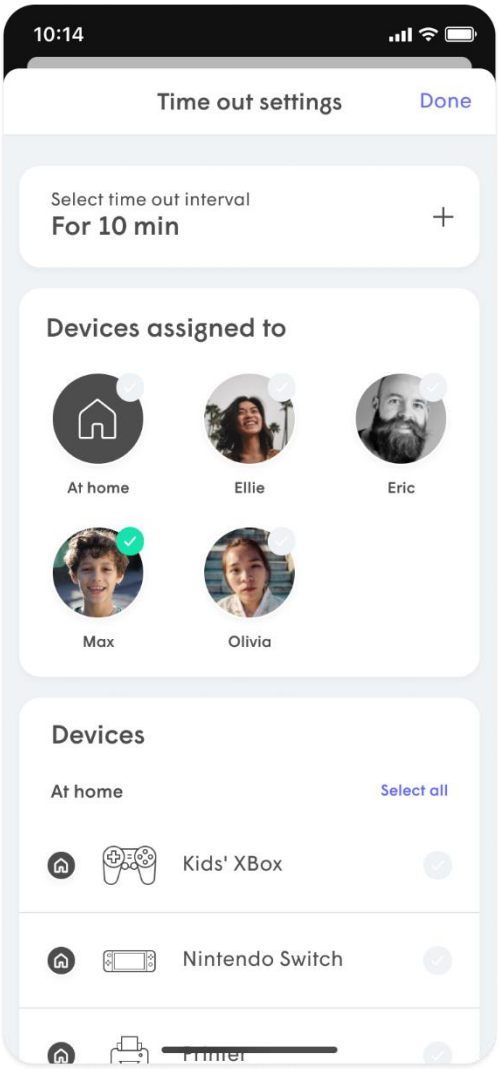

10:14
Plume
HomePass
Guard
Advanced IoT protection
23 devices humming away safely!
Ads blocked
83
Control
Time out
At Home
10 devices
Maximillian
4 devices
Olivia
2 devices
Time out
30 min, 5 devices
Sense
Motion detected near
10:14
Time out settings
Done
Select time out interval
For 10 min
Devices assigned to
At home
Ellie
Eric
Max
Olivia
Devices
At home
Select all
Kids' XBox
Nintendo Switch



Setting a custom Time Out / Global Time Out (All devices)

1. From the **home screen** scroll to **Control Section** and find the **Time Out** menu.
2. Tap on the **pencil icon** to edit who will be put in a Time Out and the length of the Time Out.
3. Use the **+** to increase the Time Out period in 10-minute increments. Use the - to reduce the duration.
4. Under **Devices at home**, tap on the devices individually or you can use the **black checkmark** to select all devices.
5. Tap on **Done** to return to the previous screen.
6. Tap on the **pause icon** to activate the Time Out. All devices selected will now have Internet access blocked. The Time Out timer will count down until expiry.
7. Use the **+**, **-** or **x** to modify the duration or cancel the Time Out.


10:14
Plume
HomePass
Guard
Advanced IoT protection
23 devices humming away safely!
Ads blocked
83
Control
Time out
At Home
10 devices
Maximillian
4 devices
Olivia
2 devices
Time out
30 min, 5 devices
Sense
Motion detected near


10:14
Time out settings
Done
Select time out interval
For 10 min
Devices assigned to
At home
Ellie
Eric
Max
Olivia
Devices
At home
Select all
Kids' XBox
Nintendo Switch

