

WorkPass

Mobile App Manual

Contents

App navigation

Managing Network Settings

Managing Network Access

- Wi-Fi Zones
- Secure Wi-Fi Zone

Managing Employee Wi-Fi

Managing Guest Wi-Fi Access

Managing Digital Access

Plume Shield™

- Online Protection
- Advanced IoT™ Protection
- AdBlocking
- Privacy Mode

Managing the Account

Speed Tests



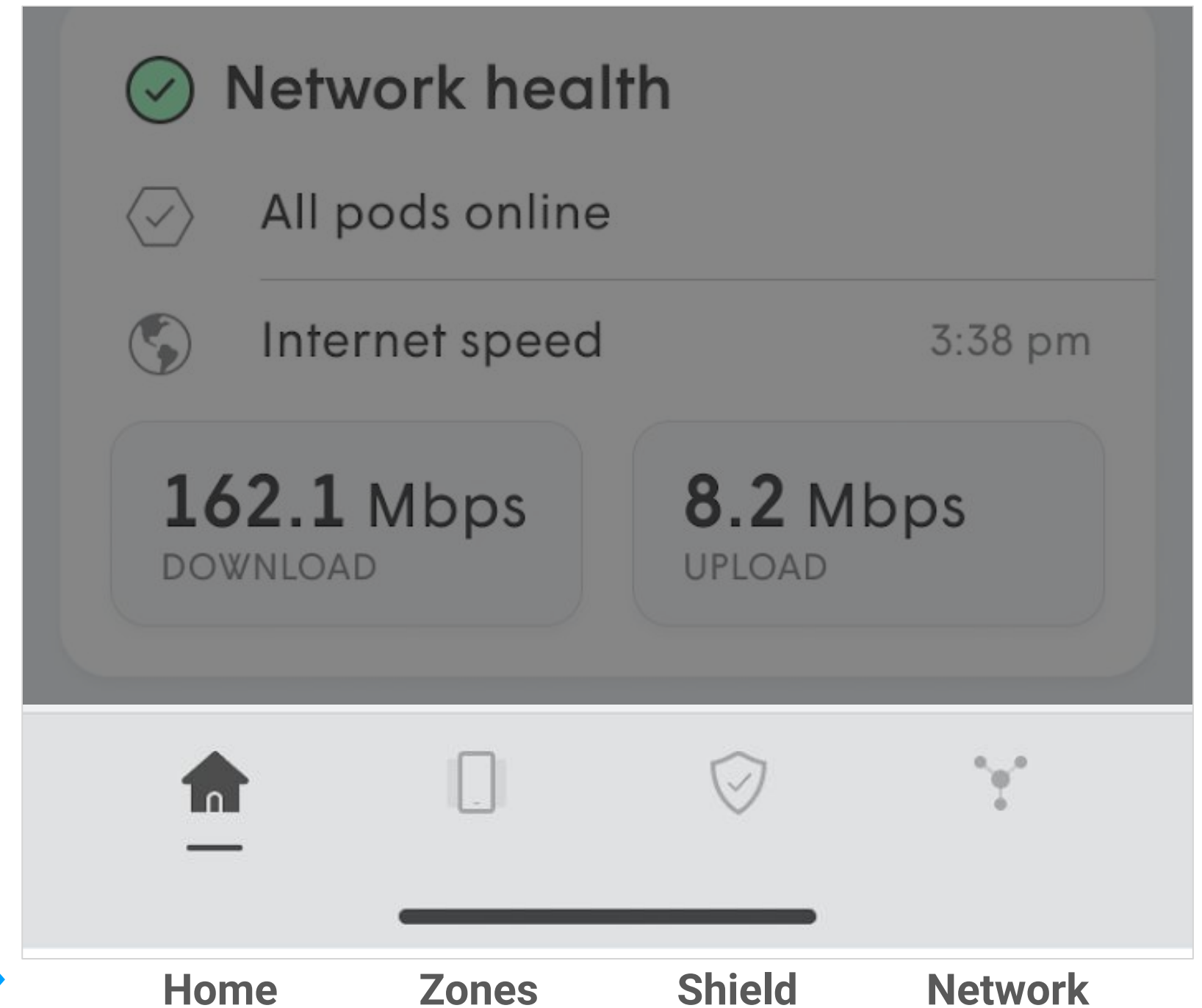
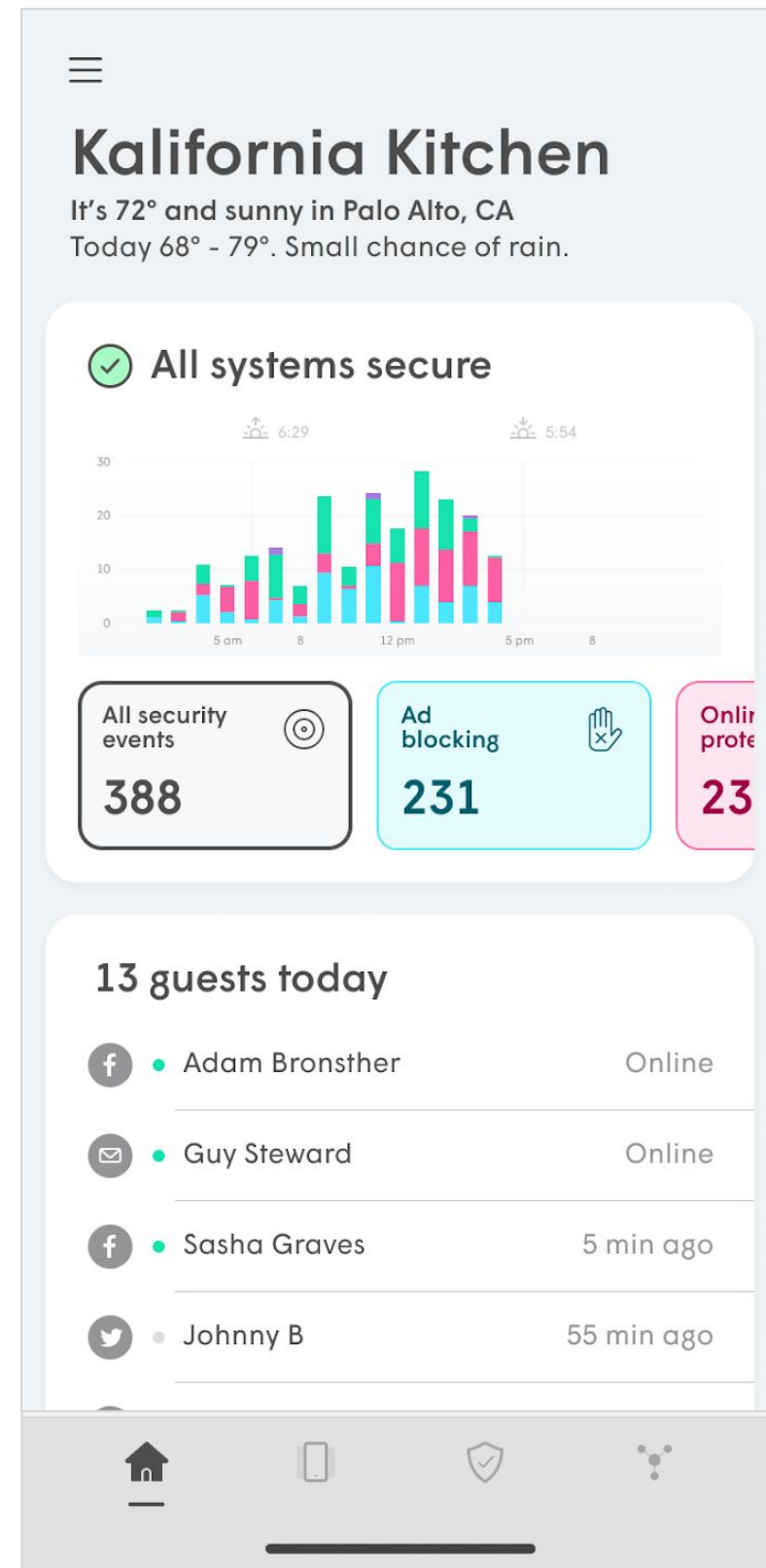
App Navigation

App Navigation

Main Menu

The majority of daily network admin and monitoring can be found in these four tabs.

- **Home** - Overview of current network (24 hrs), including Guests, Security status, Employees at Work, Network Health. **Settings** and the associated pages are also from here.
- **Devices** - Manage Zones, Devices, People and Wi-Fi access.
- **Security** – Shield features such as: Online Protection, Advanced IoT™ Protection, Ad Blocking.
- **Network** – Topology View



App Navigation

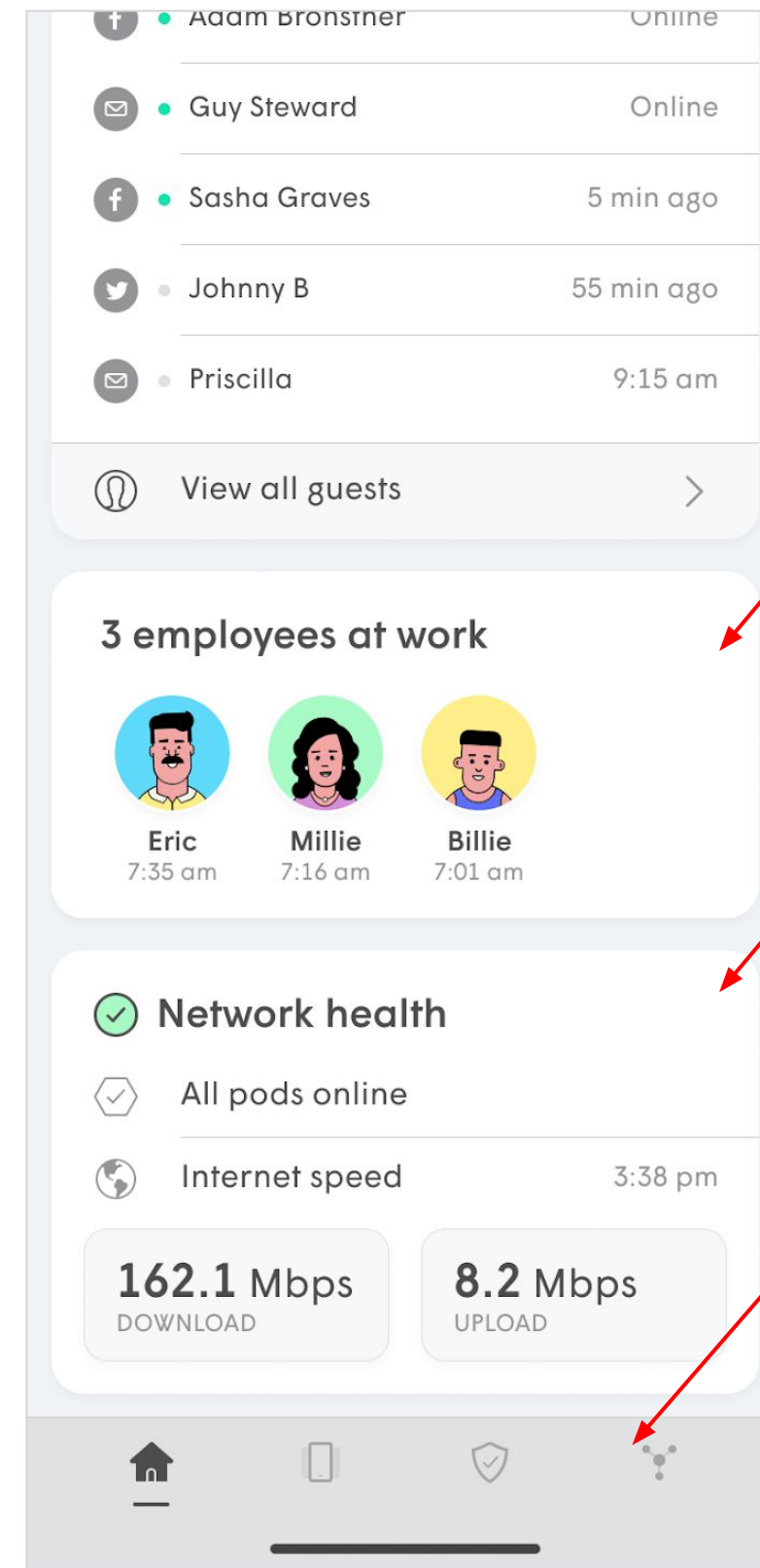
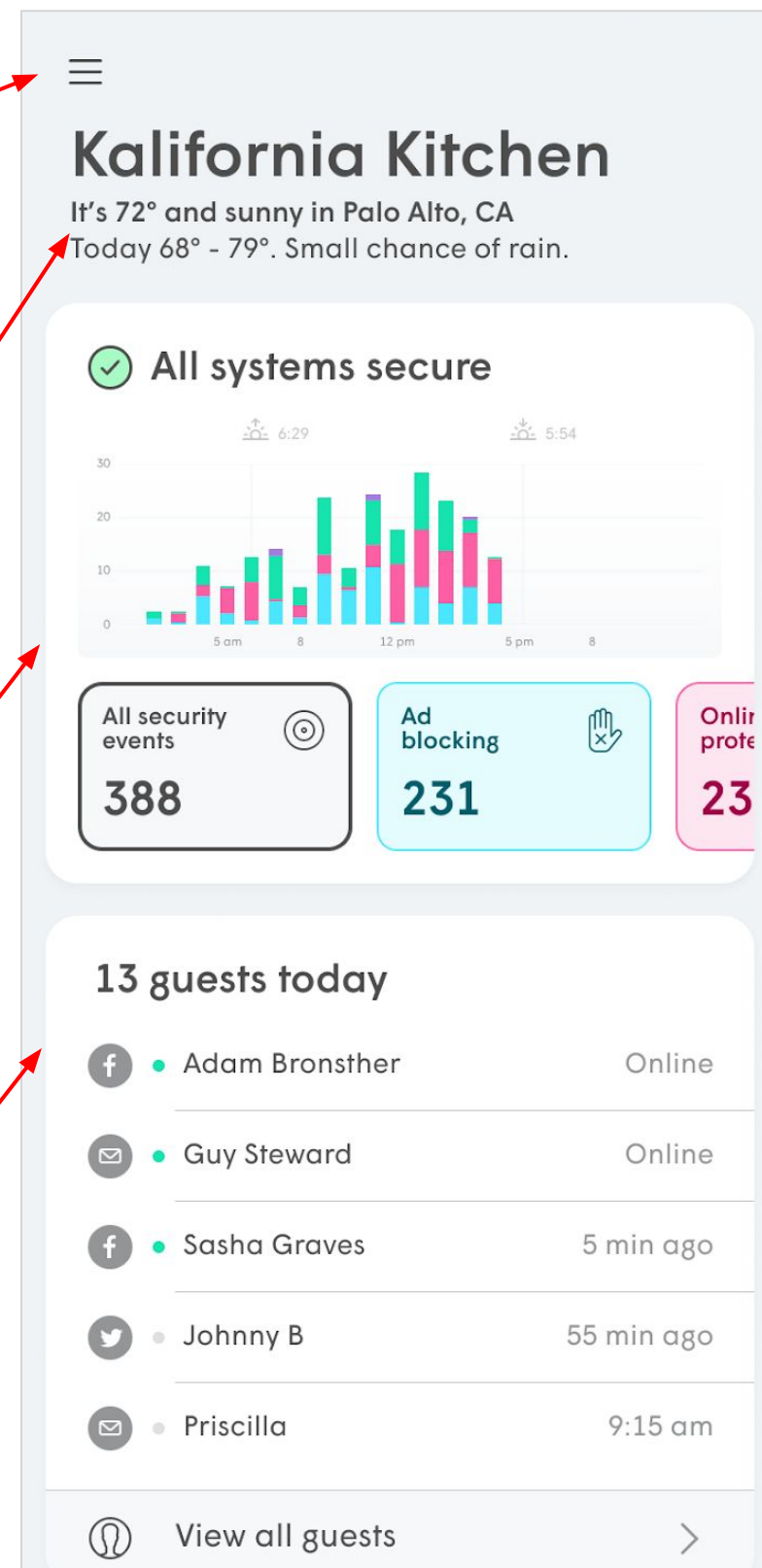
Home Screen

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

Location – Provides location information, including weather.

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

Guests – Display a list of guest that have connected to the network today



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

Network health overview – Shows current status of network (pods online) and recent speed test results

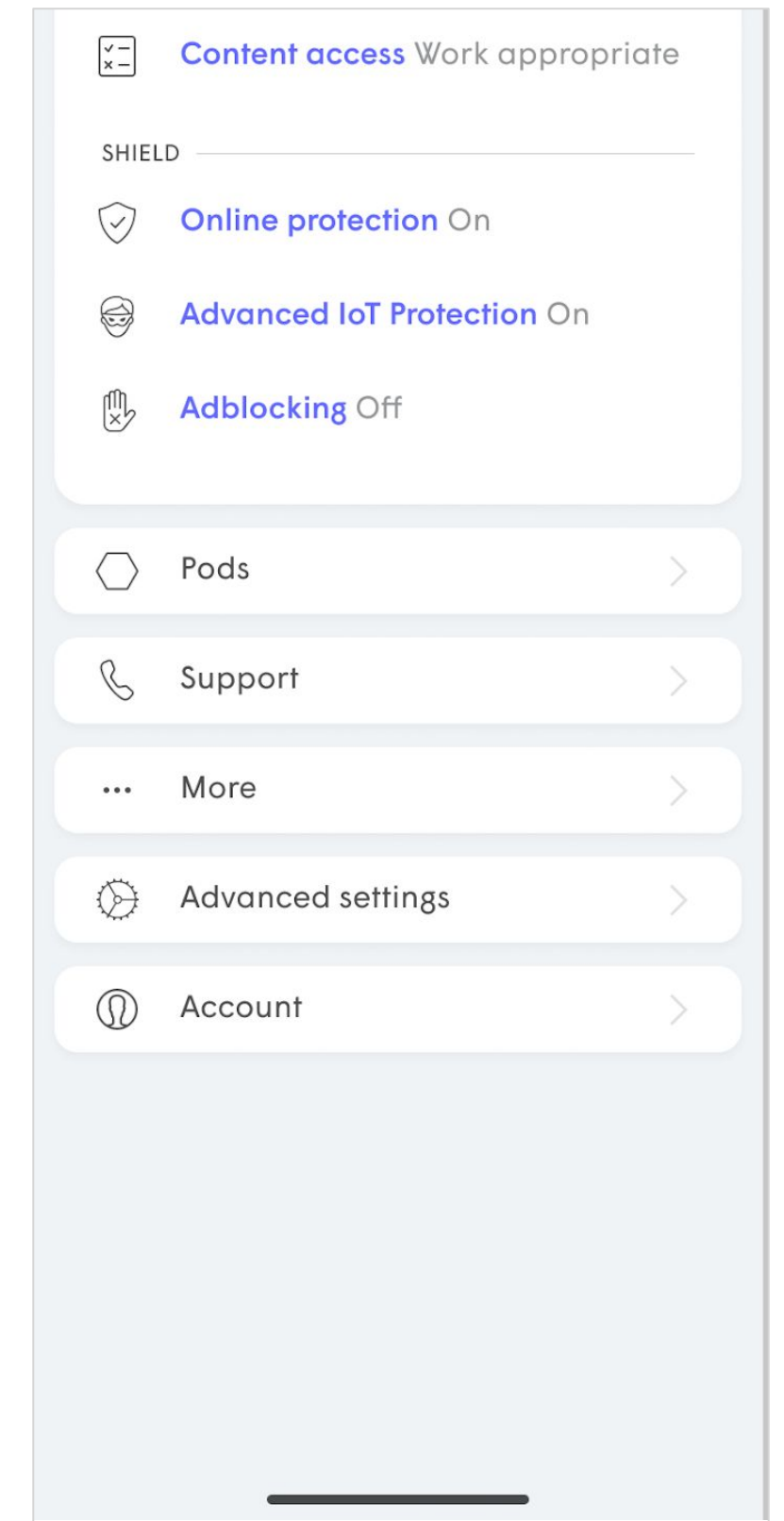
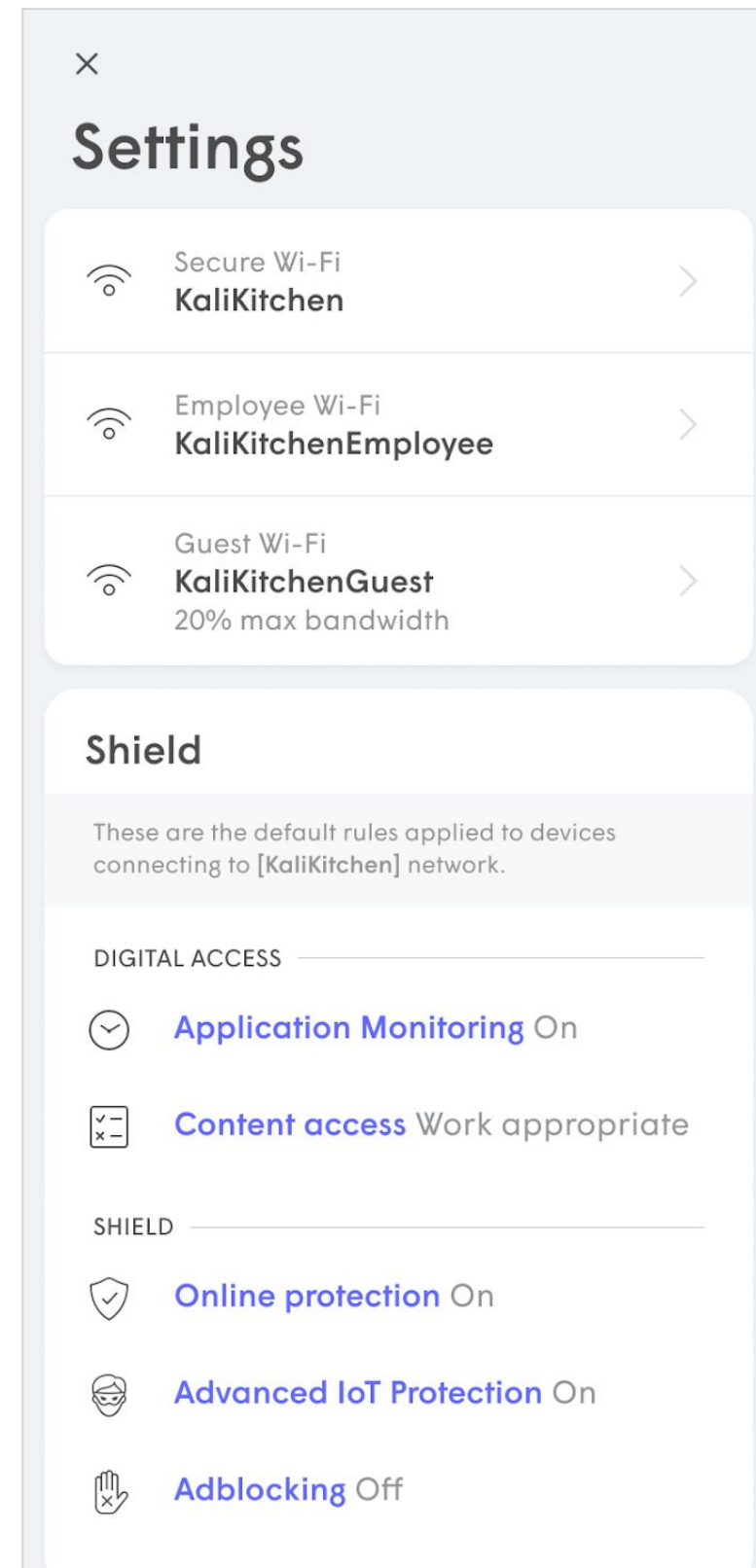
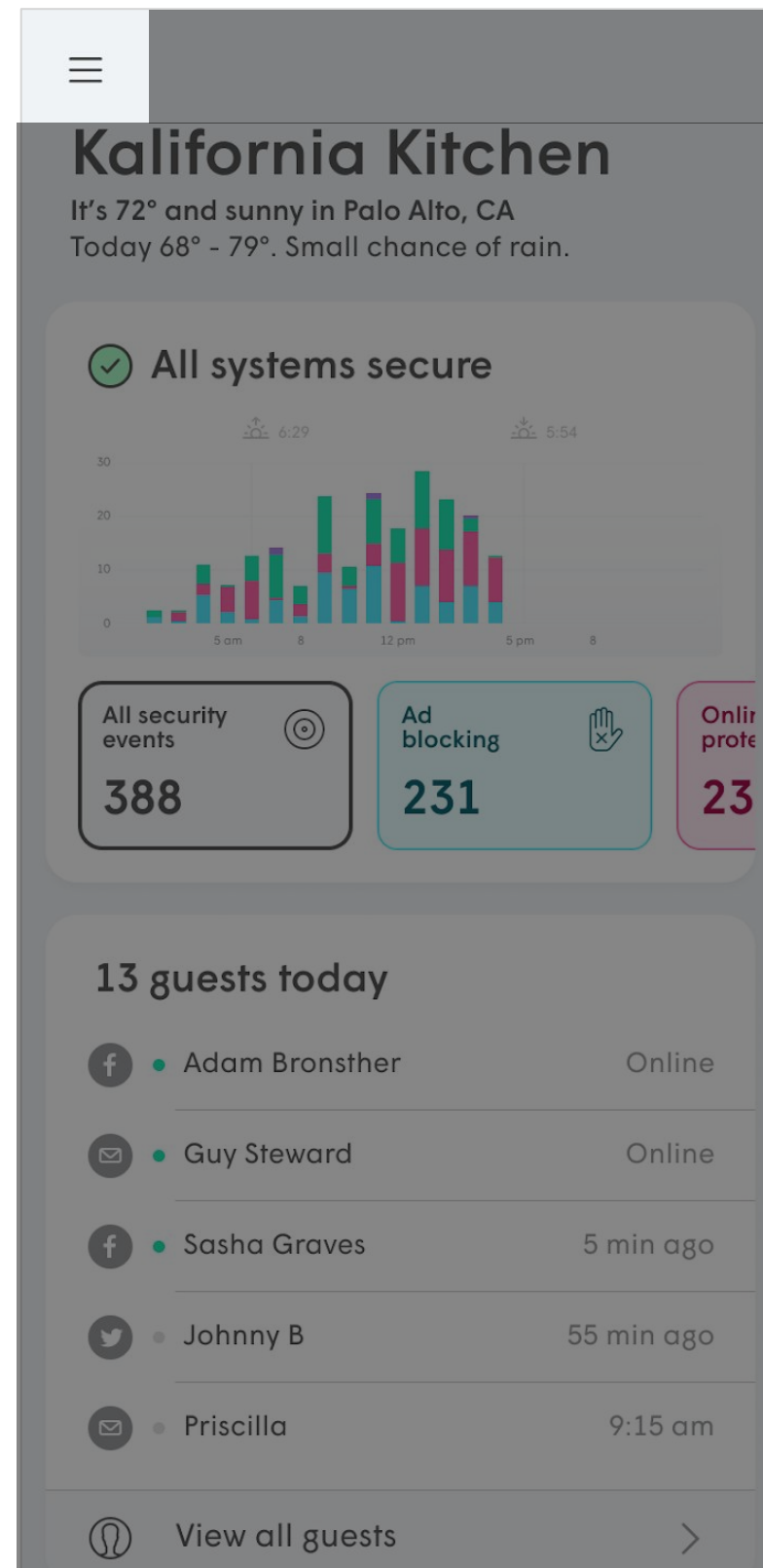
Menu bar - Switches between **Home, Zones, Security** and **Network** tabs

All information presented in the **Home** screen is based on the last 24 hours.

App Navigation

Settings


- **Settings** menu can be accessed from the **Home** tab using ☰
- Settings contains several menus and settings that are network-wide and were mostly configured during the initial onboarding flow.
- Unless changes need to be made, the admin will rarely need to access these controls on a regular basis.

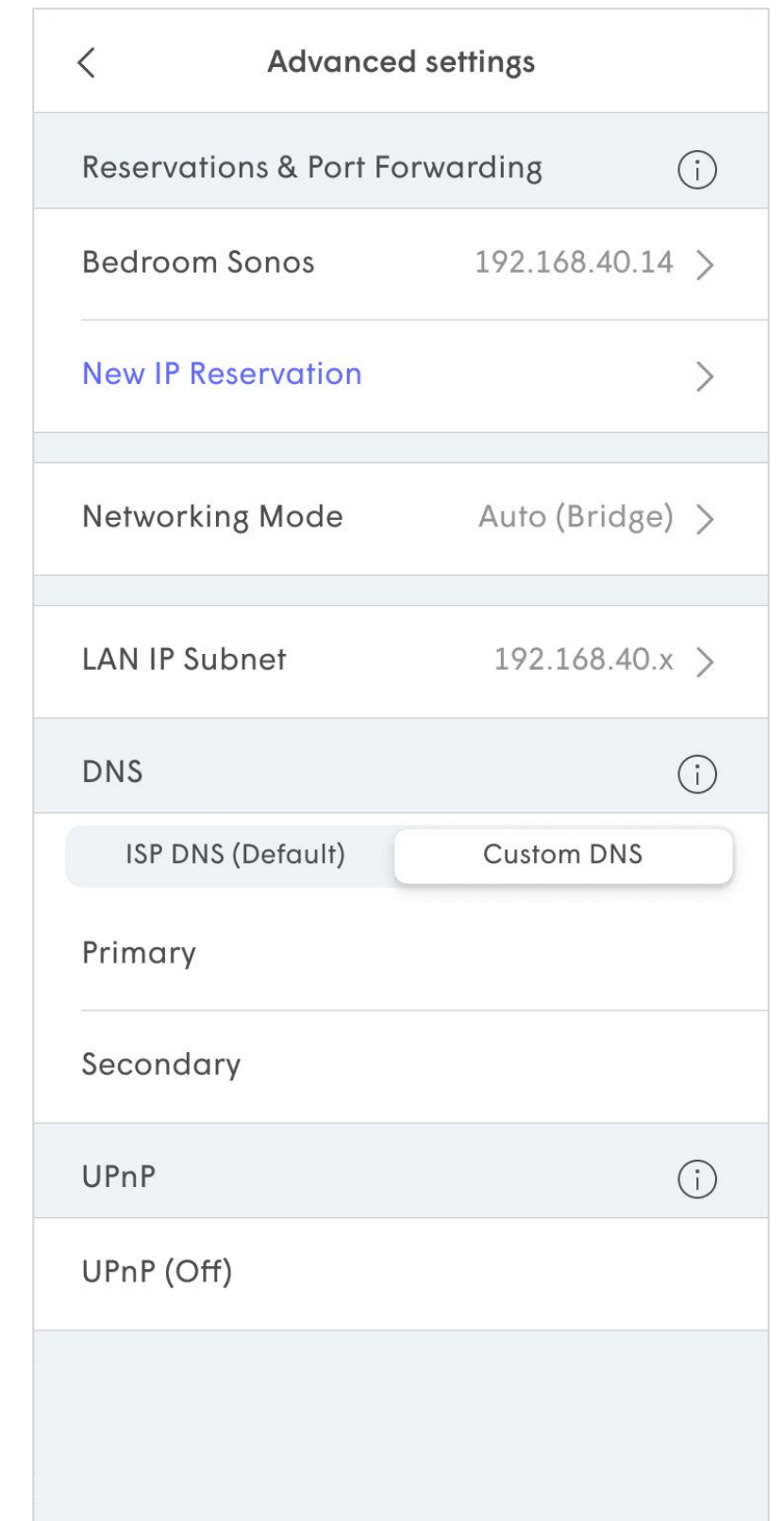
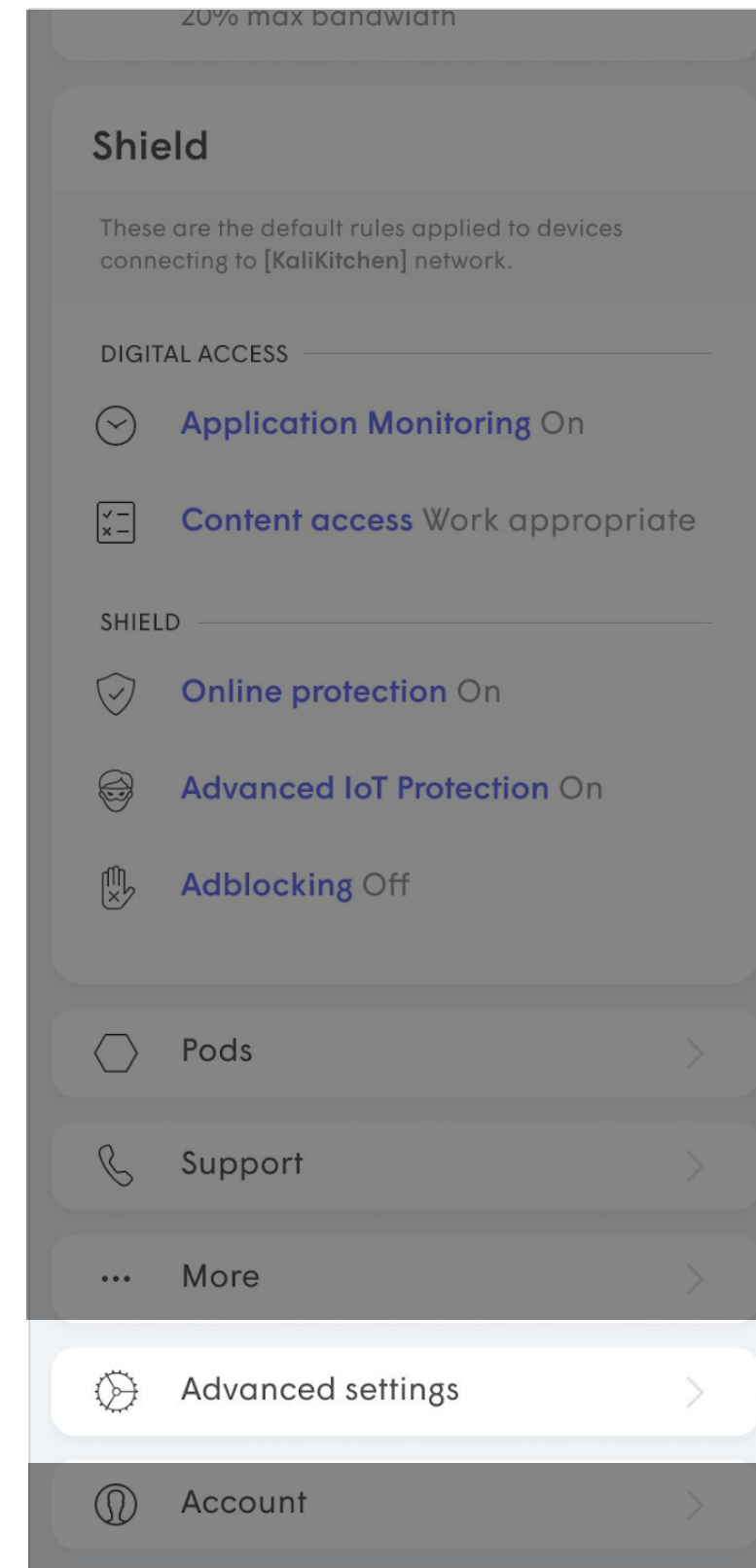
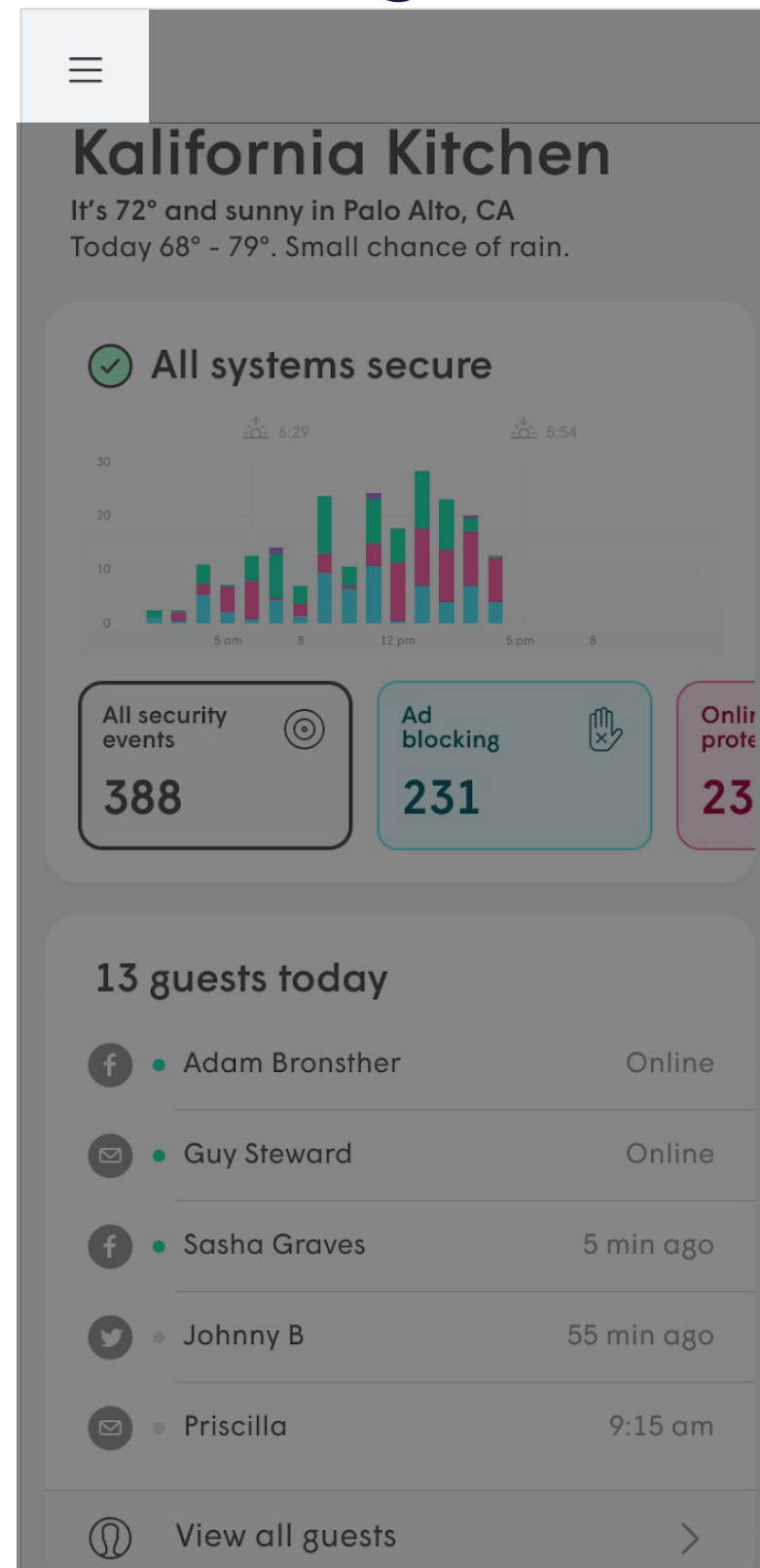


Managing Network Settings

Managing Router Settings

Accessing Router Settings

- Open Settings from the home screen by tapping 
- From the Settings page, Router settings can be found in **Advanced Settings**.

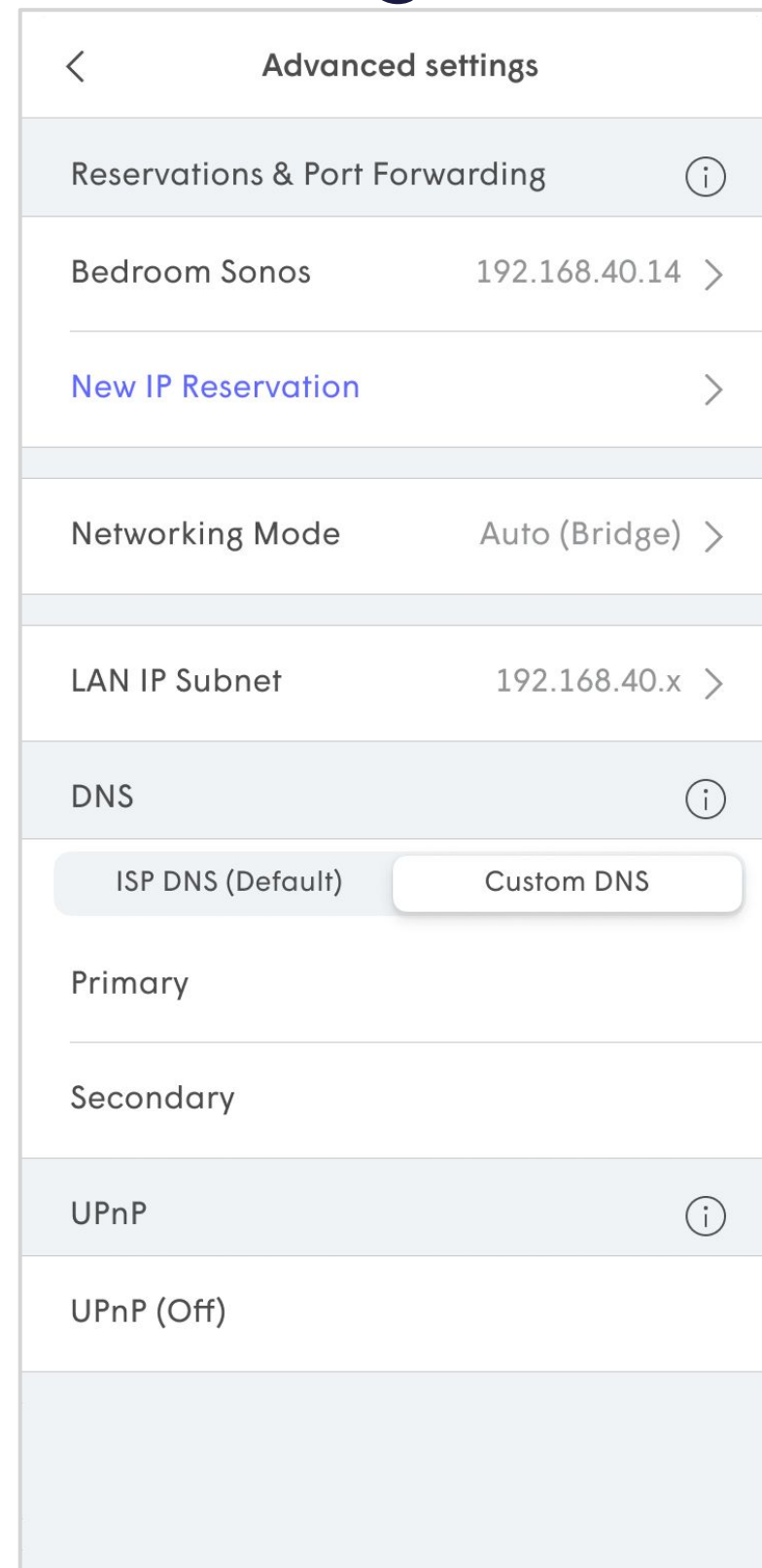


Managing Router Settings

Accessing Router Settings

Router settings will be greyed out unless the network is operating in Router Mode.

If the customer continues to use their existing router, most of these settings will be managed on the router upstream.



Managing Router Settings

Networking Mode

By default Plume pods are shipped with the Network mode set to **Auto**.

When the Gateway pod is plugged in, the IP address assigned to it determines the operating mode:

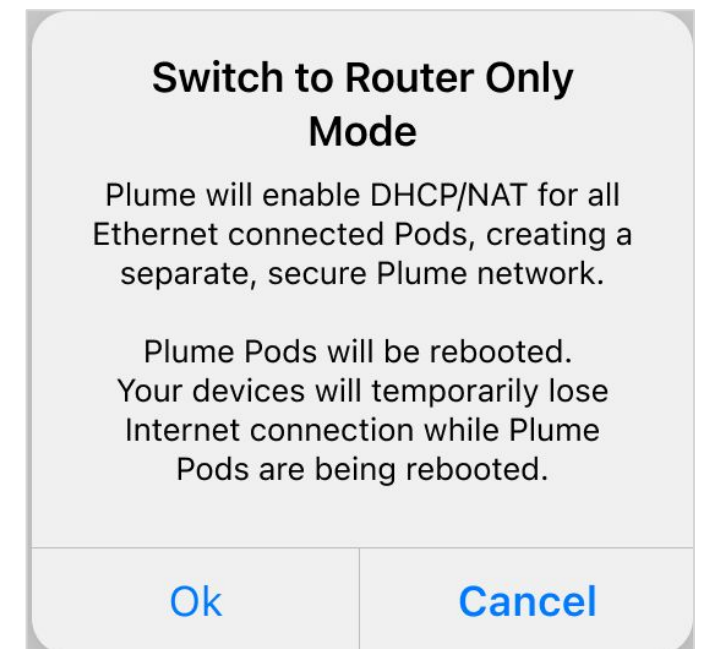
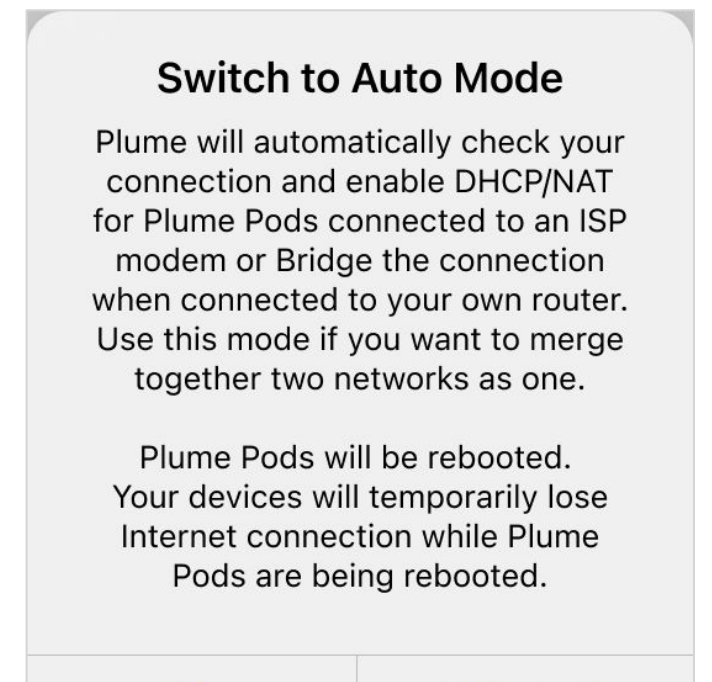
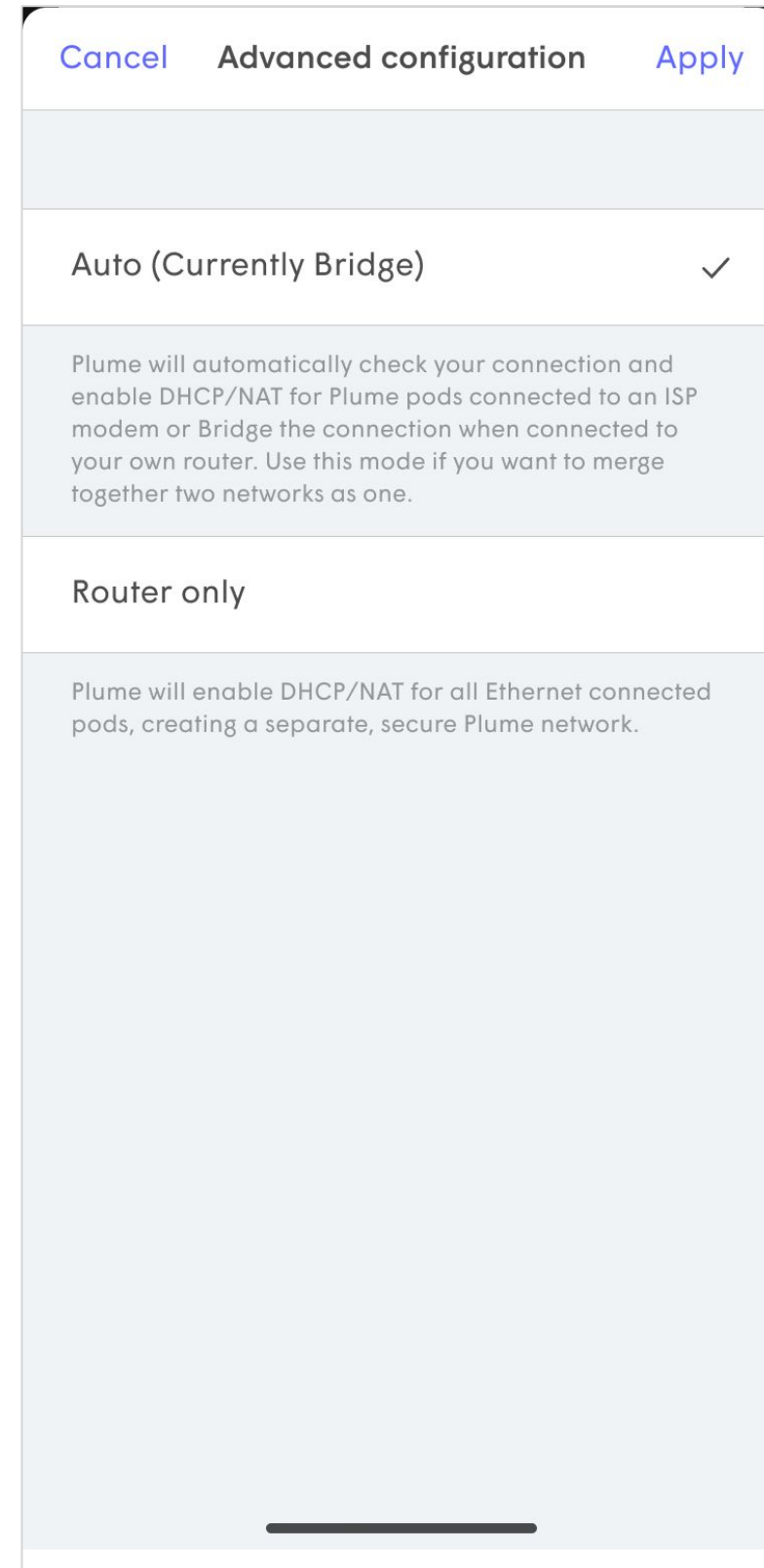
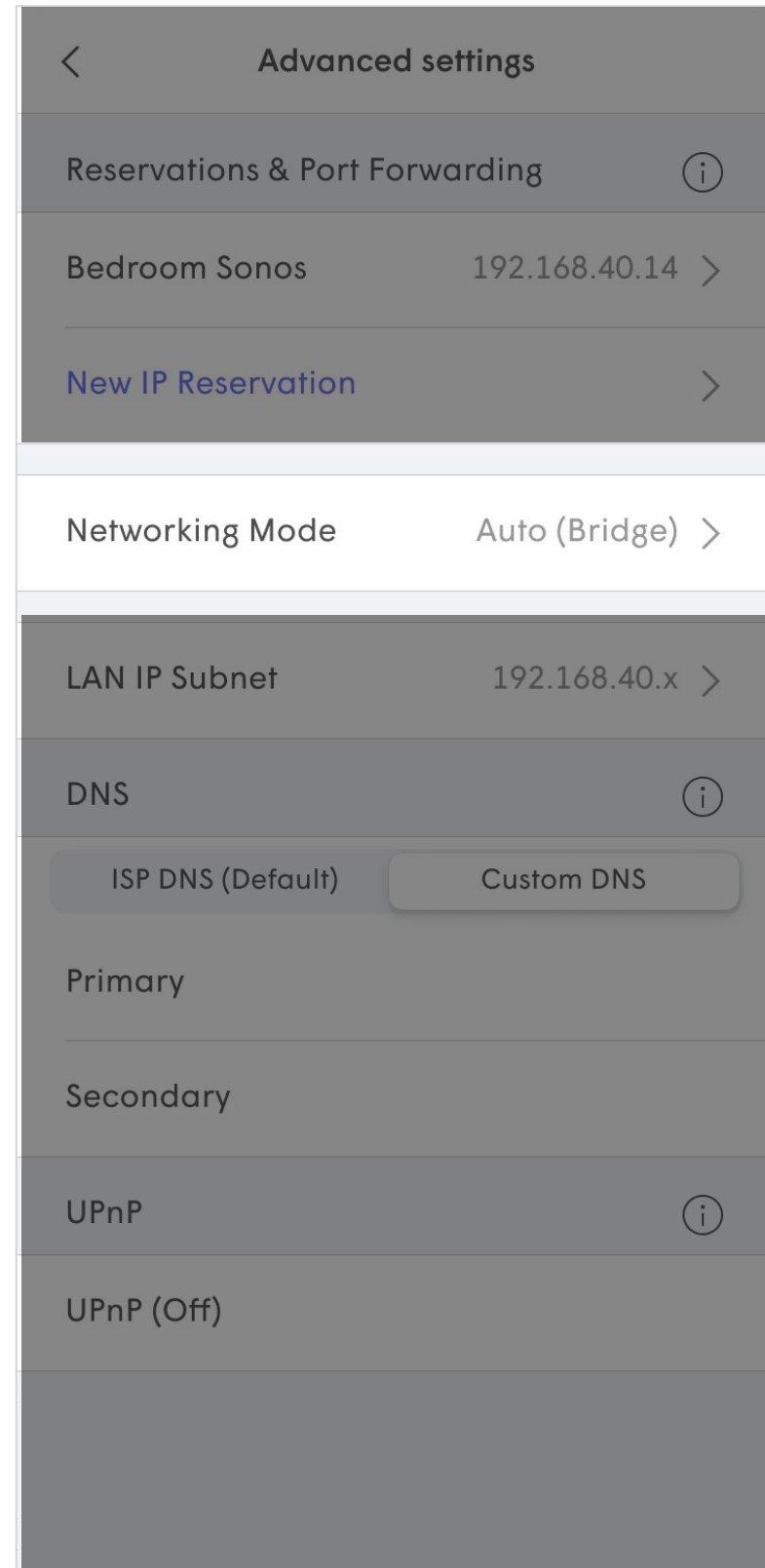
- (Auto) Bridge - private IP assigned
- (Auto) Router - public IP assigned

When operating in Bridge mode, Plume does not handle router functions such as NAT, DHCP and Firewall.