Setting up Port Forwarding

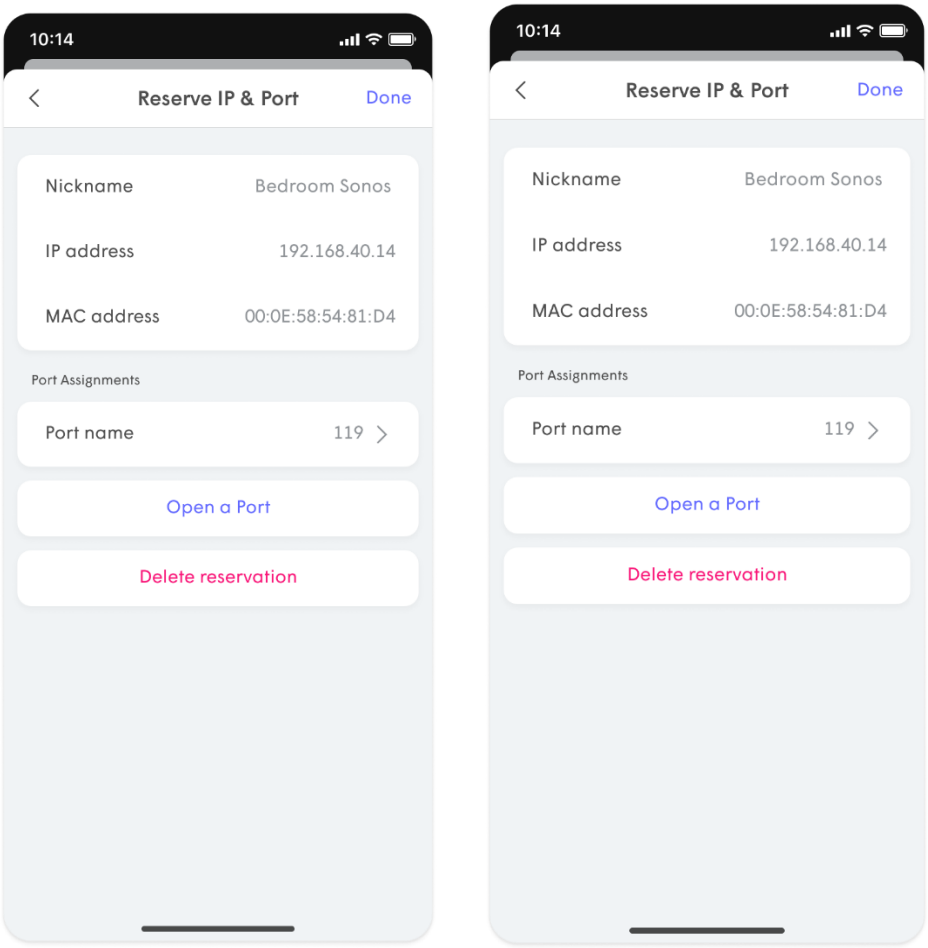
What is Port Forwarding?

Port forwarding (opening ports) allows you to open specific ports in the router's firewall which are needed by some services to communicate to devices on your network. A port has an internal and external value called the port number. Multiple external hosts can use the same external port number, but each internal port must be different, this allows Network Address Translation (NAT) to identify the destination for inbound traffic.
Port forwarding is necessary when you are having issues related to a restricted NAT.

Where do I find Port Forwarding settings?

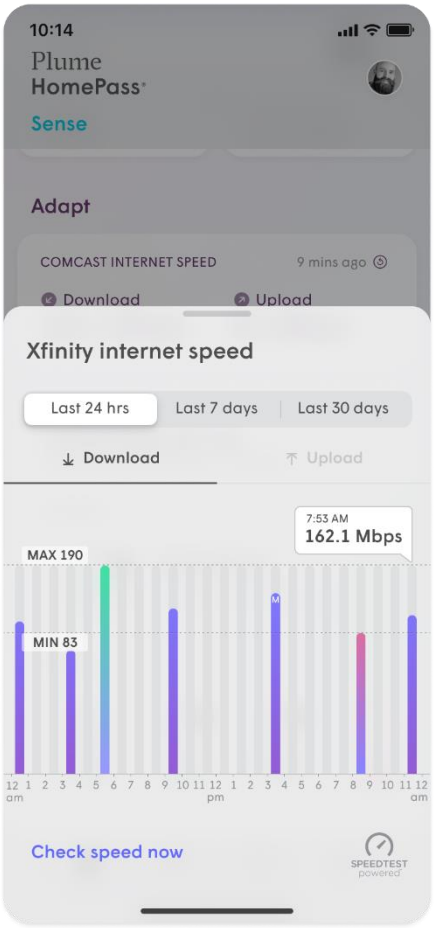
UPnP allows services to automatically set up port forwarding rules, although you can also manually set up port forwarding. Manual set up can be tedious if you are setting rules for multiple services and multiple devices. You should not enable UPnP and set up port forwarding at the same time.
Because you are opening/forwarding ports in the firewall, this setting must set in the router. If Plume is in bridge mode, you will need to set up port forwarding rules in your router. If you are using Plume in router mode, port forwarding can be set up in the HomePass app:

1. In the **Adapt** menu open the **Advanced Settings** or through the gear icon at menu ▫▫▫ ▫▫▫.
2. You need to set an IP reservation for the local device.
3. From the IP reservation, tap on **Open Port.**
4. Enter a **name** for the rule (each name need to be unique).
5. Enter the **External Port** number the service requires.
6. Enter the **Internal Port** number* to be used on the device.
    - Use the same number as the external to just open the port or another number to route the traffic to a different port.
7. Choose the required **Protocol.**
8. Tap on **Save.**
9. Repeat these steps for each rule needed.
    - If the external port has already been used for one service, it is not necessary to set it again for a different service on the same device.
    - The external port number for each rule can be the same, however, the internal port number must always be unique. This means you will need to choose another internal port number for each local device.

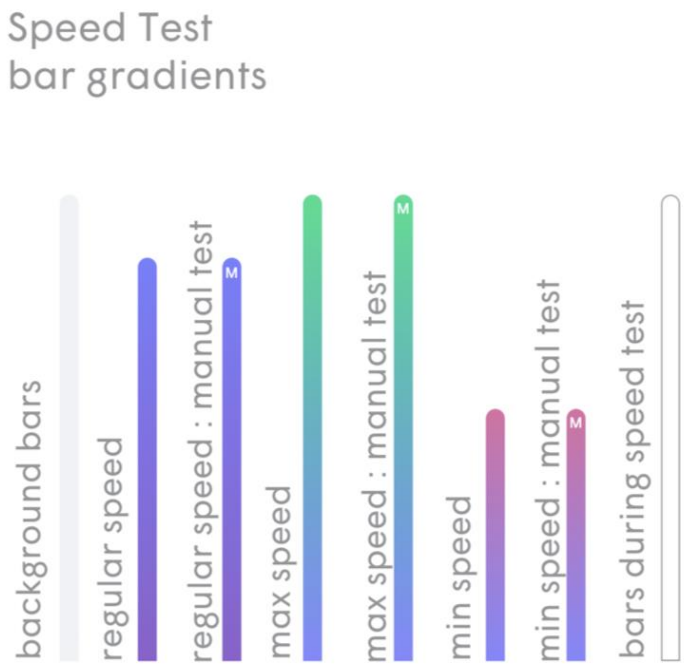

10:14
Reserve IP & Port
Done
Nickname
Bedroom Sonos
IP address
192.168.40.14
MAC address
00:0E:58:54:81:D4
Port Assignments
Port name
119
Open a Port
Delete reservation
10:14
Reserve IP & Port
Done
Nickname
Bedroom Sonos
IP address
192.168.40.14
MAC address
00:0E:58:54:81:D4
Port Assignments
Port name
119
Open a Port
Delete reservation

What do the colours of my ISP speed test results mean?

If you've run some ISP Speed Tests on your network already (or if they've run automatically), you may have noticed some beautifully colored bars appear on your chart!

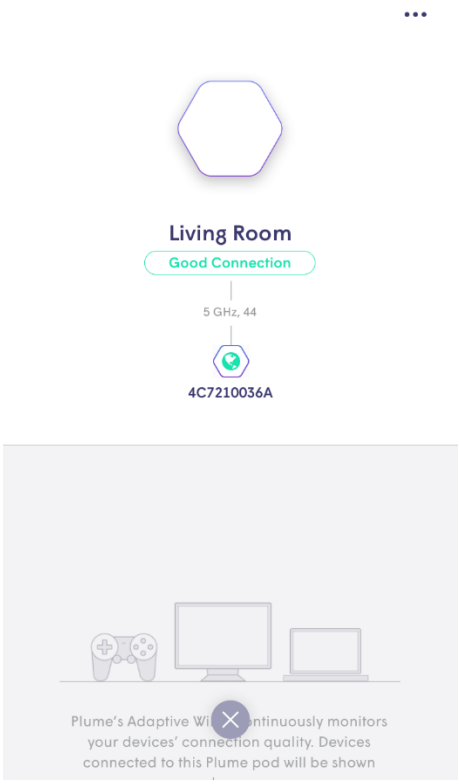


Each gradient actually represents the status of your network during the time the speed test was run.



The fastest speed test from your selected time frame (24 hrs, 7 days, or 30 days) will always appear with a green gradient. Conversely, the slowest will be red. The results between these two will appear in purple.
Additionally, manual speed tests will appear with an "M" on top of the graph.
Note: When many speed tests are run in a short amount of time, the results may be averaged into one bar to avoid overpopulating the chart.

What does the health of my pod mean?



On the pod detail screen above, the app reports the current pod Health. Pod health describes the connection quality of the link between this pod and its immediate parent pod.

Pod health takes into account the Wi-Fi signal strength, the speed of data transmission, and available airtime to send and receive data from the upstream connected pod.