The customer can also force Plume to operate in **Router Only** mode.

This can potentially create a double NAT.

Switching modes always requires a reboot.



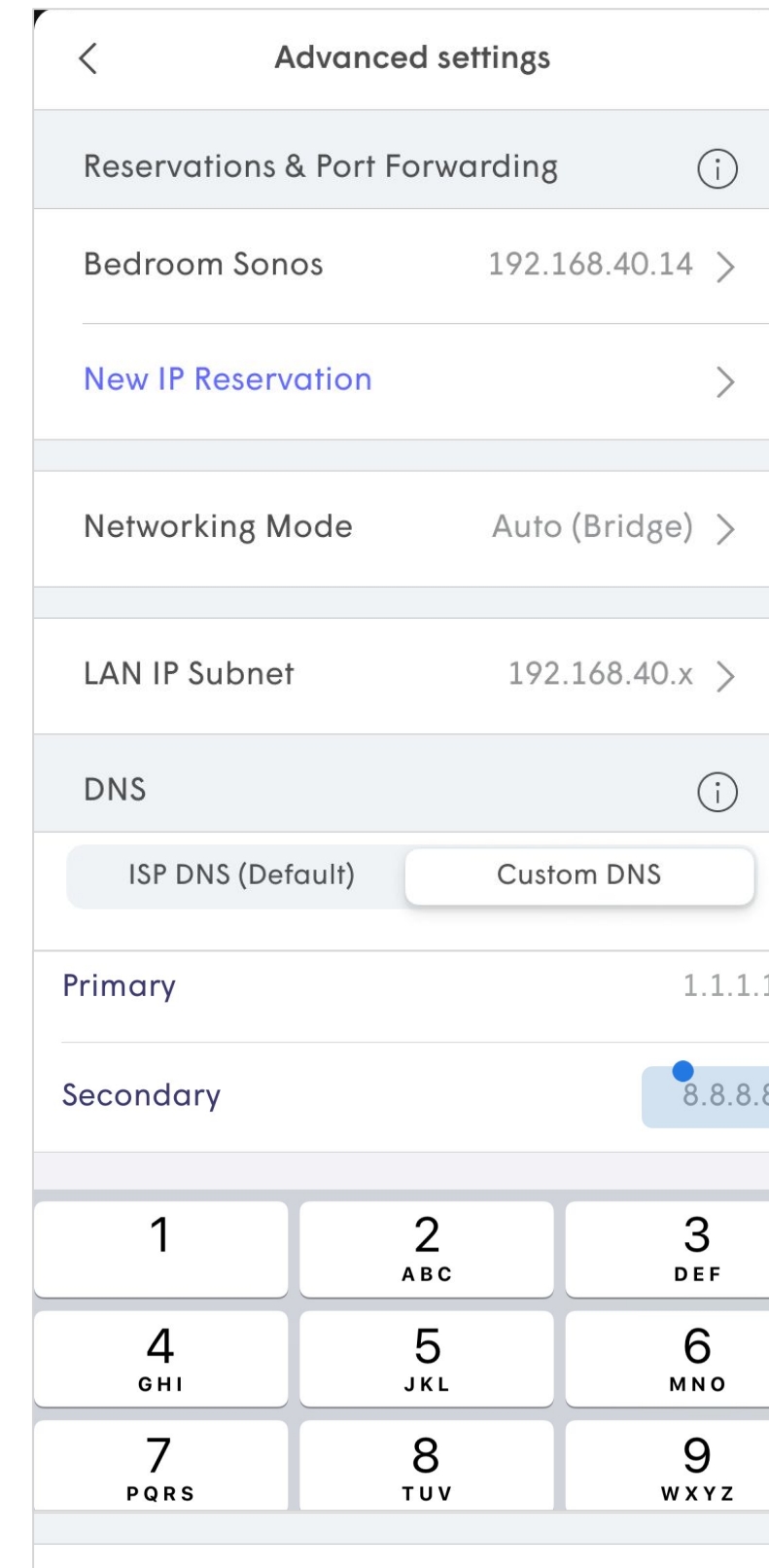
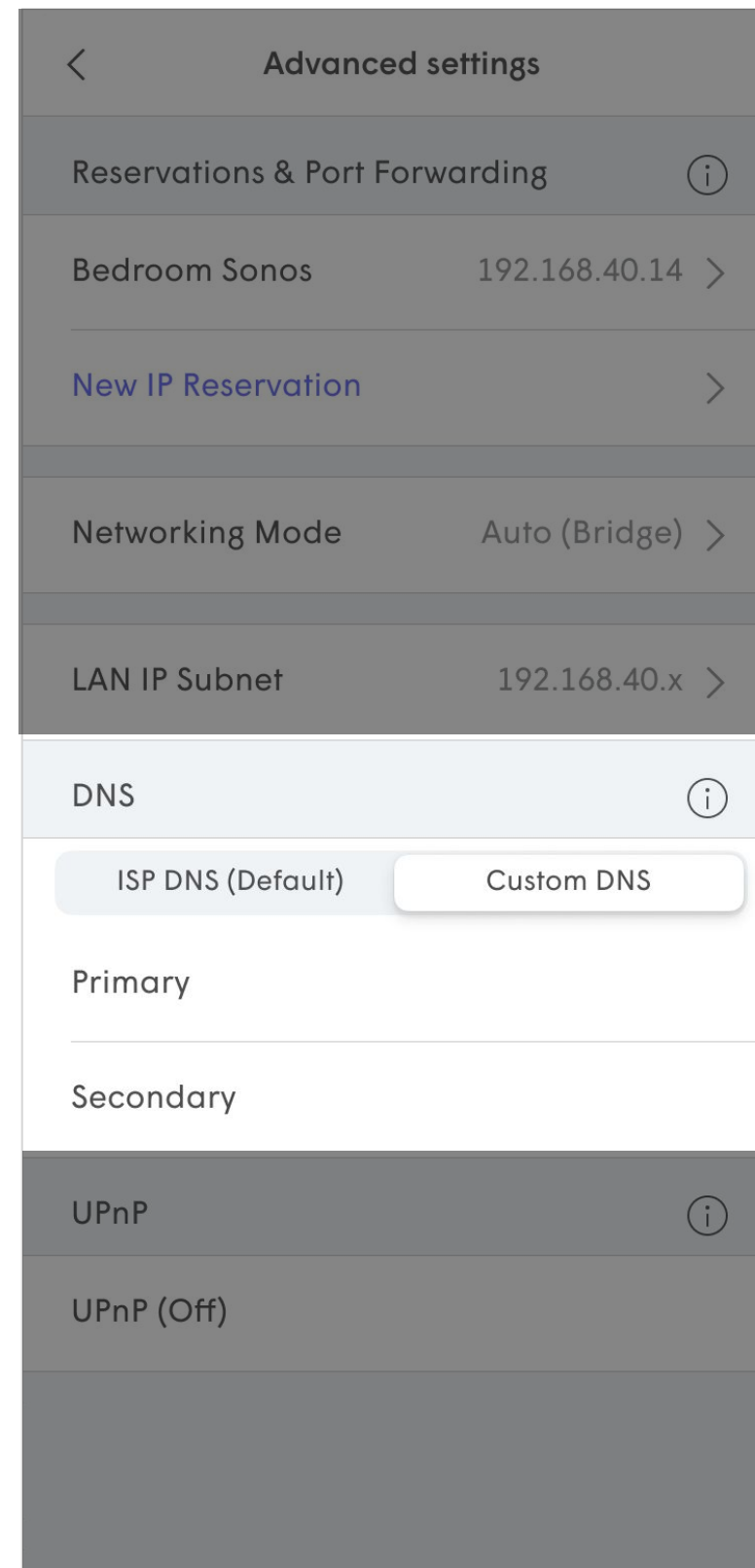
Managing Router Settings

Custom DNS

When Plume is operating in Router mode, you can set a custom DNS through the WorkPass app.

By default the ISP DNS is used, although a custom DNS can be used such as Google, Cloudflare, OpenDNS, etc.

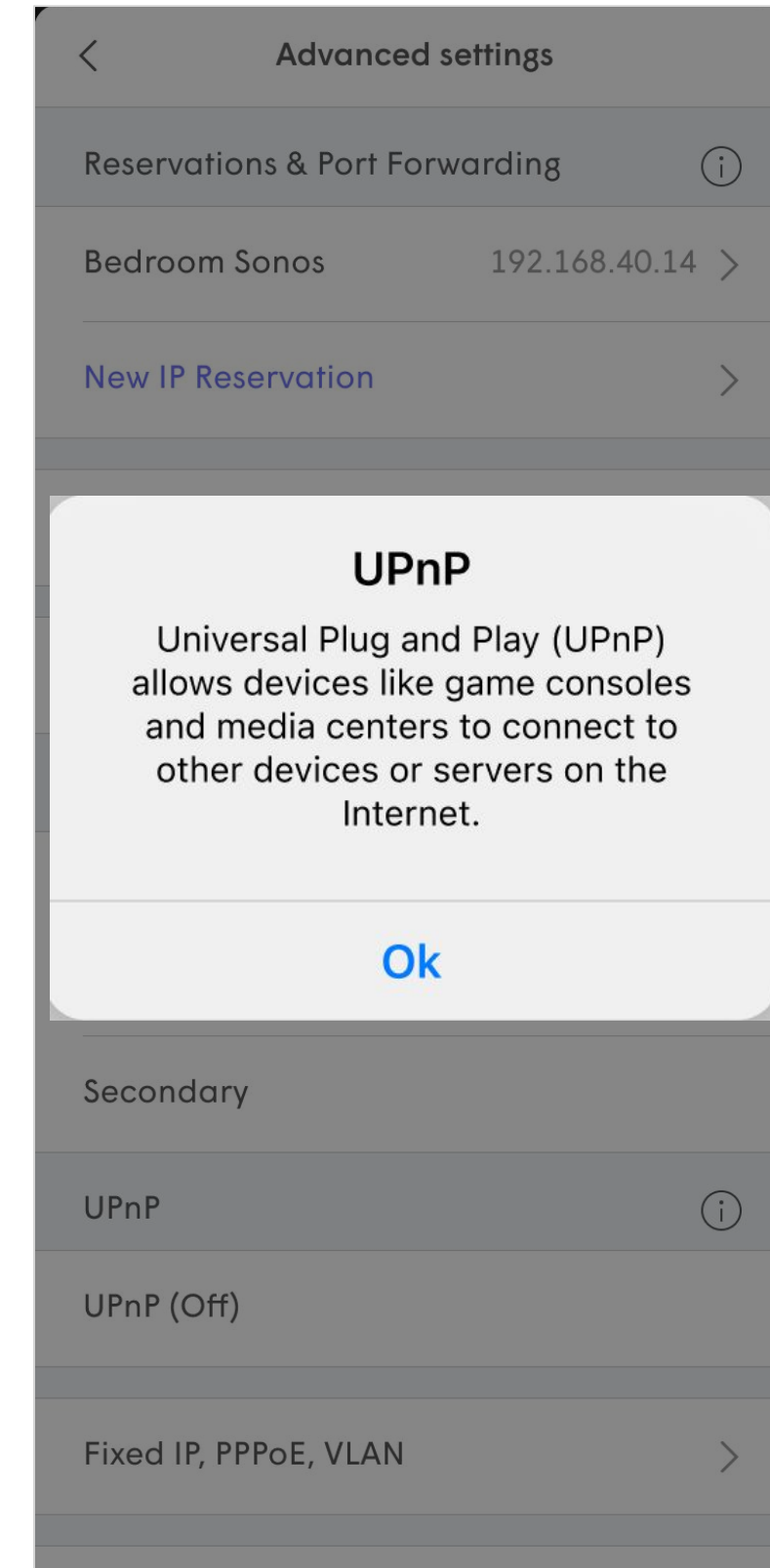
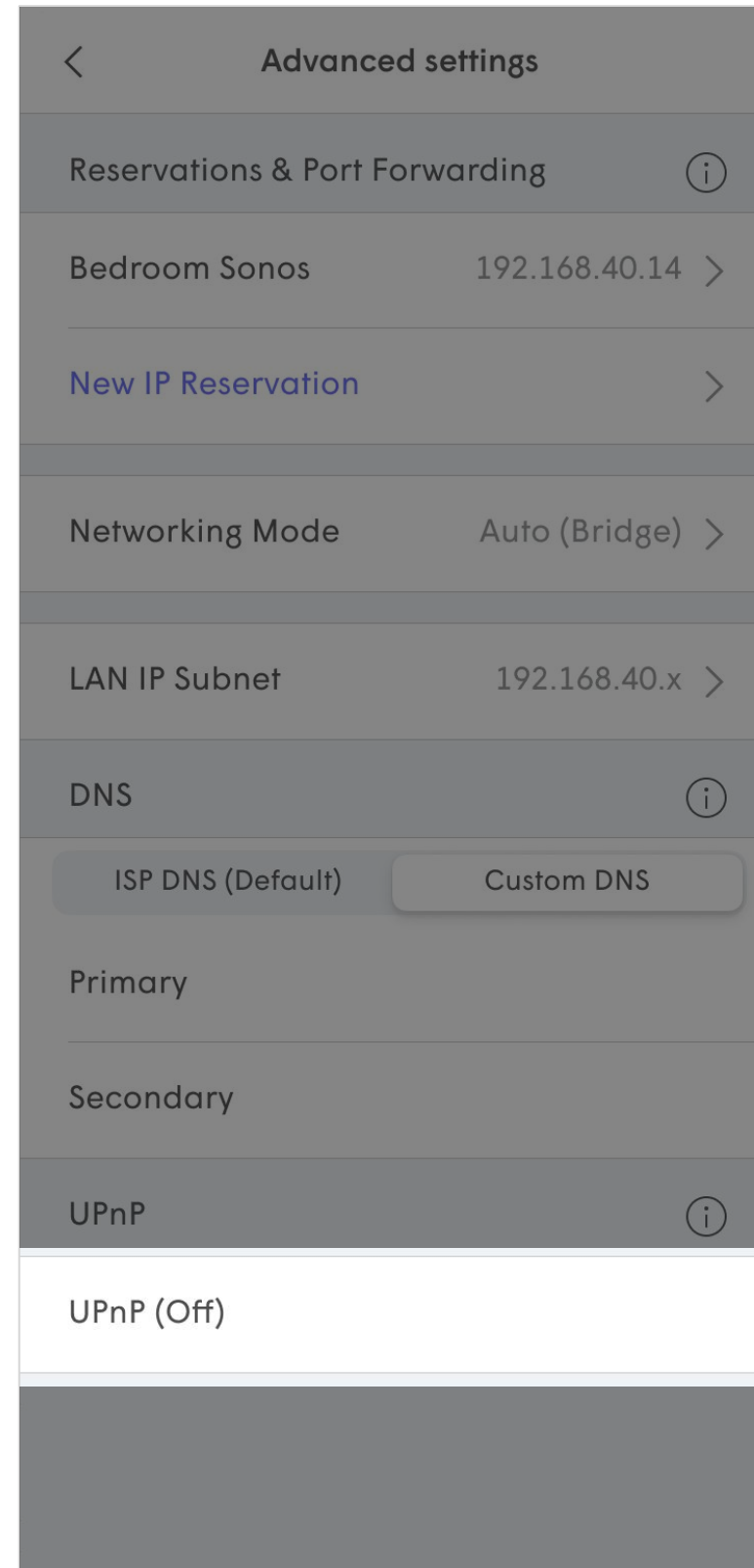
Custom DNS settings will not impact the operation of Plume features like Shield.



Managing Router Settings

UPnP

When Plume is operating in Router mode, Universal Plug and Play (UPnP) can be toggled On or Off.



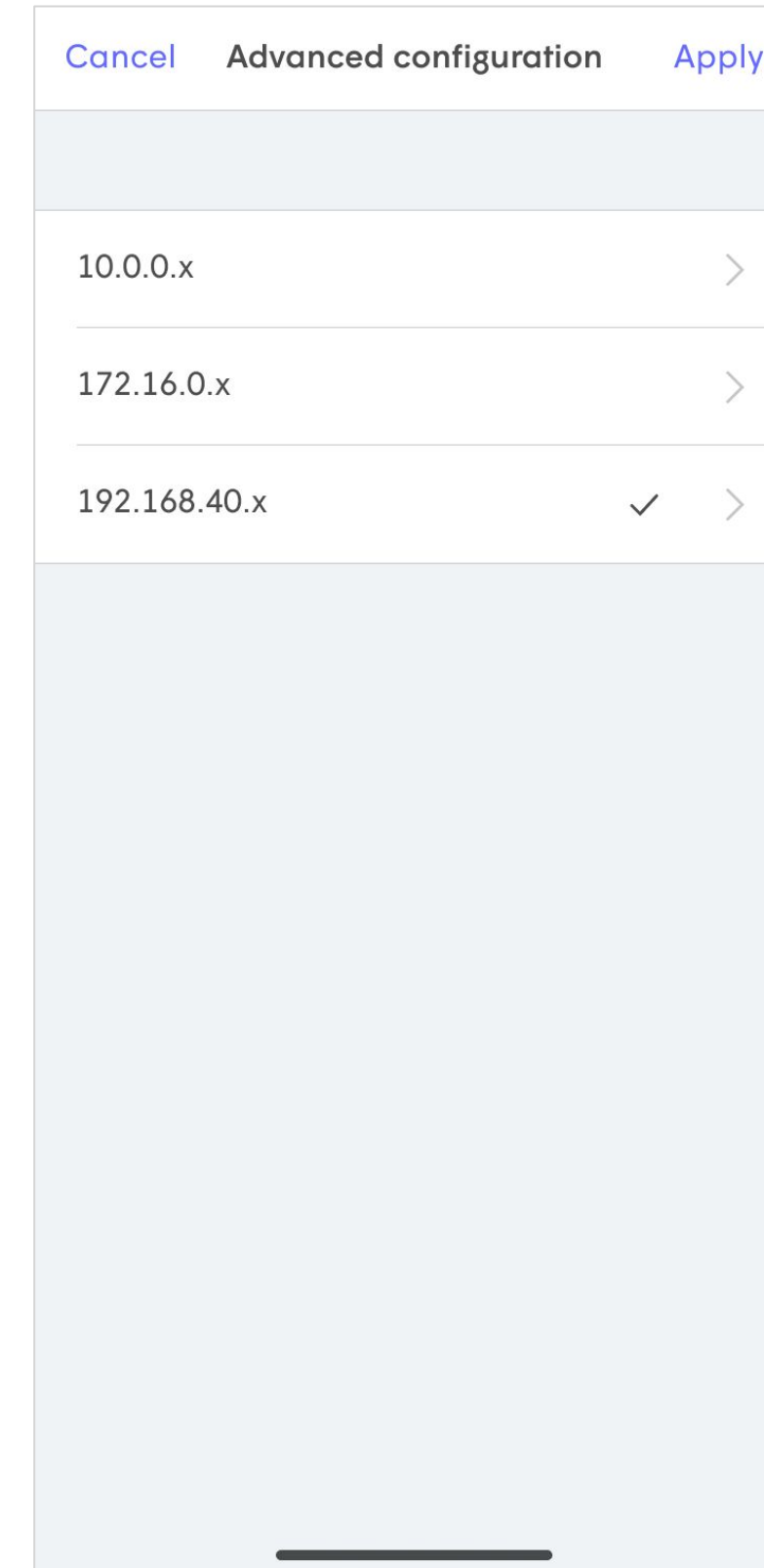
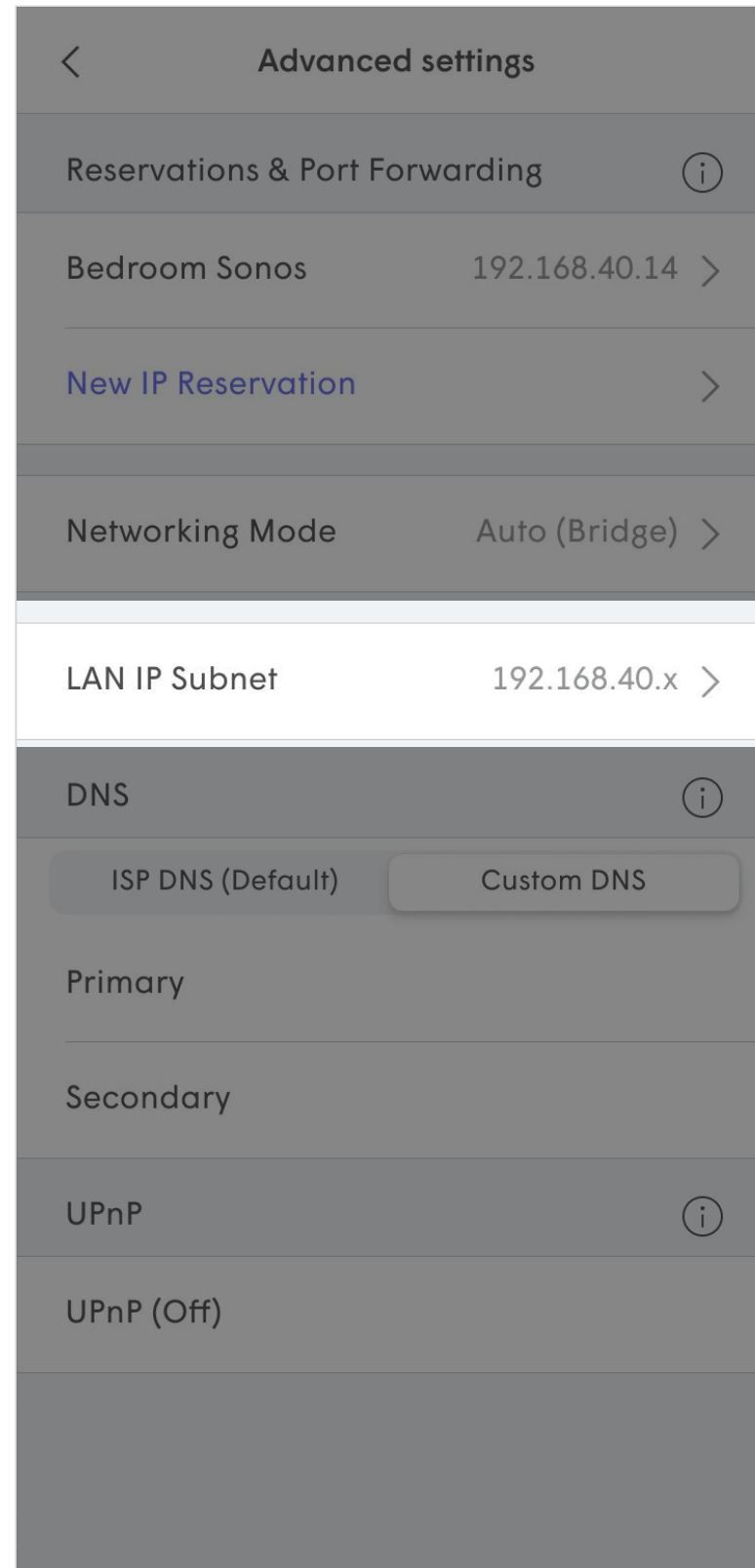
Managing Router Settings

LAN IP Subnet

You can specify what IP subnet is used for your Secure and Employee Plume network.

Tap **LAN IP Subnet** and choose the range you wish to use:

- 10.0.0.x
- 172.16.0.x
- 192.168.1.x



Managing Router Settings

LAN IP Subnet

Enter the specific range you wish to use. All private IP ranges are available to use.

- 10.0.0.x – 10.255.255.x
- 172.16.0.x – 172.31.255.x
- 192.168.0.x – 192.168.255.x

Once you tap **Update**, the network will need to reboot to apply the changes.

After the reboot IP reservations will automatically match the new range.

Cancel Advanced configuration Apply

192 . 168 . 40 . x

Pick a number between 0 - 255.

Cancel Advanced configuration Apply

192 . 168 . 40 . x

Pick a number between 0 - 255.

Update LAN IP Subnet
DHCP reservations will automatically change to match the new address.

Your Wi-Fi system will be rebooted.
Your devices will temporarily lose Internet connection until the system is back online.

Update Cancel

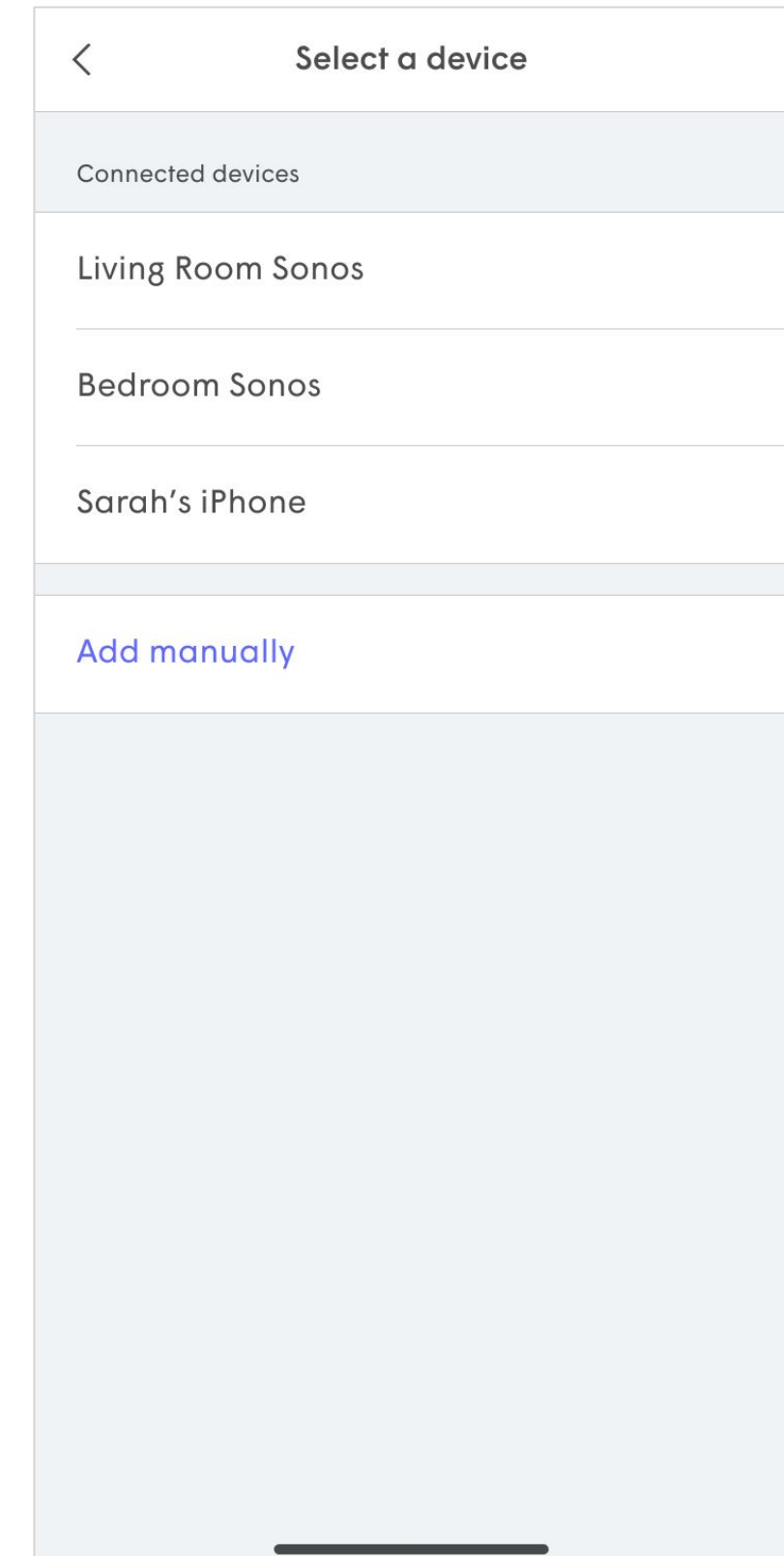
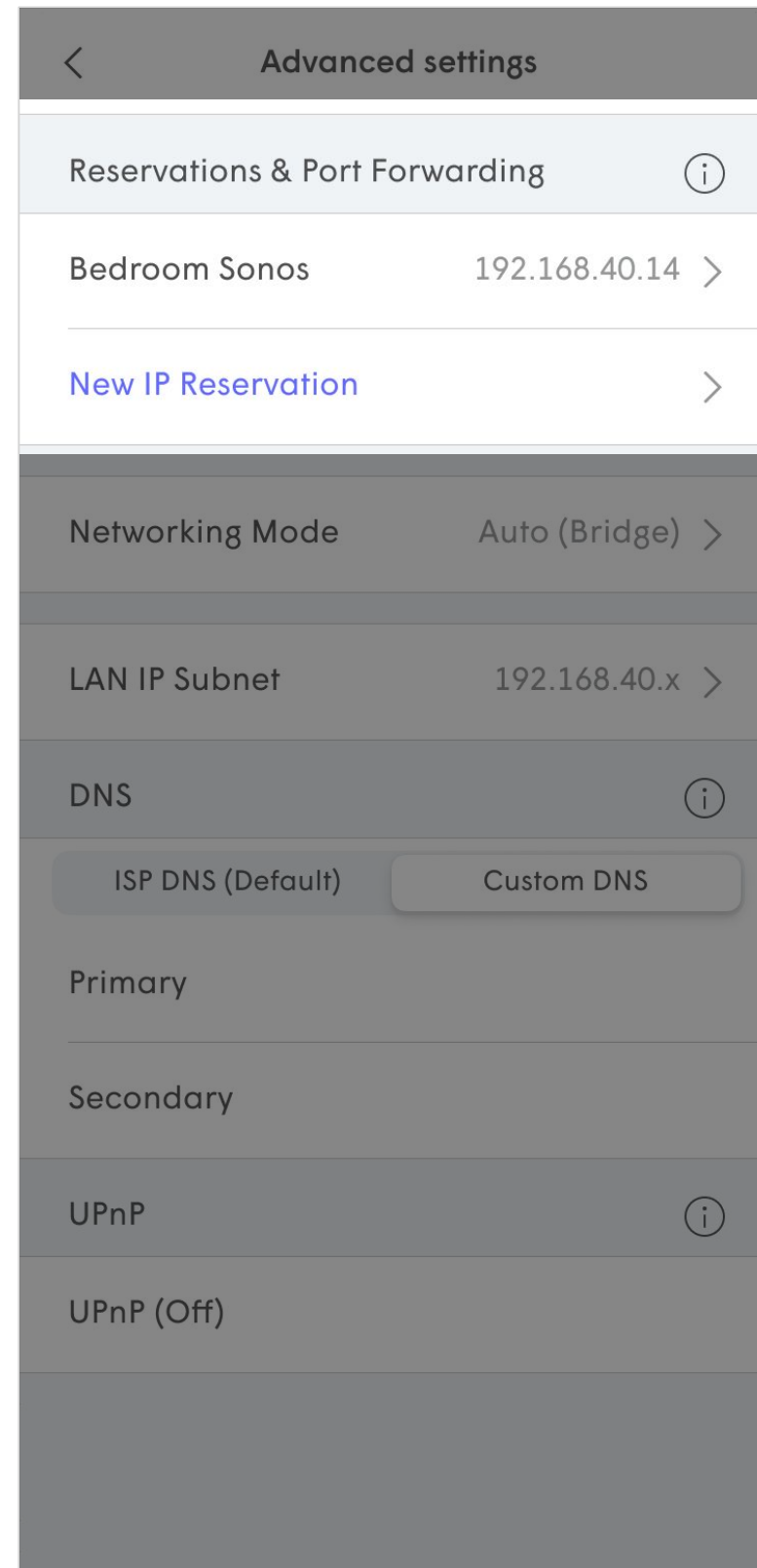
Managing Router Settings

IP Reservations

When Plume is operating in Router mode, IP addresses can be reserved. Once a device has an IP reservation, port forwarding rules can then be applied to it.

Tap **New IP Reservation** and choose the device from the list you want to apply the IP reservation to.

You can use the **Add Manually** option to set an IP reservation to a device that has not connected to the network yet.



Managing Router Settings

IP Reservations

Once a device is chosen from the list, type in the IP address you wish to reserve.

In the case of Manually reserving an IP, you have to type in a nickname, the IP address and the device's MAC address.

Tap on **Done** and the reservation will be saved or you can continue to **Open a Port** for that device.

Cancel Advanced configuration Apply

Nickname

IP address 192.168.40.xxx

MAC address

Port Assignments

Open a Port

Cancel Advanced configuration Apply

Nickname Bedroom Sonos

IP address 192.168.40.14

MAC address 00:0E:58:54:81:D4

Port Assignments

Port name Speaker >

Open a Port

Delete Reservation

Managing Router Settings

Port Forwarding

Once a device has an IP reservation you can continue to **Open a Port** for that device.

Enter the **Port Name** for the port forwarding rules you are setting up.

Type in the **External port**, **Internal port** and the protocol.

Tap **Save** and then continue to Open other ports under this reservation.

Cancel Advanced configuration Apply

Nickname	Bedroom Sonos
IP address	192.168.40.14
MAC address	00:0E:58:54:81:D4

Port Assignments

Port name	Speaker >
-----------	-----------

Open a Port

Delete Reservation

Cancel Advanced configuration Apply

Port name	Speaker
External port	8080
Internal port	8080

Protocol

TCP & UDP TCP UDP

Delete Port Assignment

Managing Wi-Fi Access

Managing Wi-Fi Passwords

The Wi-Fi password management features of WorkPass allows businesses to set up 3 different SSIDs and passwords for the network. This means that 3 separate credentials and access levels are used for the network.

There are three separate access zones:


- **Secure** - Wi-Fi access for devices that must be segregated from the rest of the network. This zone should be used for Point of Sale (POS) systems, security cameras and other business infrastructure that requires controlled access. Devices in this zone can be further segmented into groups. Ethernet connected devices will be added to the zone.
- **Employees (Limited Access)** --Create a custom password to be shared with employees, including the admin. Access to local (Secure) devices can be controlled, while still allowing for internet access.
- **Guest** - Devices in this zone will only have access to the internet with no access to local devices on the network. A password is not created and access is handled through a captive portal, requiring the registration of users of this zone. Bandwidth can also be limited for users in this zone, to ensure adequate bandwidth remains for business infrastructure and employees.



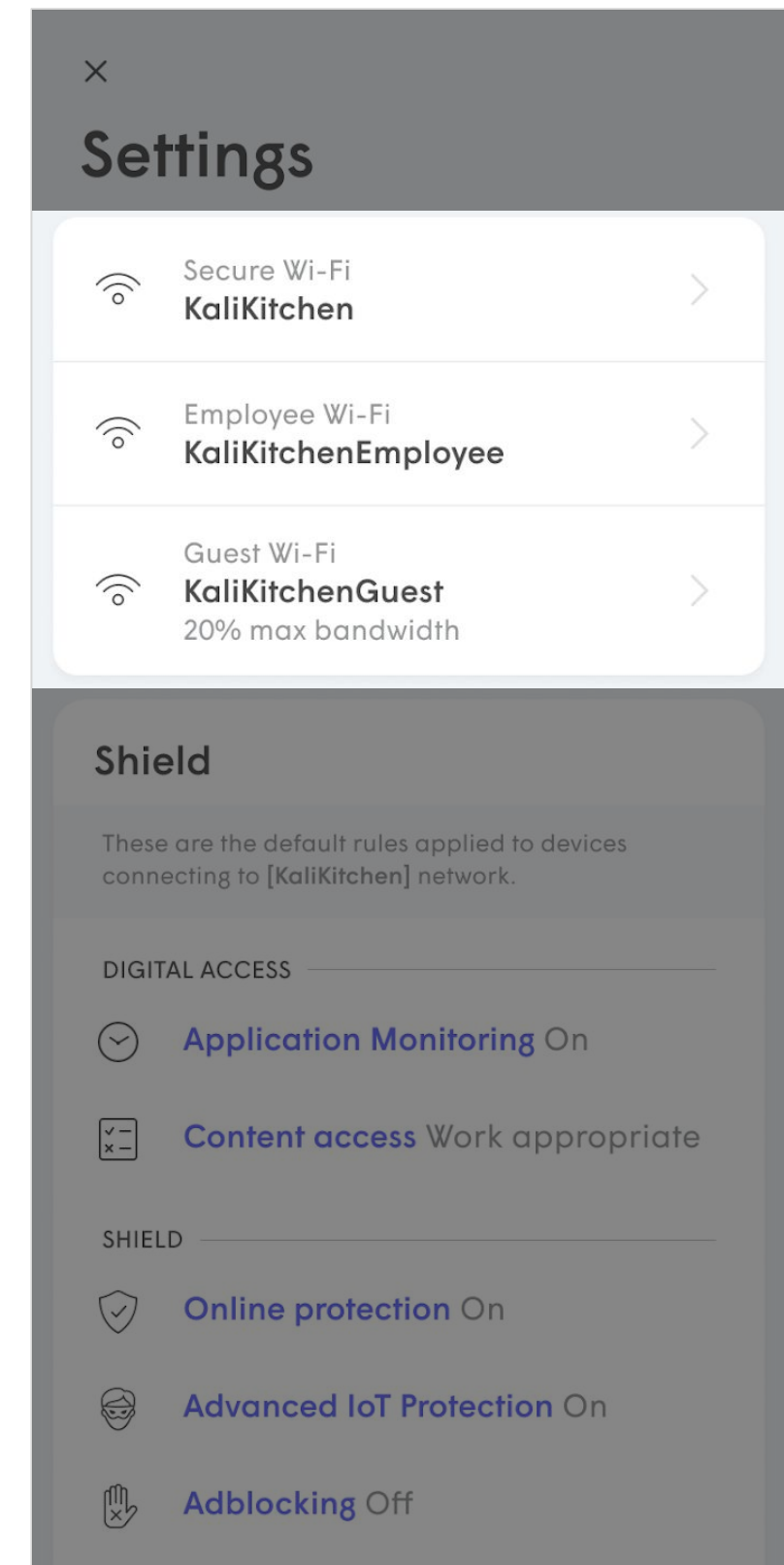
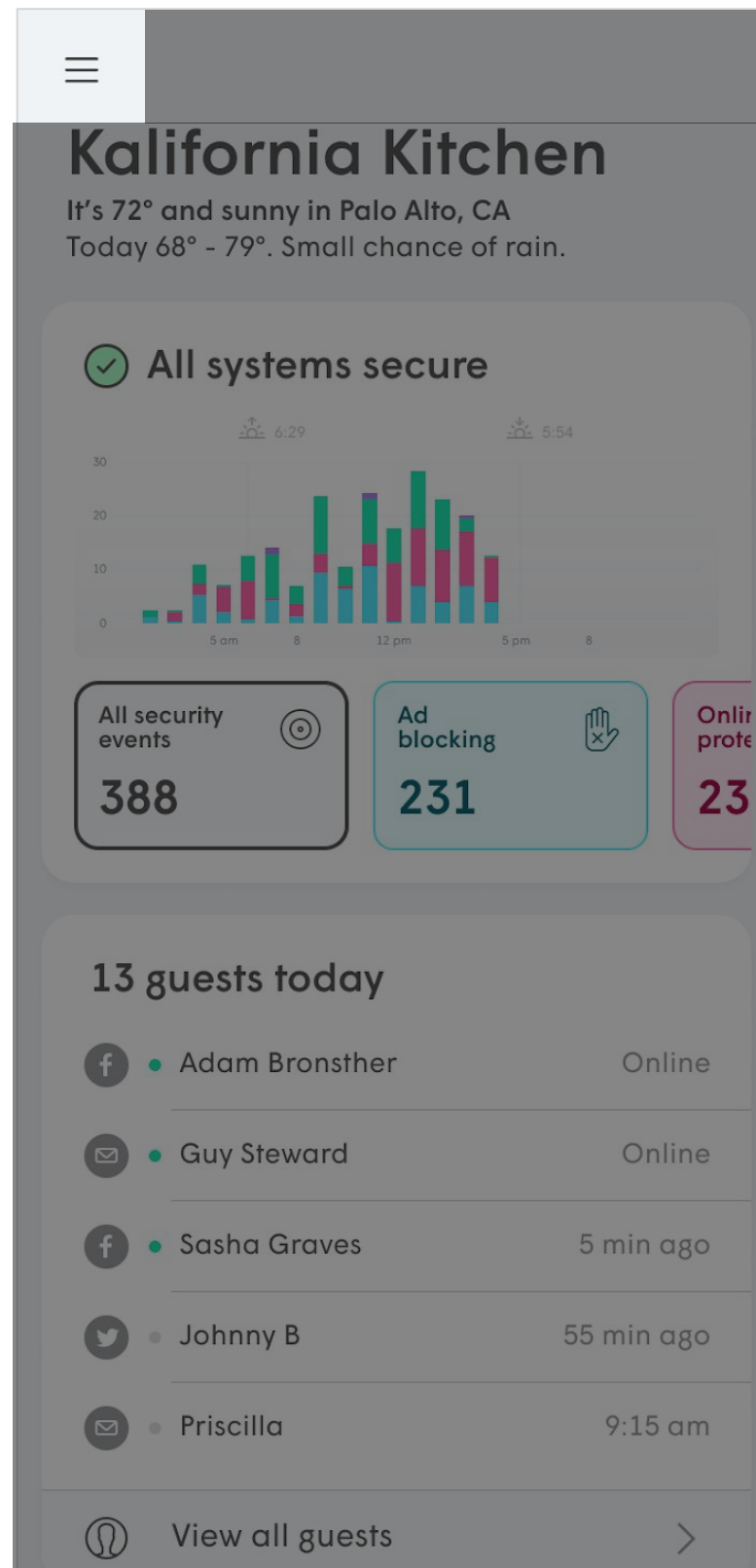
Optionally, devices attempting to connect to both the Secure and Employees zones can require manual approval to be granted by the admin to ensure only trusted devices connect to these zones. Using the WorkPass app connection to the Plume Cloud allows network access to be managed from anywhere with an internet connection.

Managing Wi-Fi Access

Managing Wi-Fi Passwords

From the home screen tap  to access **Settings**.

The SSIDs for each access zone created during initial setup are at the top of the Settings page. Tap on an SSID to modify that zone's settings.



Managing Wi-Fi Access

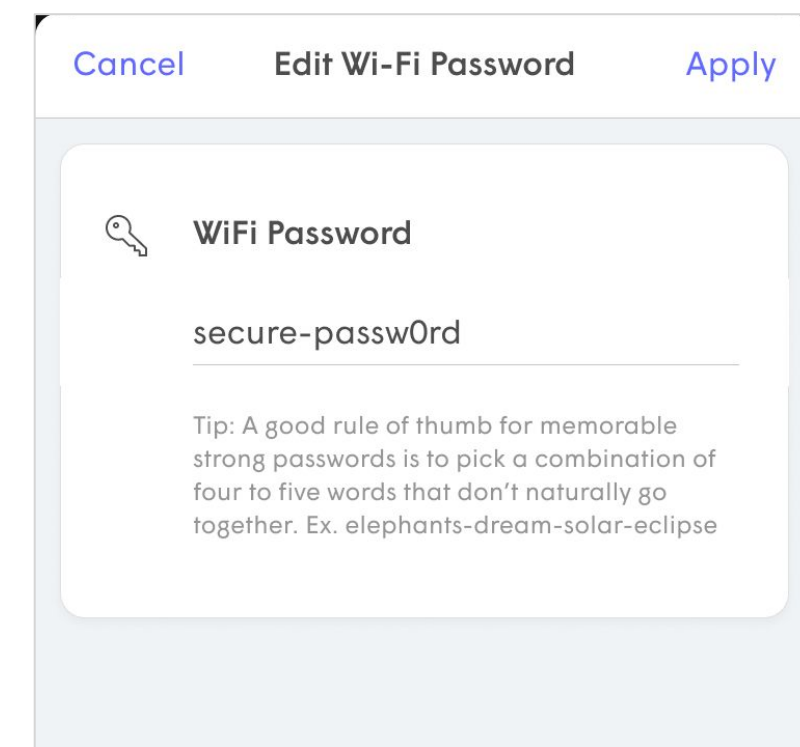
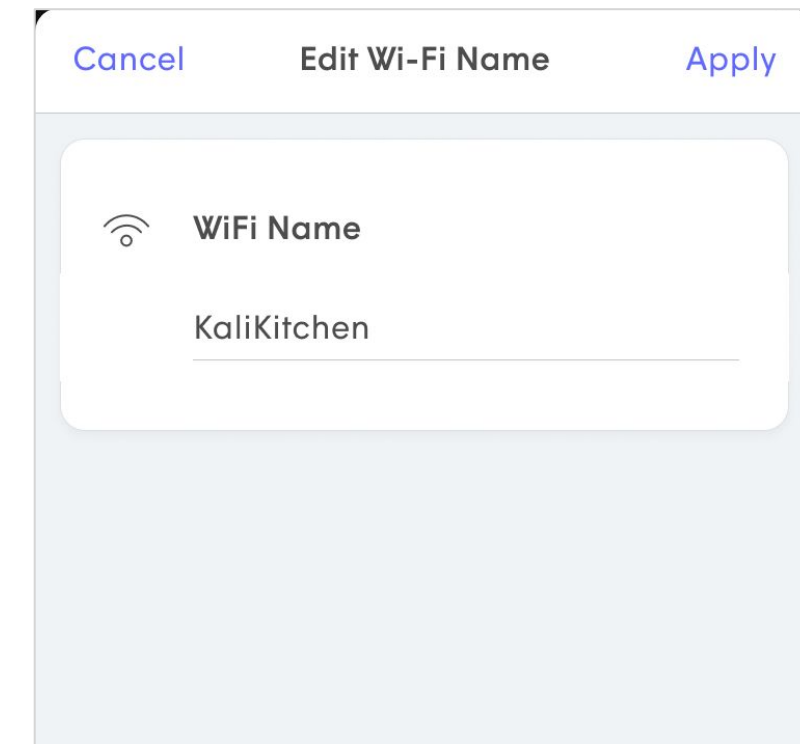
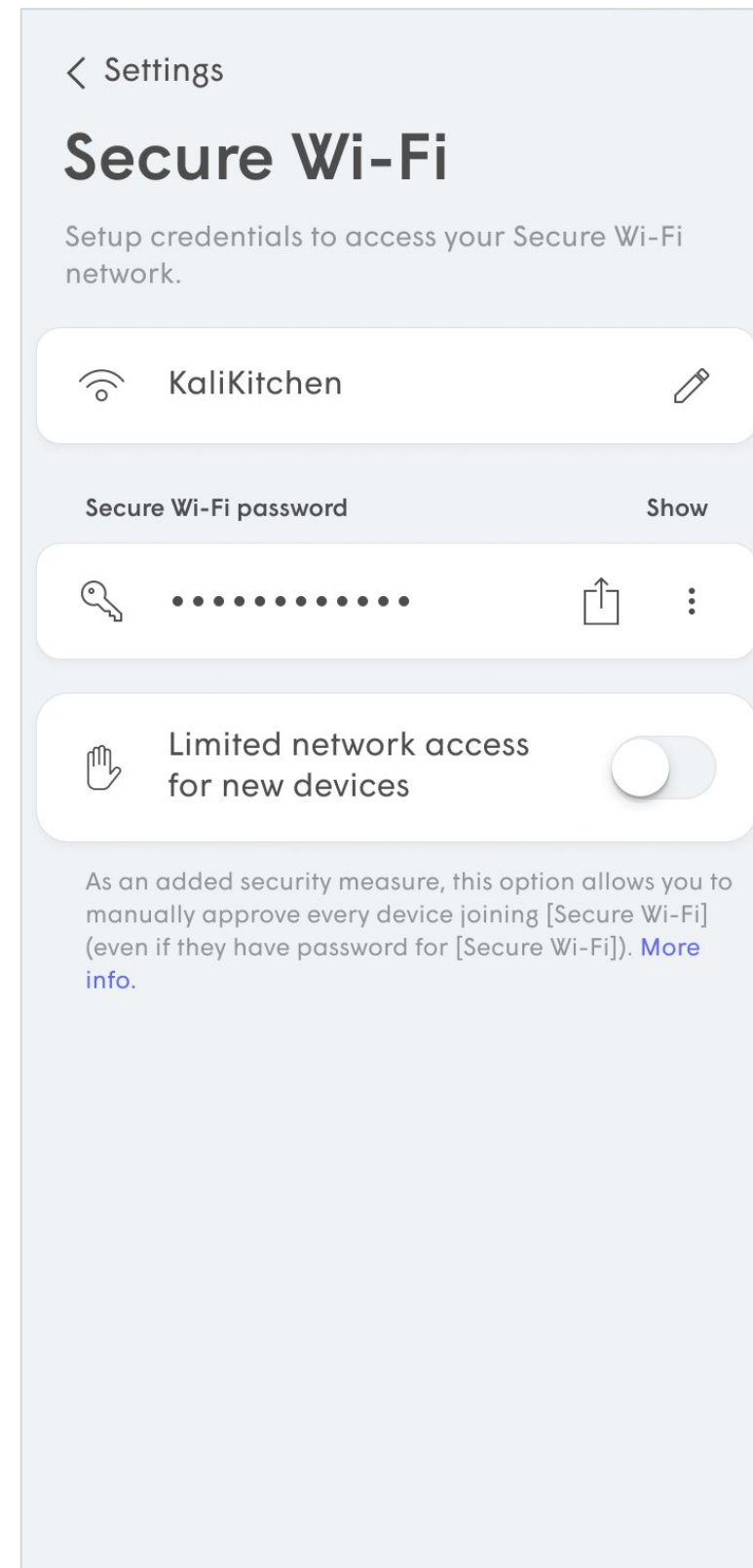
Secure Wi-Fi

The Secure Wi-Fi zone is used for devices that must be segregated from the rest of the network. This zone should be used for Point of Sale (POS) systems, security cameras and other business infrastructure that requires controlled access.

All Ethernet connected devices are added to this zone.

Tap on the pencil next to the SSID to change it, although any currently connected devices will disconnect until their settings are updated.

The Password can be revealed using the show button. Tapping on the options on the right of the password will allow you to edit or copy the password.