When your pod is moved, Plume recalculates the pod health to keep this information current. Pod health ranges from Excellent to Poor and is described below.

Excellent

Pod has a stellar connection to the upstream pod. The WiFi environment is wide open for communications between the pods. All applications should run flawlessly.

Good

The connection to the upstream pod is okay. All applications on the connected devices should run without any major impairments. Some initial buffering may happen for very high-speed applications such as 4K video streaming

Fair

The connection to the upstream pod is not ideal for real time applications or high throughput applications, like 4K video streaming.

Poor

The pod is not able to communicate well with the upstream connected pod. It may be too far from it or large amounts of interference may exist in its current location. Connected IOT devices or downstream pods and their connected IOT devices may continue to work, but real-time applications such as video conferencing or streaming may suffer.

What if Advanced IoT Protection blocks a site that is actually safe?

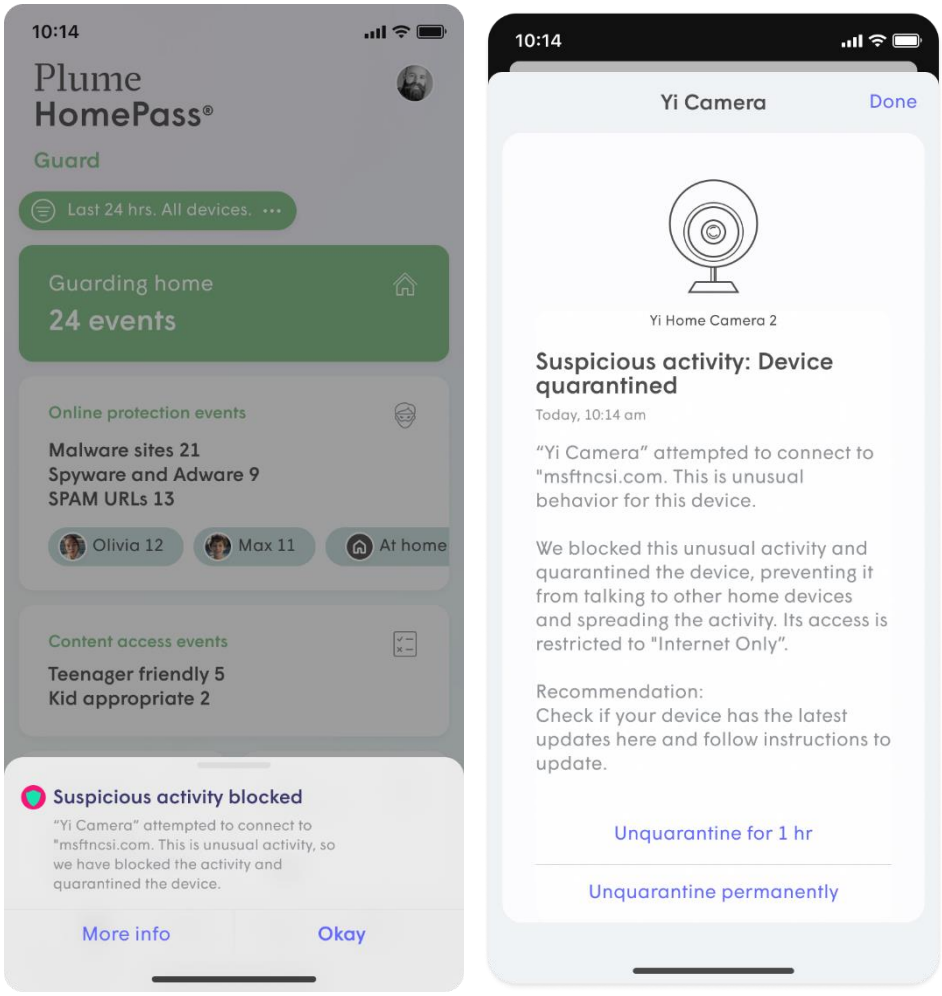
When an anomaly is detected, the device will automatically be placed into quarantine to protect the integrity of your network and the devices connected to it. Quarantining the device effectively places "Internet Only" permission on the device, allowing basic functionality while preventing access to your other home devices.
Advanced IoT Protection (AIP) uses machine learning on device network metadata to establish known behaviors. However, sometimes safe sites can be flagged as a false positive. If a new behavior comes across our large training samples or if device behaviors are updated by the vendor, the device may be incorrectly flagged. Learning happens continually to establish new normal behaviors, however can cause some alerts in the interim. If you trust the website the device is accessing, you can whitelist it for the device and for all devices in the home.