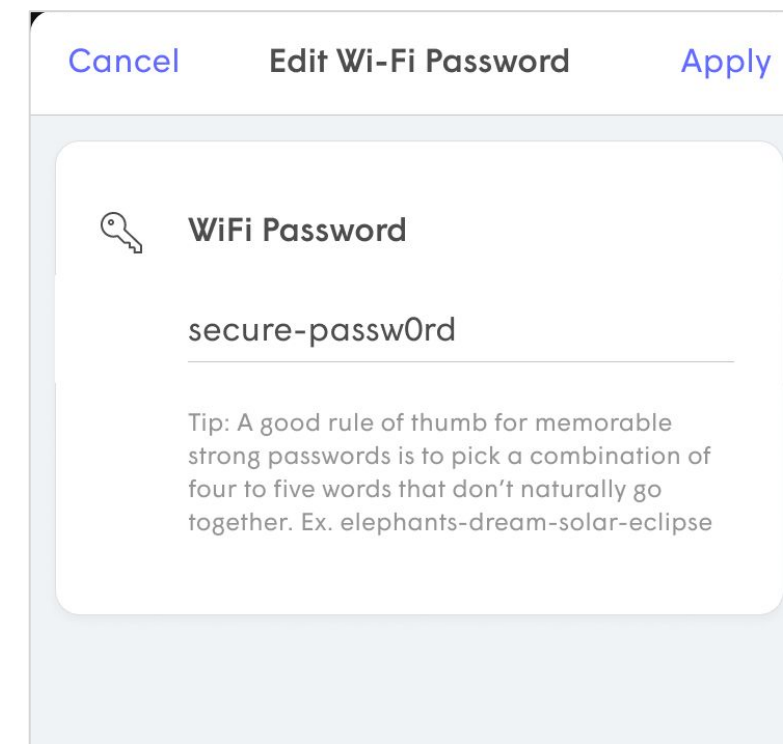
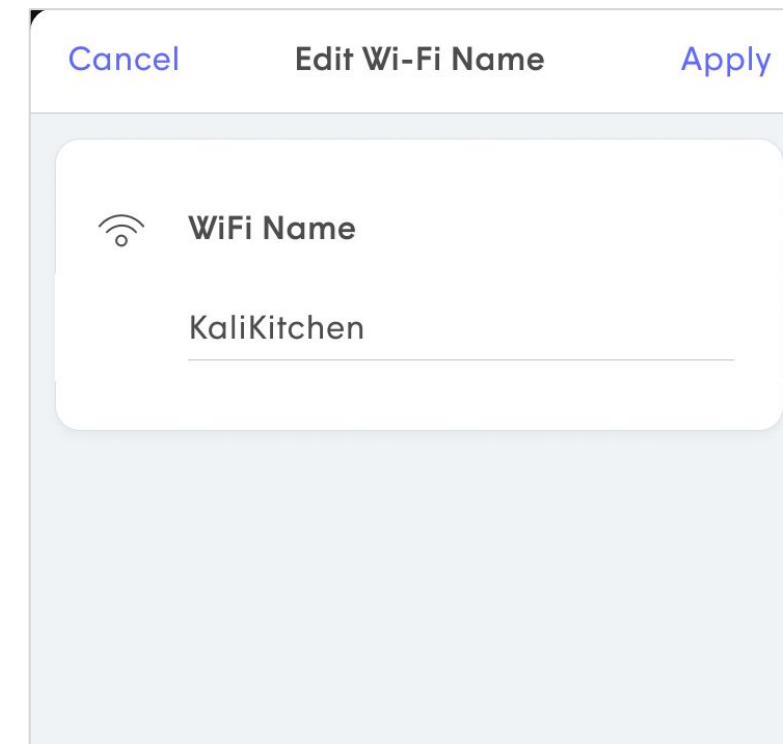
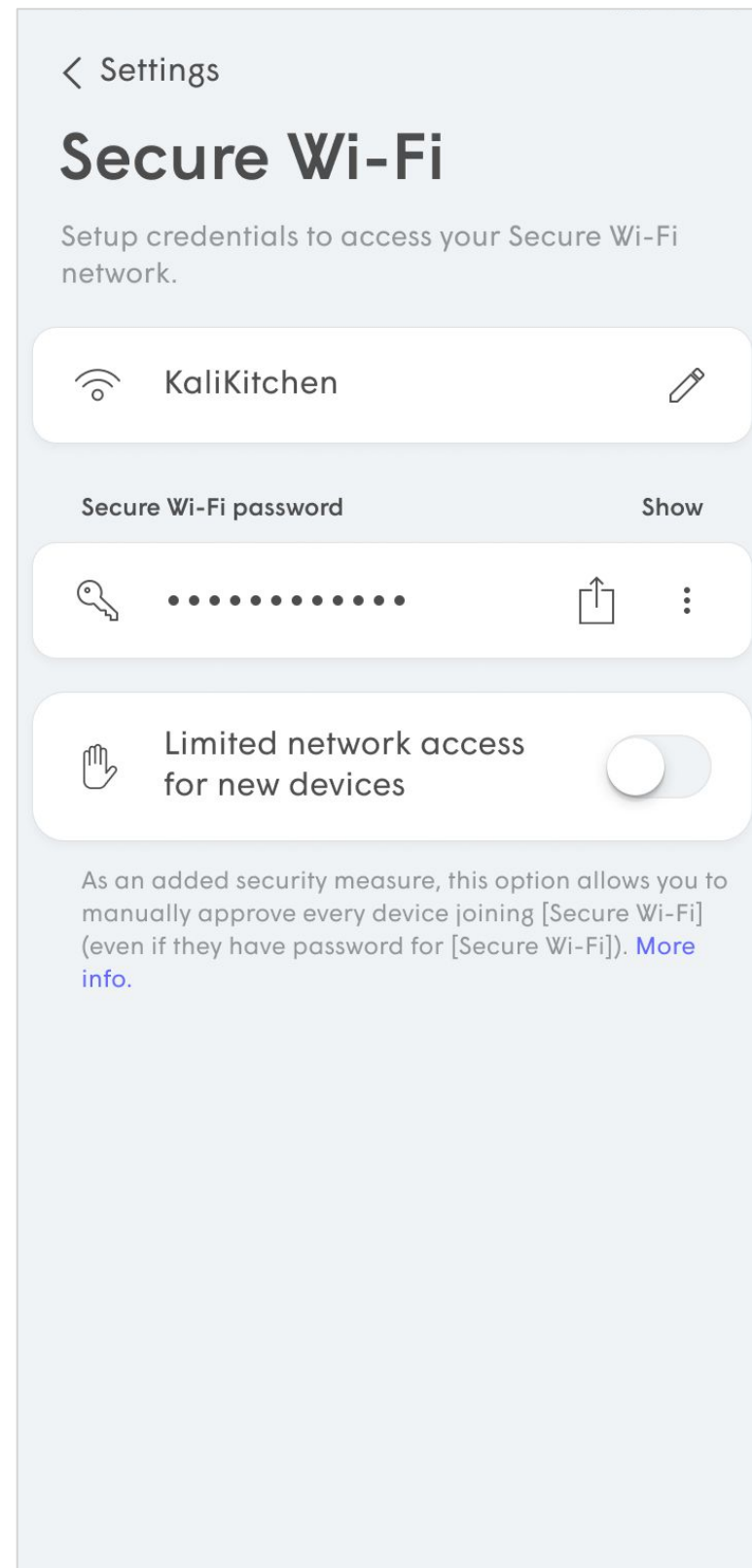
Managing Wi-Fi Access

Employee Wi-Fi

Access you the Employee Wi-Fi zone should be shared with employees, including the admin. Access to local devices can be controlled, while still allowing for internet access.

Tap on the pencil next to the SSID to change it, although any currently connected devices will disconnect until their settings are updated.

The Password can be revealed using the show button. Tapping on the options on the right of the password will allow you to edit or copy the password.



Managing Wi-Fi Access

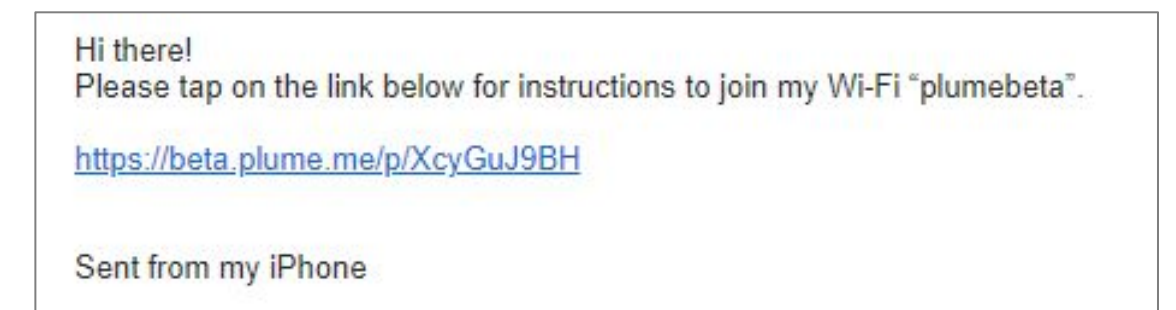
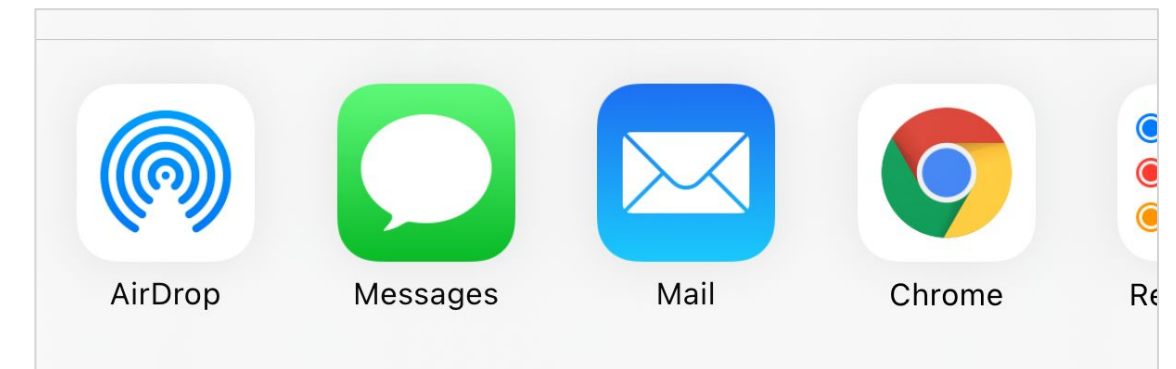
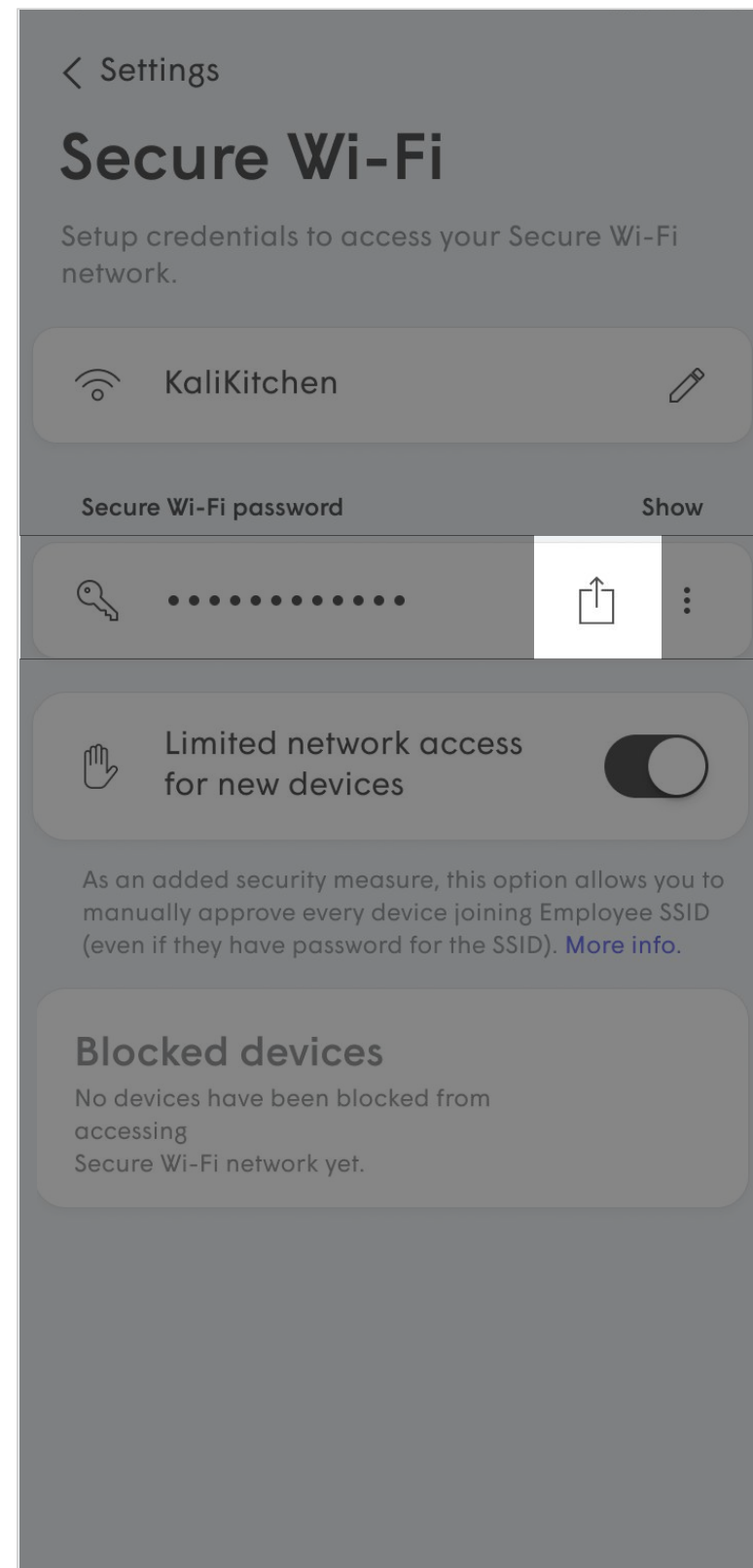
Sharing Passwords

Easily share any password created in the Secure Wi-Fi or Employee Wi-Fi zones.

Tap on the **share icon** to the left of the password you want to send.

Choose the application you want to use to send the link (SMS, iMessage, email, airdrop, android beam, etc). Only the options available on the device will be shown.

The recipient will receive a time-limited link that opens a webpage containing the SSID and their password.

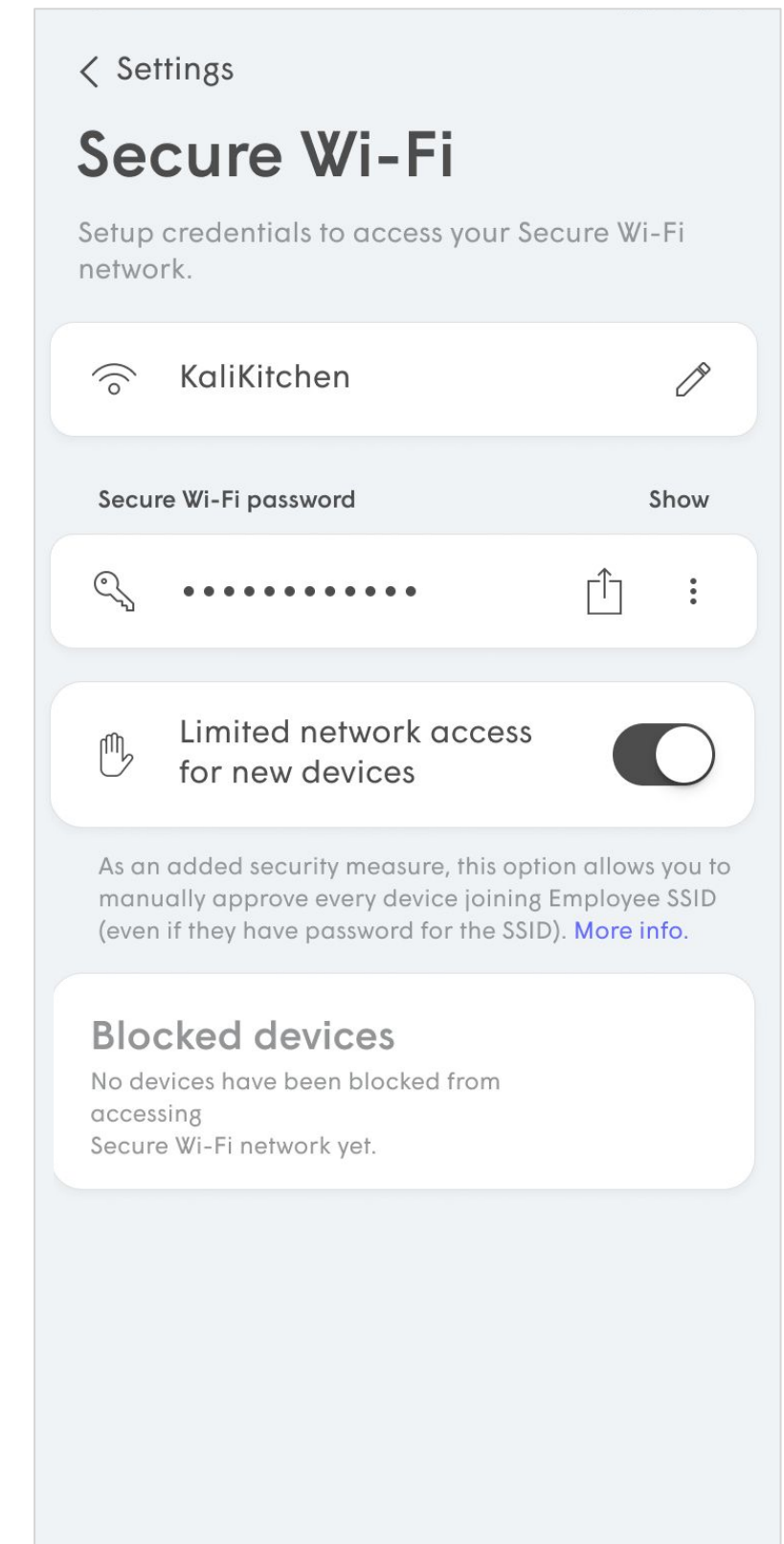
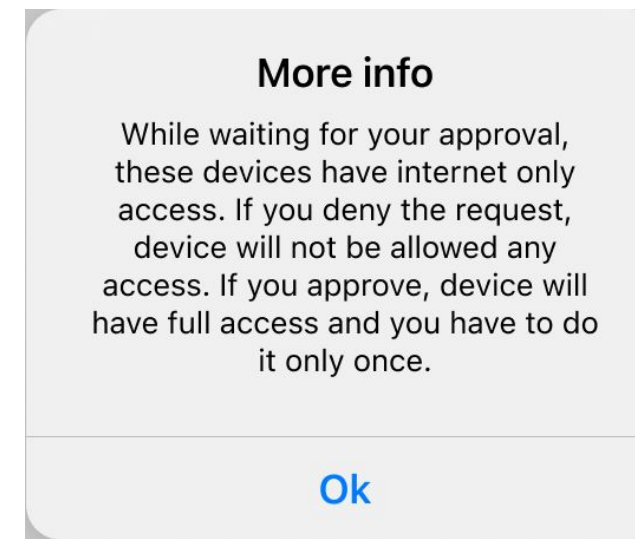
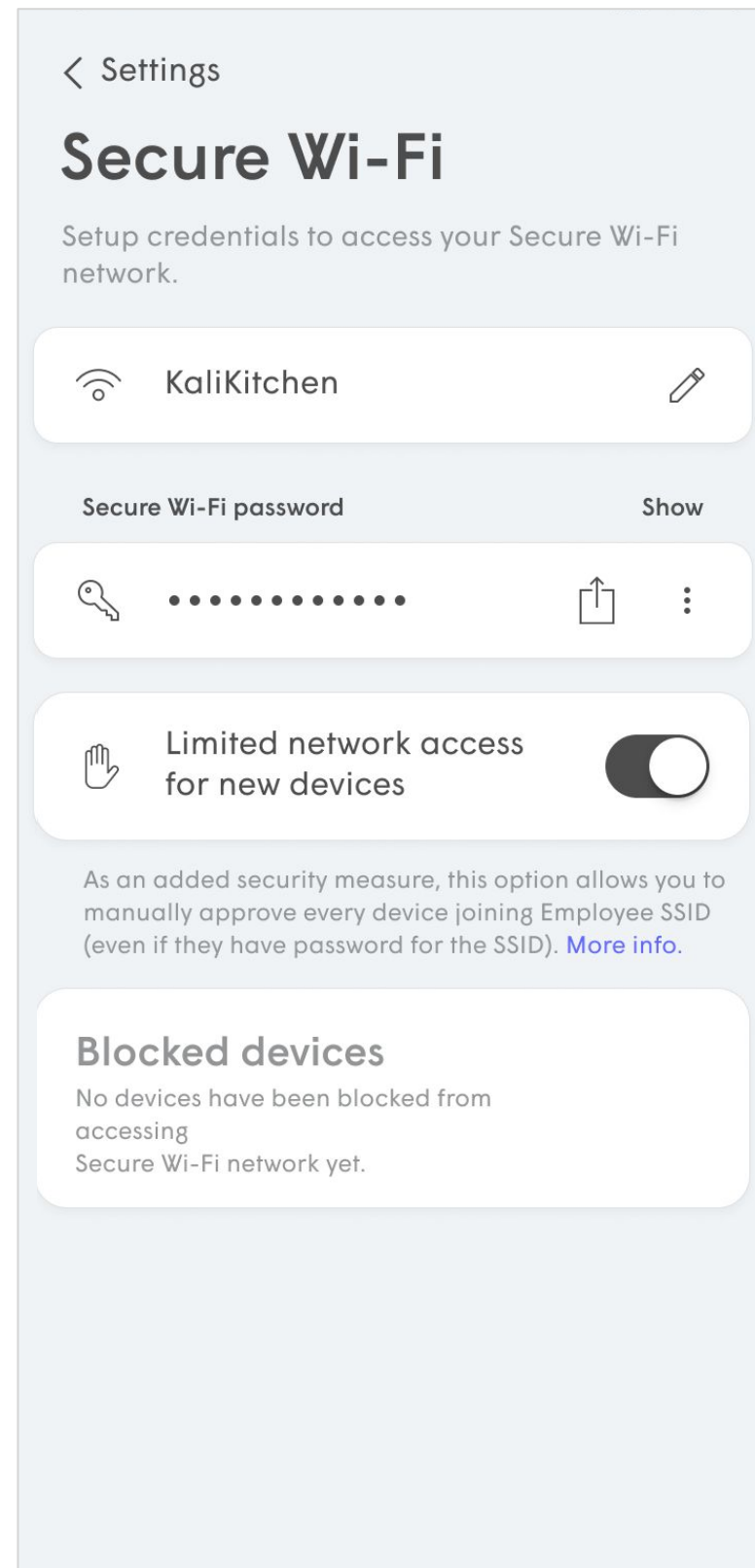


Limiting Network Access for New Devices

Enabling the **Limited network access for new devices** option can be enabled to protect both the Secure Wi-Fi and/or Employee Wi-Fi zones from new devices joining the network.

When enabled, even with the password, new devices connecting to the zone will have all local network access blocked until they are manually approved by the network's administrator. During this time in purgatory, the device will only have Internet access.

For the best Wi-Fi security, this should be enabled.



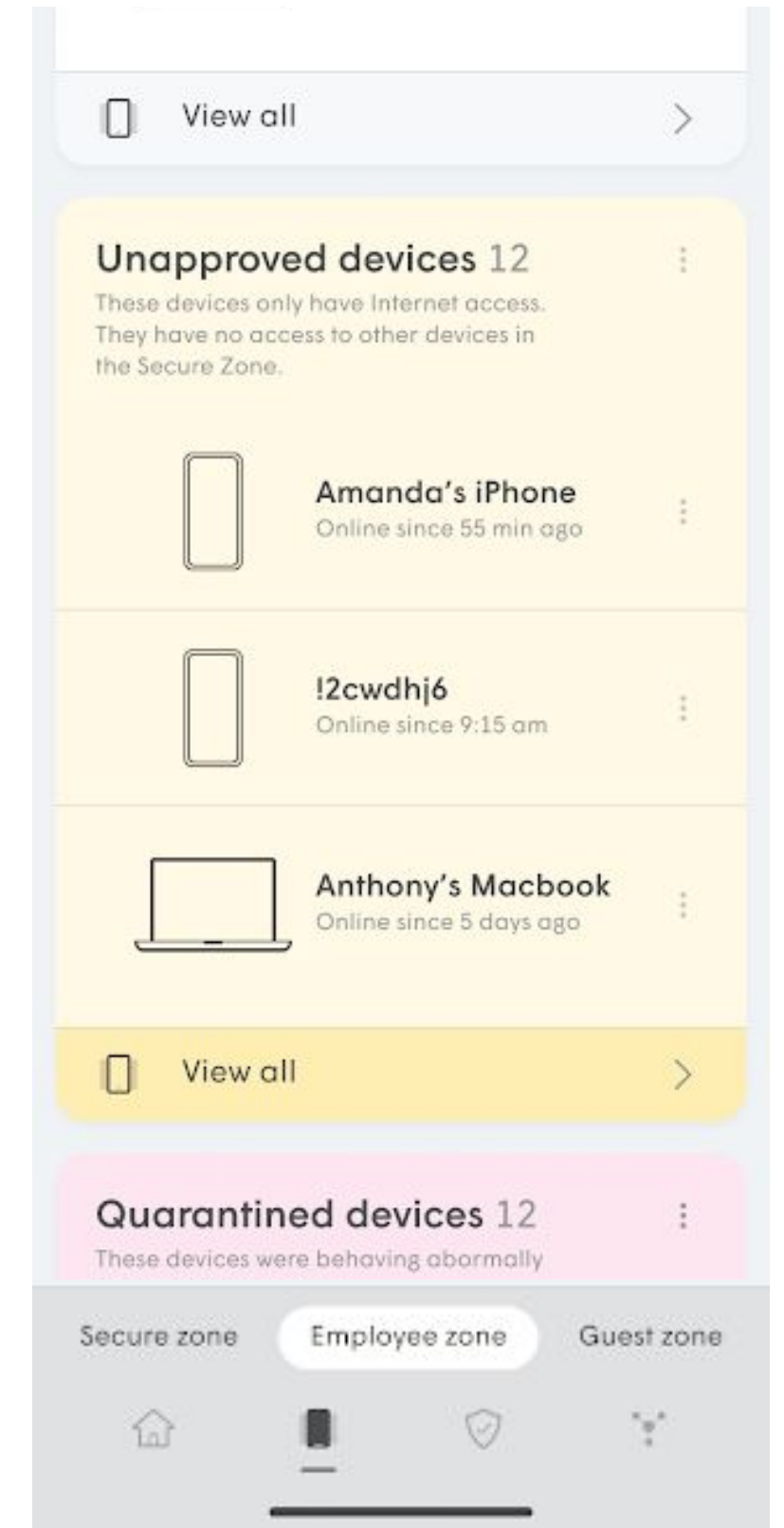
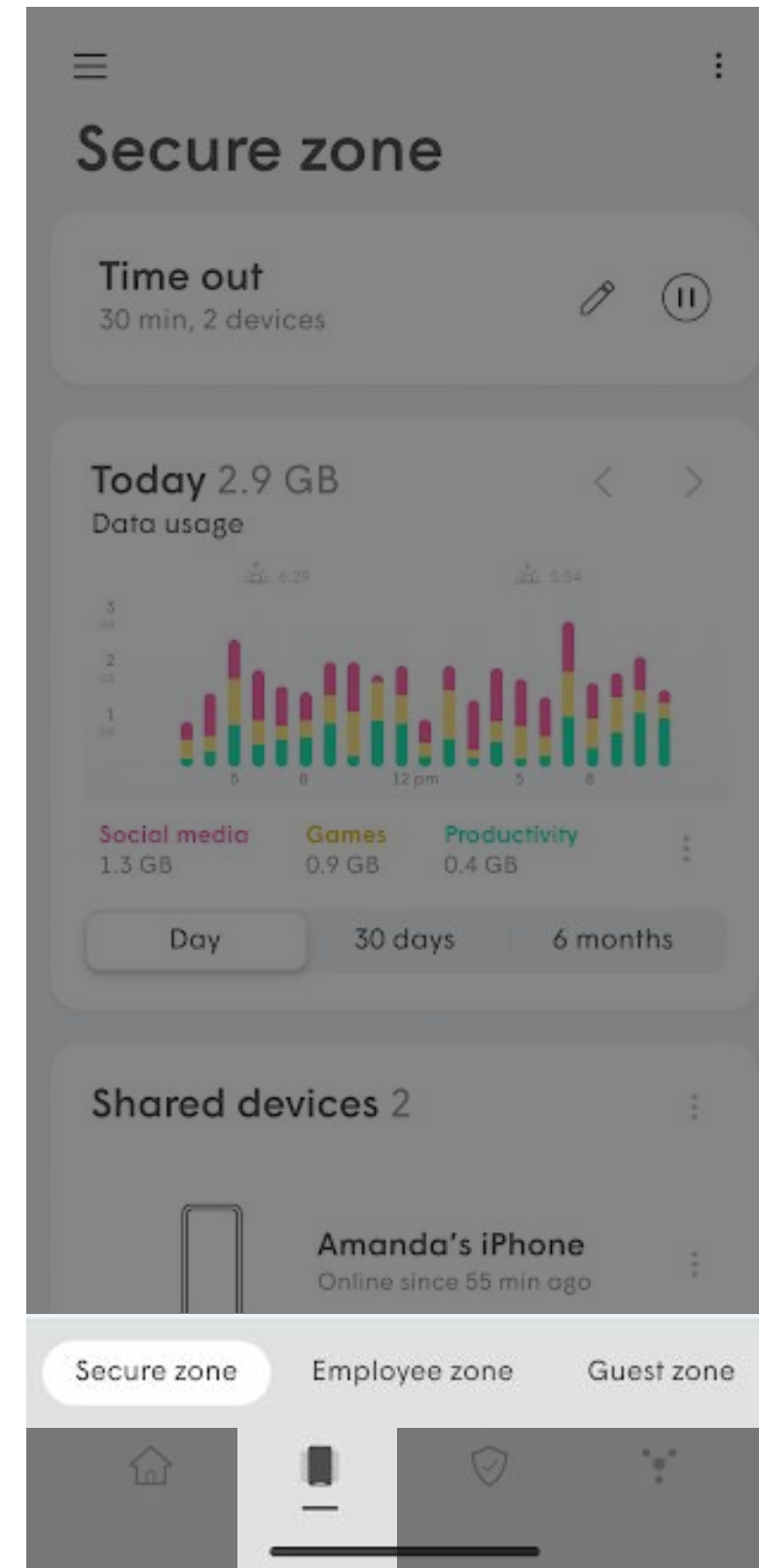
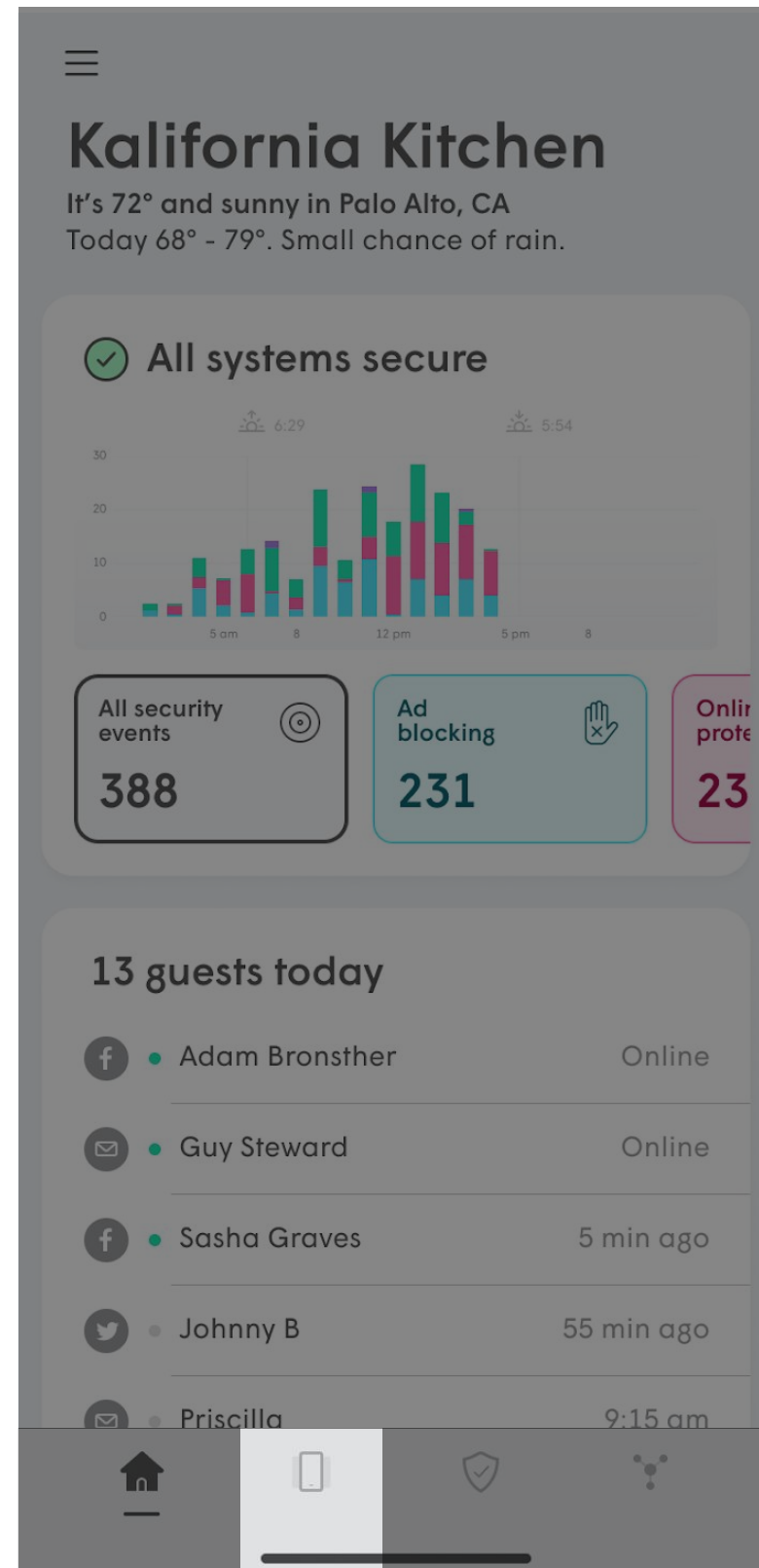
Approving Network Access for New Devices

Manually approving new devices for local access from devices currently in purgatory is handled through the **Zones** tab.

The **Zones** tab further organizes all devices based in the three available zones:

- **Secure zone**
- **Employee zone**
- **Guest zone**

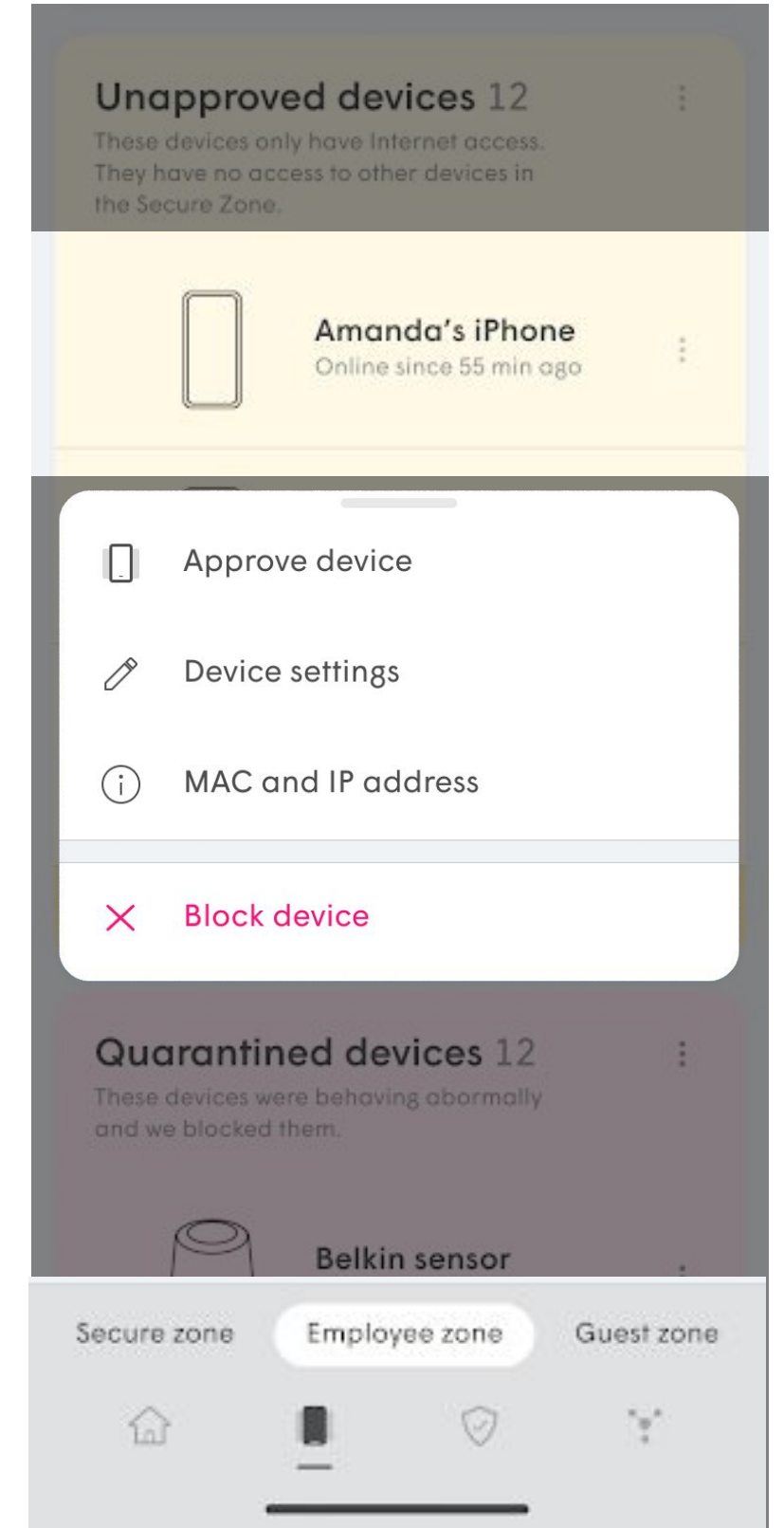
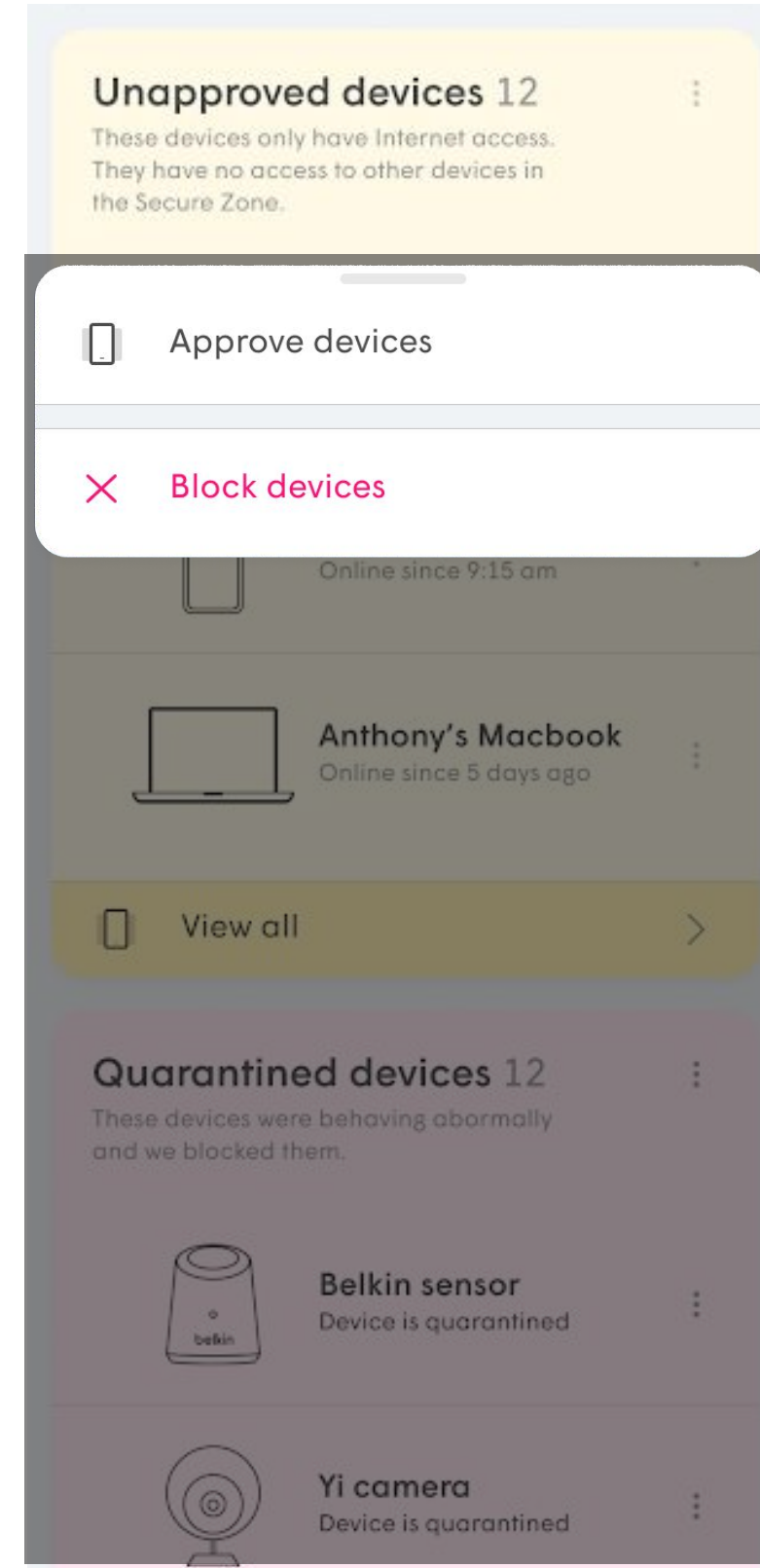
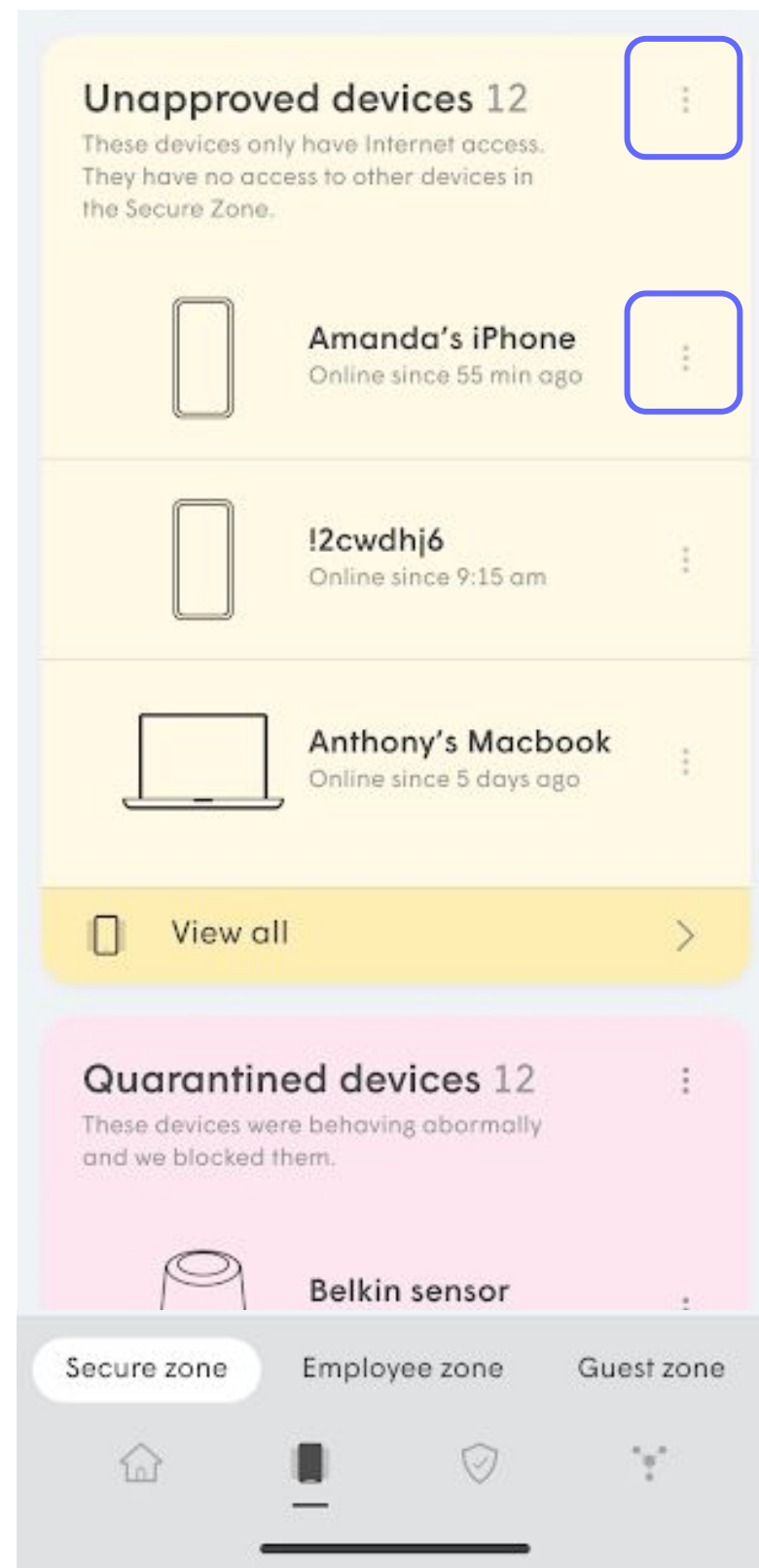
Tap on the **Secure zone** or **Employee zone** for the devices you wish to manage and scroll down to **Unapproved devices**.



Approving Network Access for New Devices

Tap the **options** icon to the right Unapproved devices to approve the devices all at once, or use the **options** icon next to the specific device to approve just that device.

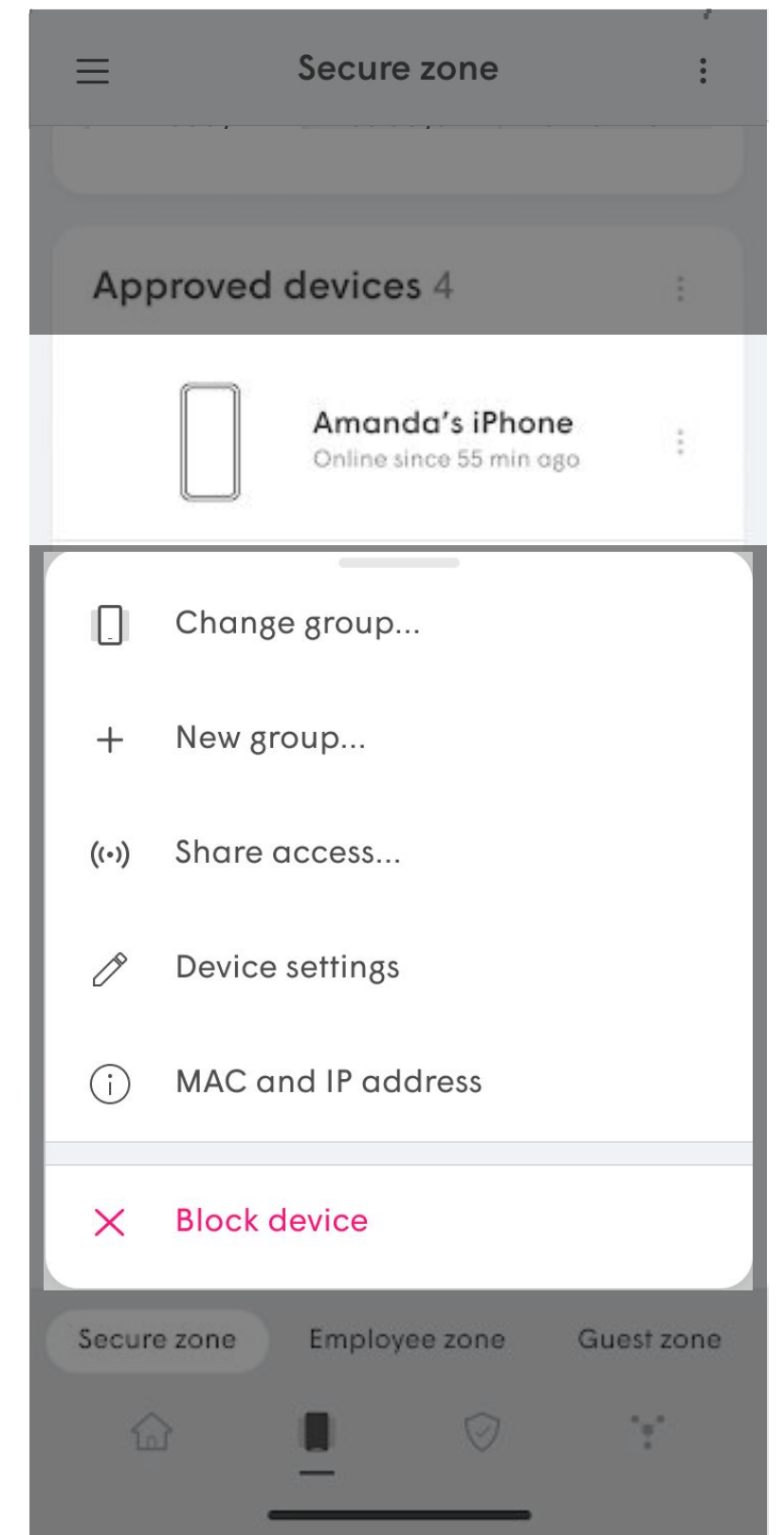
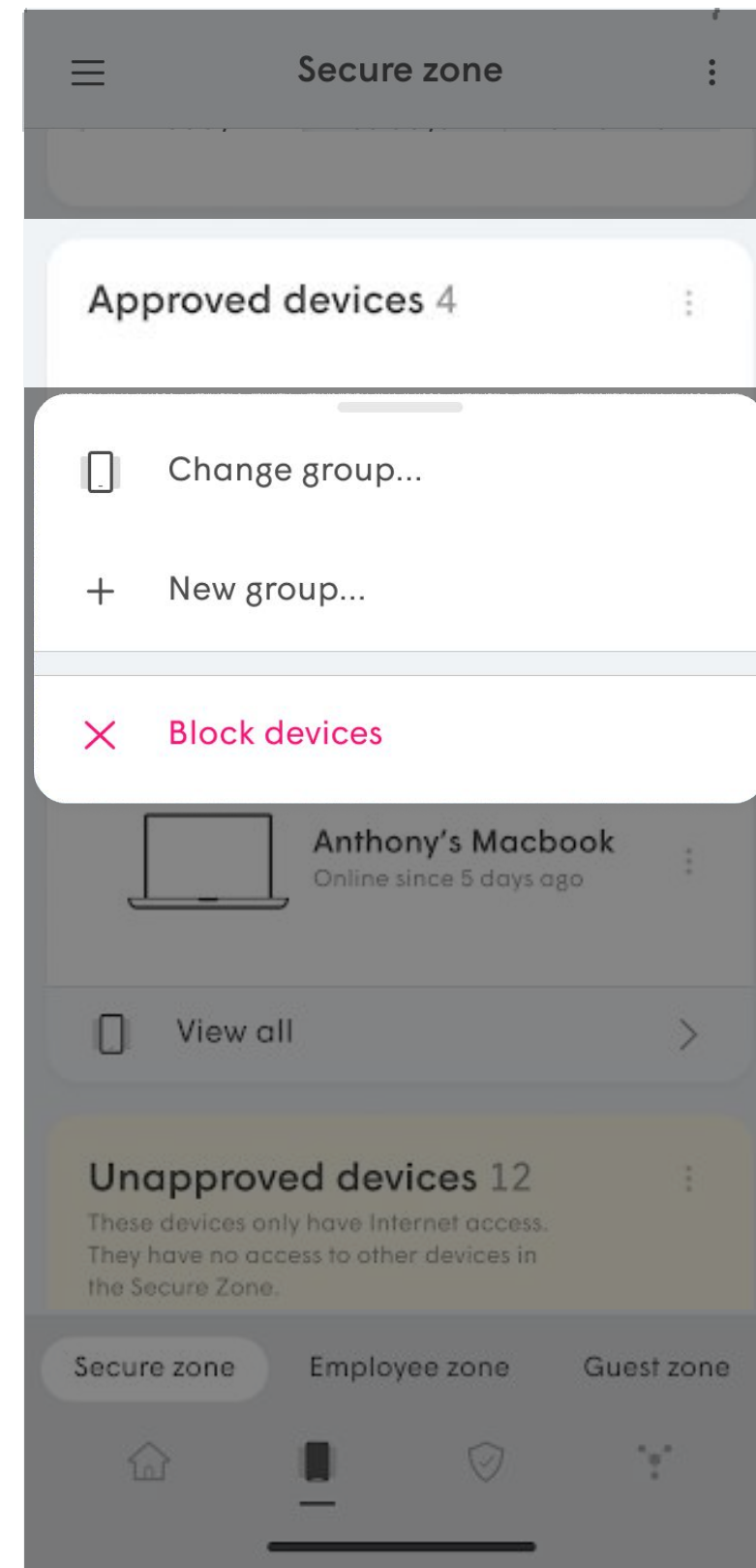
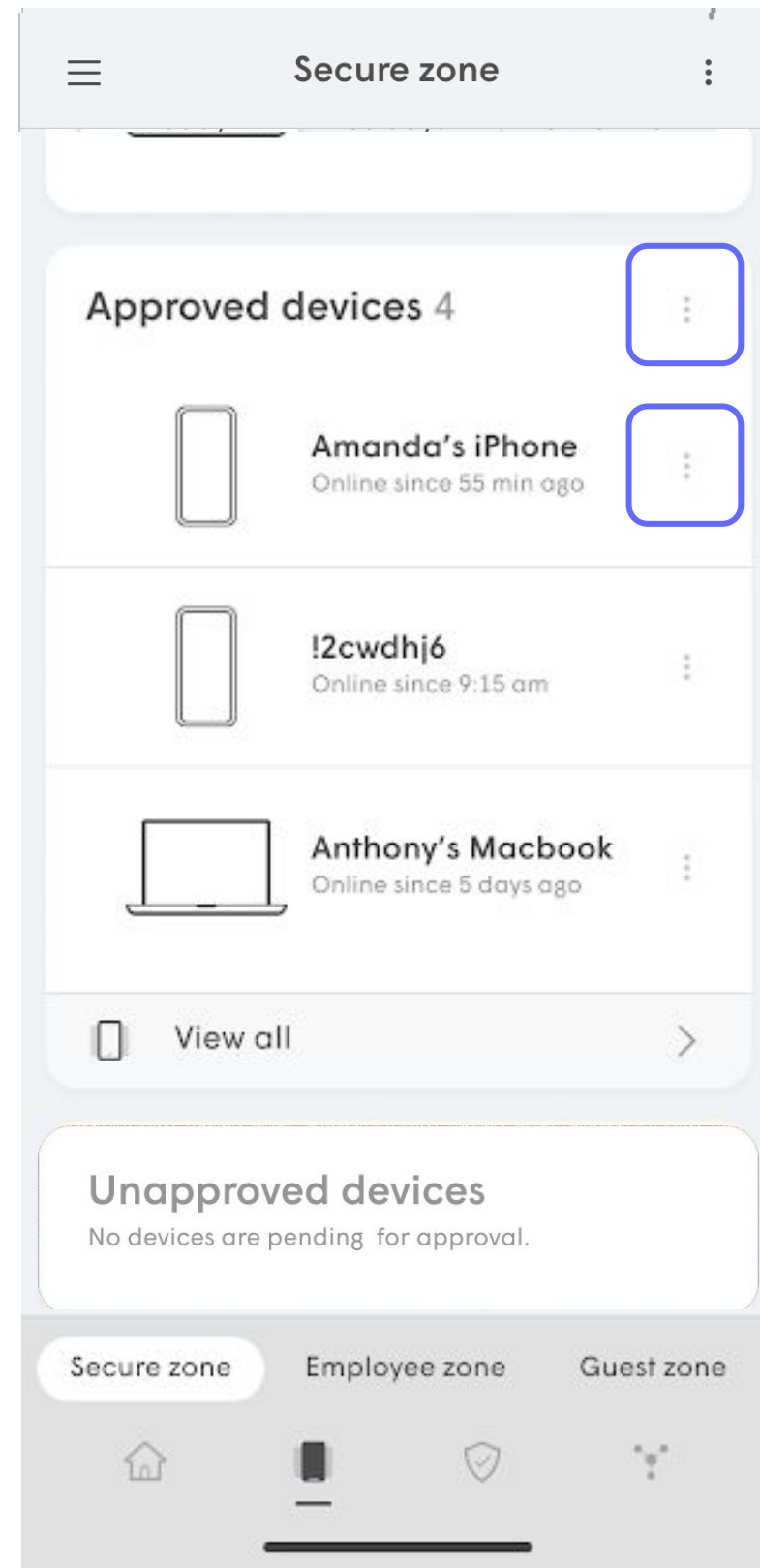
Tapping **Approve device(s)** removes the device(s) from Blocked list and allows for local access based on the current zone.



Approving Network Access for New Devices

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

Approved devices options include **Change group**, **New group**, and **Block Access**. Individual Approved devices also have the options to **Share access**, **device settings**, **MAC and IP**



Managing Wi-Fi Access

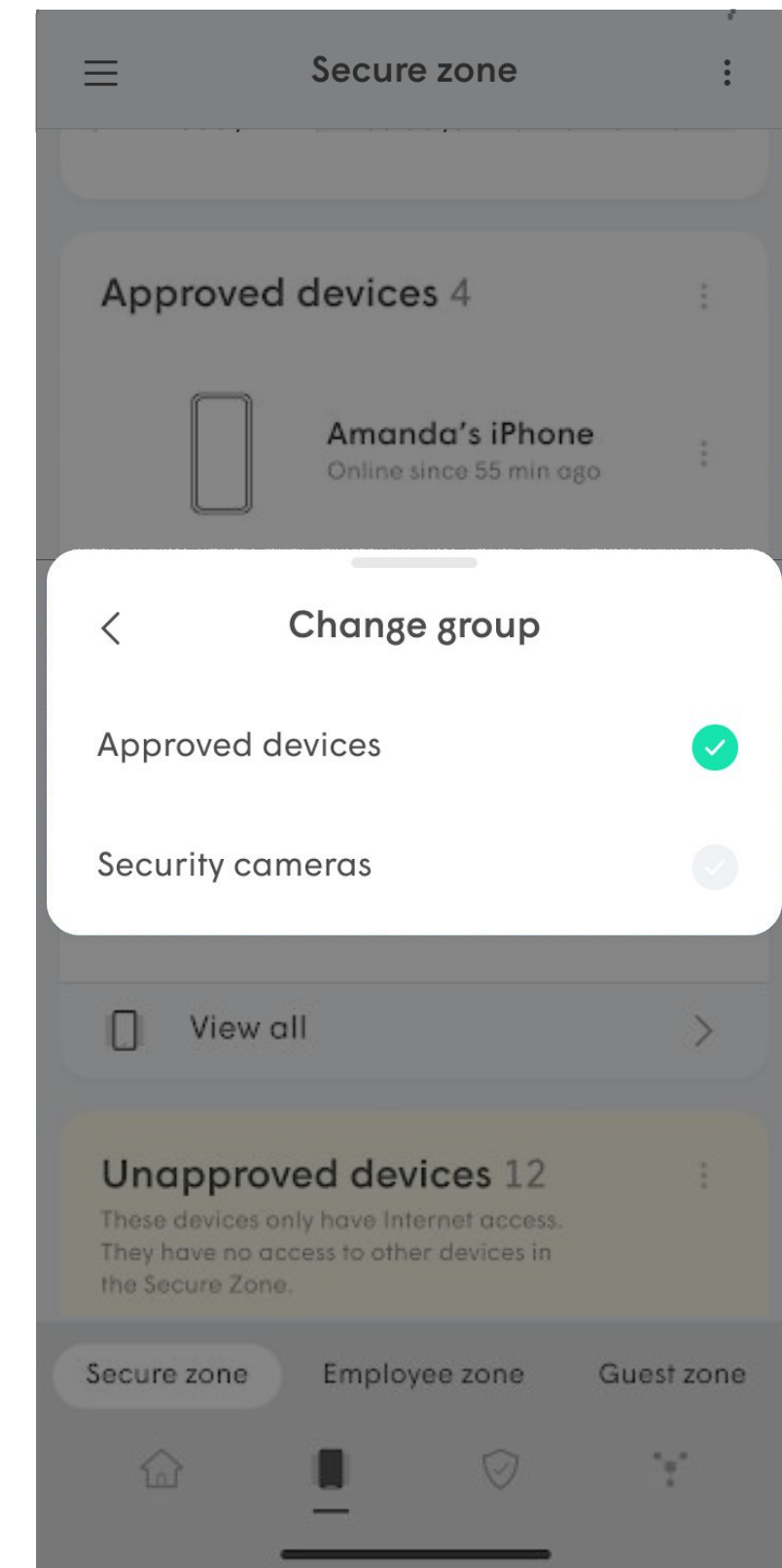
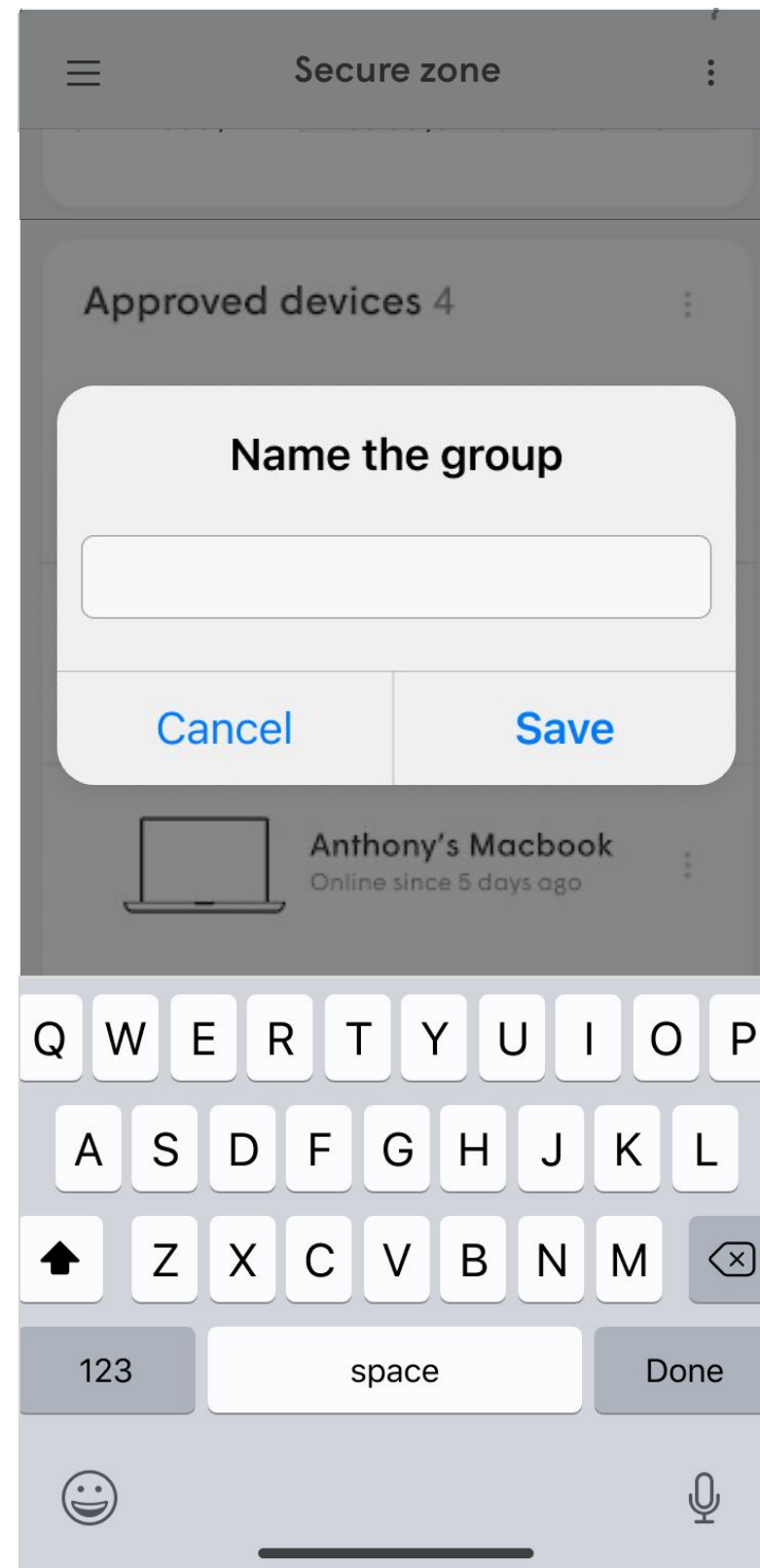
Device Groups

Devices in the Secure Wi-Fi zone can be grouped to better organize and allow them to be quickly shared as a group instead of individually.

Choose **New group** from the Approved devices option to create the group. This can also be done from the options at the top-right of the Secure zone page,

Once the group is created, use the **Change group** option to add the individual device to the new group.

IMPORTANT: Device Groups are for organization purposes only and **do not block a device from accessing another within the same zone.** Groups are used to share Secure Zone devices with employees more efficiently.

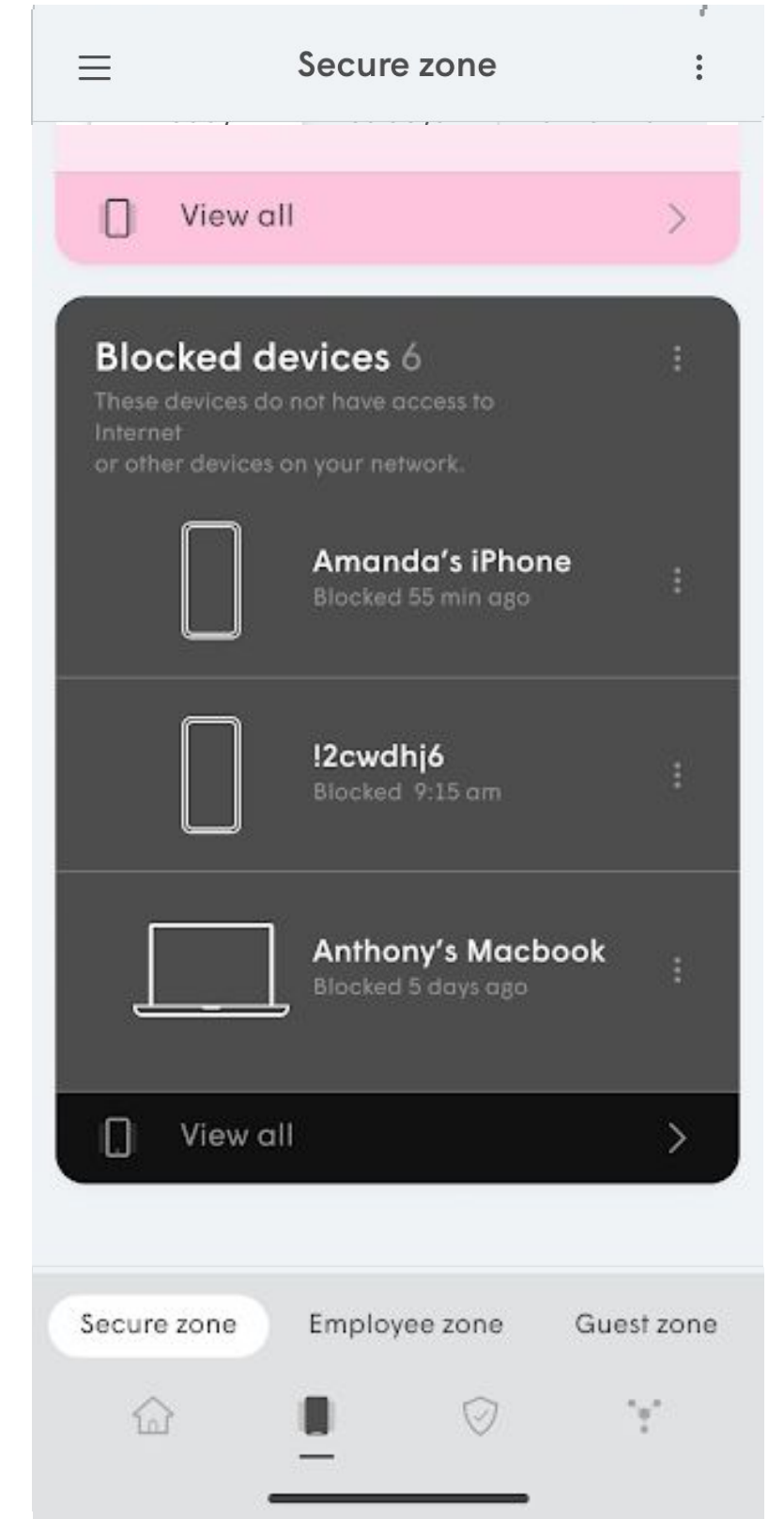
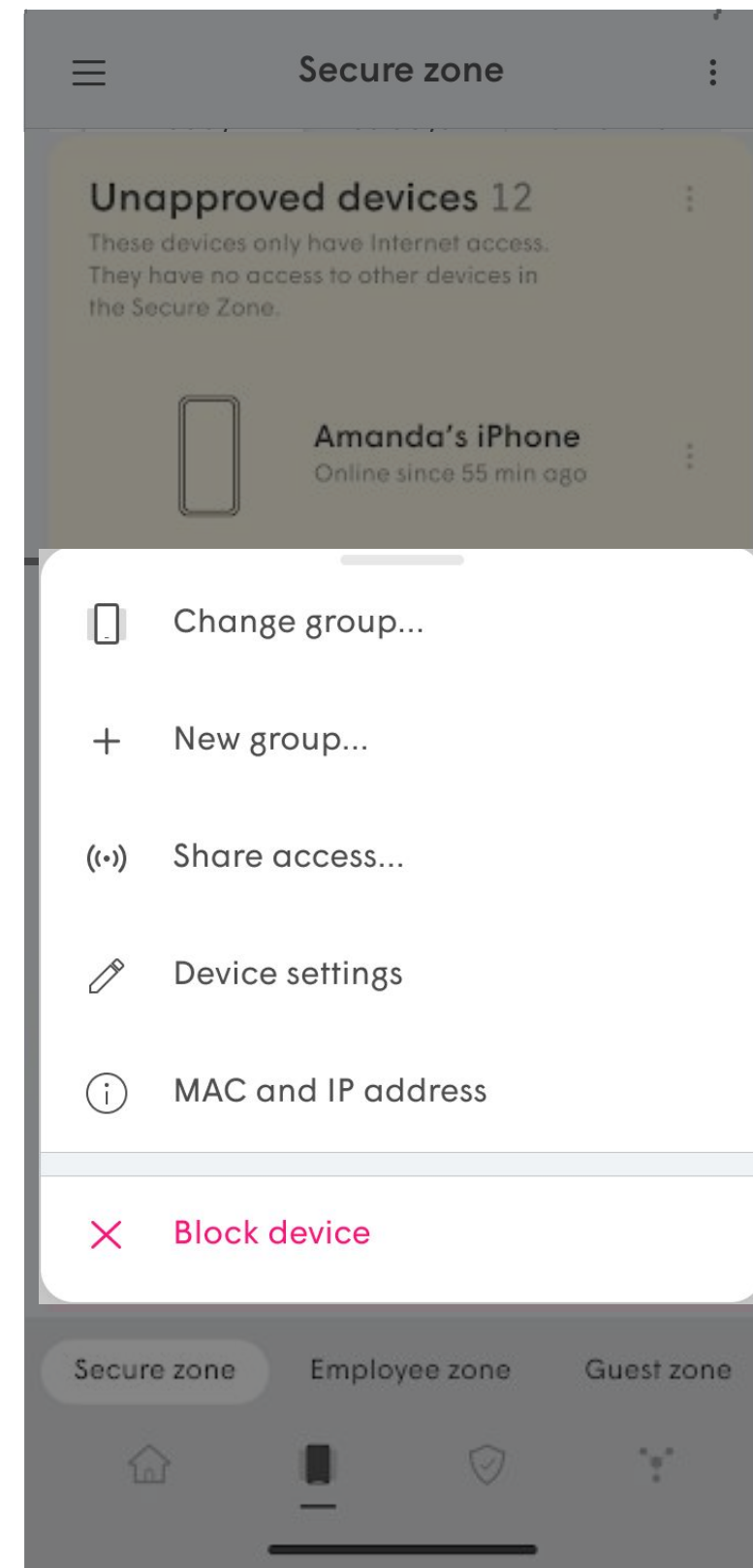
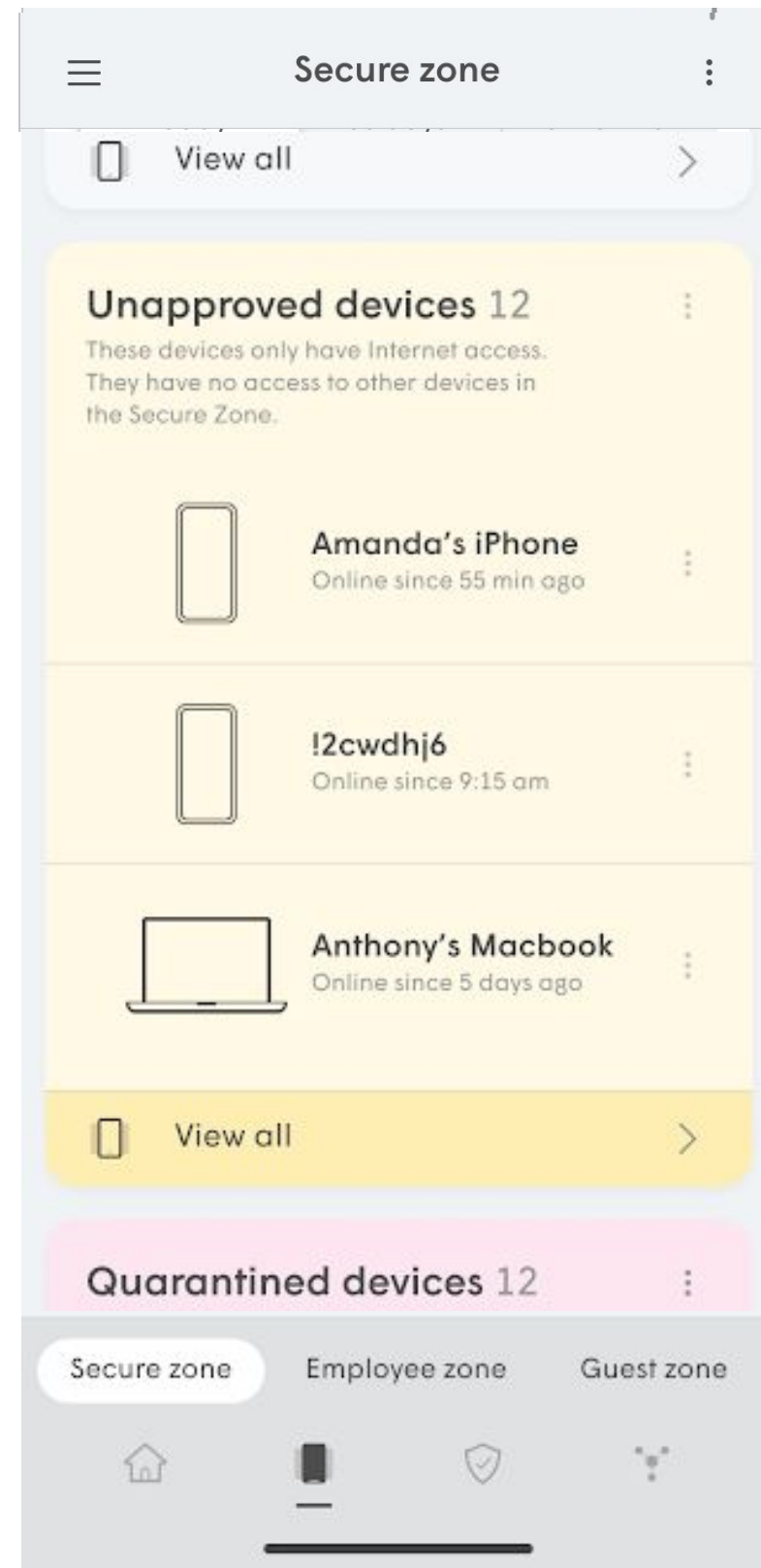


Managing Wi-Fi Access

Blocking Devices

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

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



Managing Wi-Fi Access

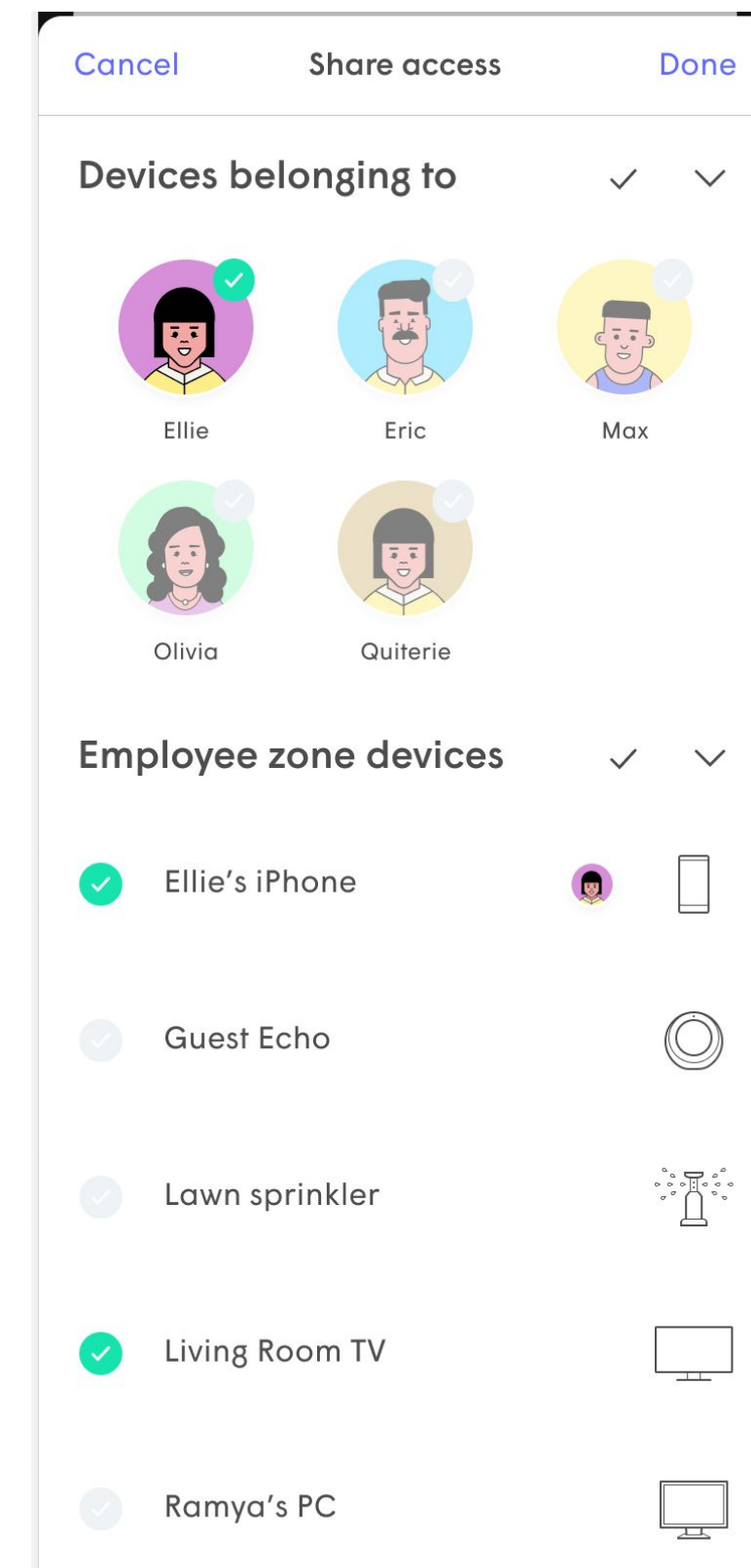
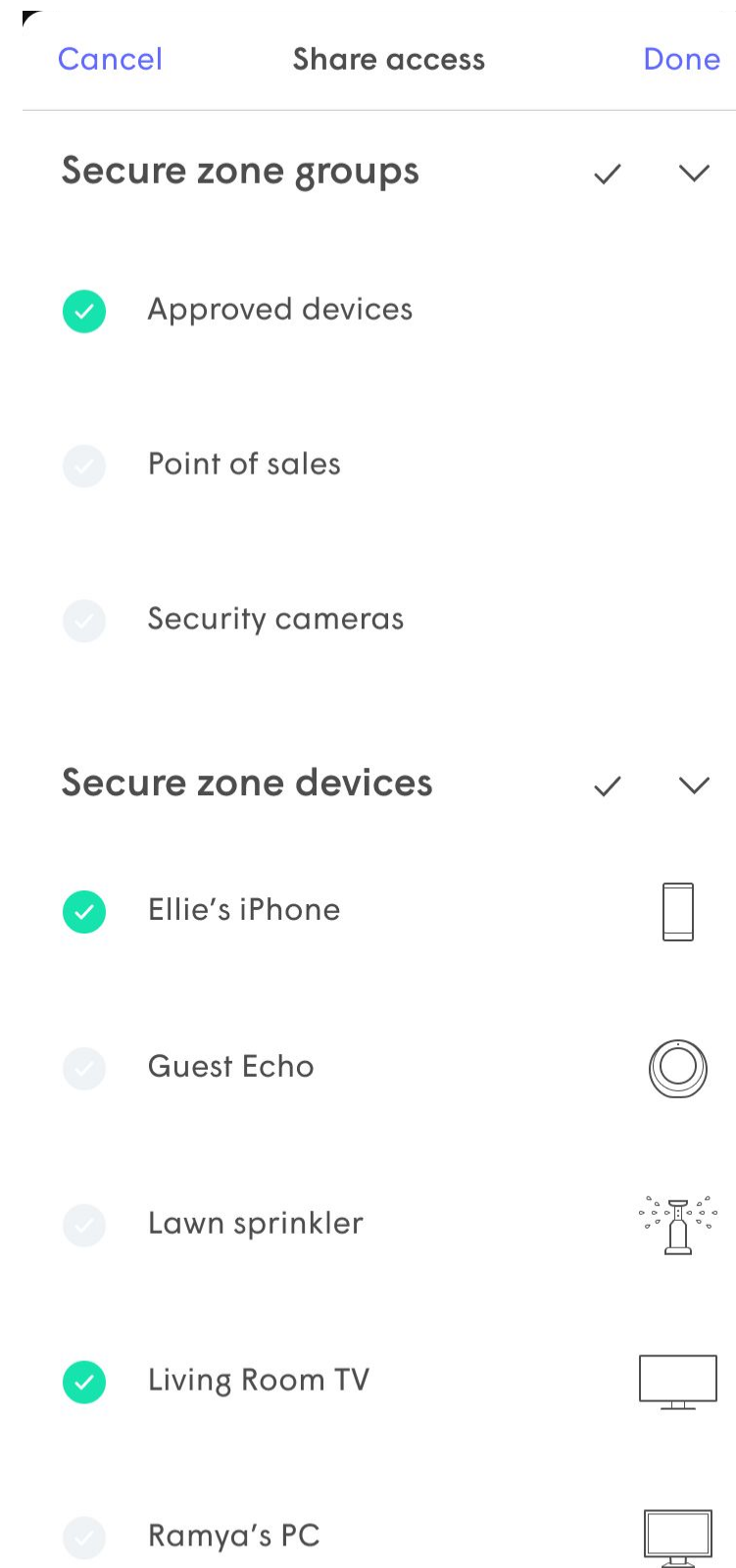
Sharing Devices

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

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

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

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

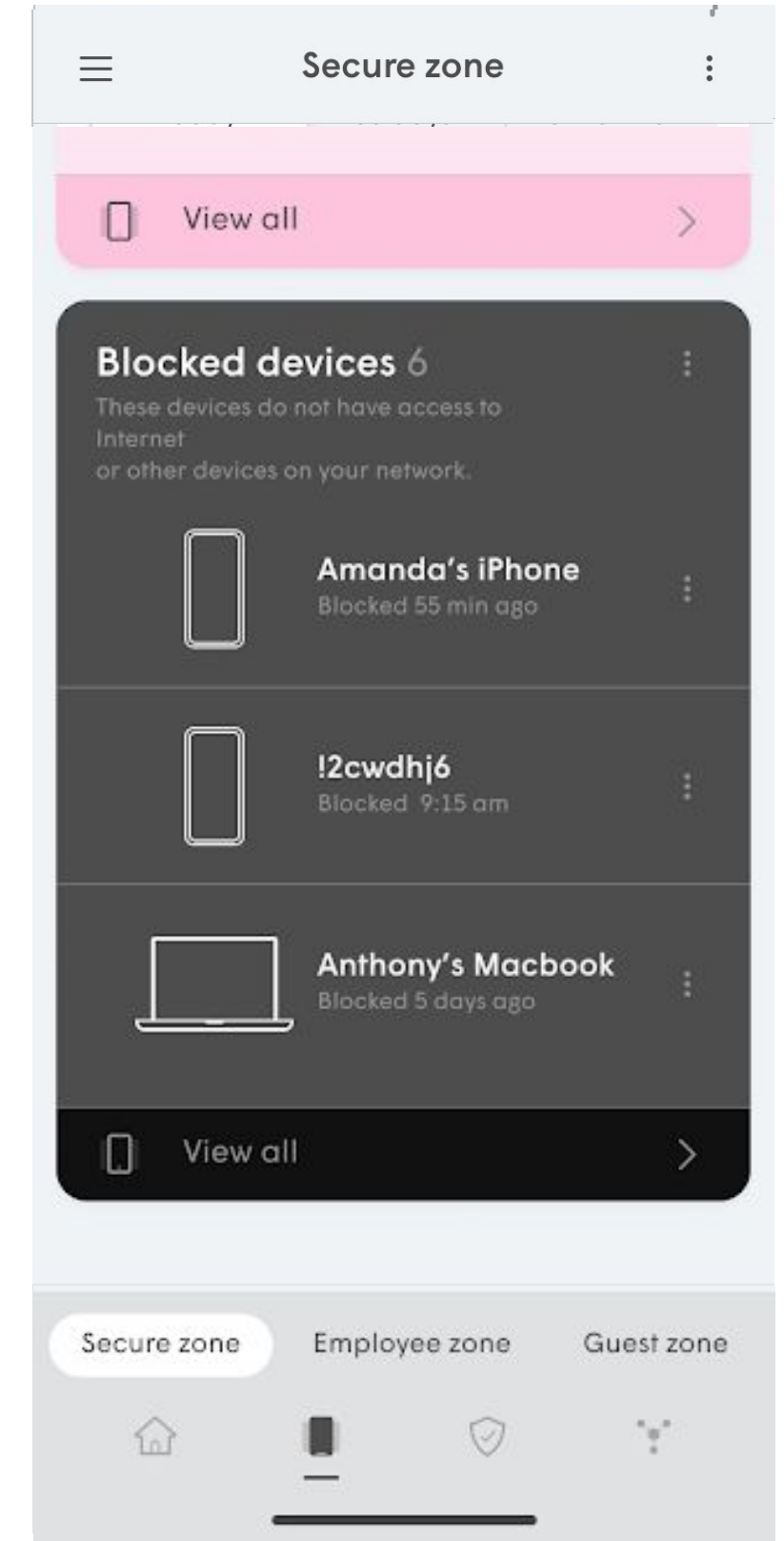
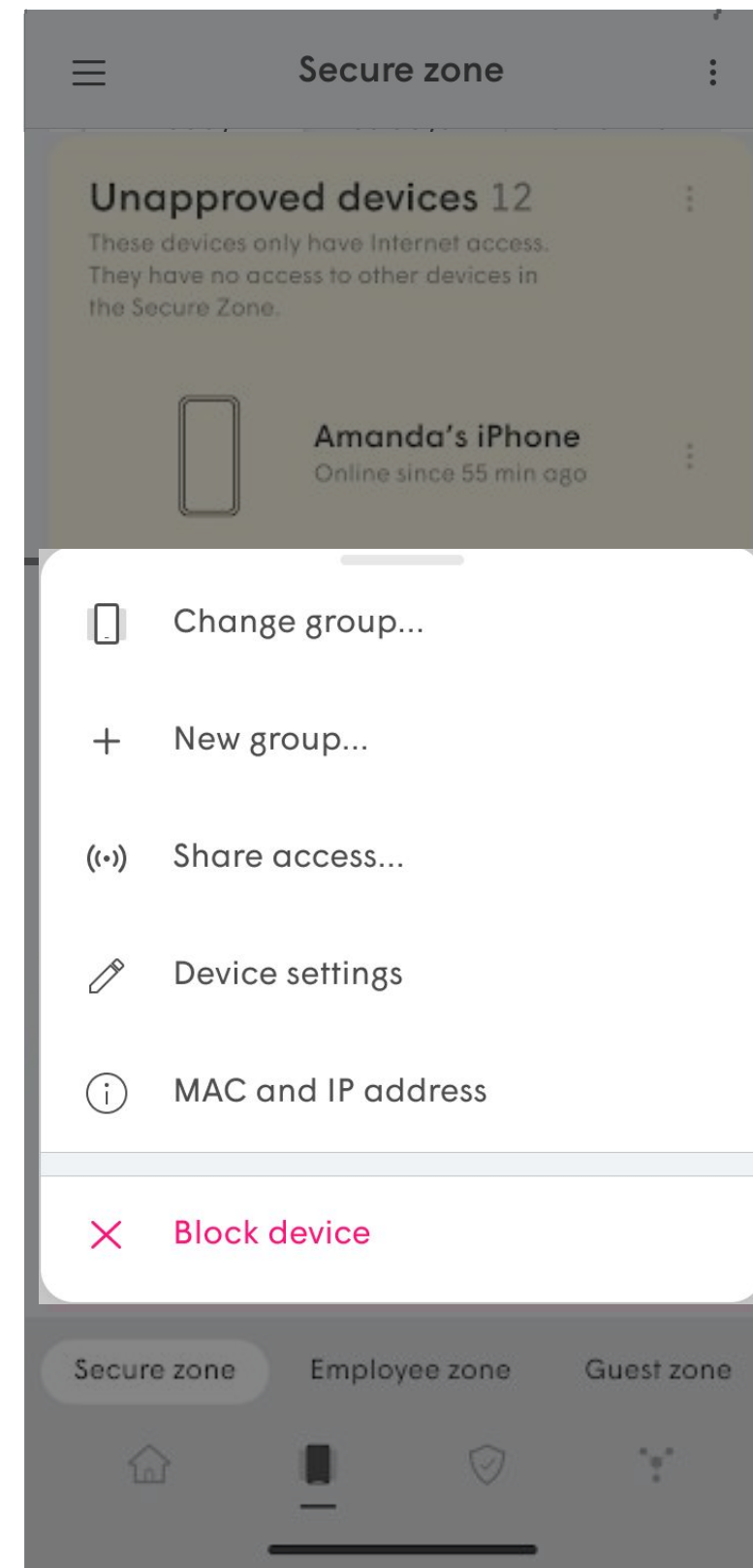
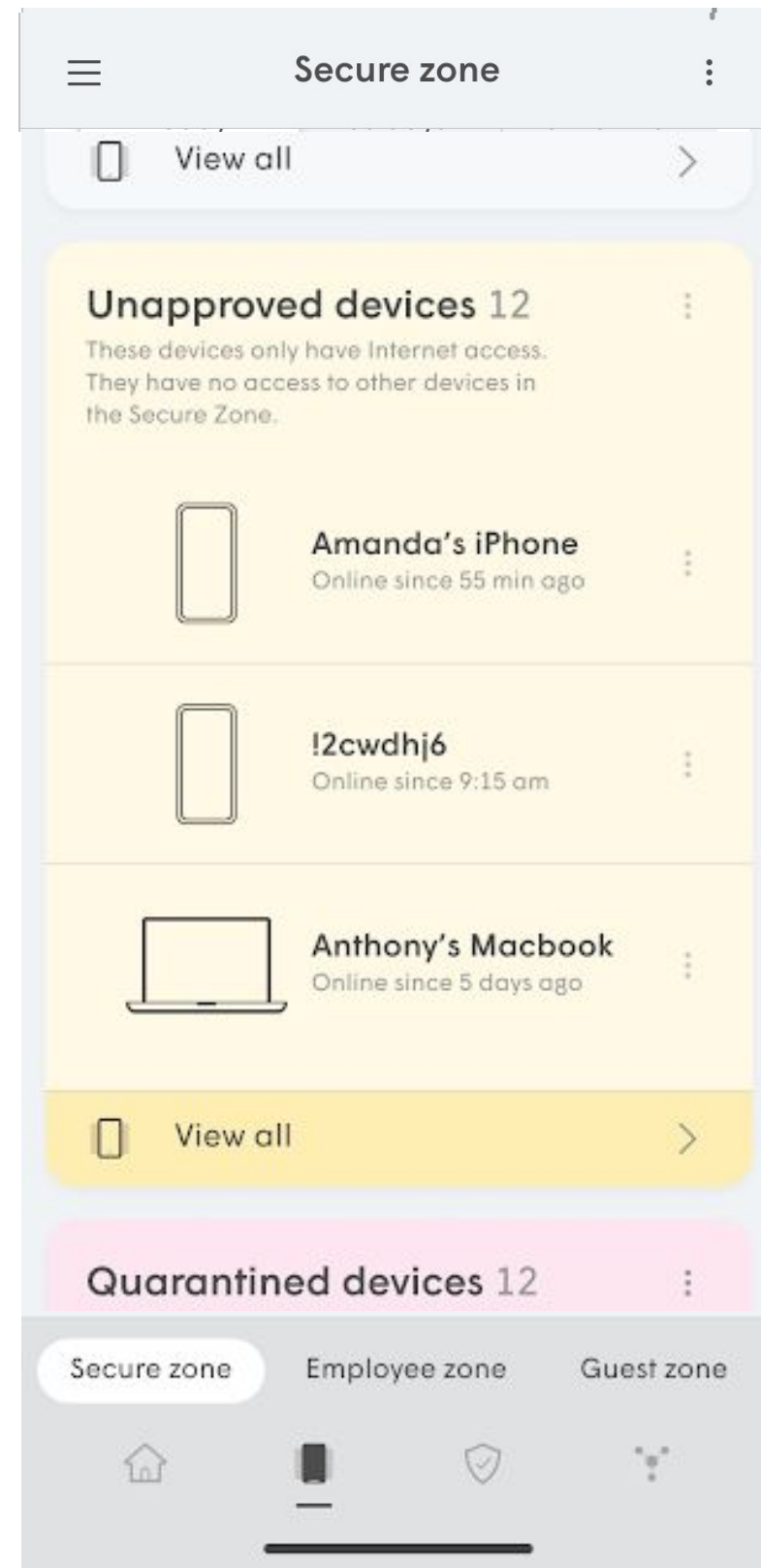


Managing Wi-Fi Access

Blocking Devices

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

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



Managing Employee Wi-Fi

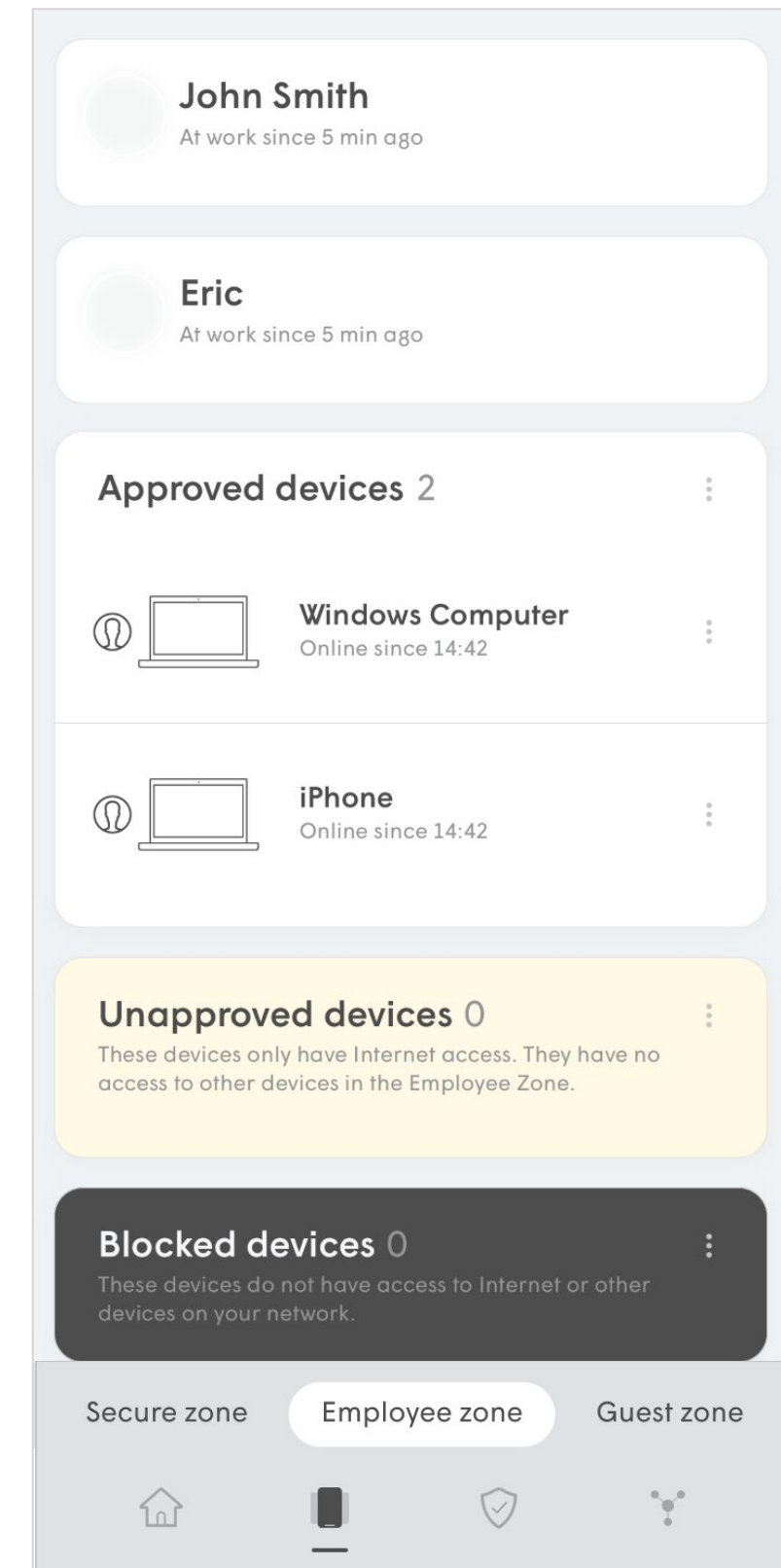
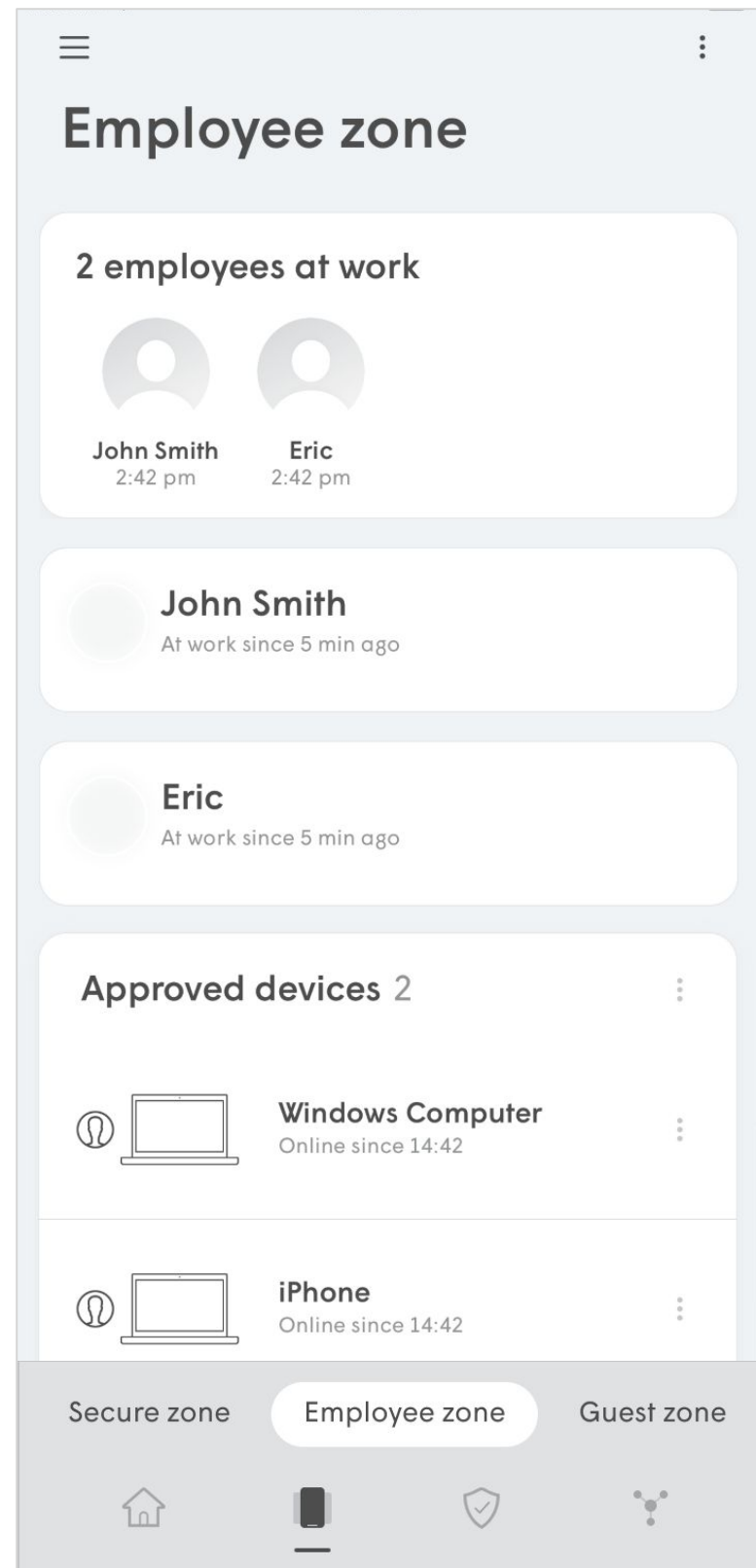
Employee Zone Overview

The **Employee zone** is managed through the **devices** menu.

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

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

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

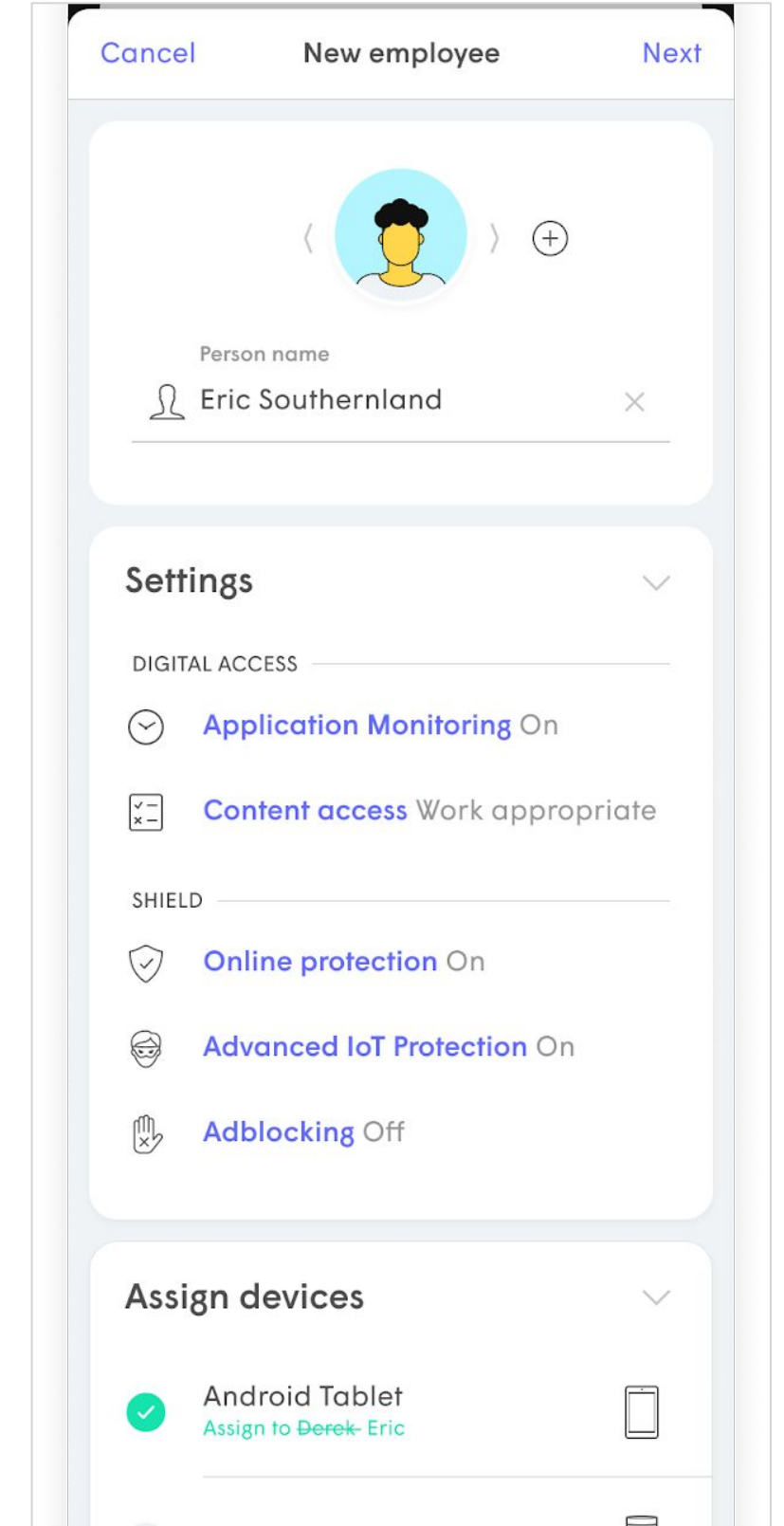
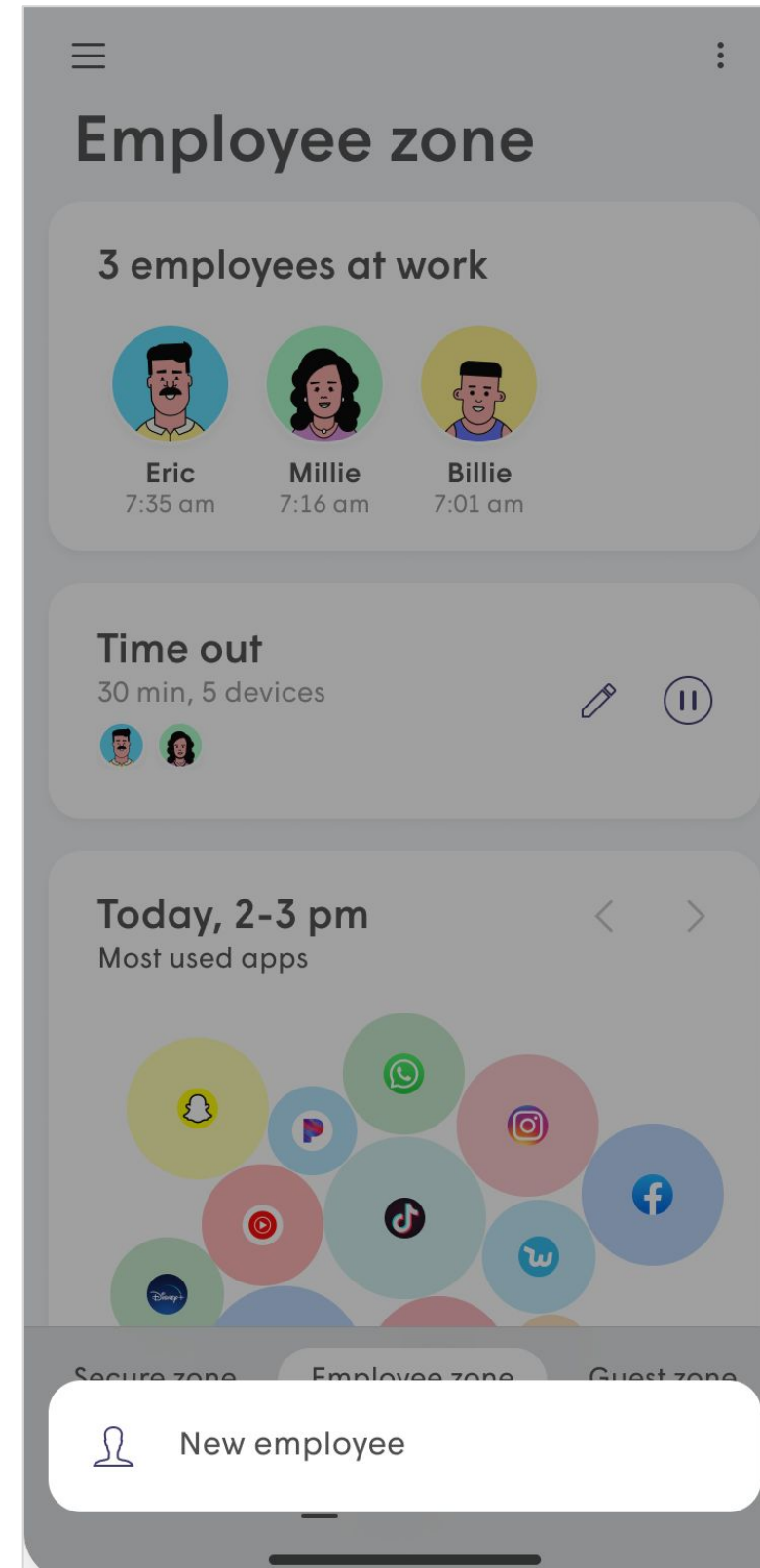
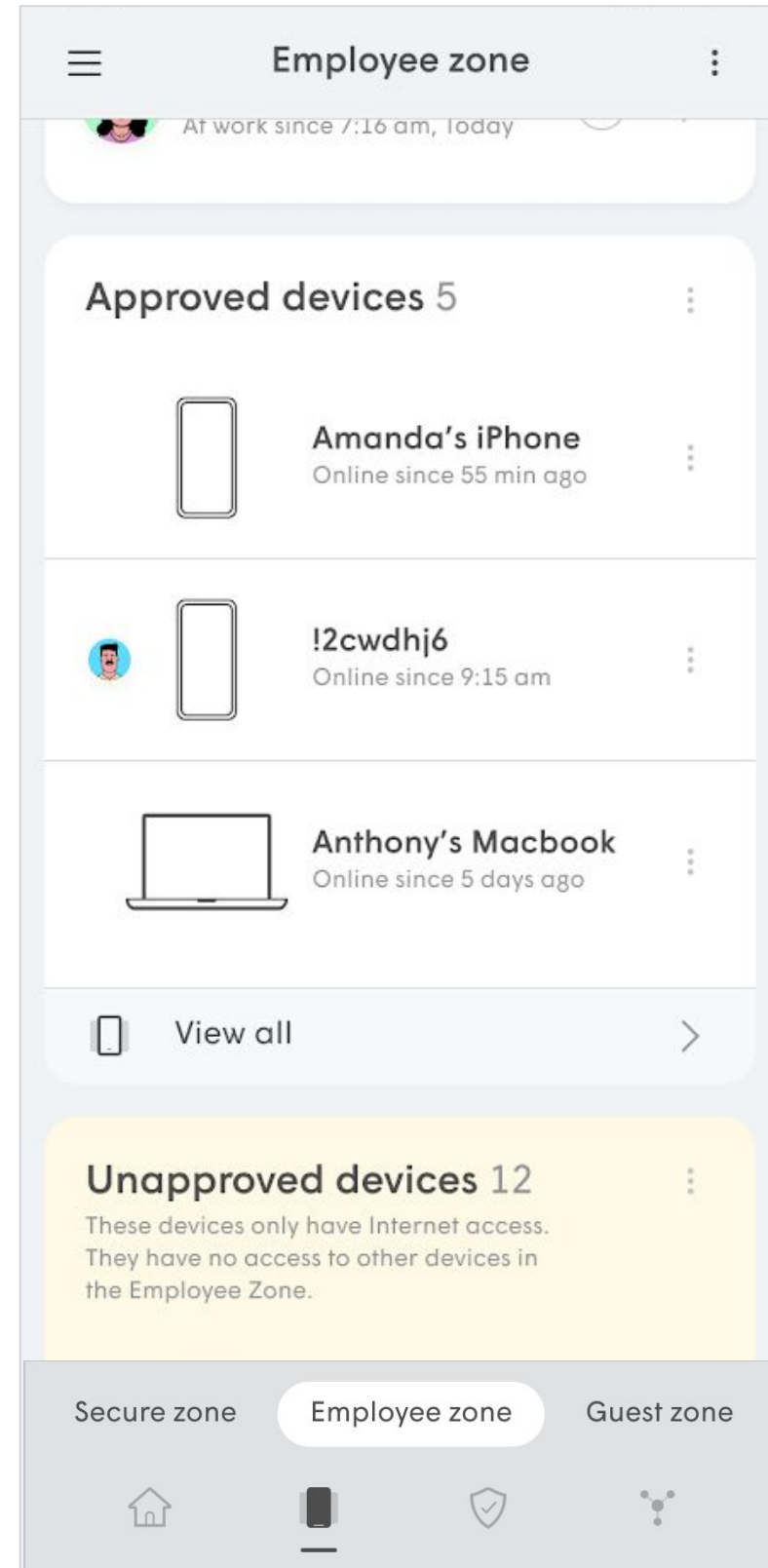


Managing Employee Wi-Fi

Adding Employees

Tapping the **options** on the top-right of the Employee zone starts the **New employee** flow.