When Should I Remove a Device From Quarantine?

You should only remove a device from quarantine if you trust the website it was trying to access. On a quarantined device, there is a **recommendation** which will open a web search for the device's manufacturer website, so you can do more research or find an updated firmware before removing the device from quarantine.

Removing a Device from Quarantine

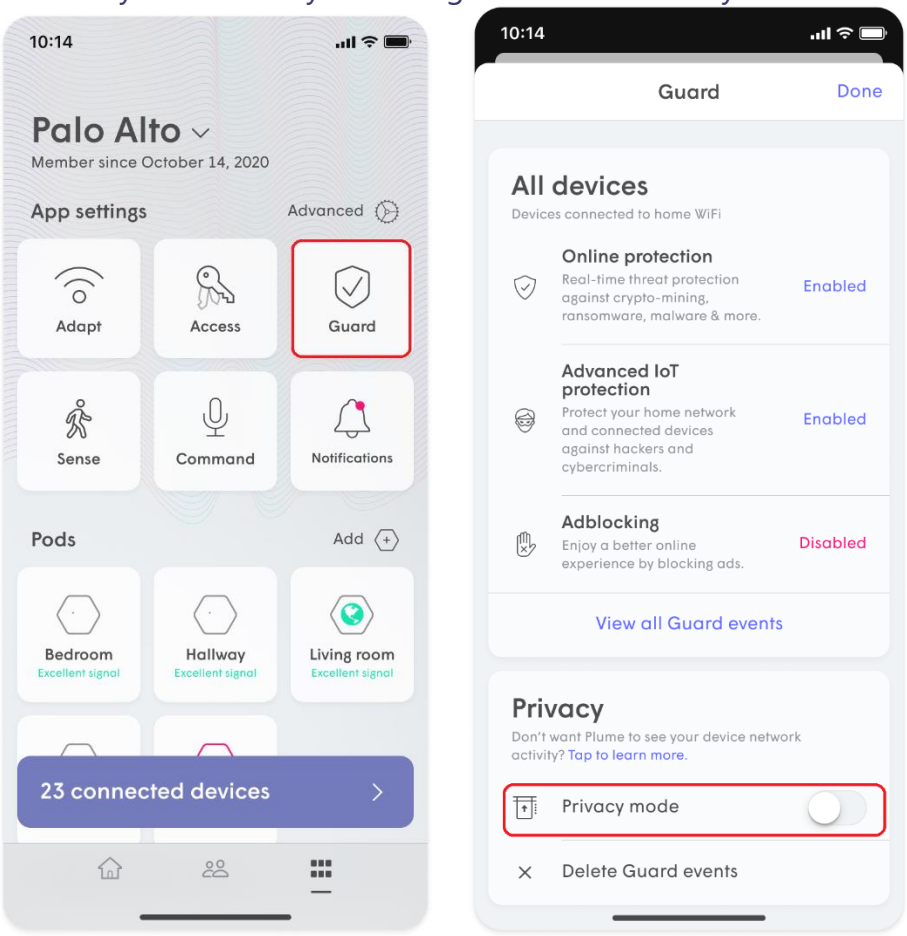
1. Open the device list and navigate to the **Internet Only** devices.
2. Find the affected device. The affected device will be labeled: **Device is quarantined**.
3. Tap on the quarantined device for more options.
4. You can choose **Unquarantine for 1 hour** or **Unquarantine permanently.**



To learn more about the blocked activity, see [How can I tell what events have been blocked by Online Protection?]

What is Privacy Mode?

Plume's Privacy Mode enables you to limit data from being sent to the Plume Cloud. This feature is configurable at the location level. It is Disabled by default, though you can always enable it by accessing the **Guard** tab of your HomePass app.