The first step is to enter the employee name.



Managing Employee Wi-Fi

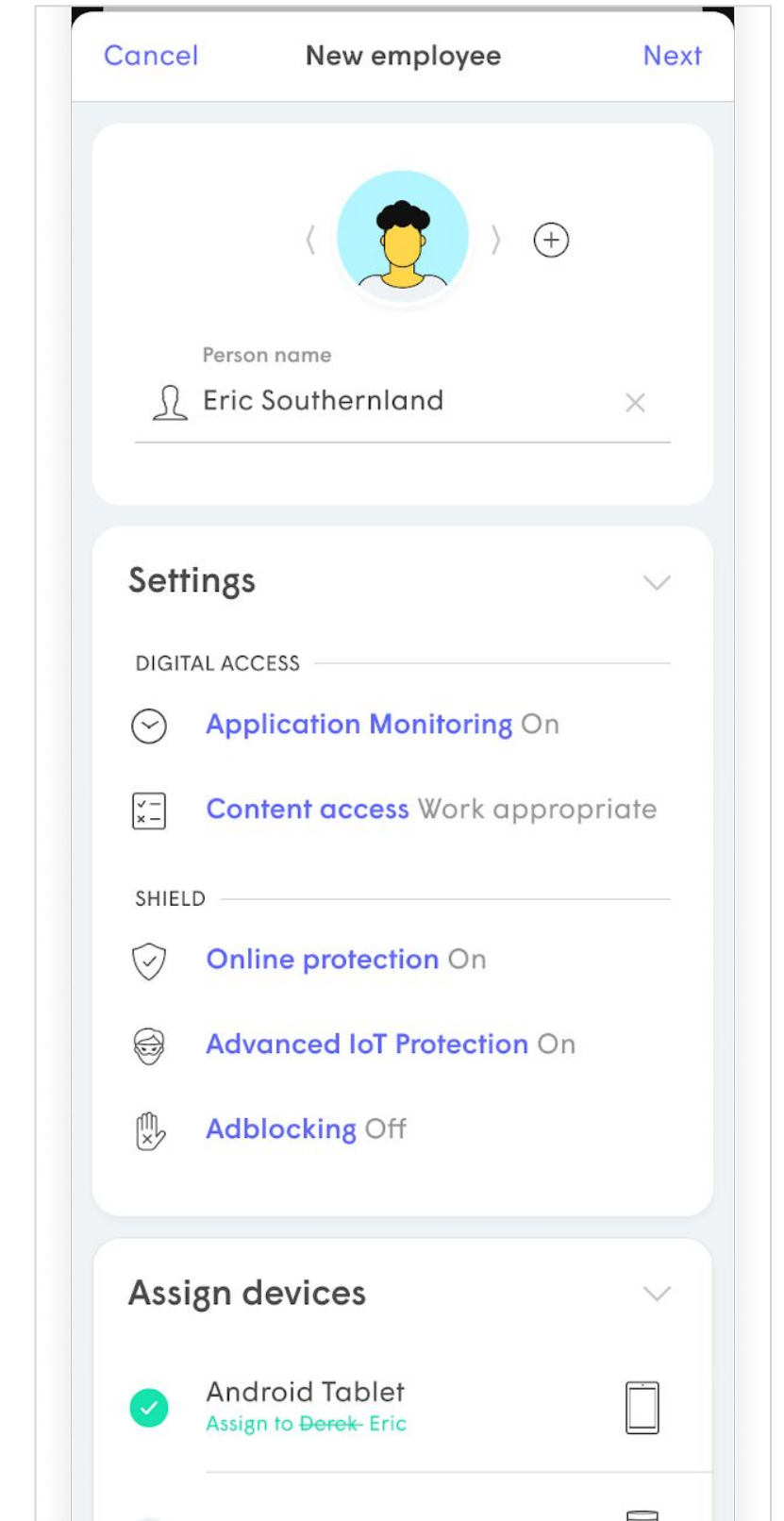
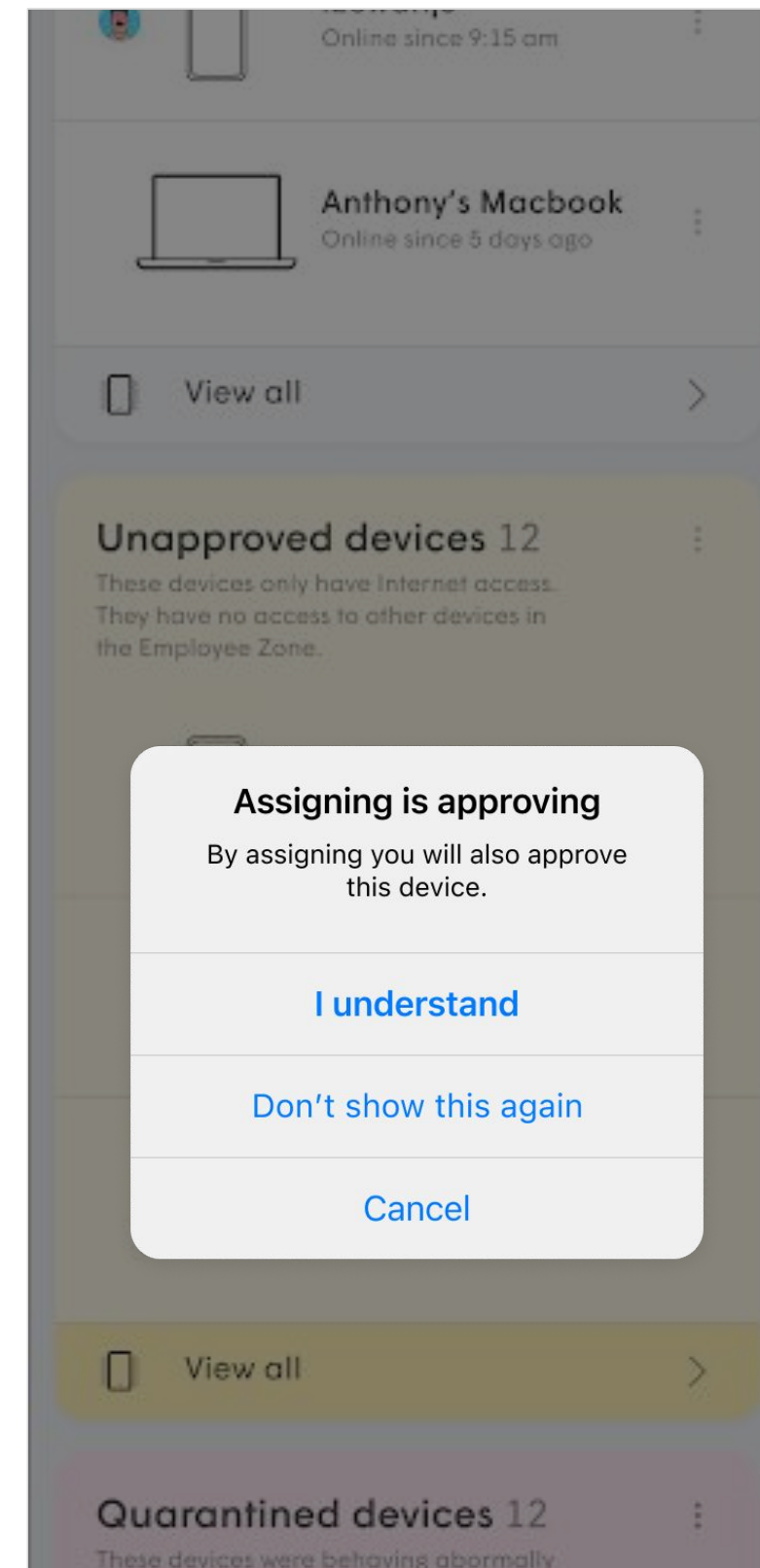
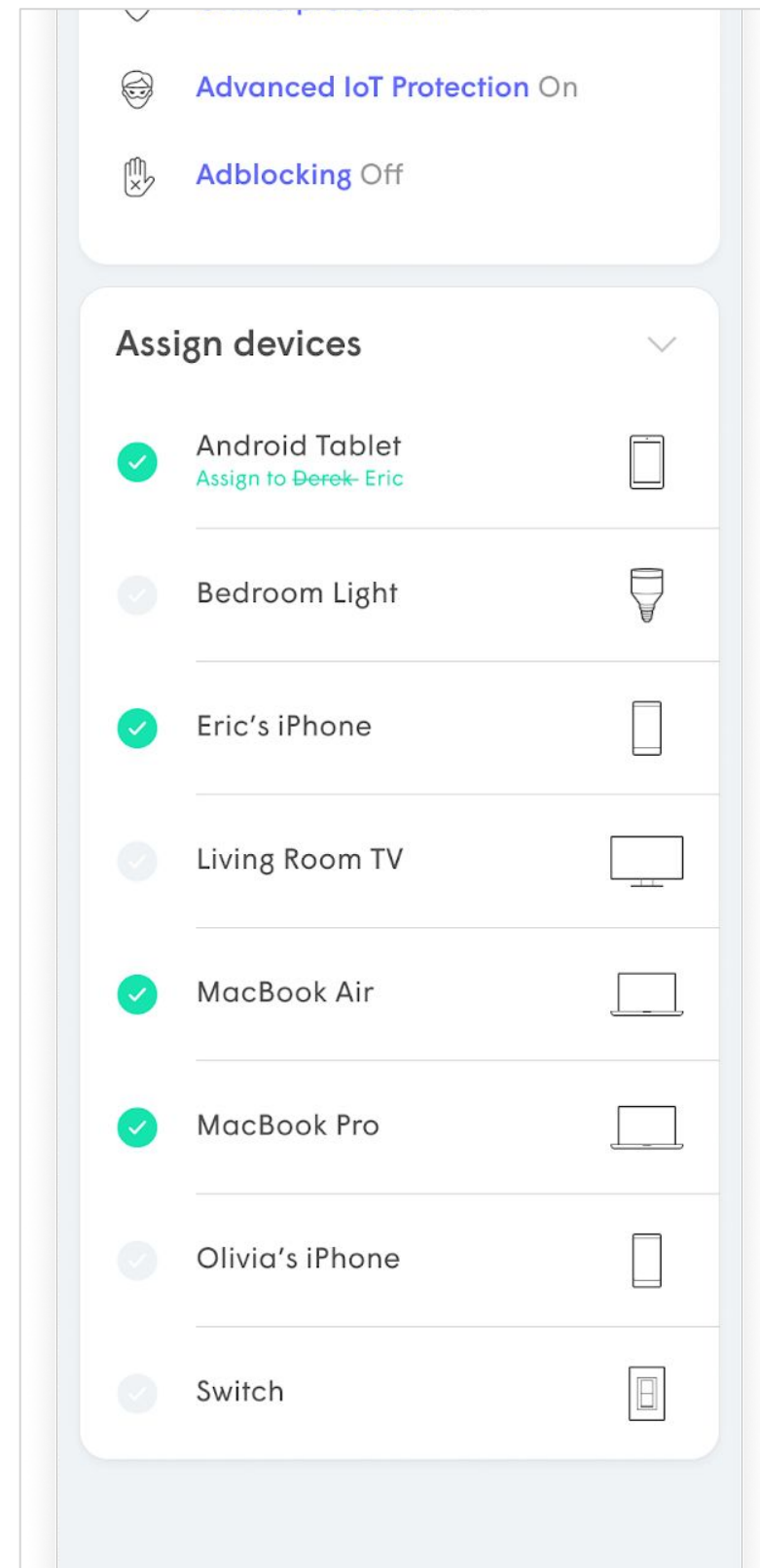
Adding Employees

The second step is to **Assign devices** to the new employee.

Additional devices can also be assigned later from the device's options.

Assigning a device from either the **Unapproved devices** list or the **Blocked devices** list to an employee automatically puts it in the **Approved devices** list and removes it from purgatory.

Once a name has been saved and devices assigned, a **Next** button will appear on the top-right.



Managing Employee Wi-Fi

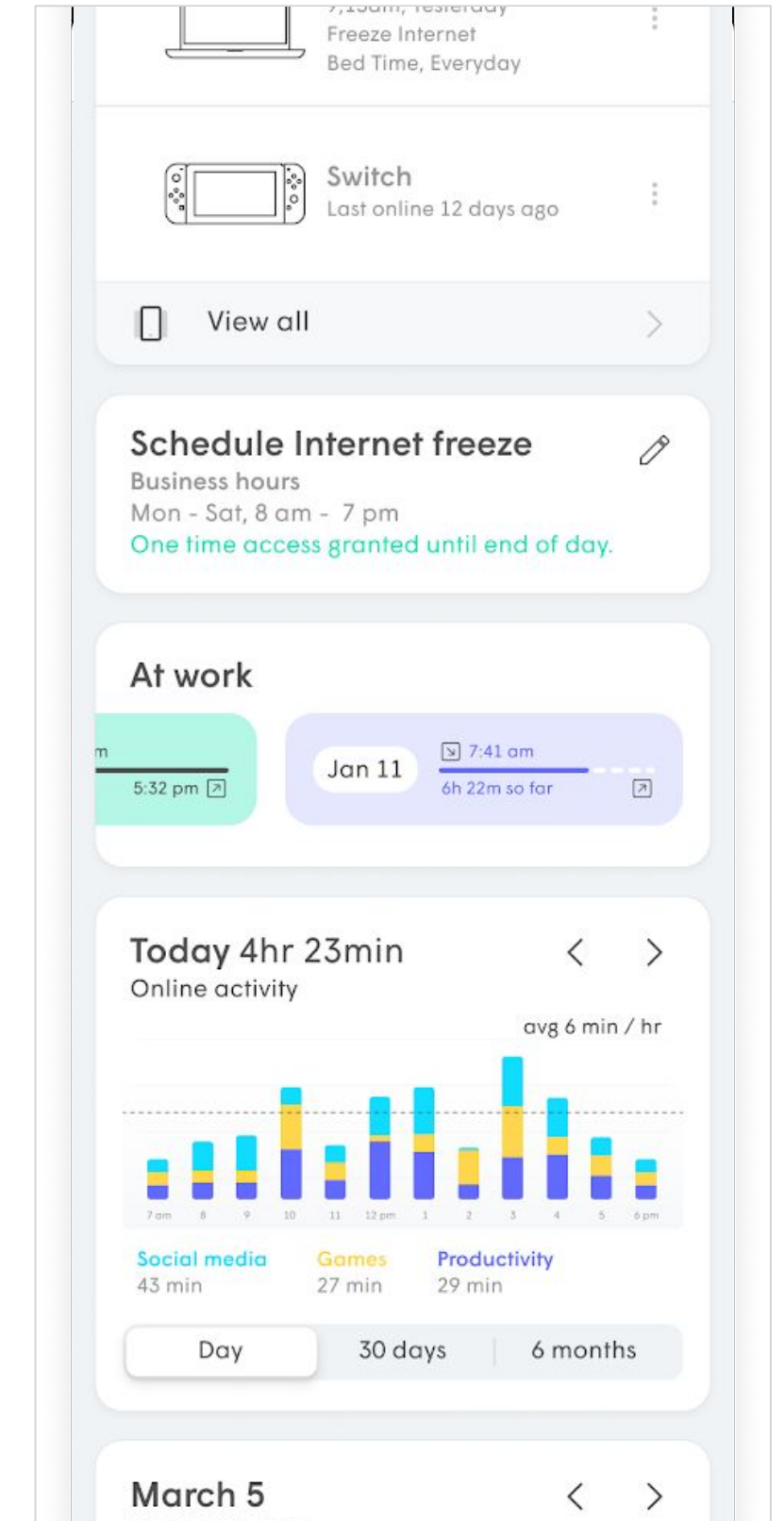
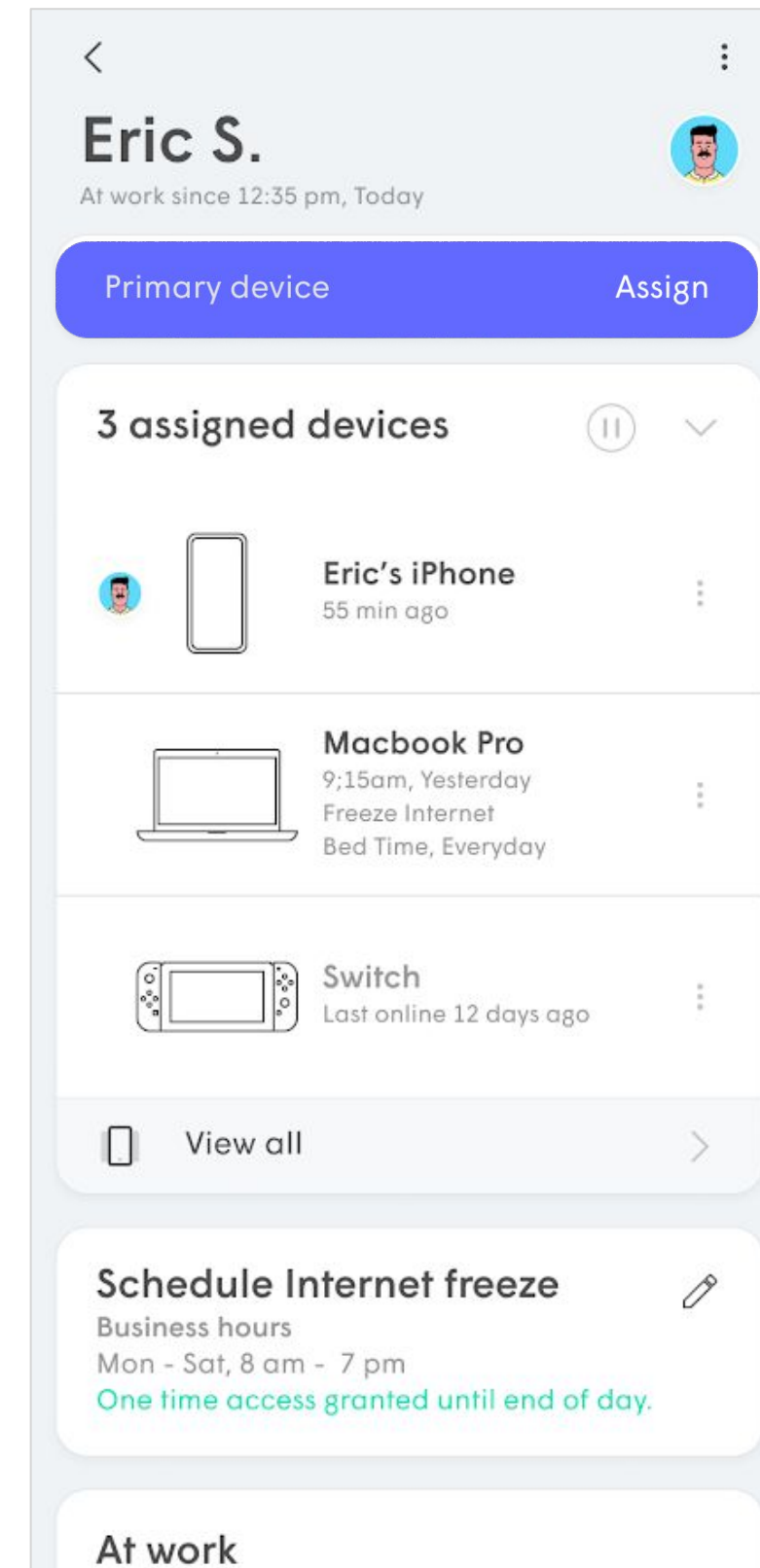
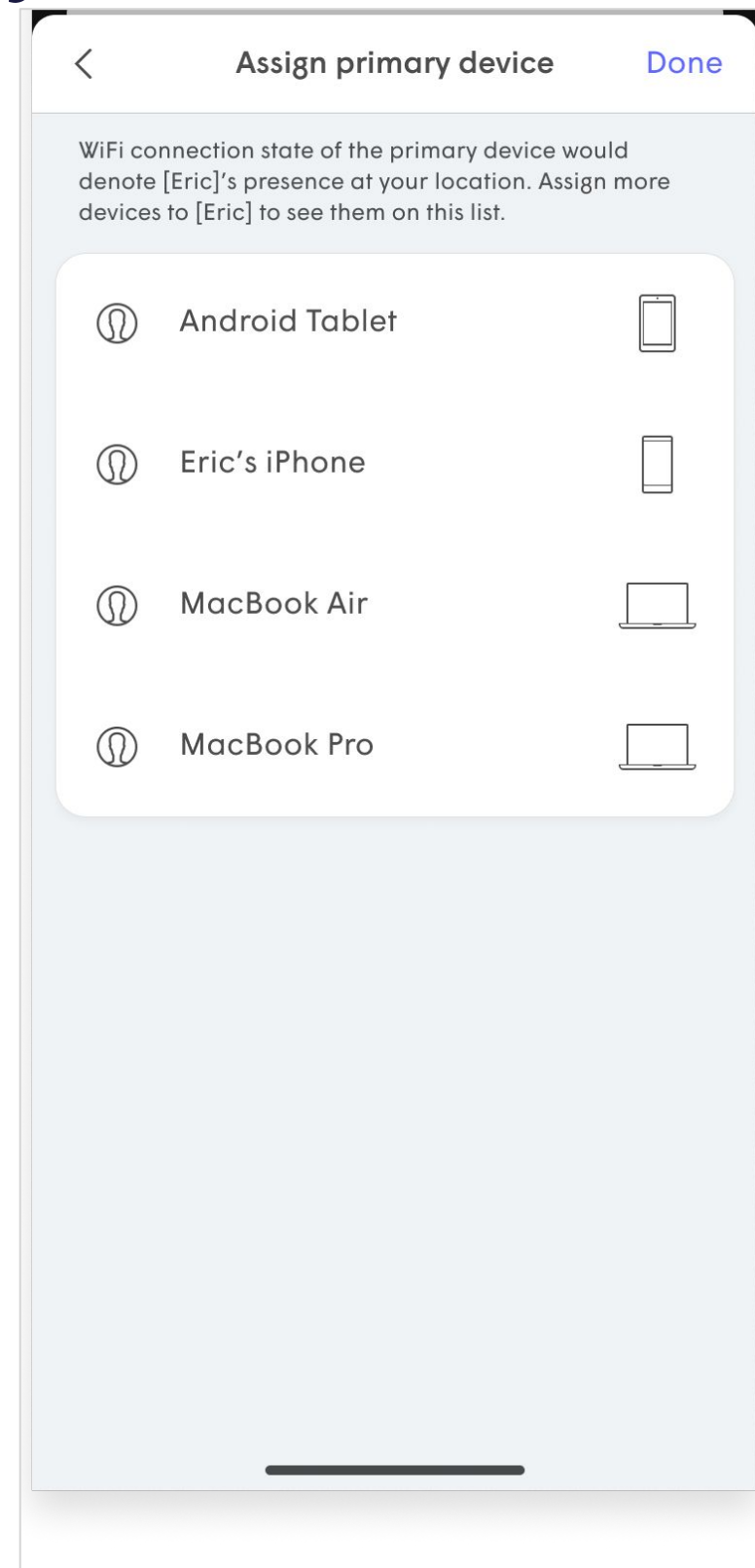
Assigning Employees

After tapping **next** from the New employee flow the admin can now **Assign a primary device** to the employee.

If unassigned during the flow, the **Primary device** can be assigned later from the Employee details screen.

The Primary device is used to determine when the employee is **at work**.

The day is defined from 12AM to 11:59PM. If an employee is working a shift that overlaps the end of day cutoff, they will be shown leaving at 11:59 PM and returning at 12 AM again.



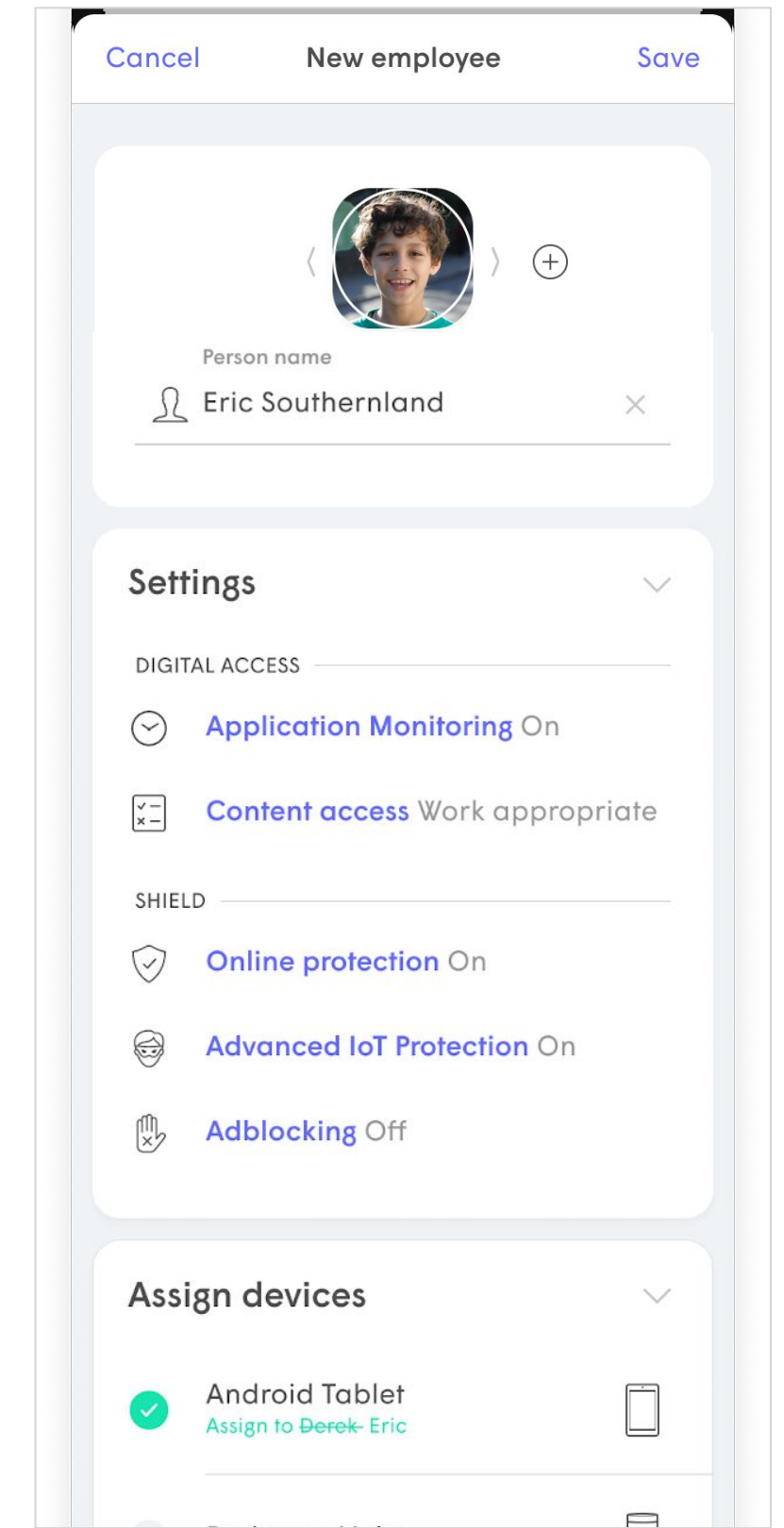
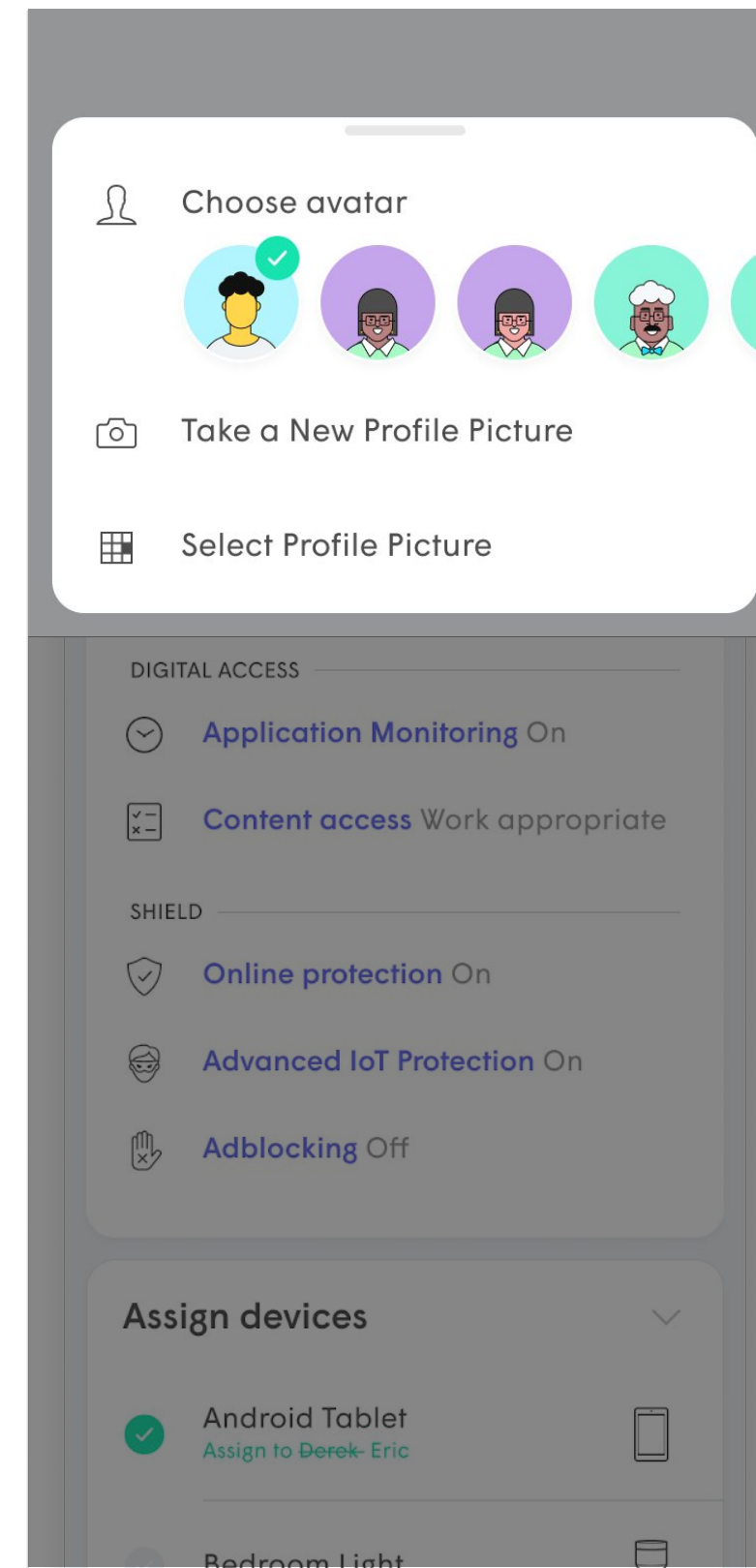
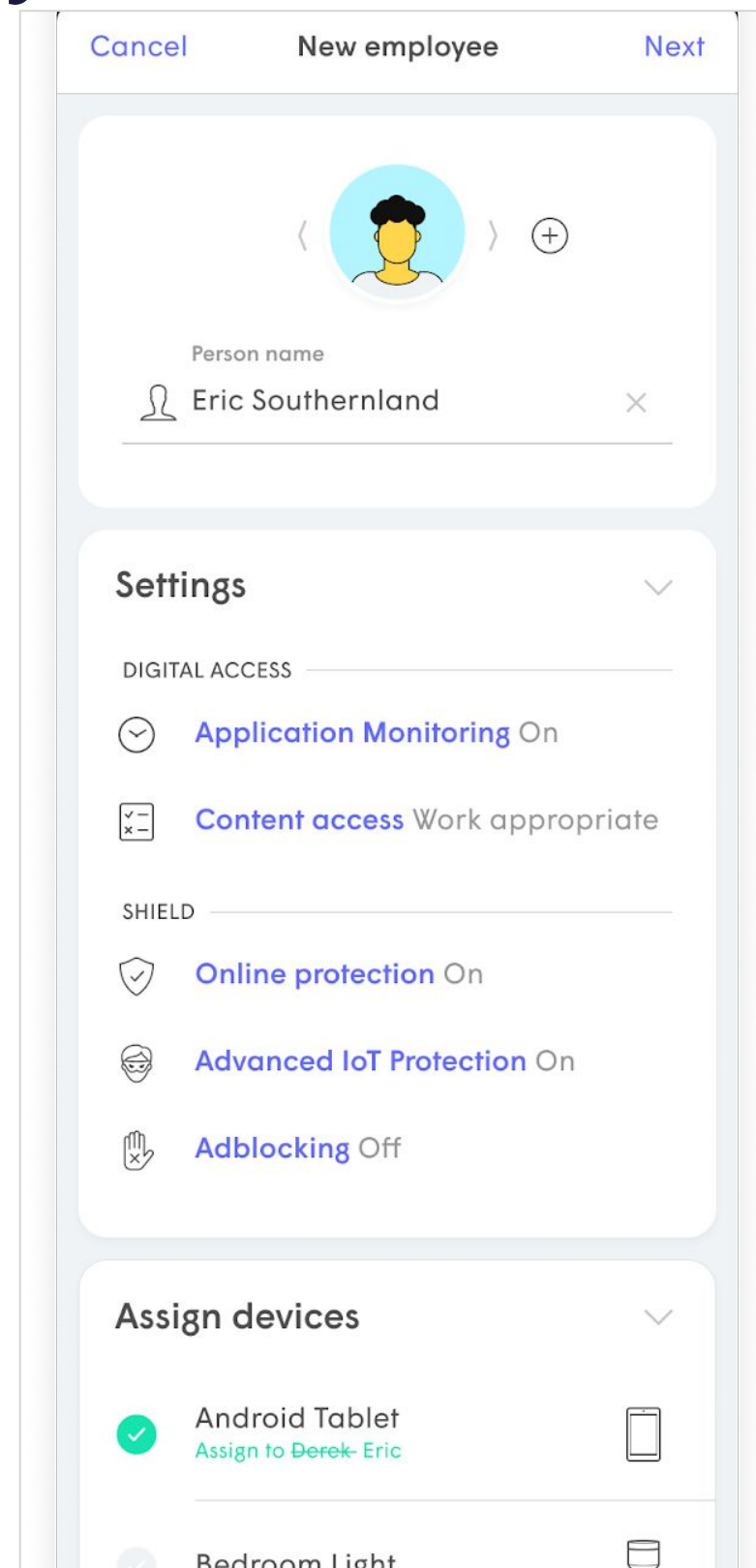
Managing Employee Wi-Fi

Assigning Employees

One of 16 generic avatars will be assigned automatically. Swiping right on the avatar will let the user choose from a further 80 more specific avatars that are available.

Tapping on the + will allow the user to choose to either **Take a New Profile Picture** or **Select Profile picture** from the device's photo gallery app.

Once the name and image have been **saved**, tapping on **Next** will bring up Primary device assignments.



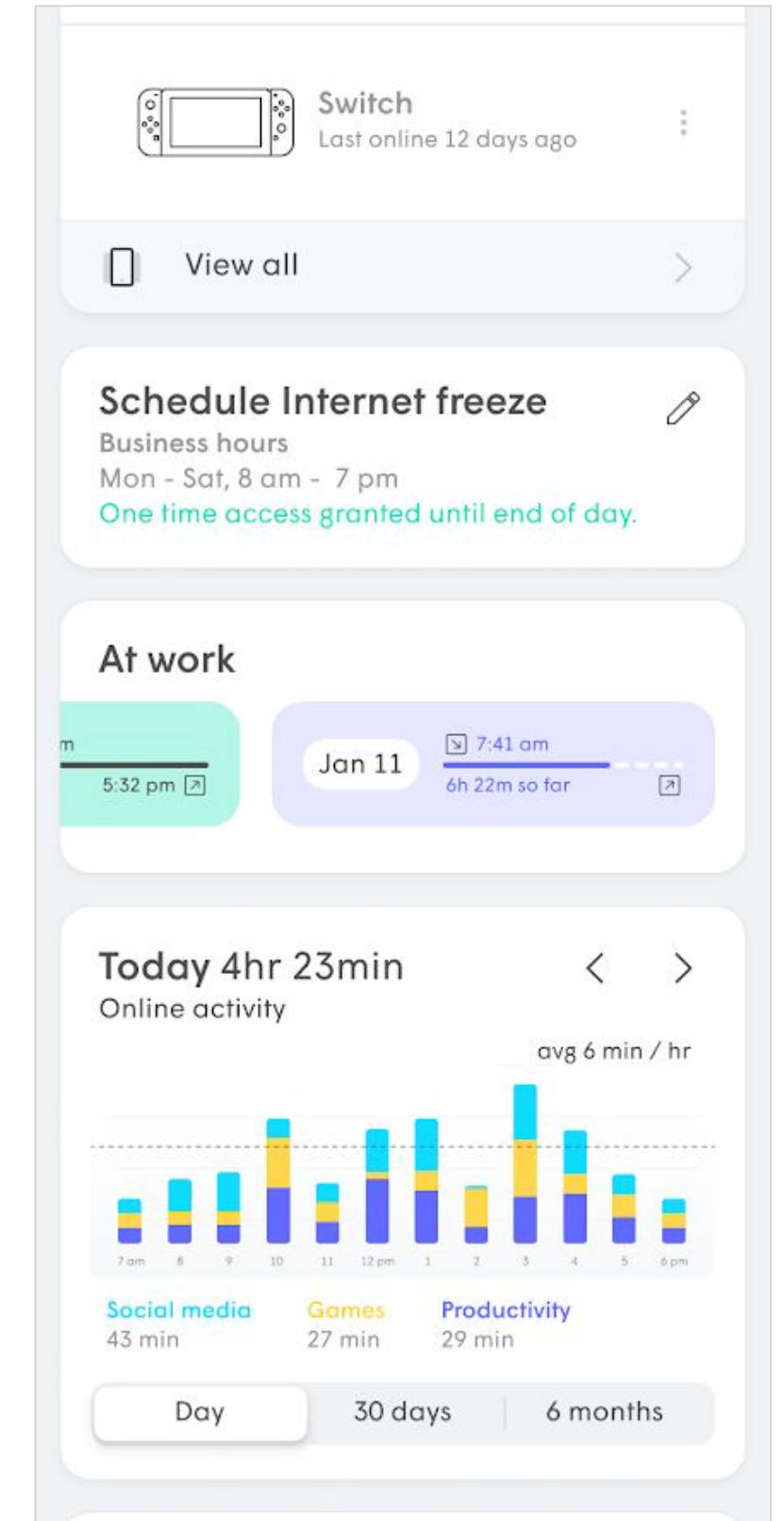
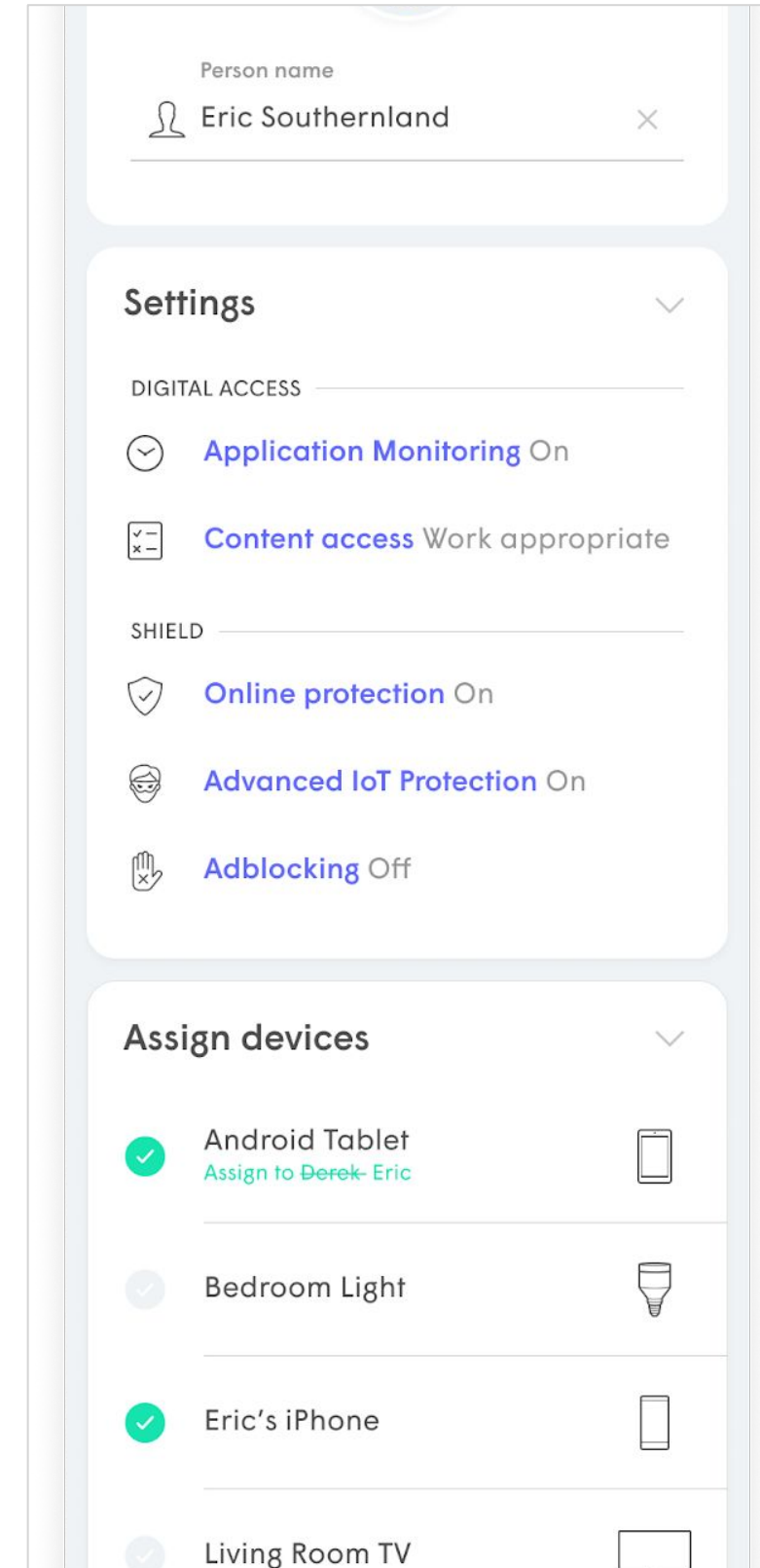
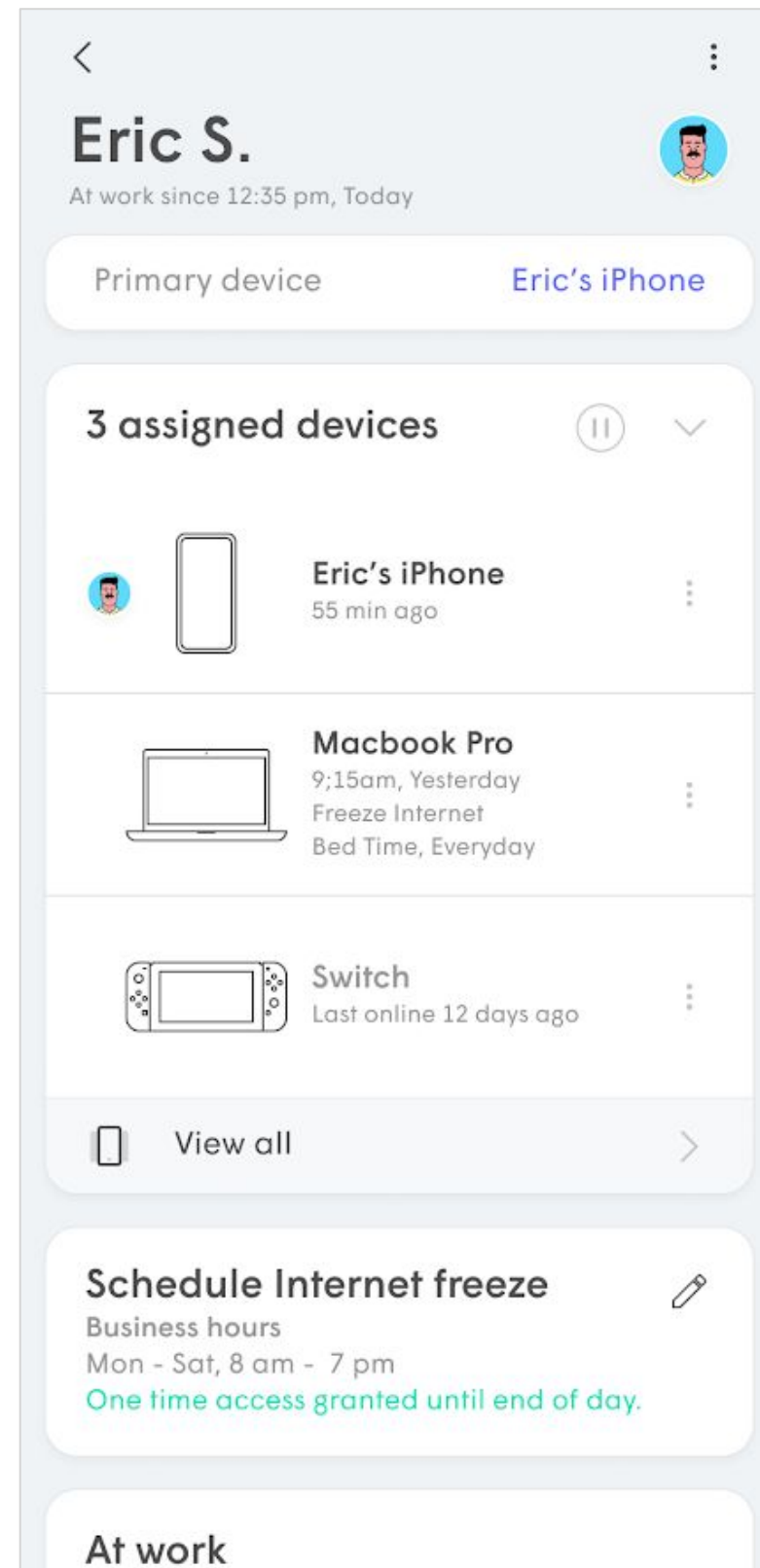
Managing Employee Wi-Fi Employee Options

Once the employee has all their devices assigned, additional employee settings can be configured.

Secure zone devices can be shared with the employee.

Shield features including **Online Protection** and **Adblocking** can now be applied at the Employee's level

Internet Freeze can be applied.



Managing Guest Access

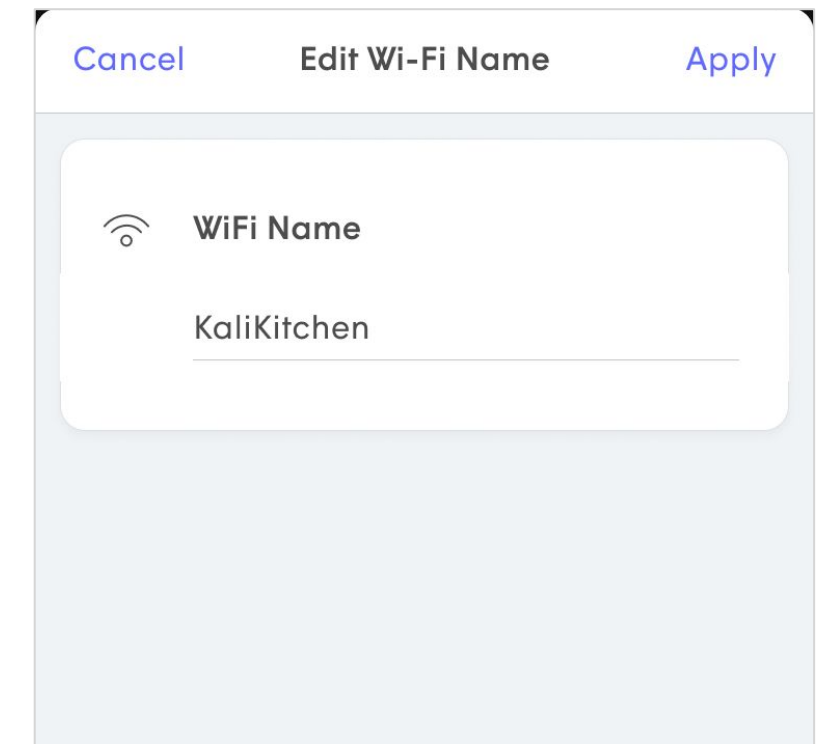
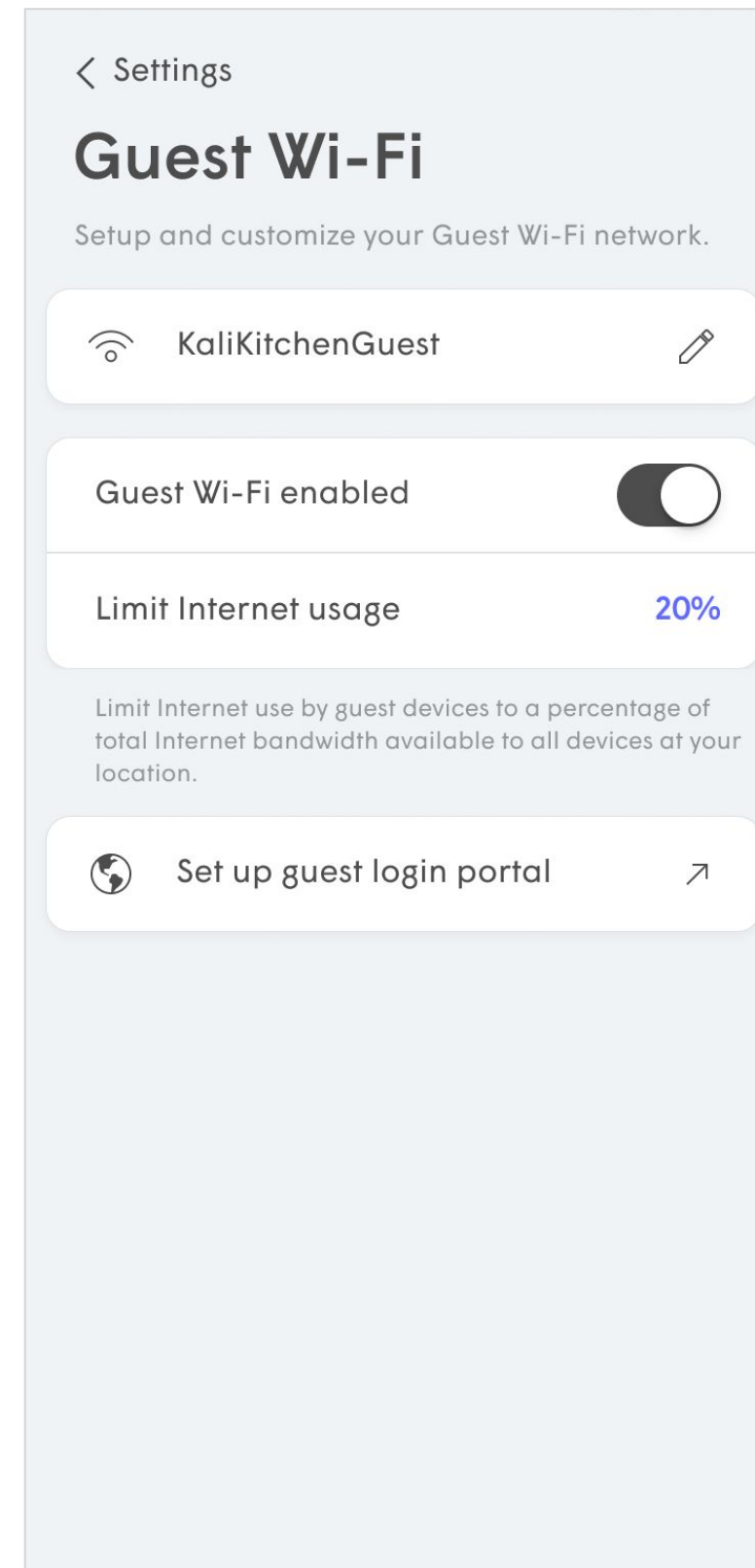
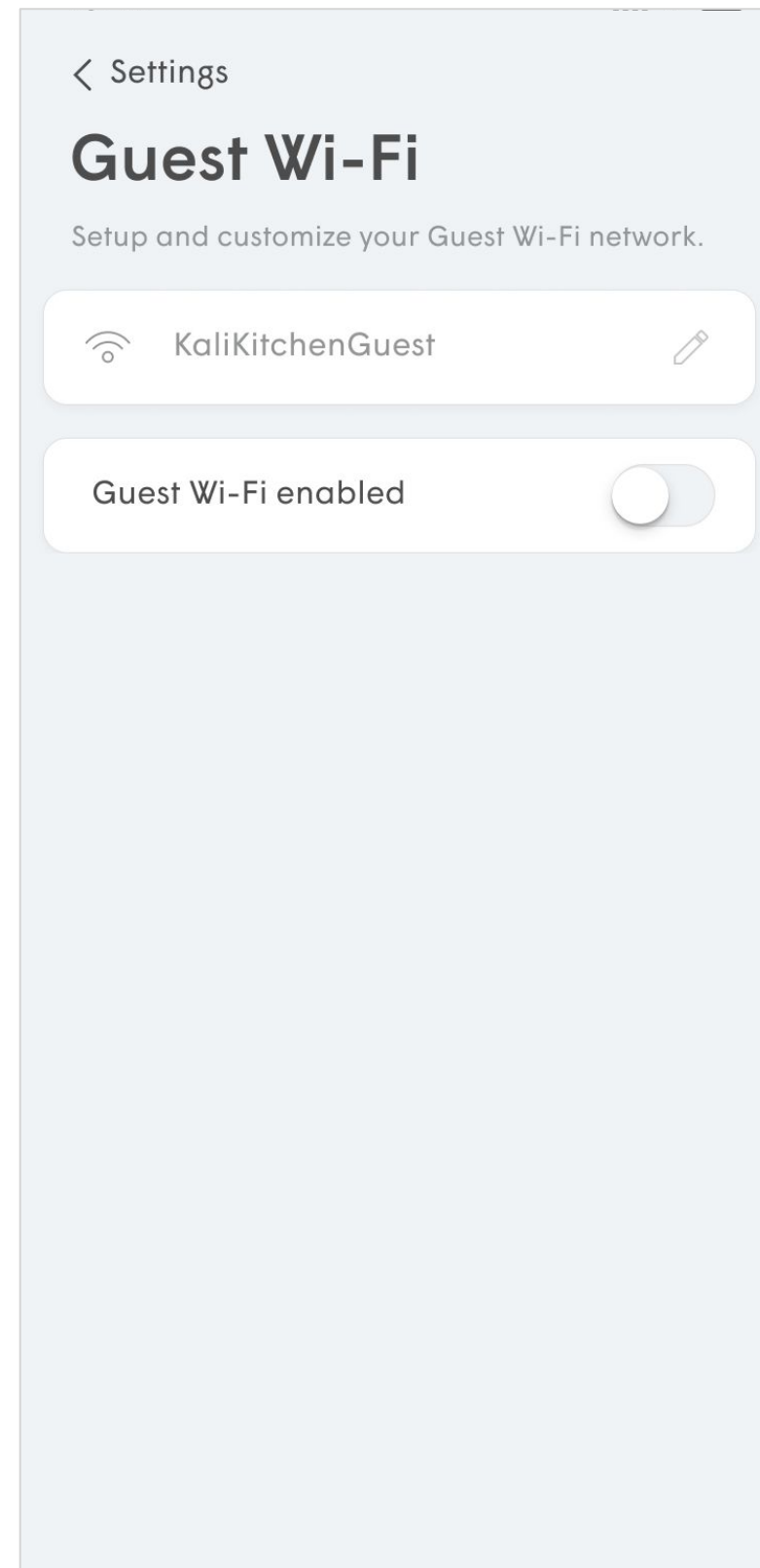
Managing Guest Access

Guest Passwords

If the Guest network was not set enabled during the initial setup, it can be created afterwards from **Settings**.

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

Unlike The Secure Wi-Fi and Employee Wi-Fi zone, the Guest Wi-Fi zone does not use a password. Guests use a captive portal which provides the device a token. You must **Set up guest login portal** before your guest can use the Wi-Fi.



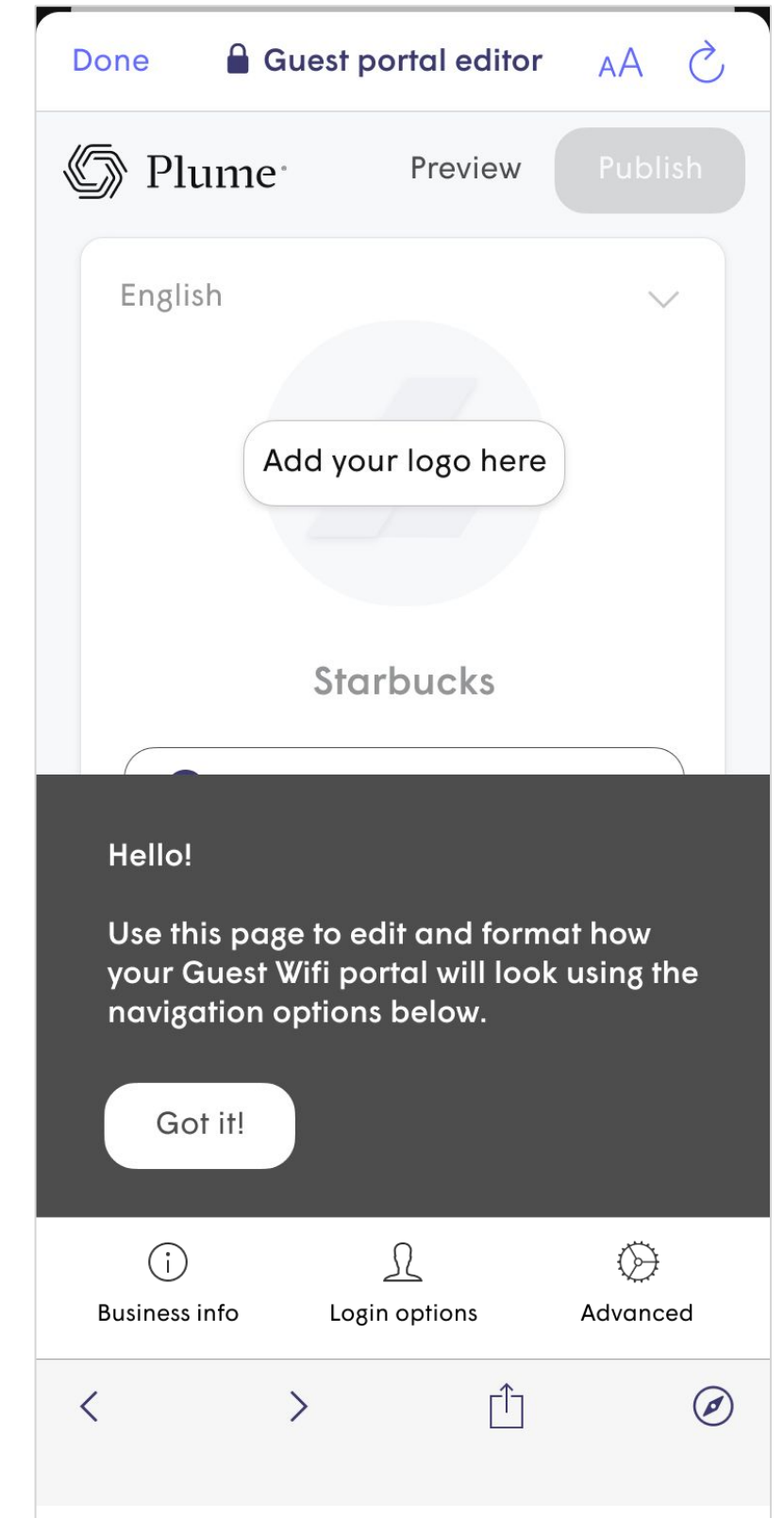
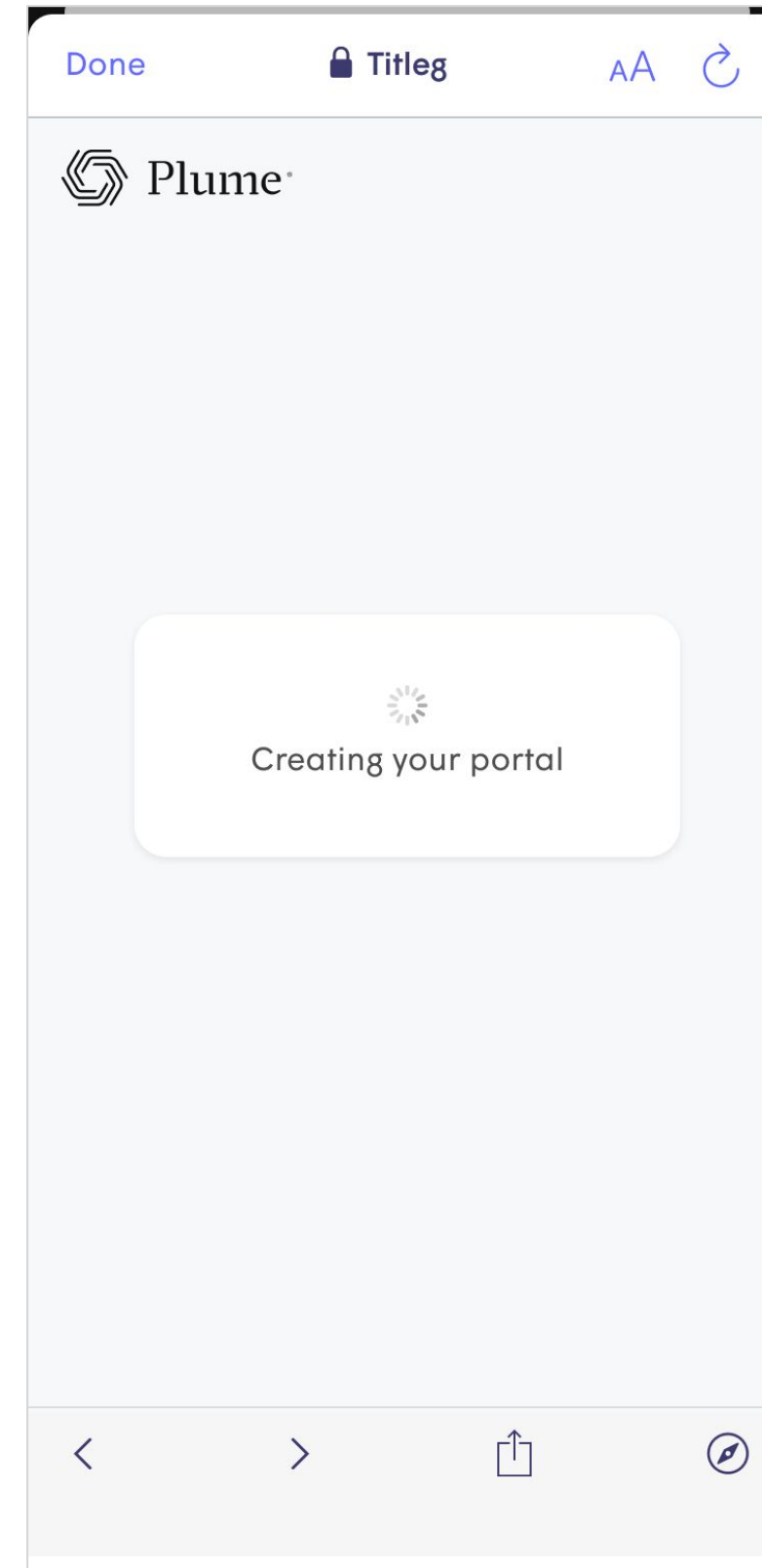
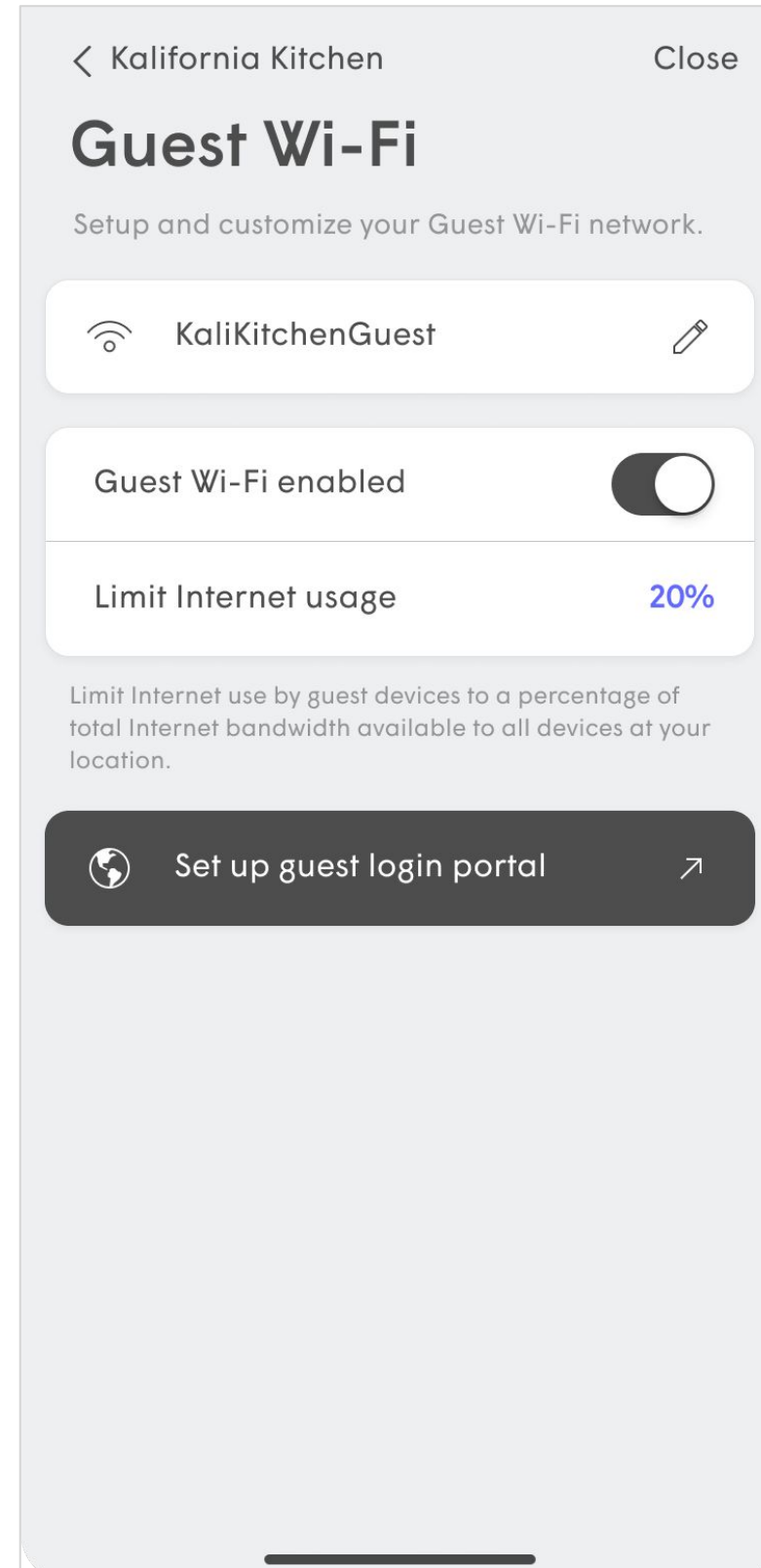
The **Limit Internet usage** percentage is a percentage of the bandwidth available and is based on the average of the last 3 days of Speed Test results and It does not limit data consumption. If enabled, speed is throttled at the Gateway.

Managing Guest Access

Guest Portal Setup

Unlike The Secure Wi-Fi and Employee Wi-Fi zone, the Guest Wi-Fi zone does not use a password. Guests use a captive portal. You must **Set up guest login portal** before your guest can use the Wi-Fi.

The set up process of the portal will open a new browser window.



Managing Guest Access

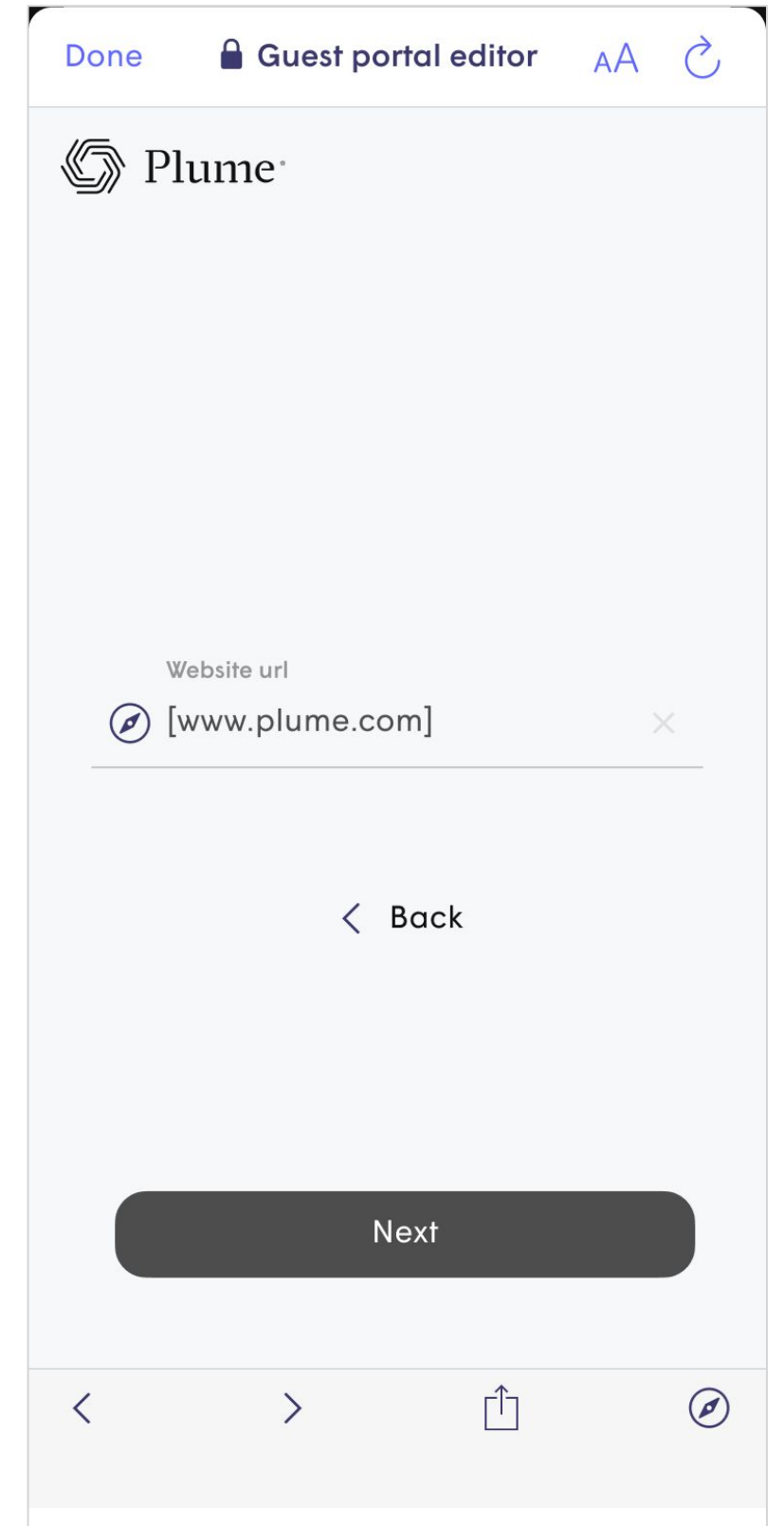
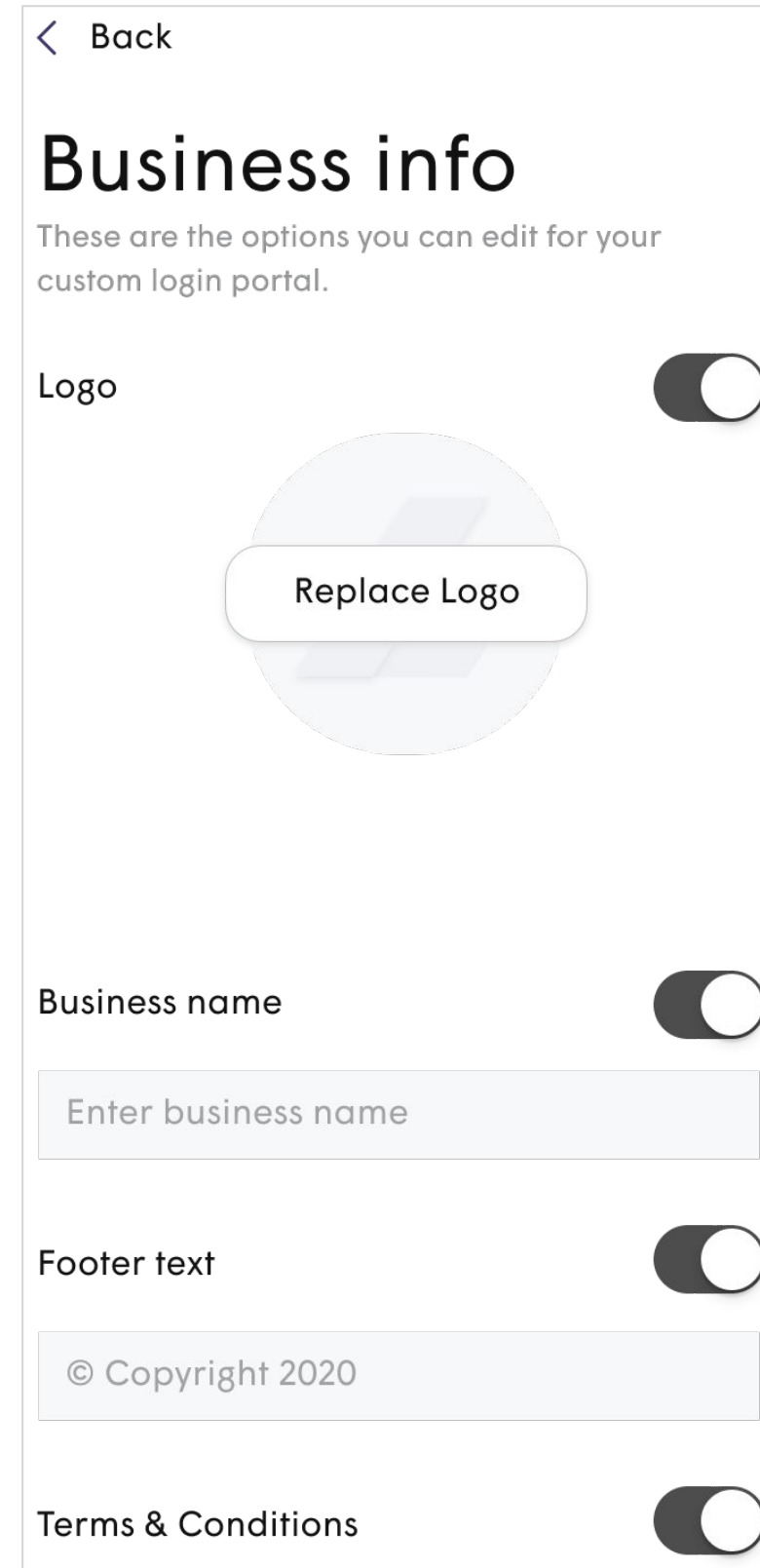
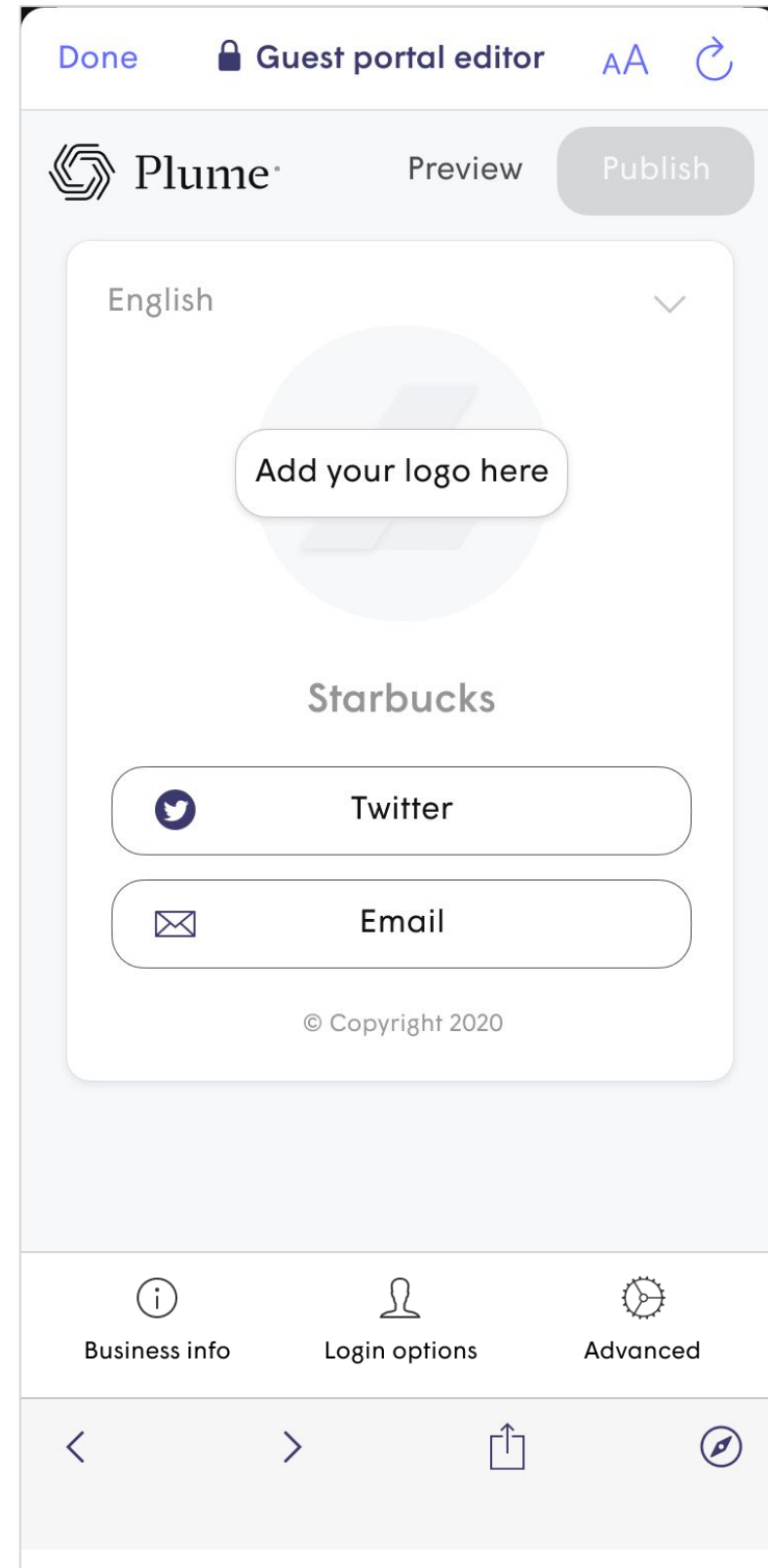
Guest Portal Setup

The first step will be to enter the Business info. This include the **Business name**, **Footer text**, **Logo** and **Terms and conditions**.

If the business has a website or facebook page, the information can be imported from the URL.*

If there is no website, the Logo can be imported from the phone's gallery and the other information entered.

*Not available in initial beta release



Managing Guest Access

Guest Portal Setup

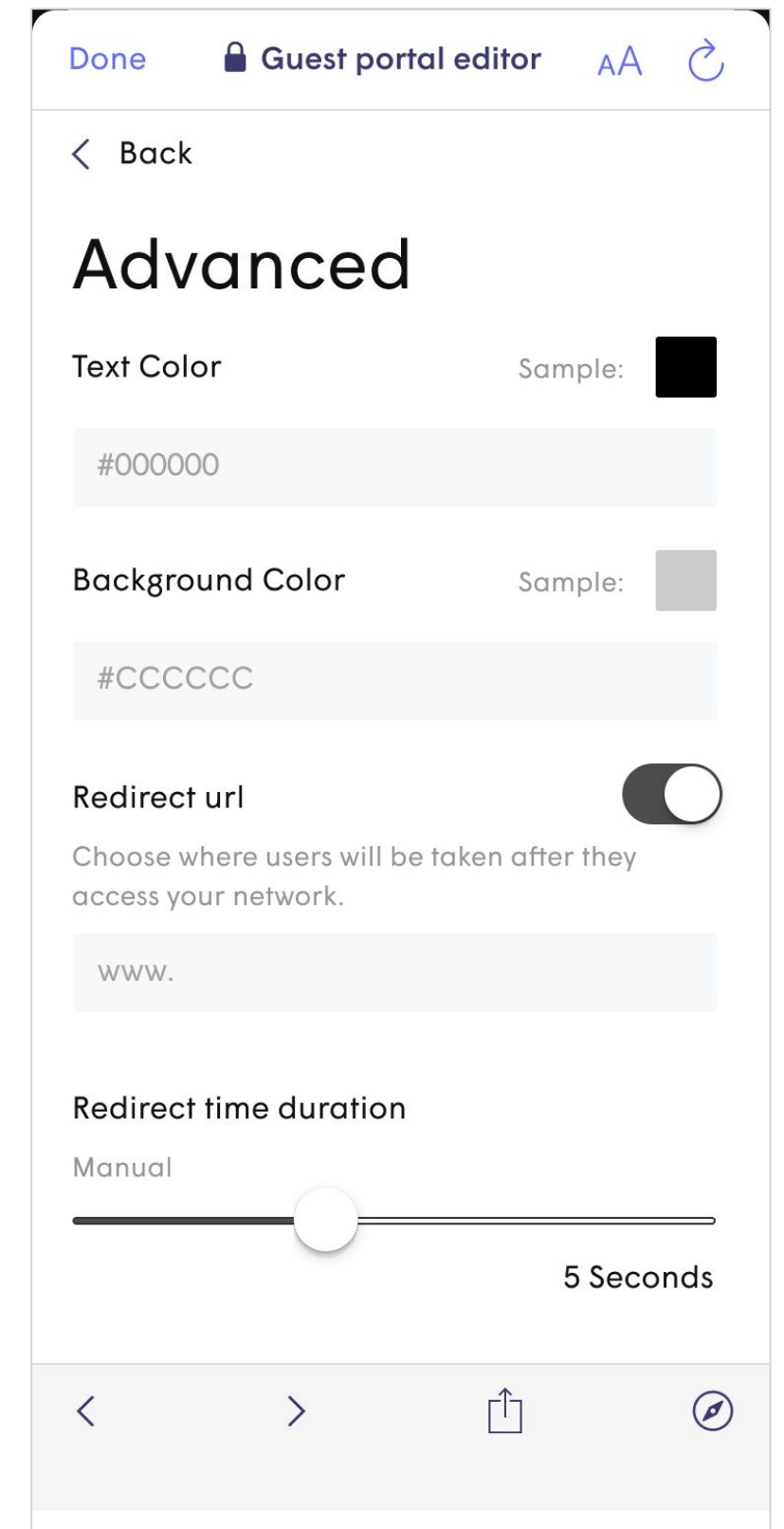
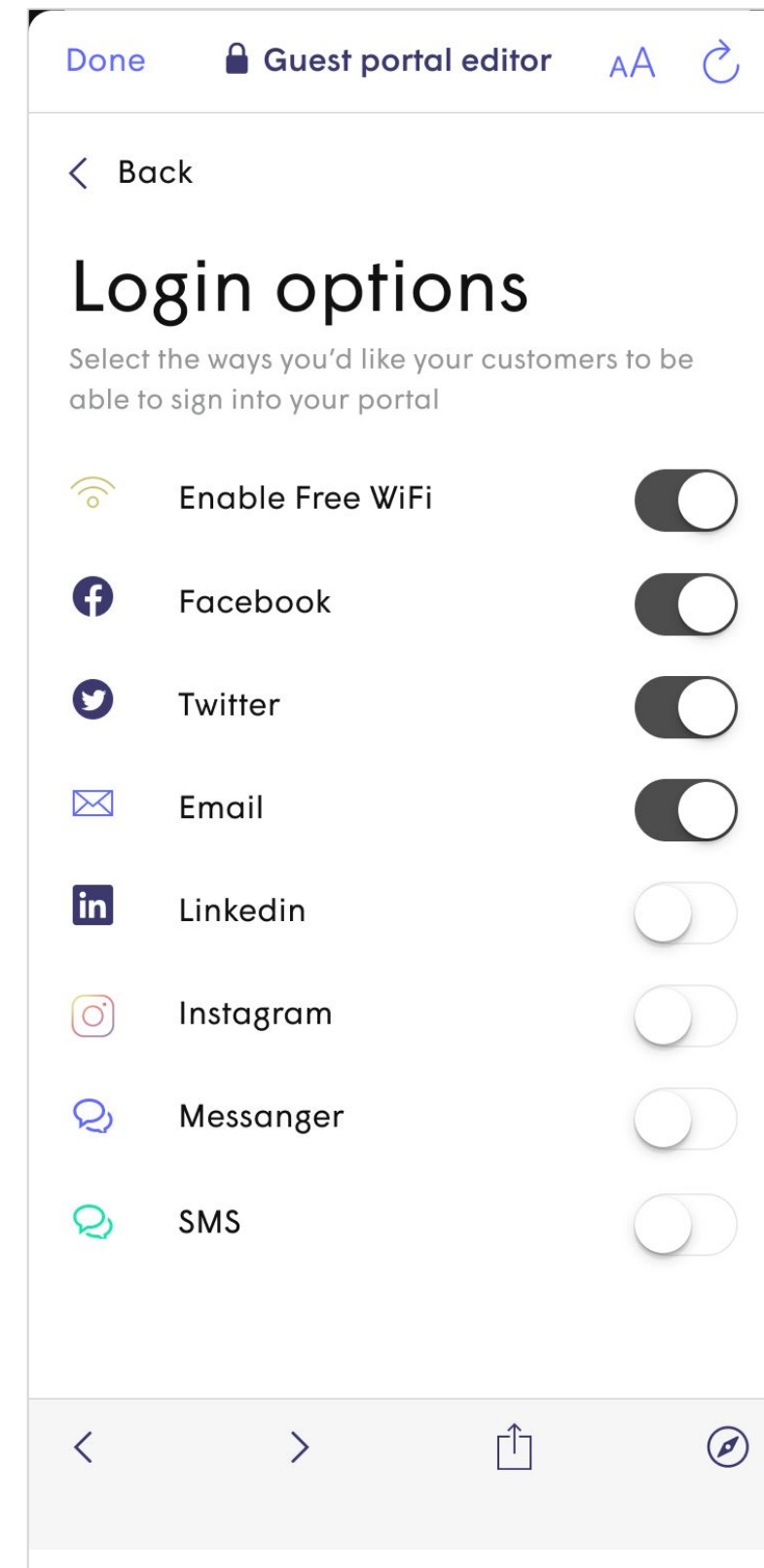
Login options allows the user to choose how the guest can sign into the portal and get internet access.

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

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

Enable Free WiFi and **Facebook** options will be available initially, with other options following in later updates.

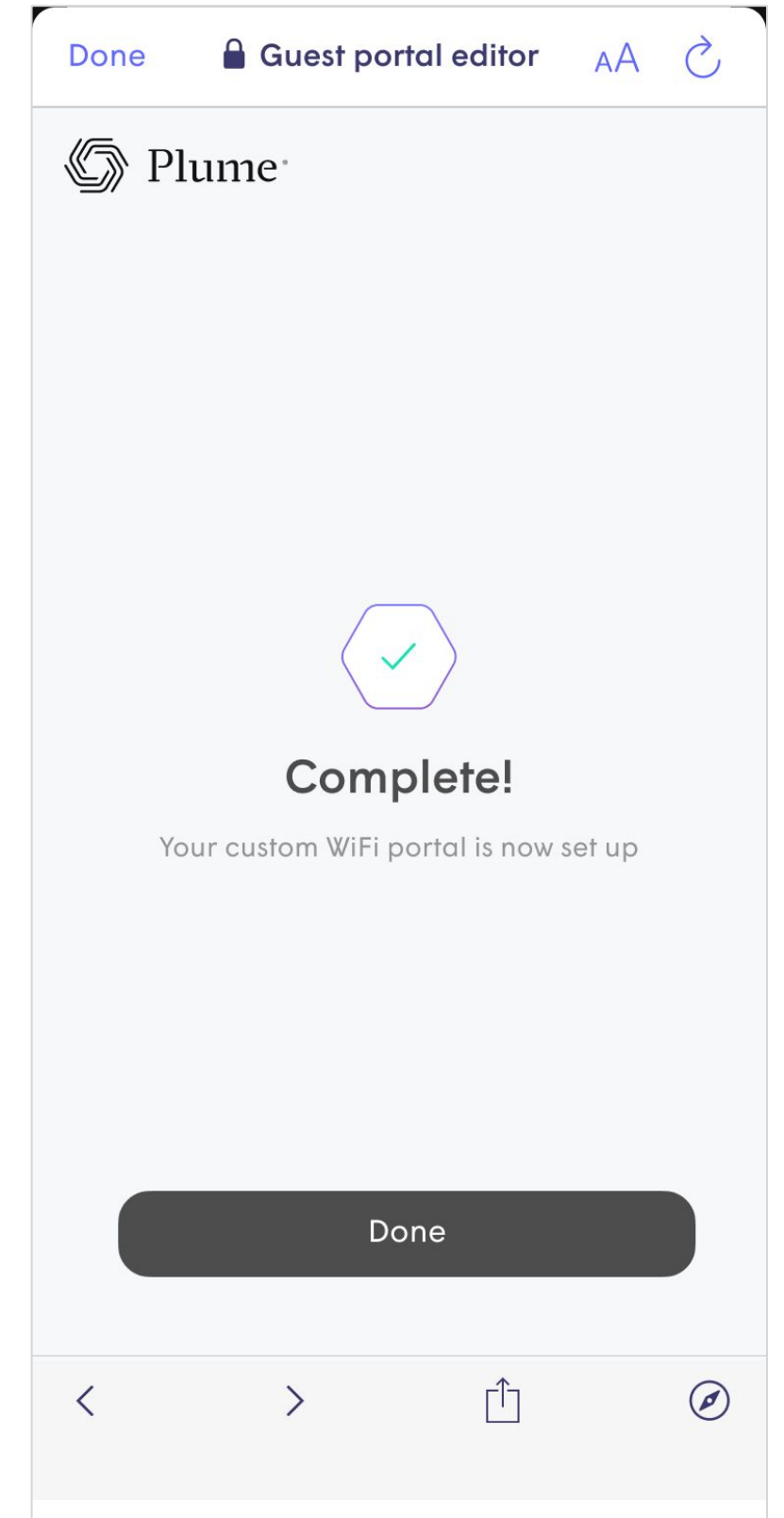
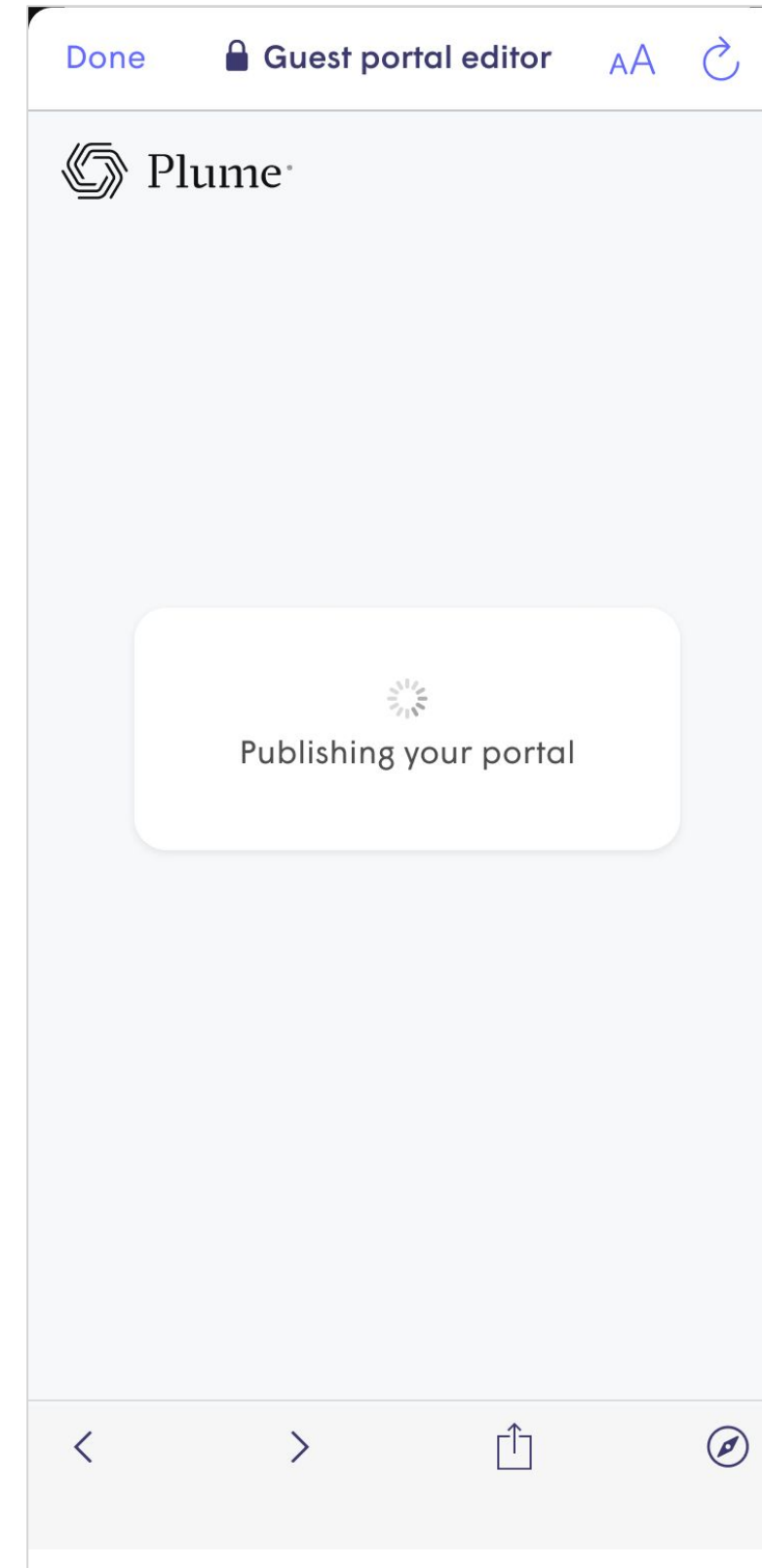
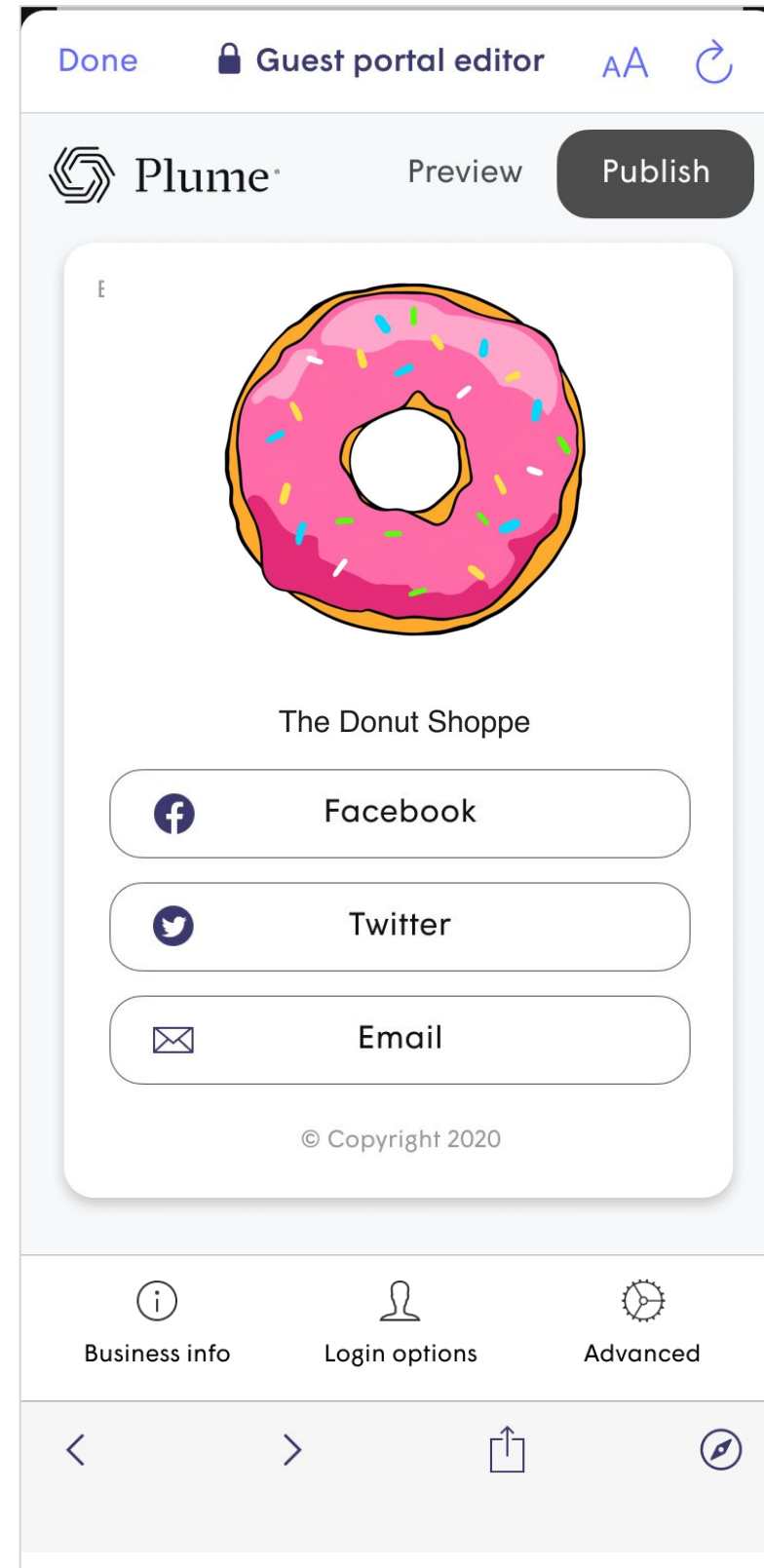
The **Enable Free WiFi** option does not require the guest to register.