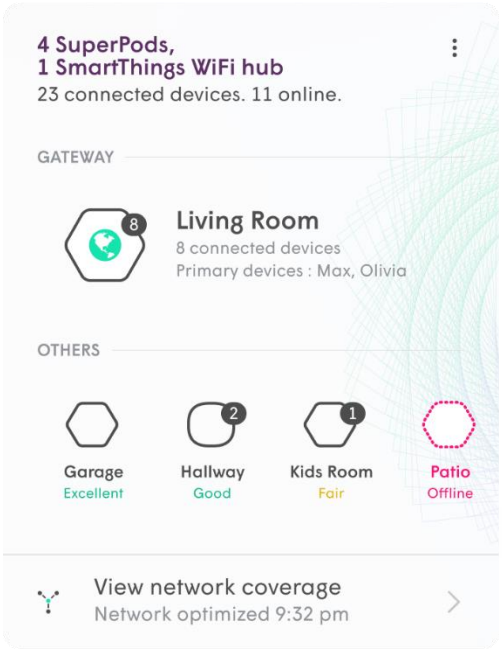
When you **Enable** Privacy mode:

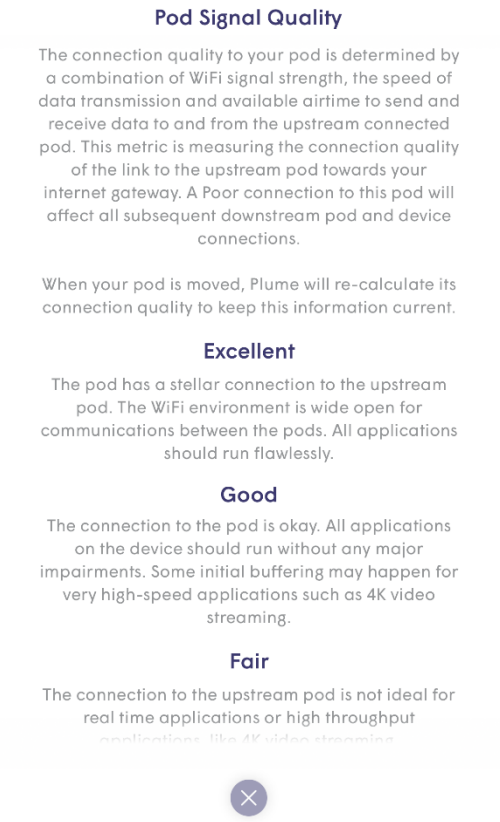
- All Guard features (Online Protection, Advanced IoT Protection, Adblocking, and Content Filters) will be disabled. Past blocked events are preserved and will be visible through the app upon disabling Privacy mode, unless you choose the **Delete Security Events** option.
- Previously quarantined devices will be un-quarantined.
- DNS sampling and user agents will not be collected at any time so Advanced Device Typing information may not be accurate.

For more on Plume's full Privacy Policy, click here.

Where can I view my Plume network status?

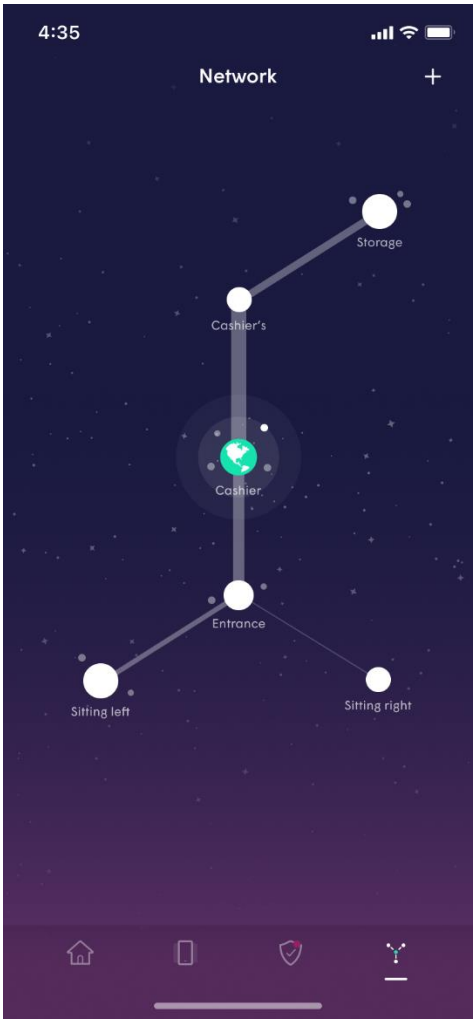
You can always view the status of your pods from the Home Screen by selecting **Adapt.** You will be able to scroll through all the pods associated with your network with its current status





.

App users have access to the network's topology where you will see a web-like structure representing each pod and connected devices on your network. This enables you to easily view the status of your pods and the devices that are actively connected to your network.



The colours of the icons signify the status of your pods:

- **Pod is Green** - pod that acts as the gateway or is connected to the gateway router.
- **Pod is White** - pod is online and has devices connecting to the internet through it.
- **Pod is Grey** - pod is online but no device is currently connected to it.
- **Pod is Red** - pod is offline.