Managing Guest Access

Guest Portal Setup

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



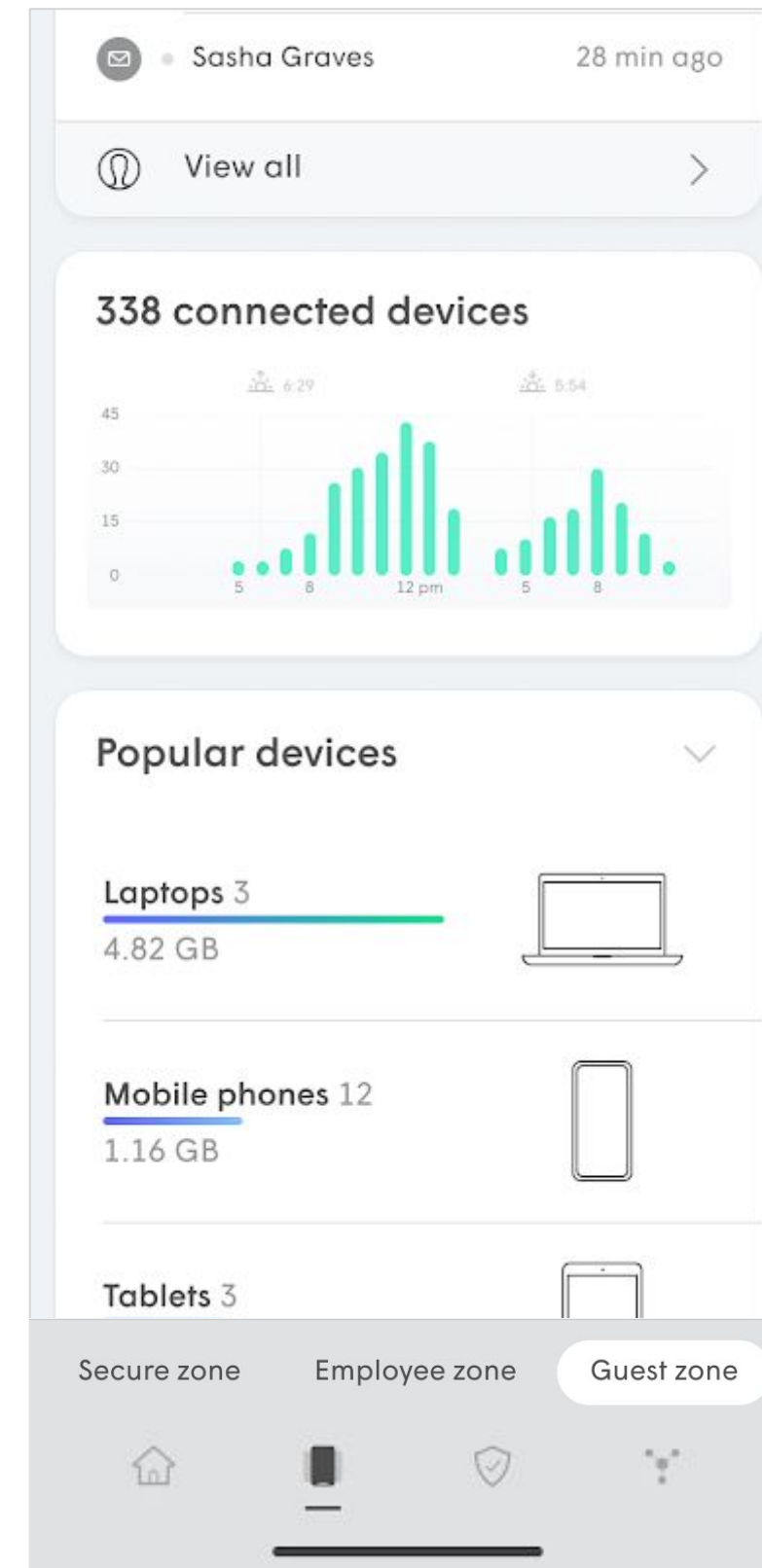
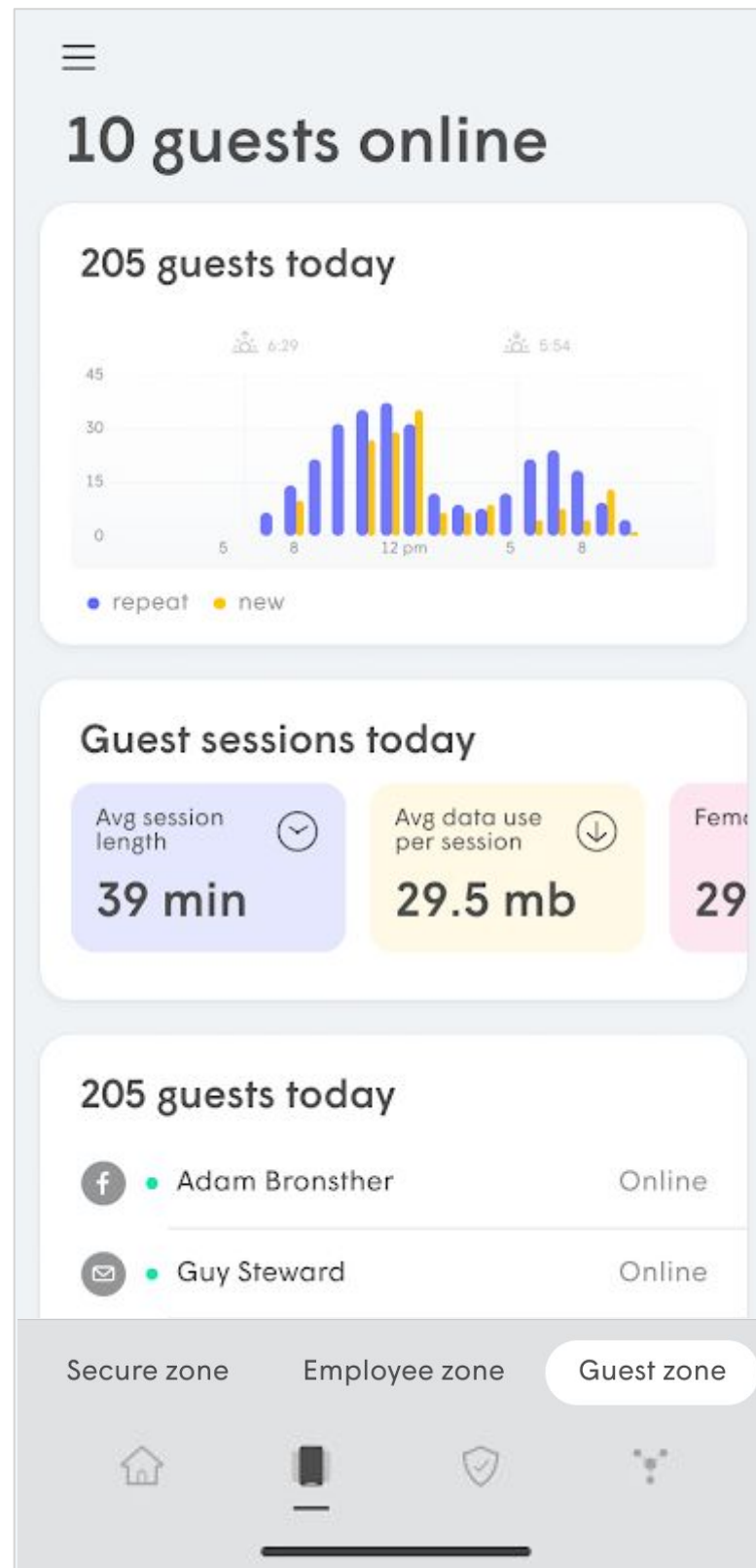
Managing Guest Access

Guest Zone Overview

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

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

The device MAC is used to recognize a device. If the random MAC feature is used, the same device will show again.



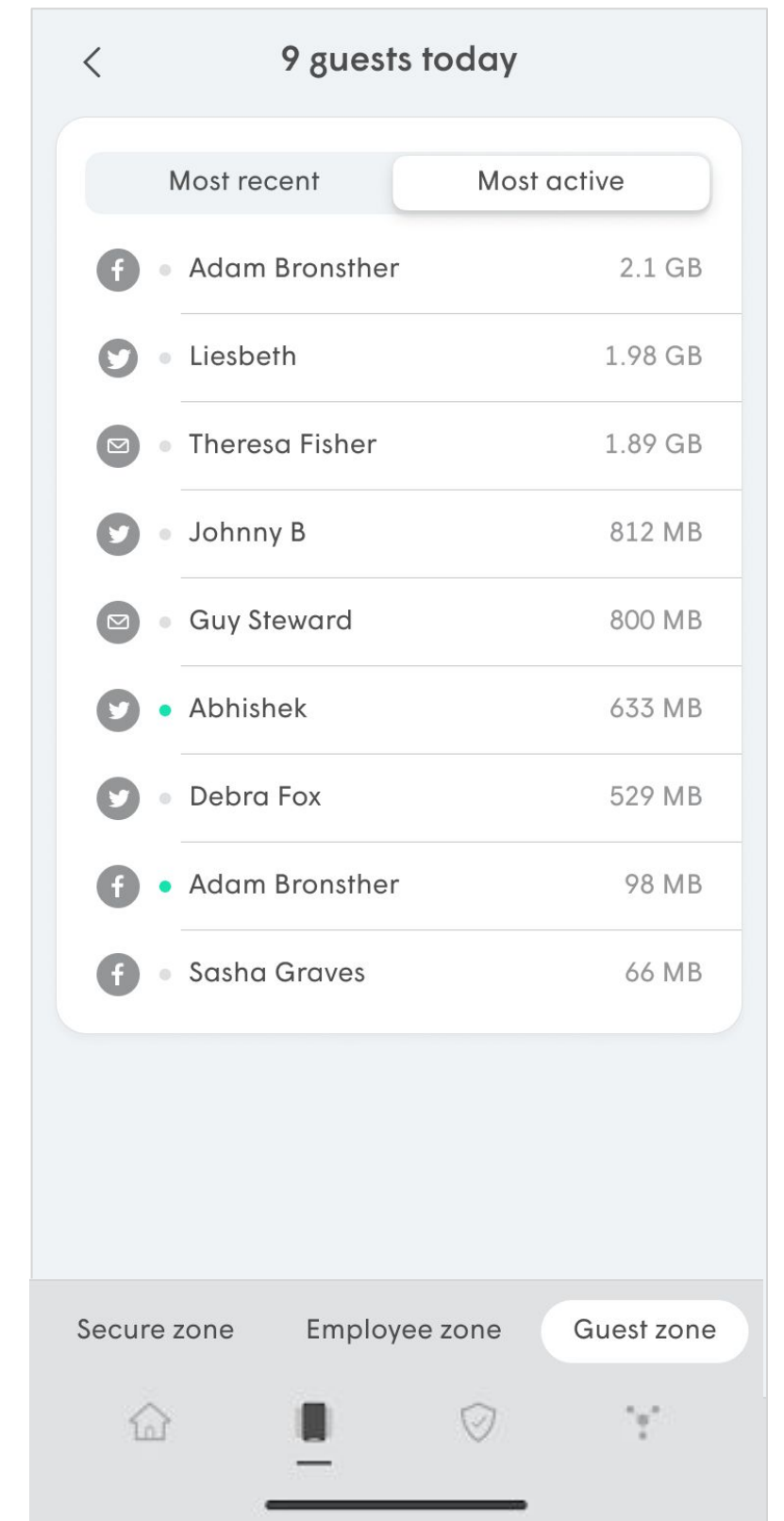
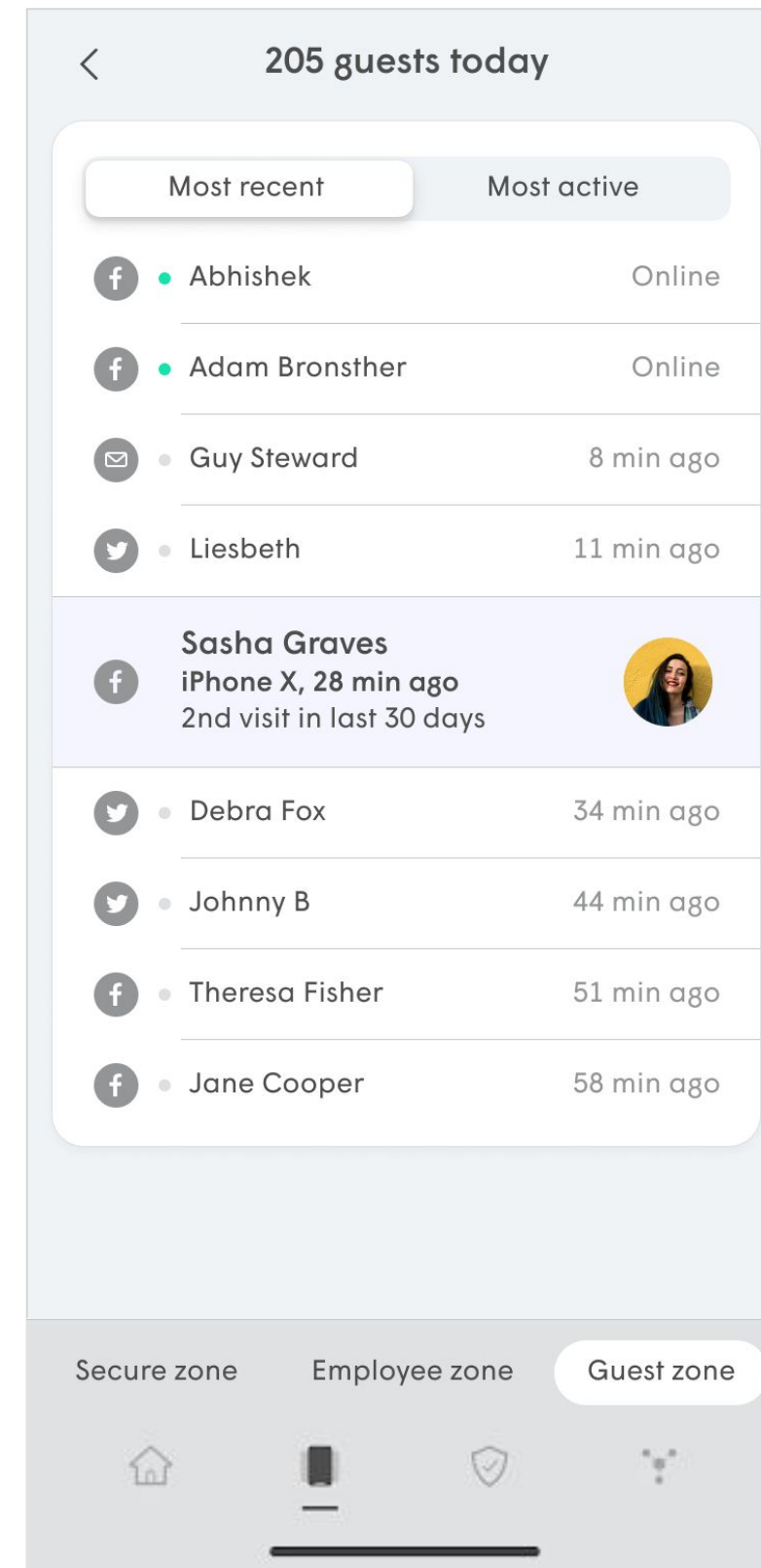
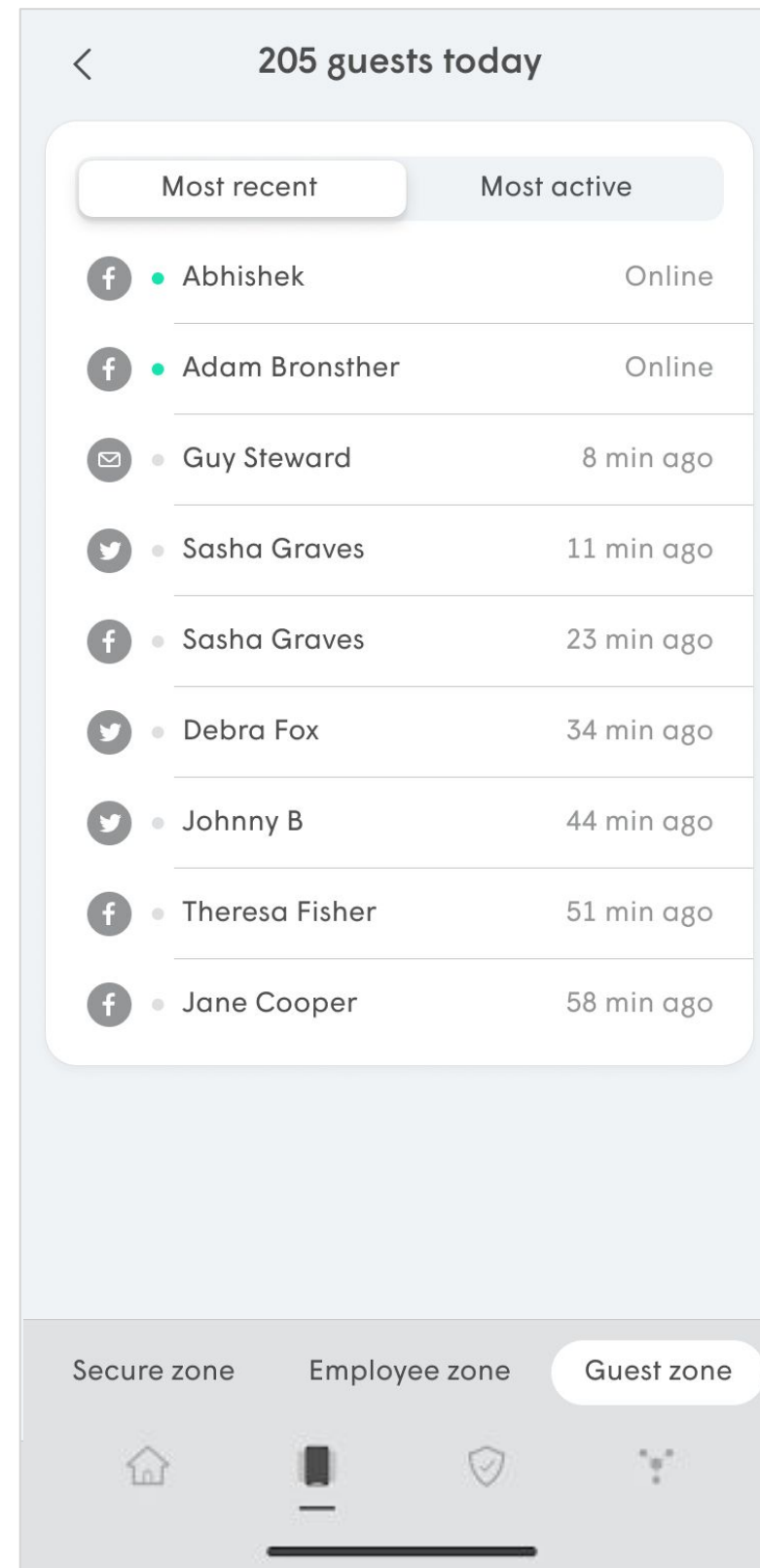
Managing Guest Access

Guest Zone Overview

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

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

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



Plume Shield™

What is Shield™?

When enabled Plume Shield protects your network by preventing access to malicious websites that can harm the devices on your network, without impacting the performance of your browsing experience.

There are three components to Shield:

- **Online Protection** – Enabled at the network, person or device level, Online protection block you devices from accessing known malicious websites.
- **Advanced IoT™ Protection (AIP)** – Advanced IoT™ Protection quarantines smart home devices when we detect unusual behavior. AIP can only be enabled at the network level.
- **Adblocking** – Enabled at the network, person or device level, Adblocker makes your web experience more enjoyable by blocking known advertising servers.



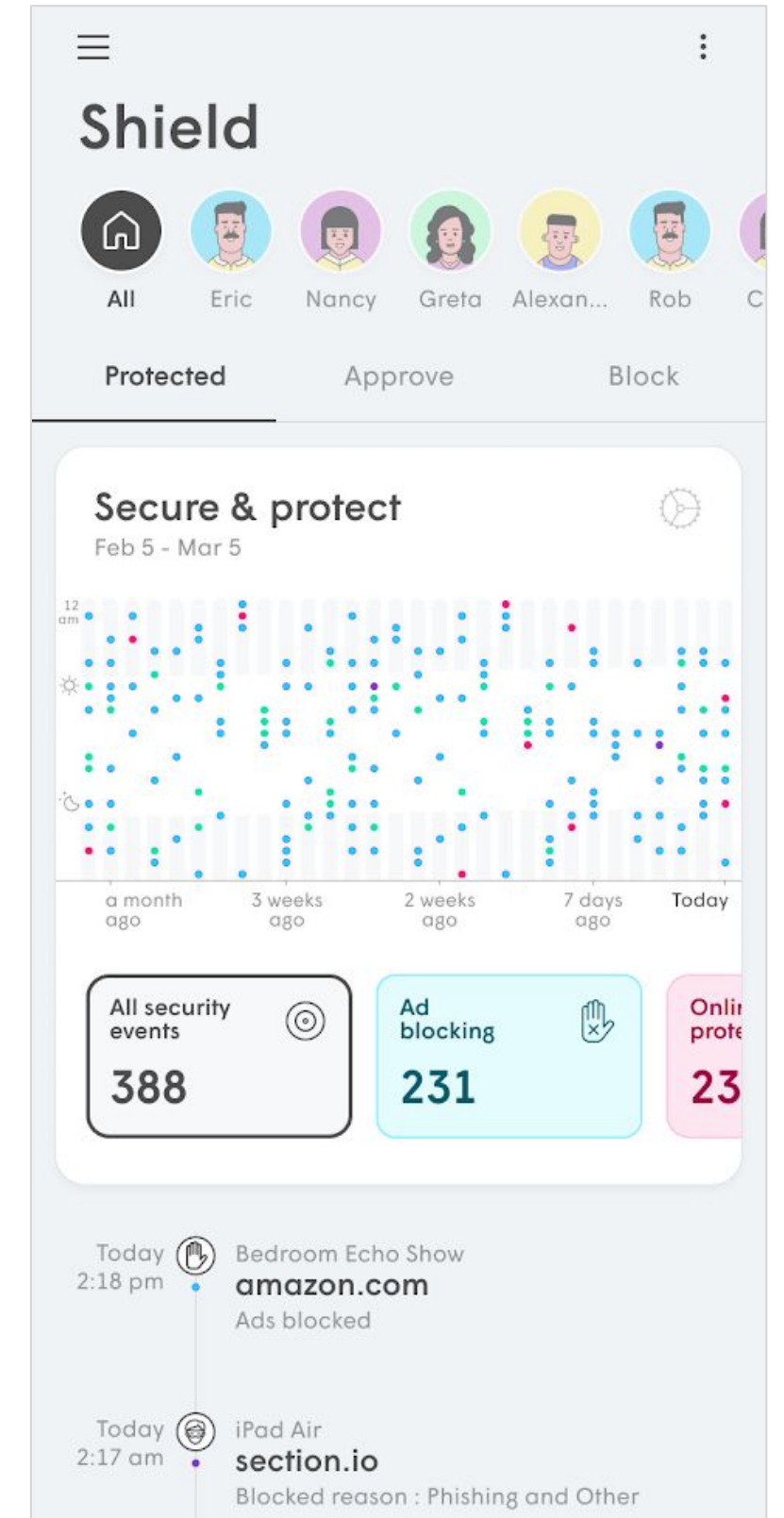
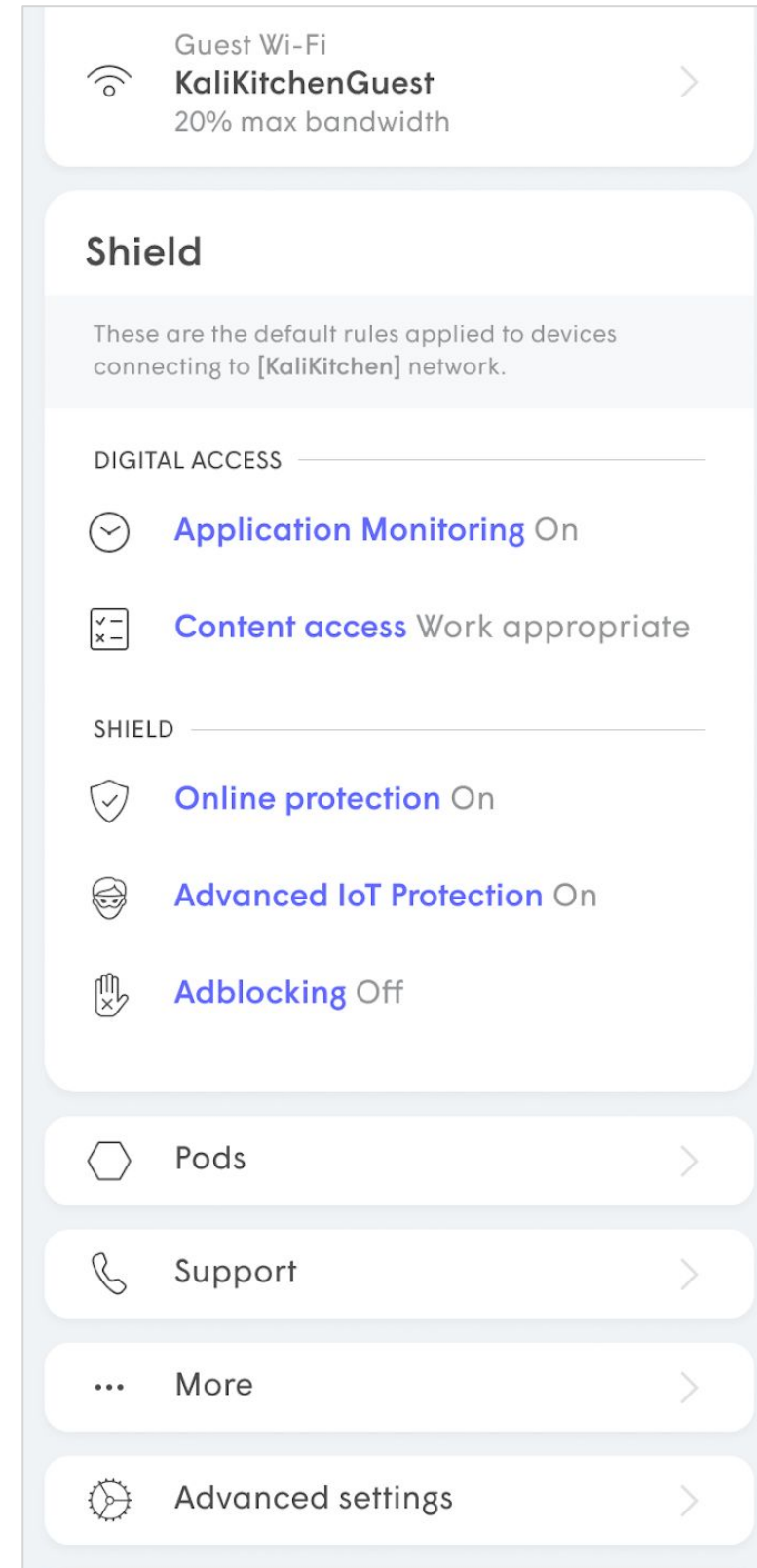
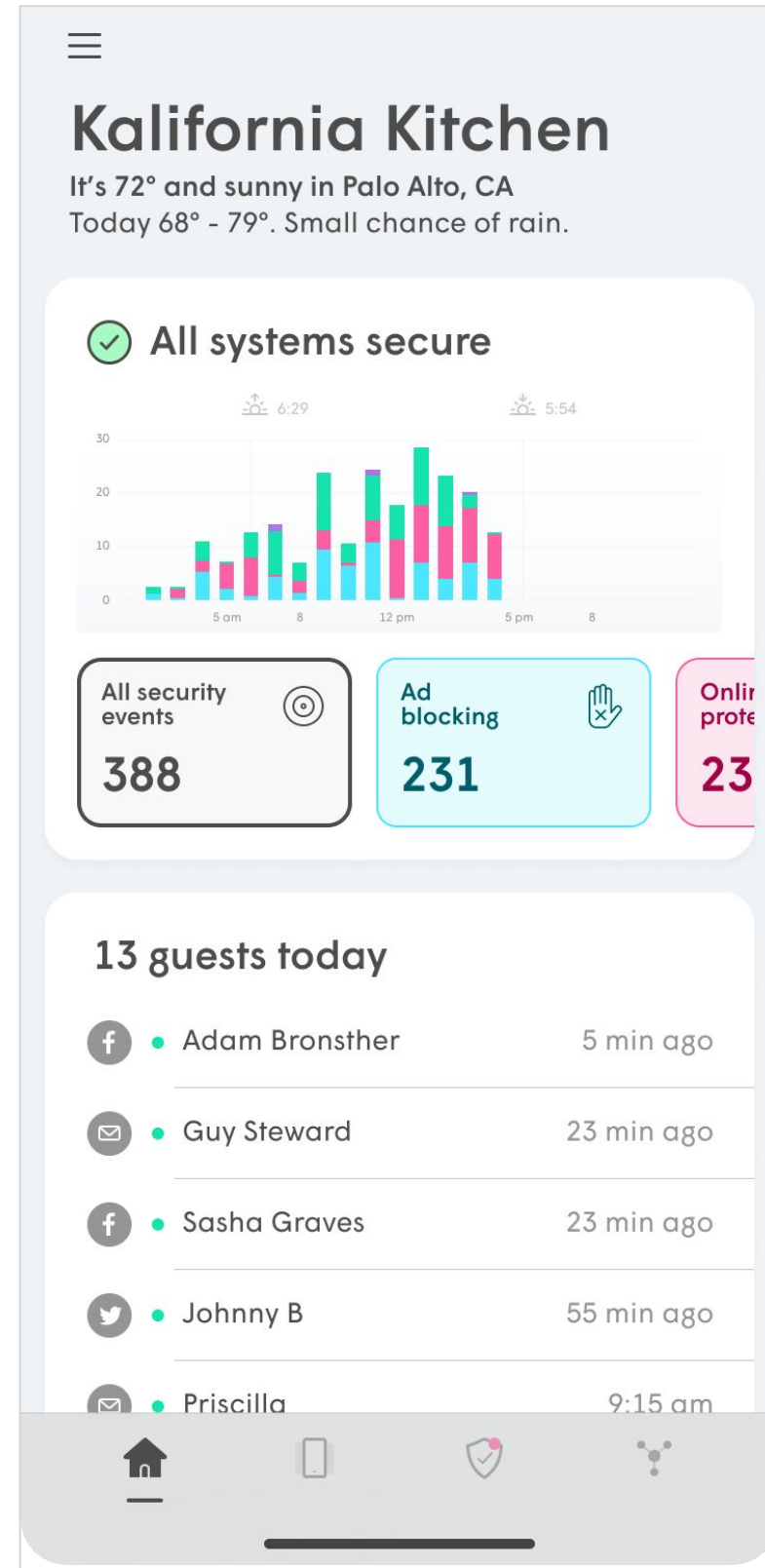
Plume Shield

AI Plume Shield

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

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

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



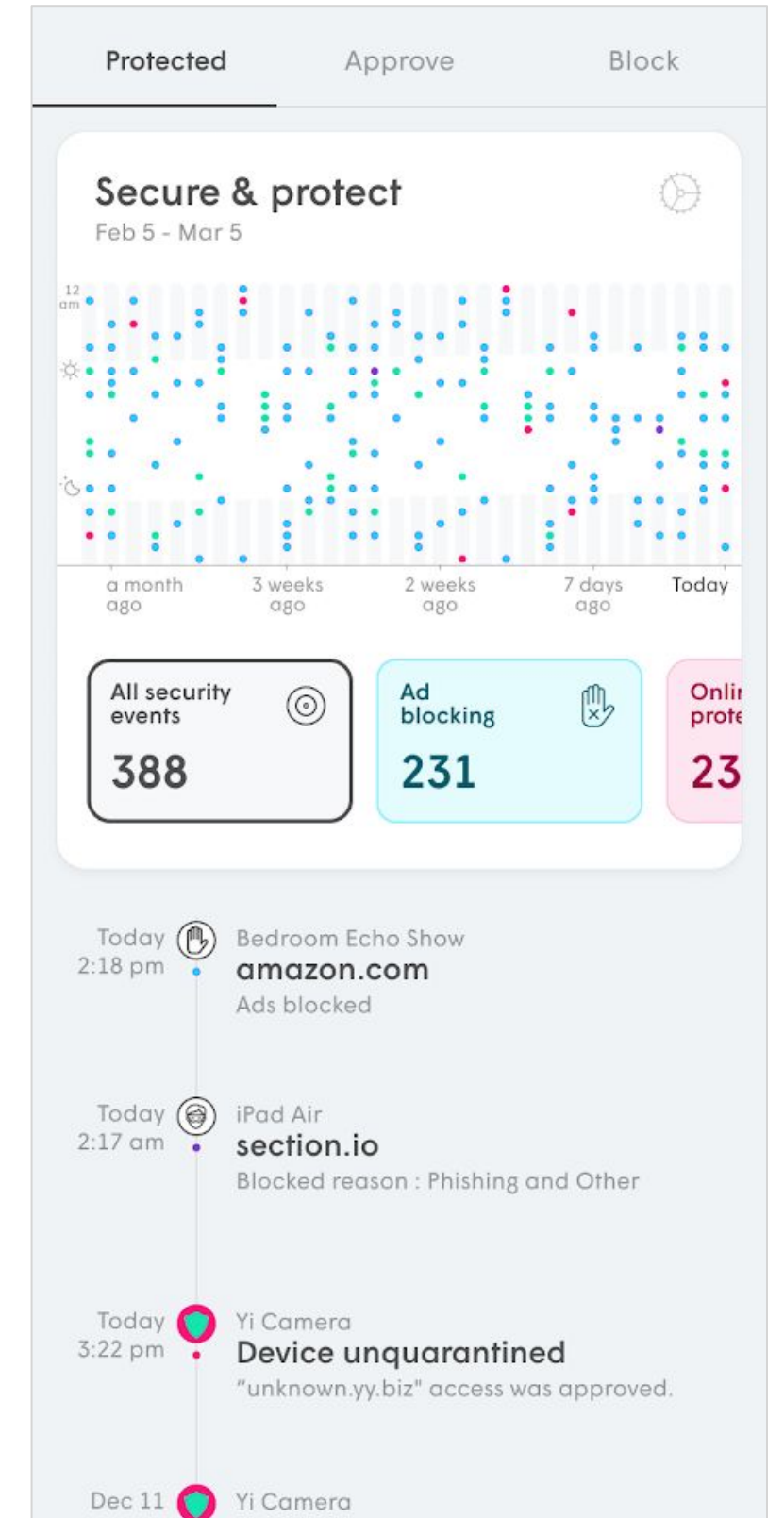
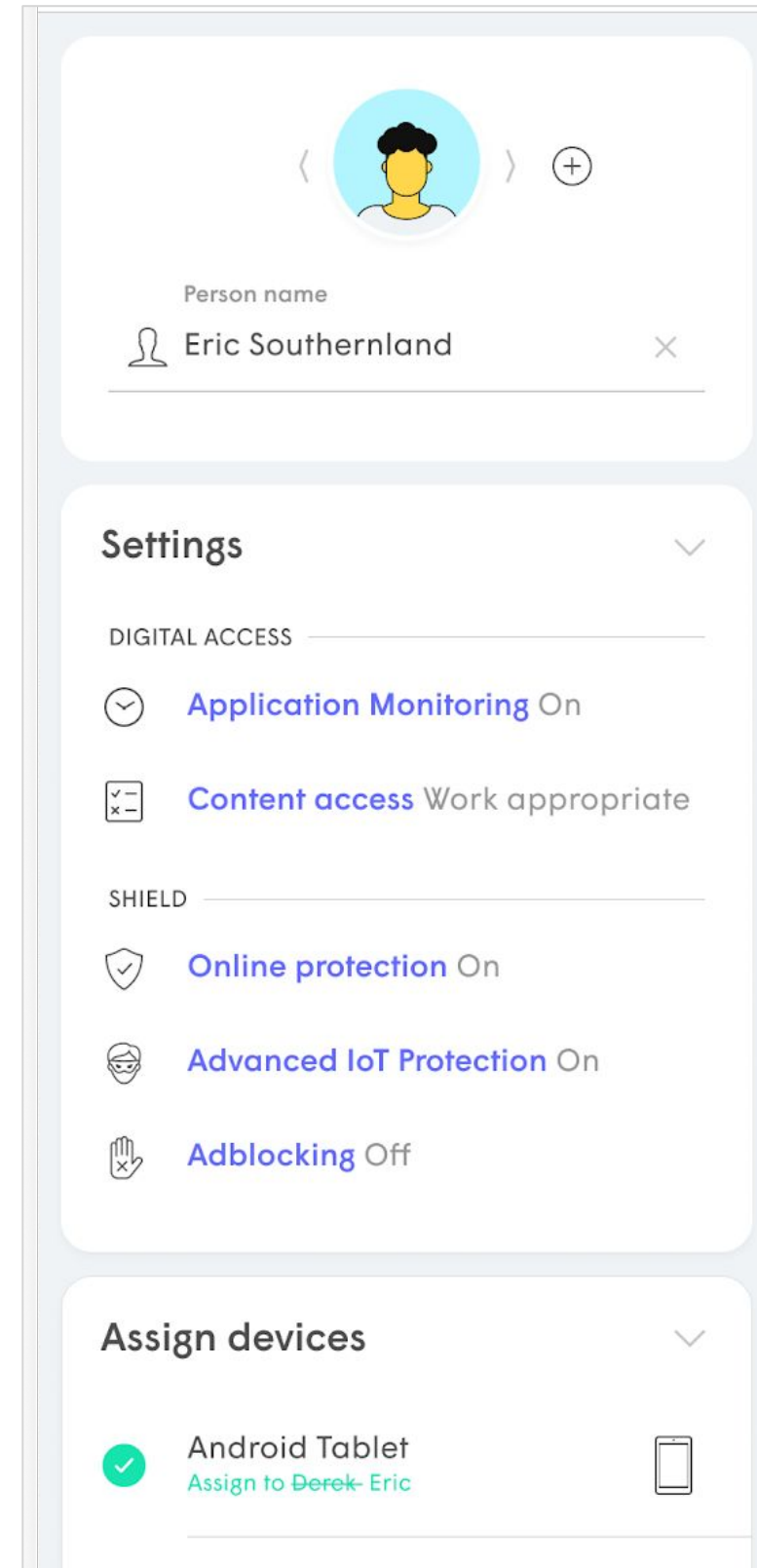
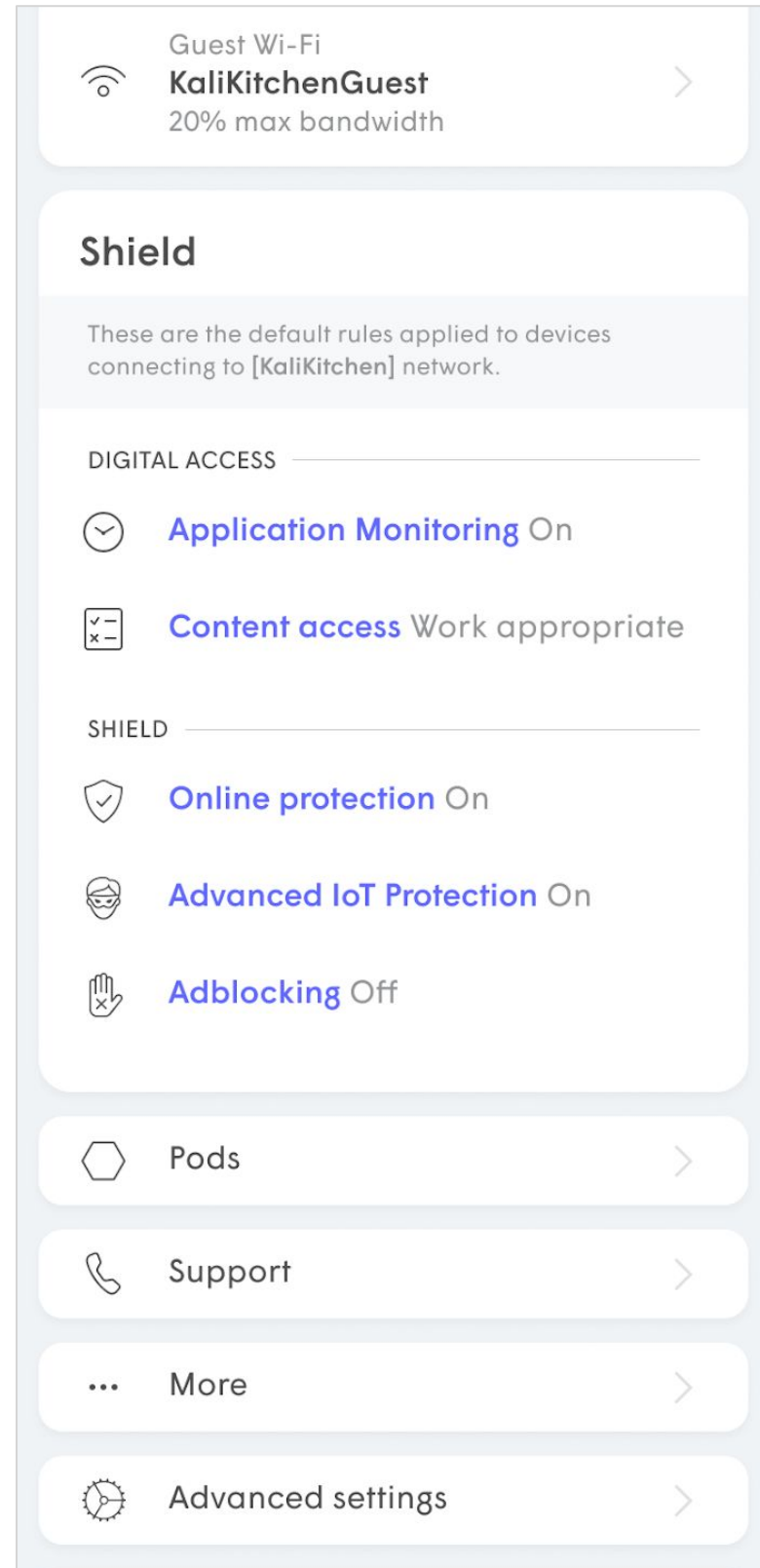
Plume Shield

Online Protection

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

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

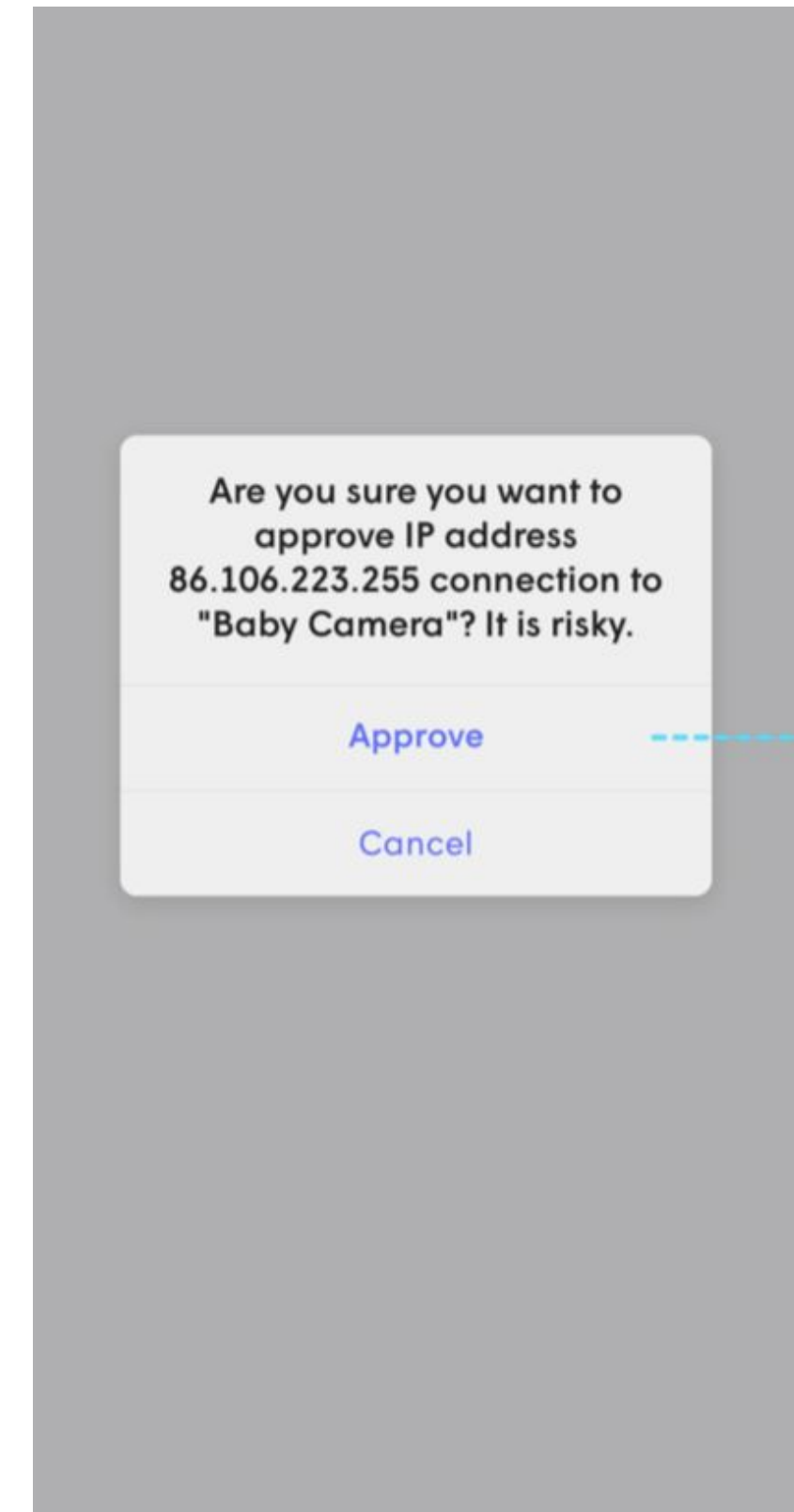
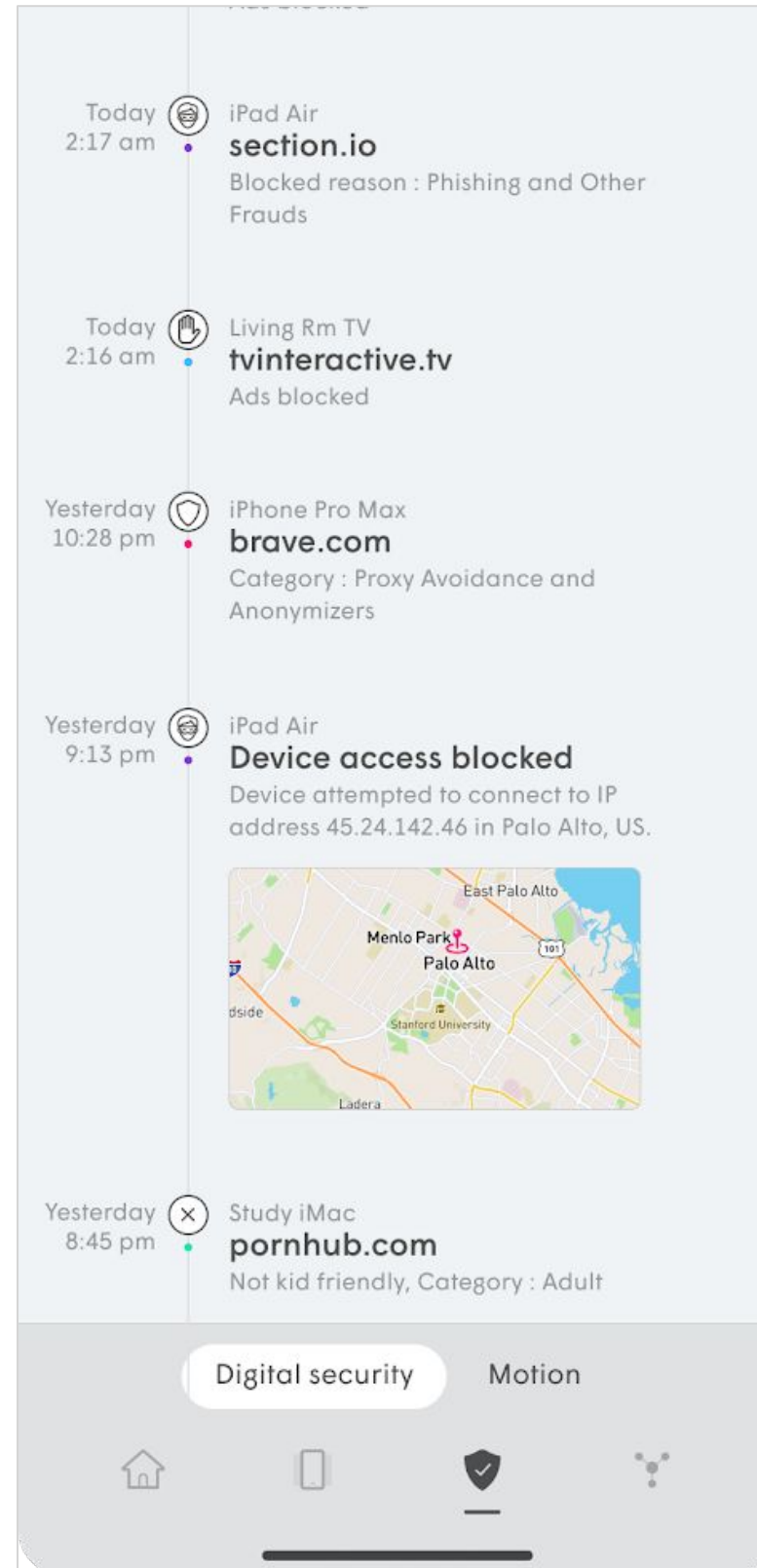
Online Protection can be set at the network, device, or employee level.



Outbound IP Protection and Intrusion Prevention

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

Outbound IP Protection and Intrusion Prevention is enabled by turning on Online Protection as long as you have a SuperPod connected as the Gateway Pod running firmware 2.4.3 or later.

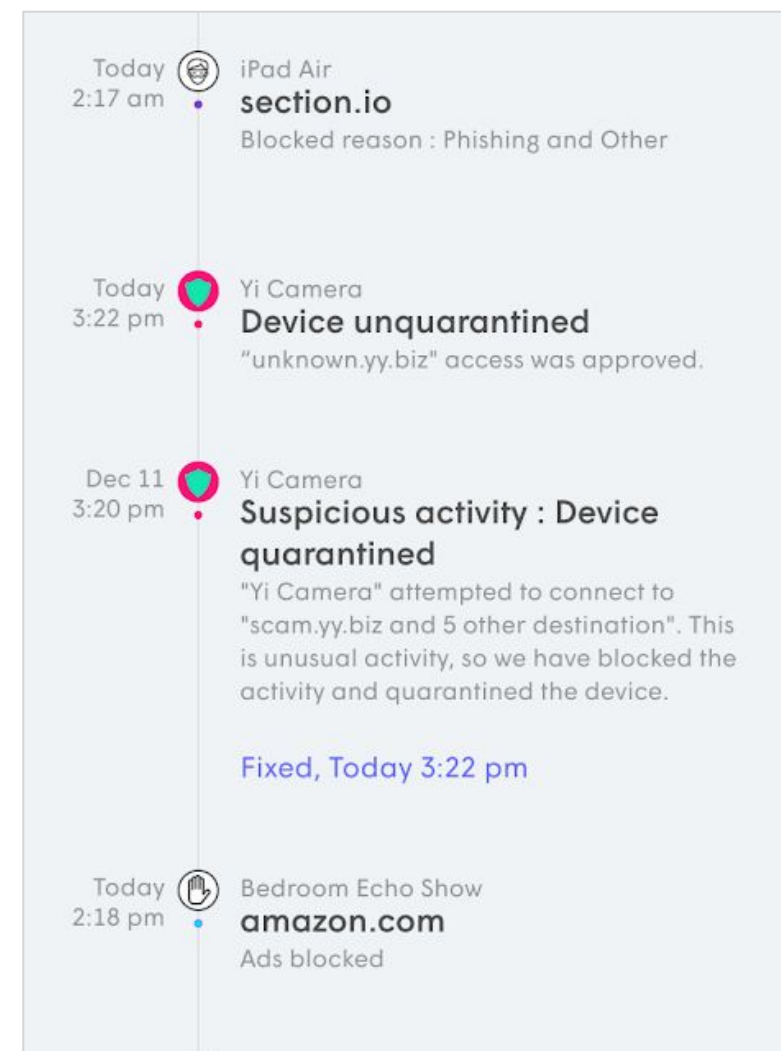
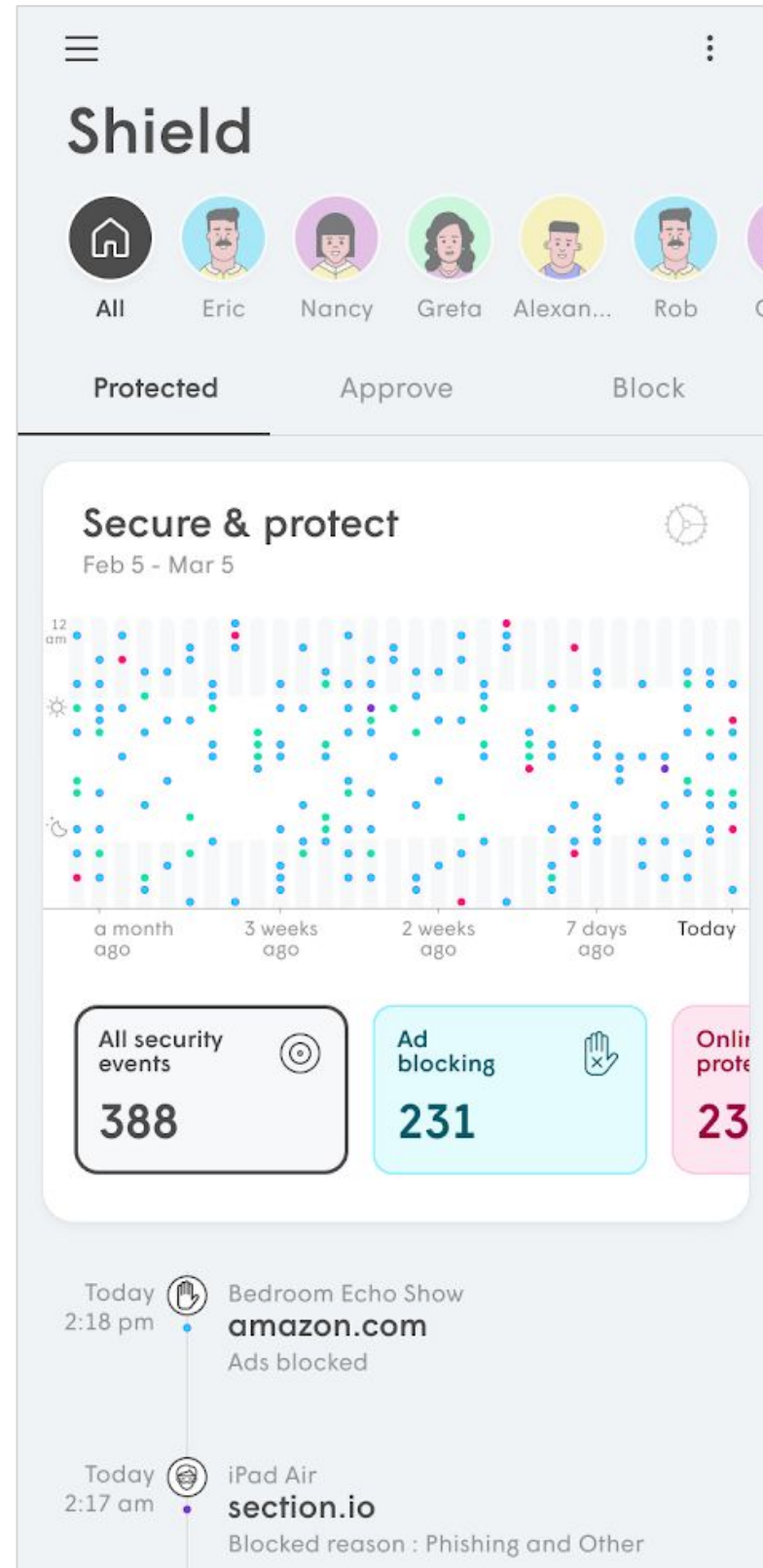


Managing Security Events

The **Shield** tab brings up a list with a graphic showing all blocked events, including Shield security events and Content Access blocked events..

The list contains 30 days worth data and the tapping on the graphic will highlight the number of events during that day.

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



- Ad blocking
- Online protection
- Content access
- Advanced IoT protection
- Quarantined device

Managing Security Events

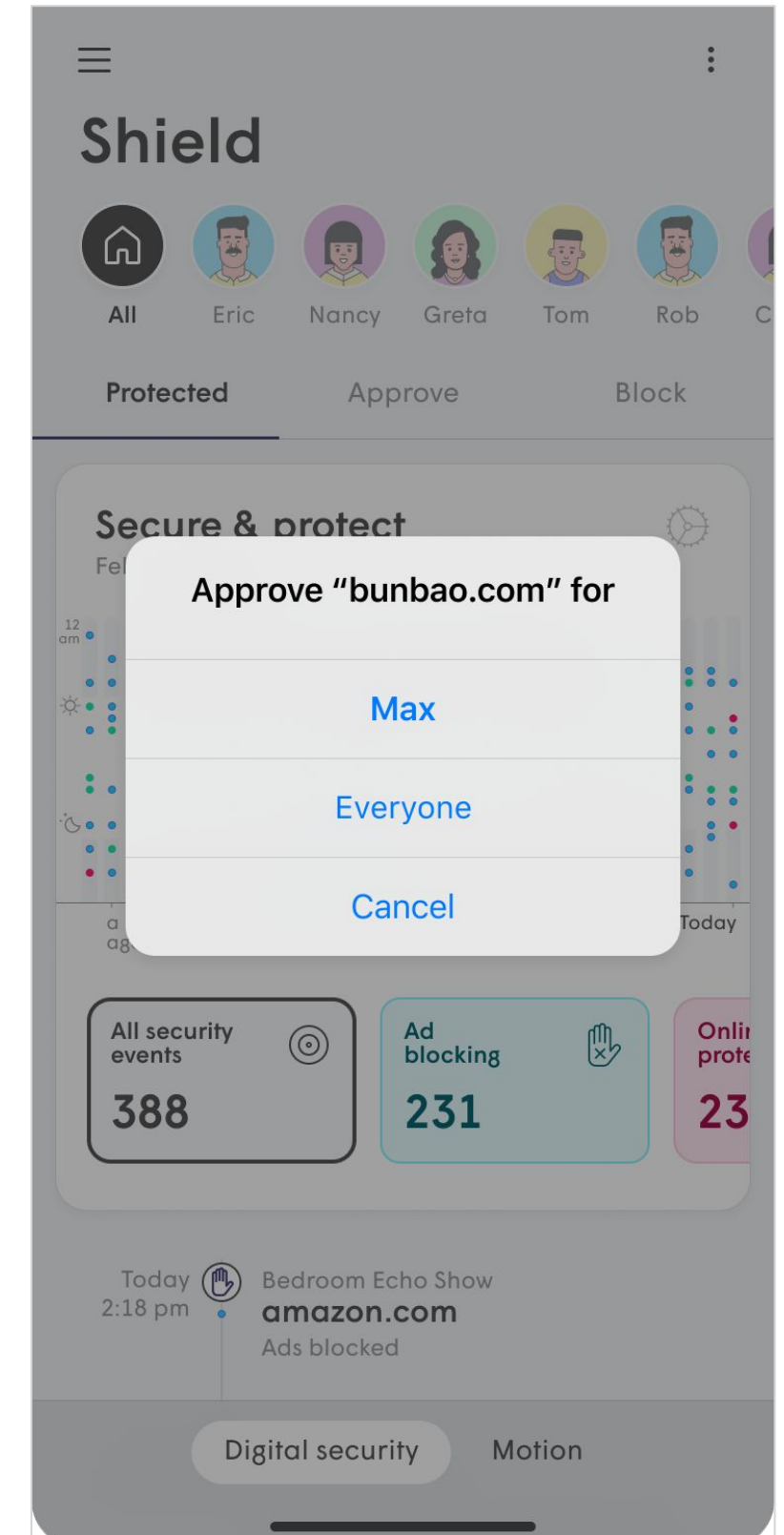
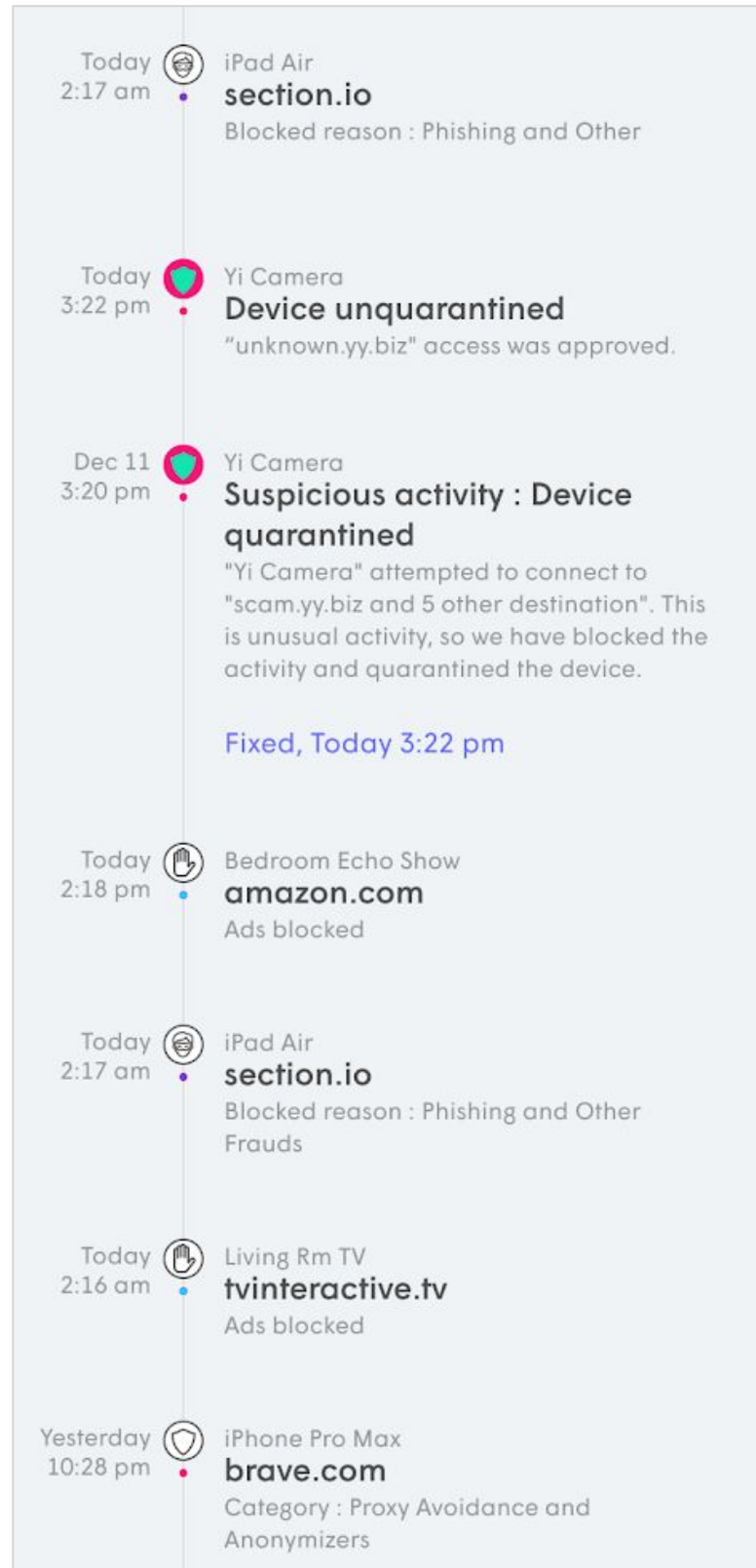
A brief description under each event provides more information on why it was blocked and which device was trying to access it.

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

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

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

Up to 20 entries in total can be manually whitelisted.



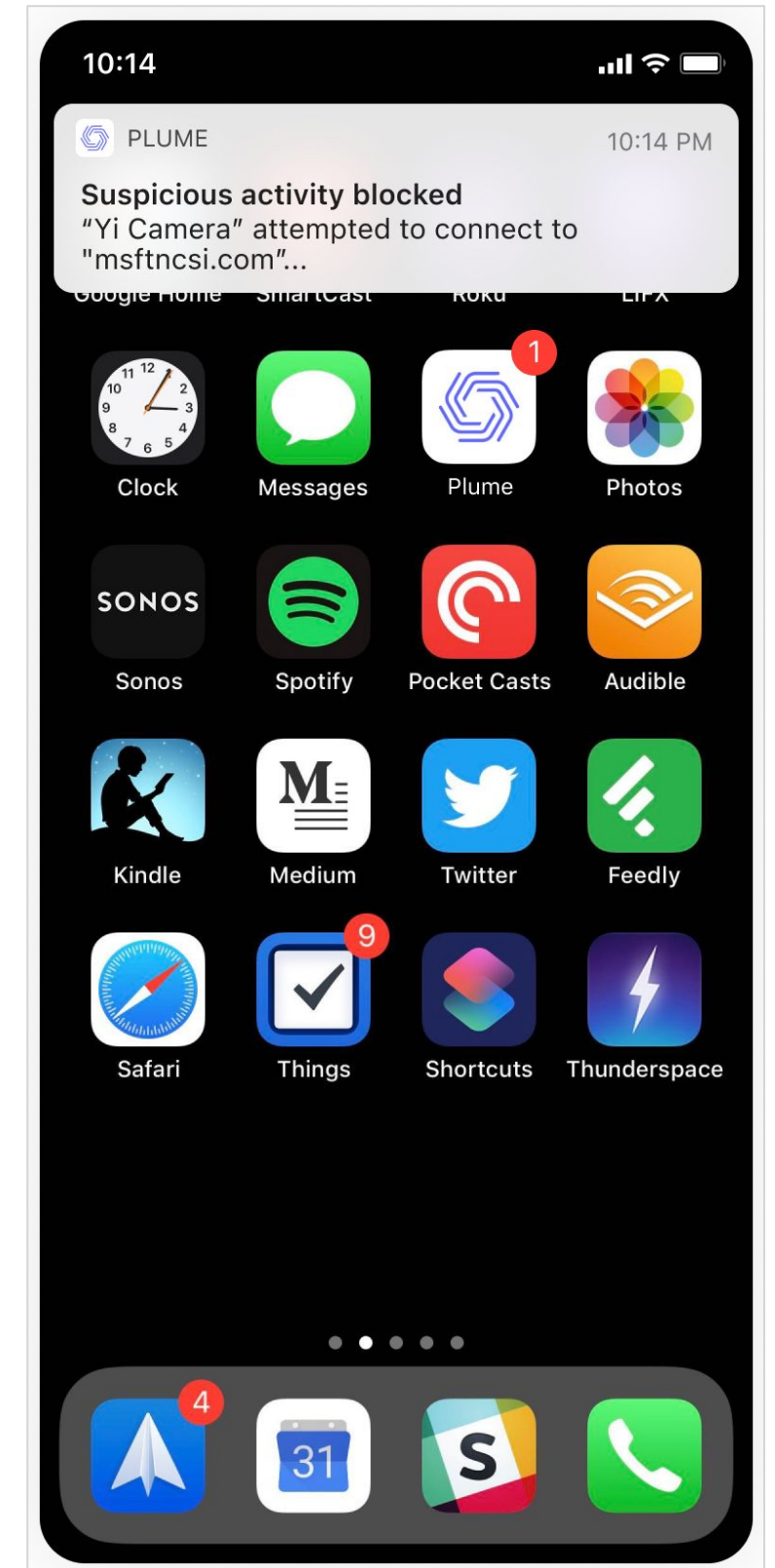
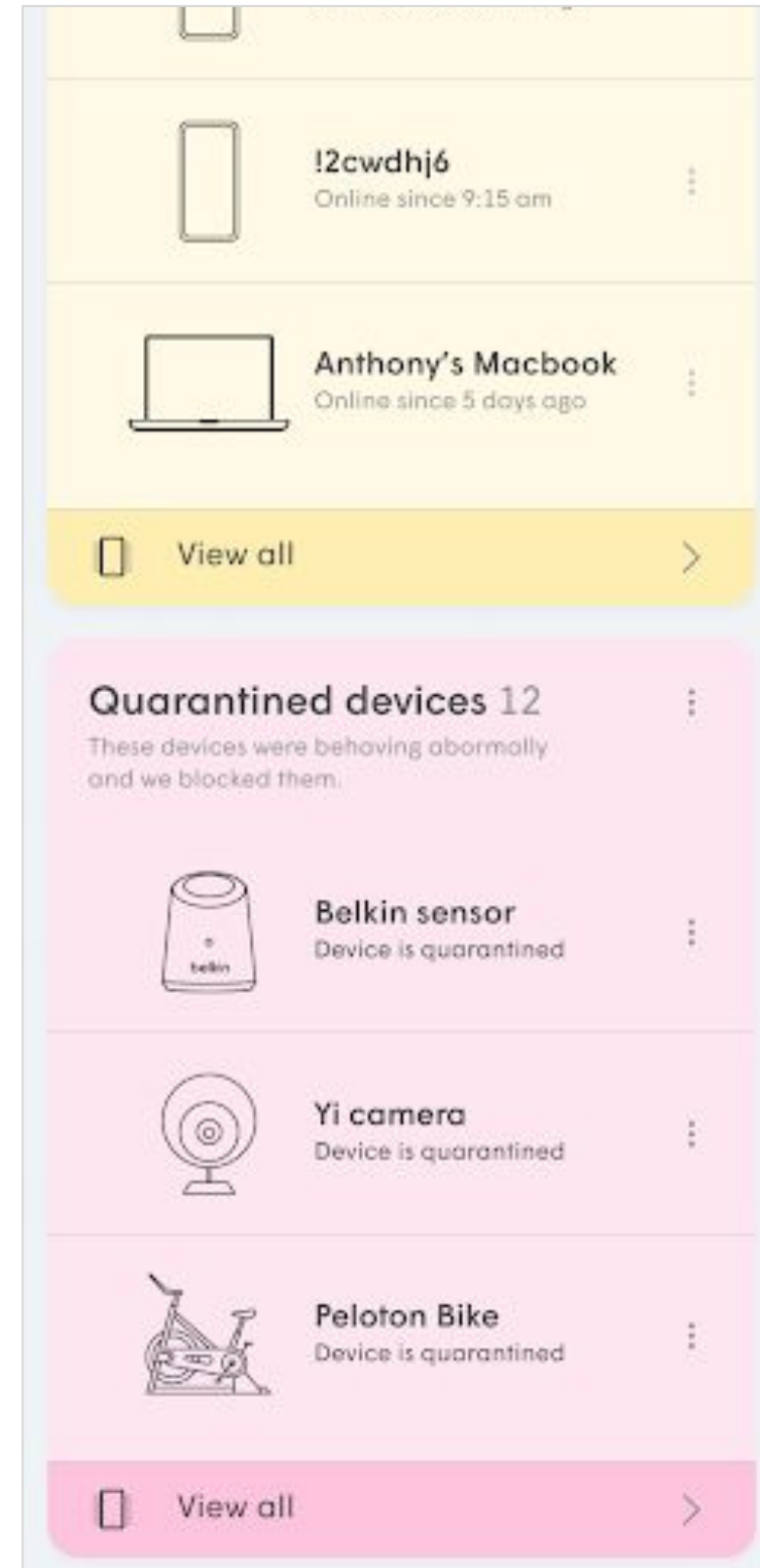
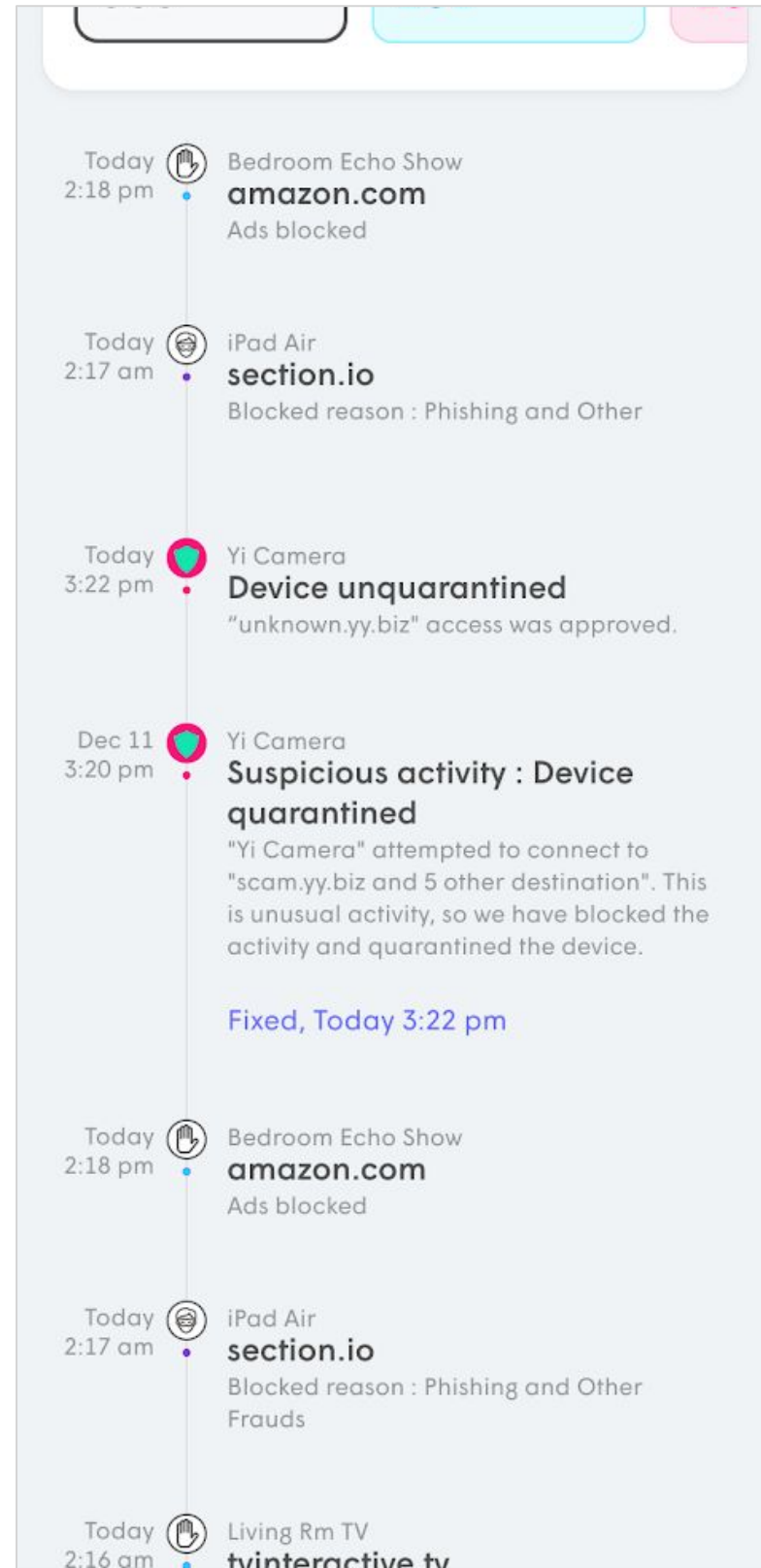
Plume Shield

Advanced IoT™ Protection

Advanced IoT™ protection studies device behavior.

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

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



Plume Shield

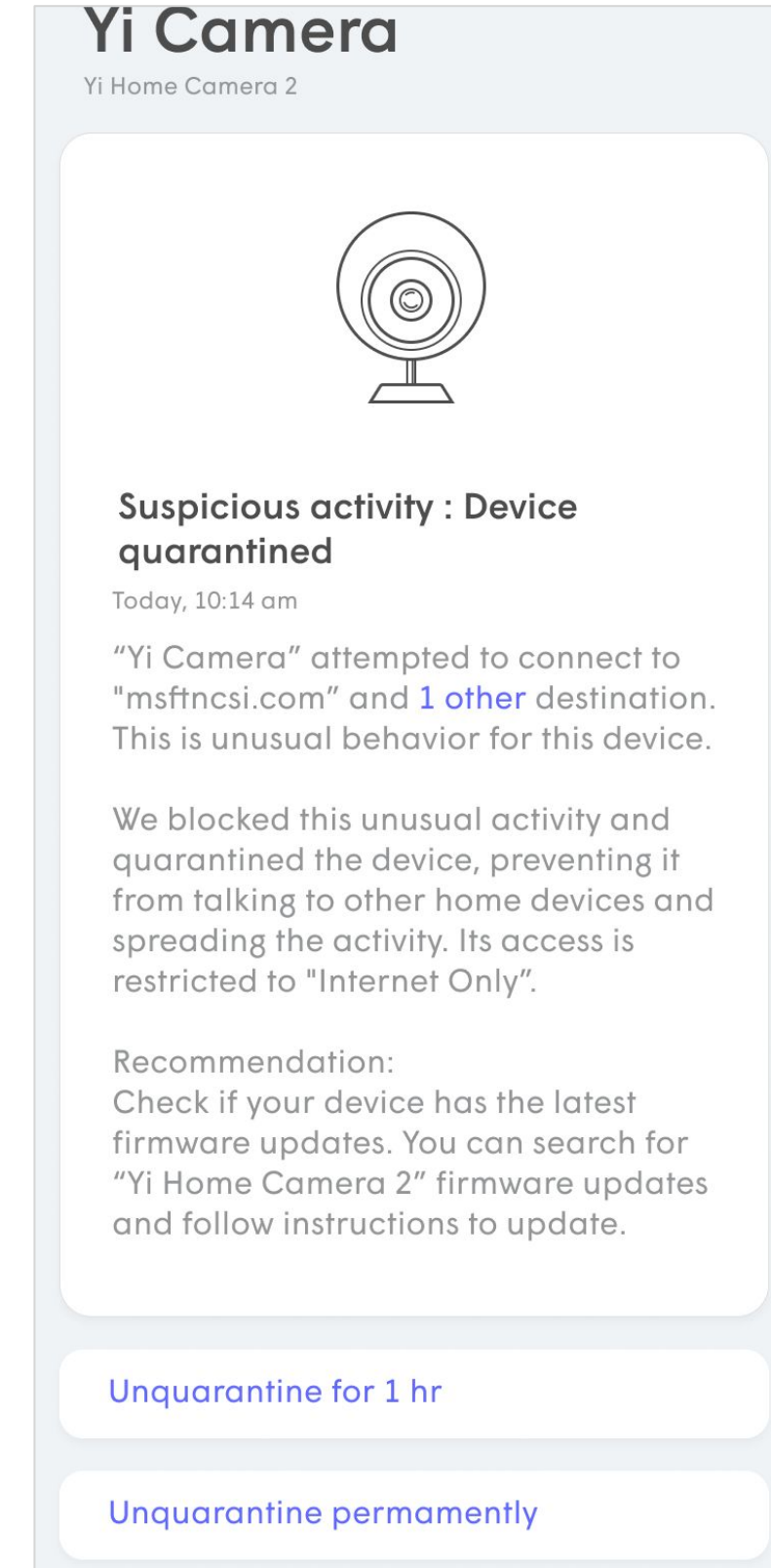
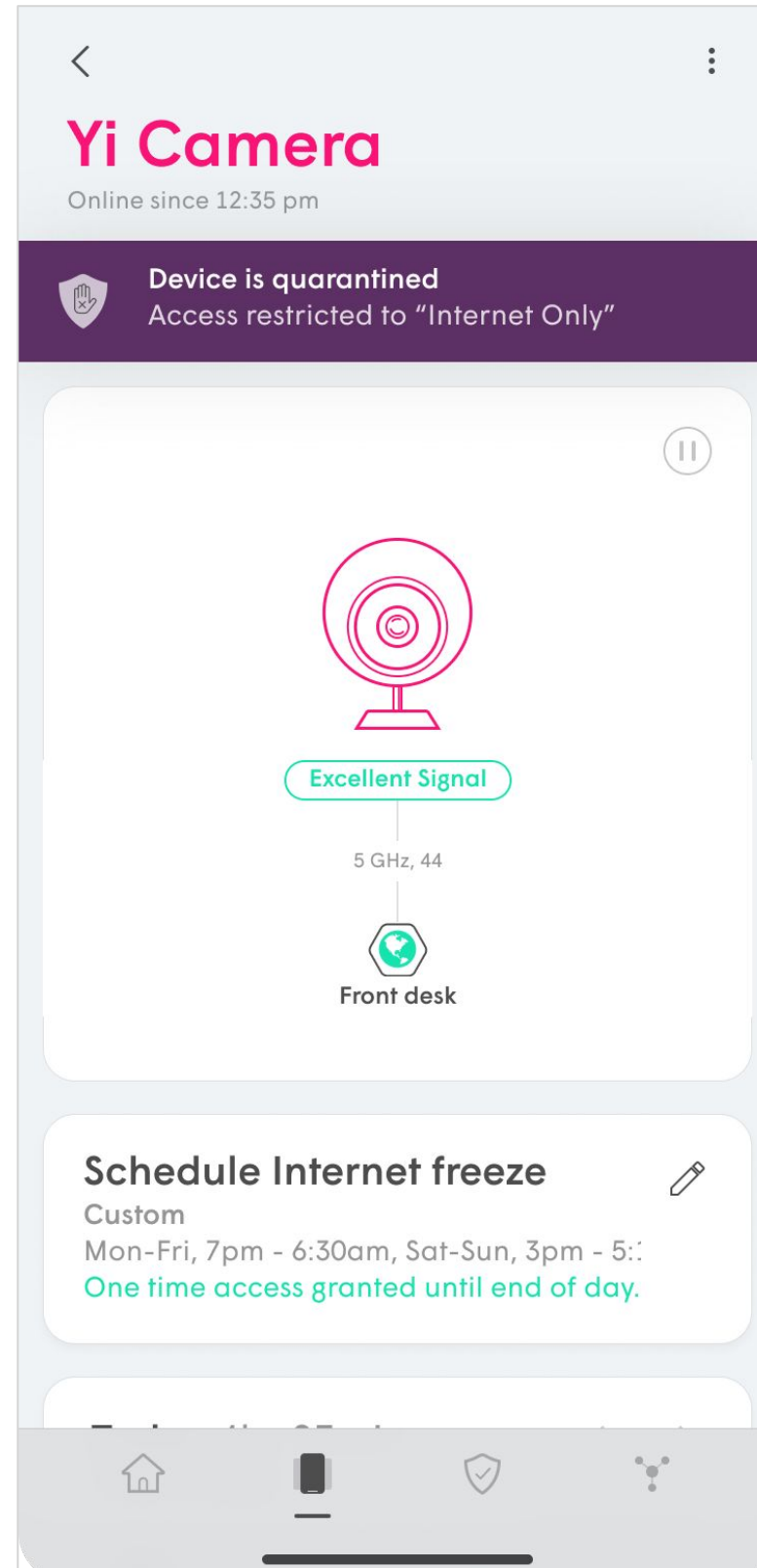
Advanced IoT Protection

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

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

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

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

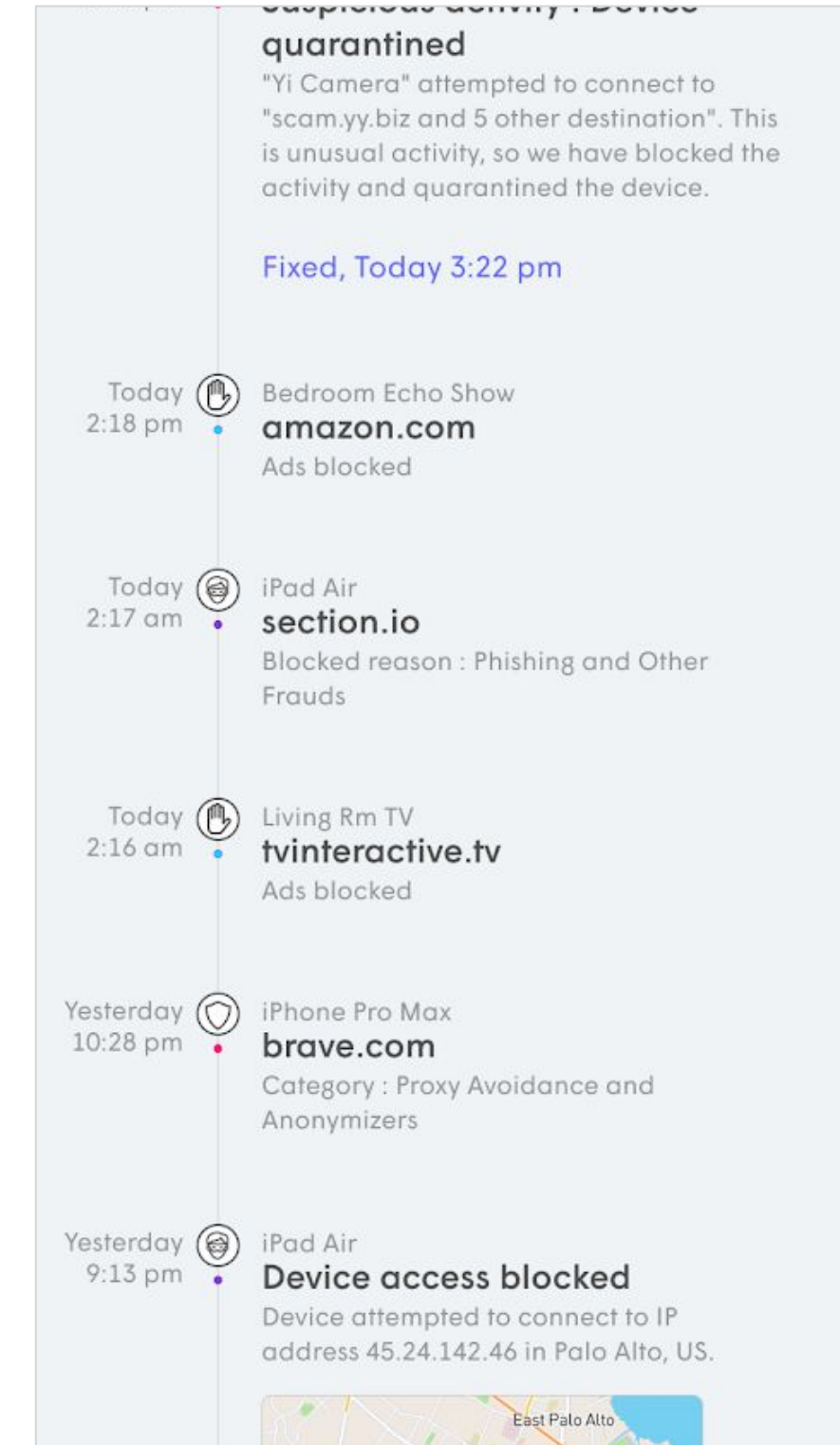


Plume Shield

Adblocking

Enabled at the network, person, or device level.

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

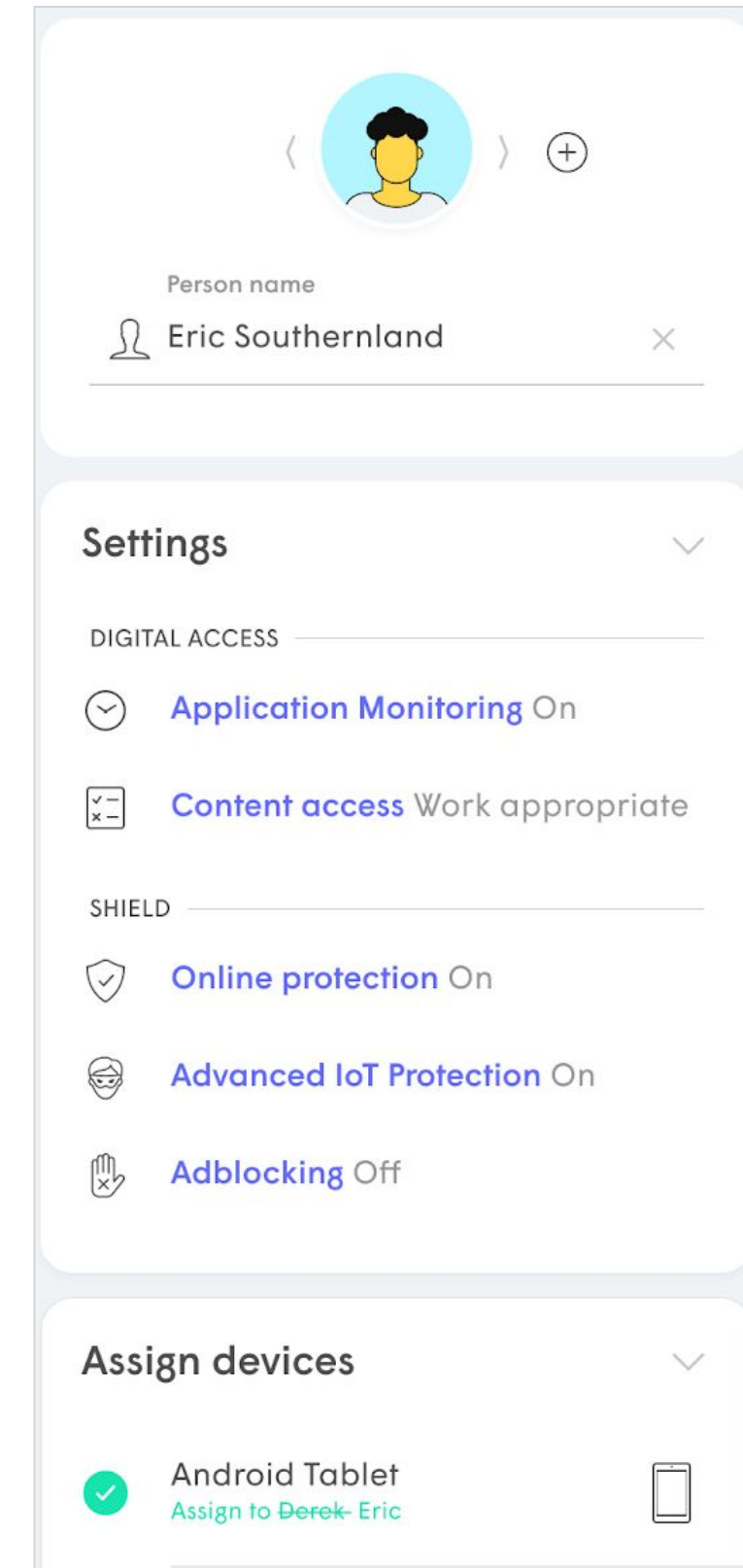
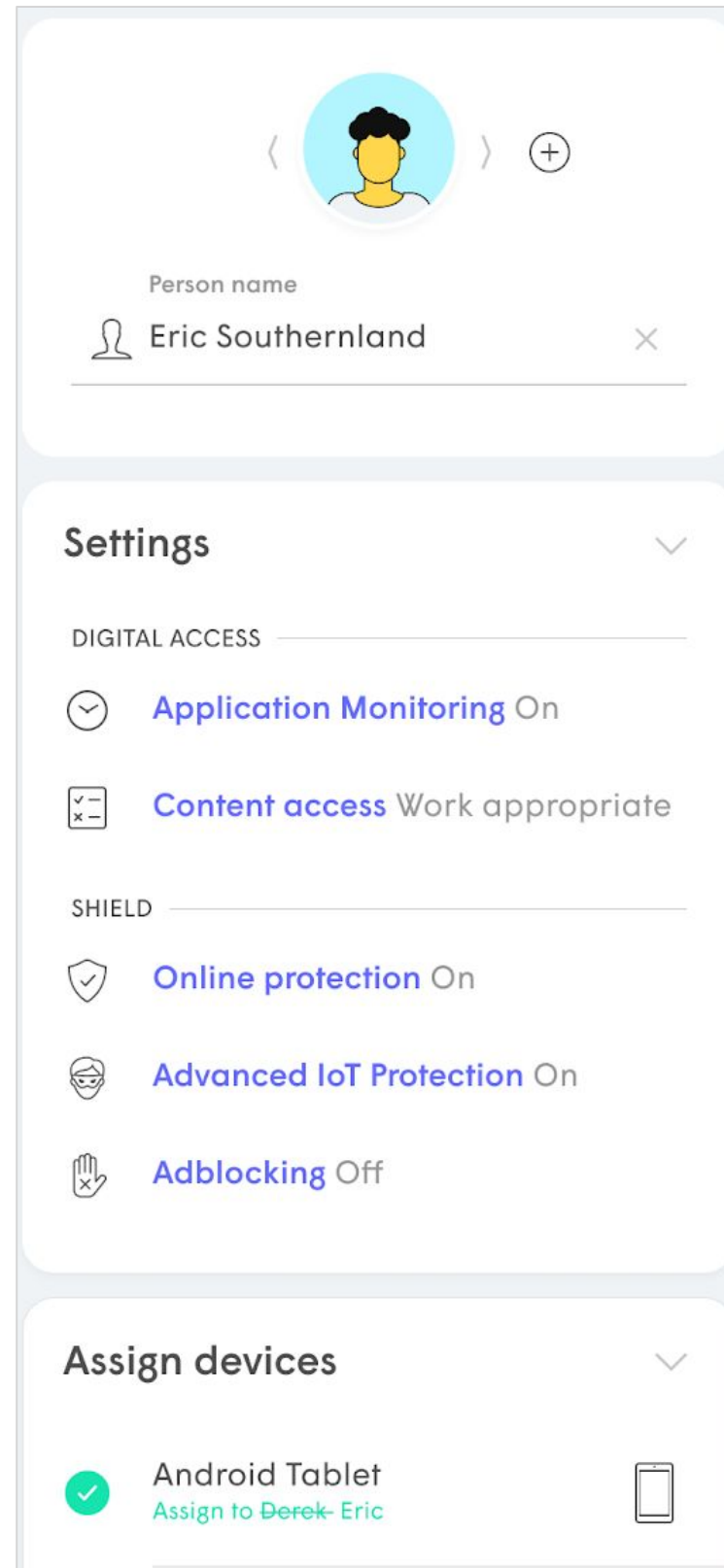


Content Access

Content Access rules, can be set at the network level.

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

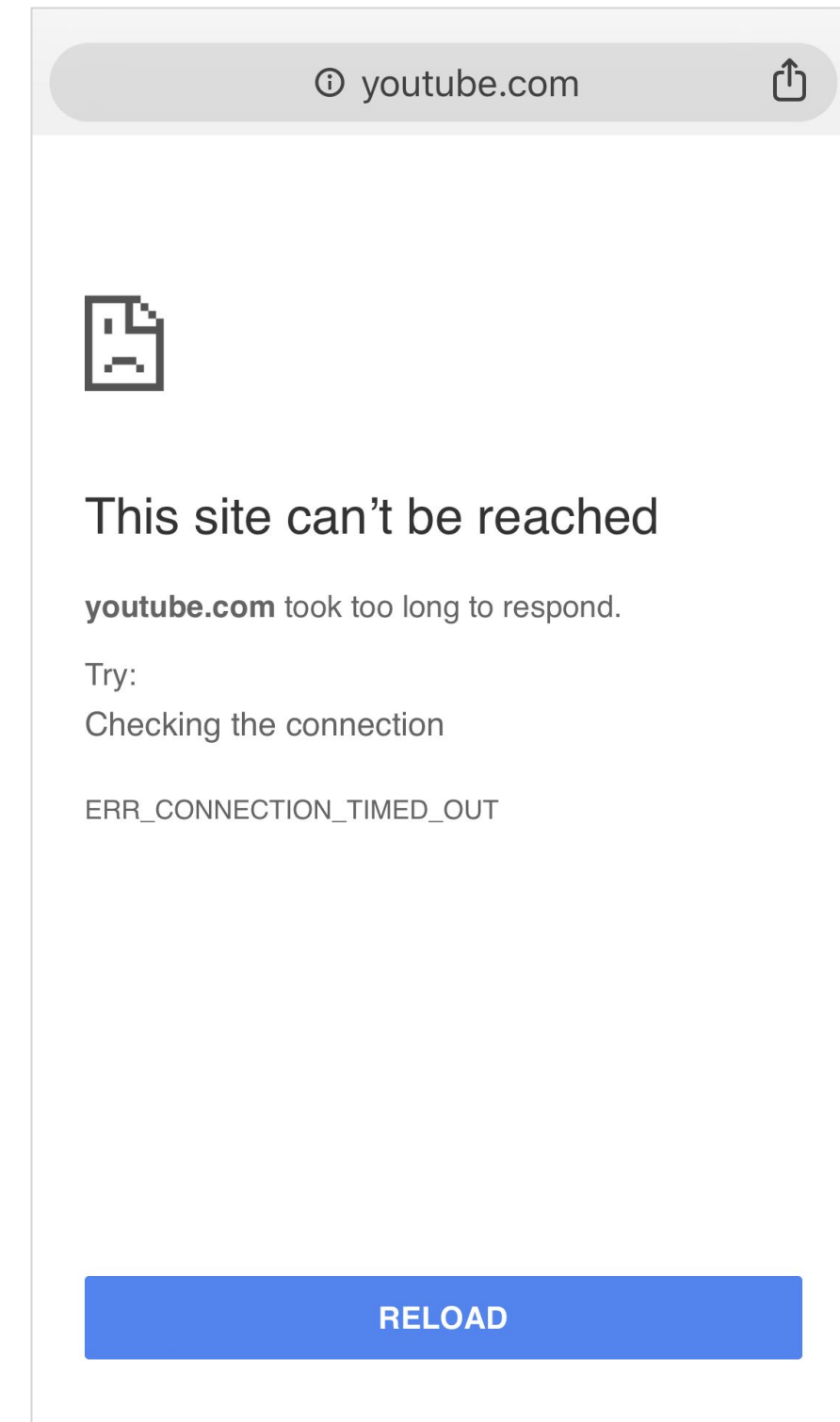
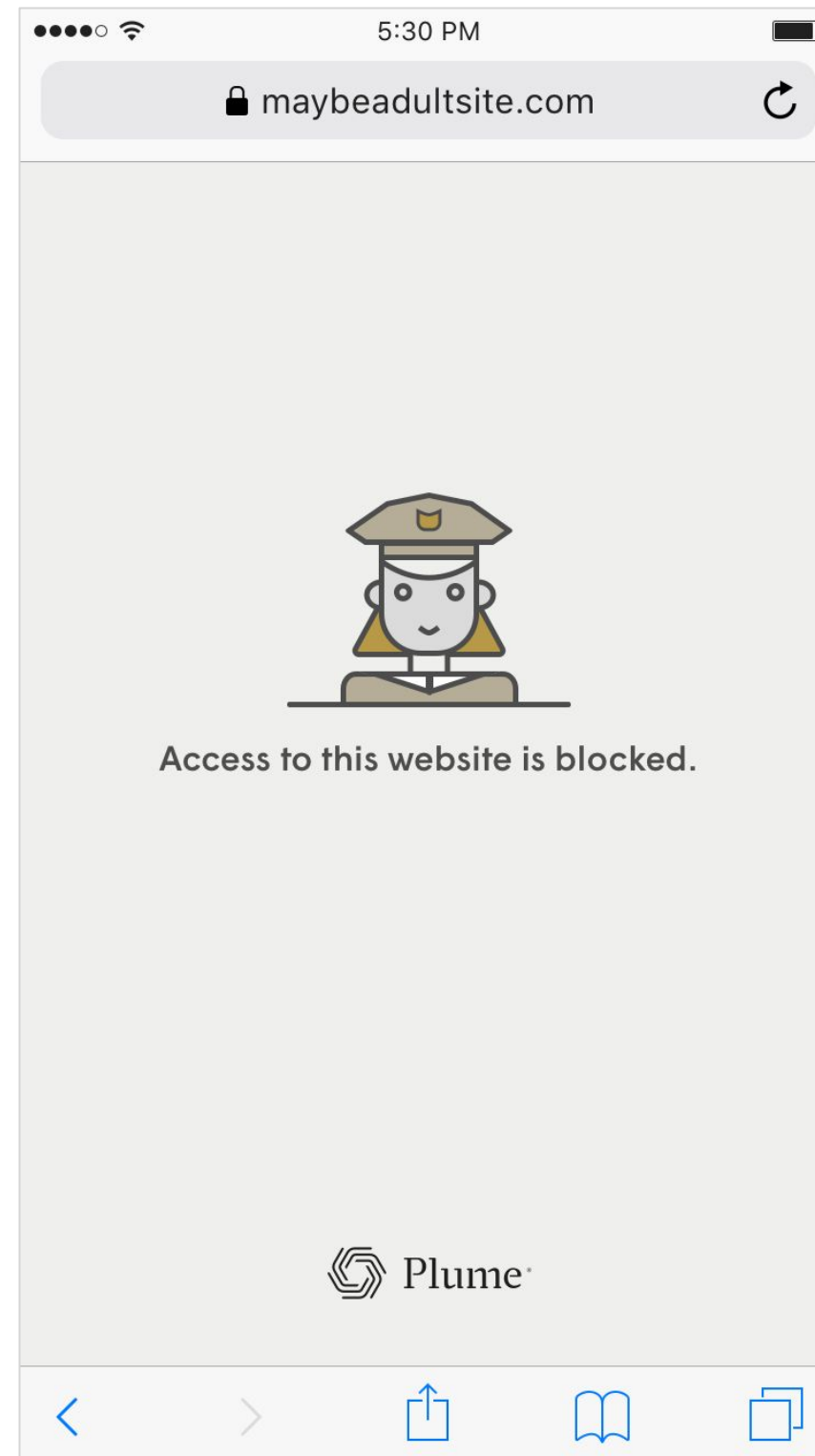
- **No Restrictions** (default) - No restriction on content other than what is being applied by Shield
- **Work Appropriate** – Content that can add potential liability to the business is blocked.



Content Access

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

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



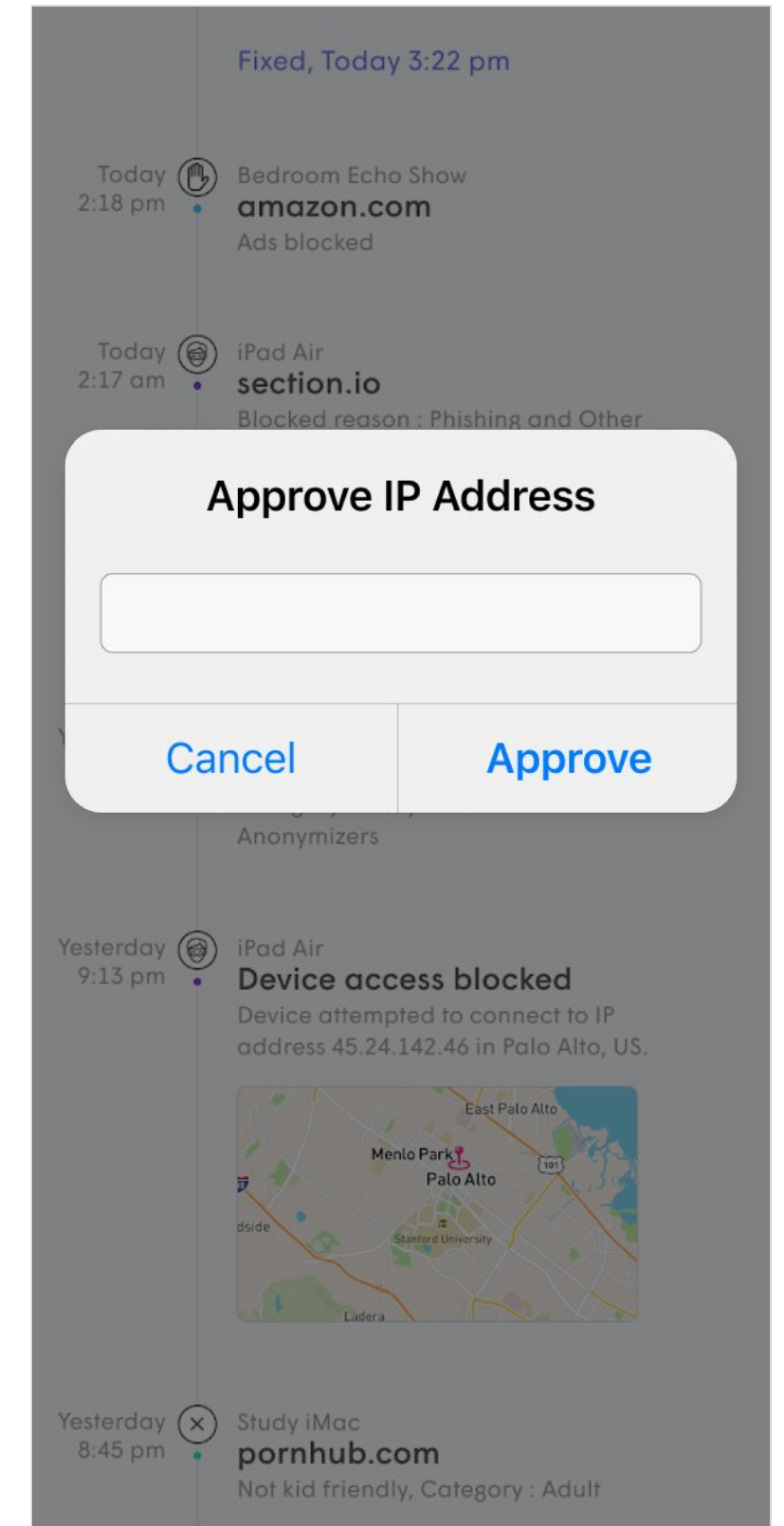
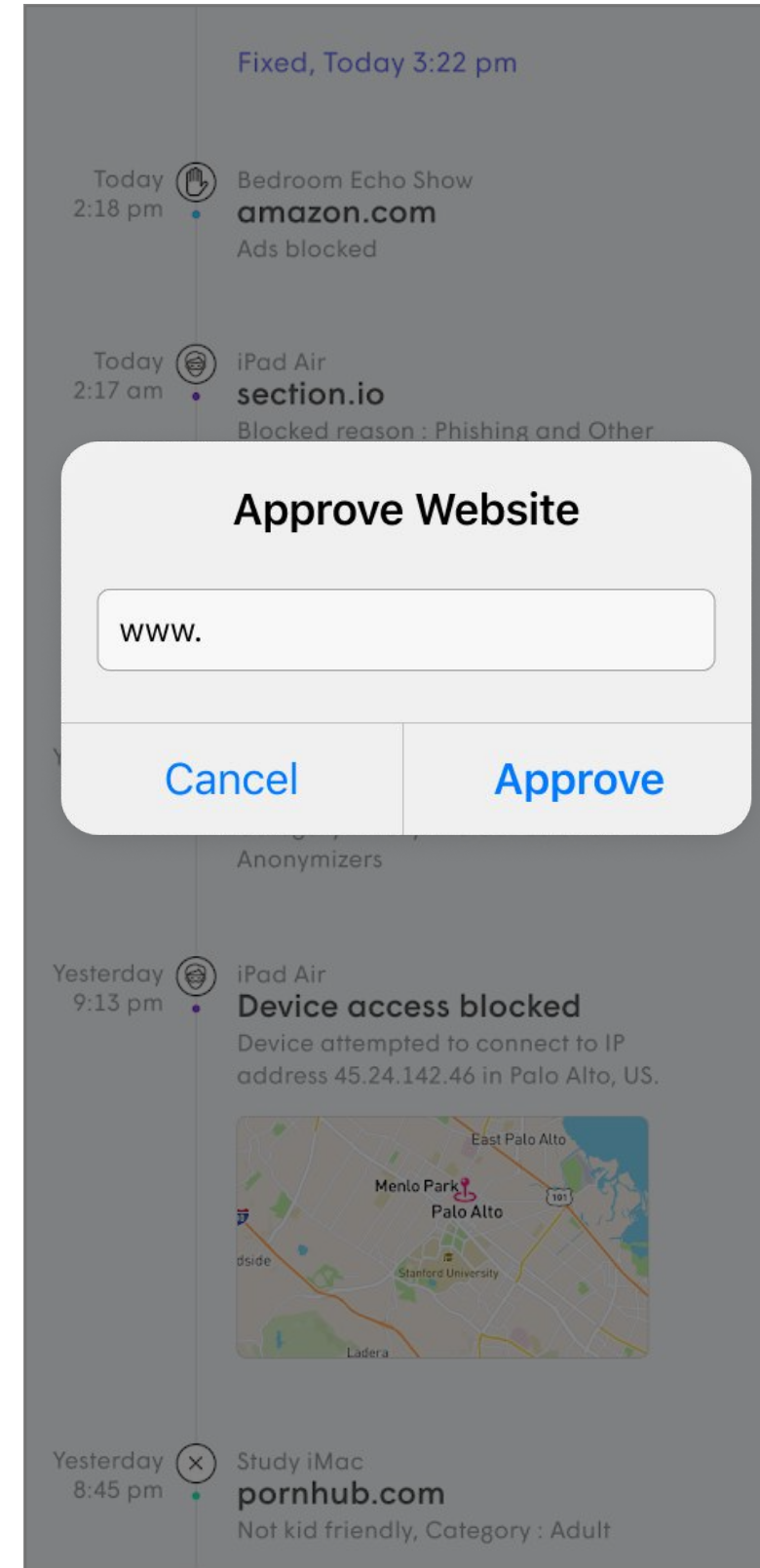
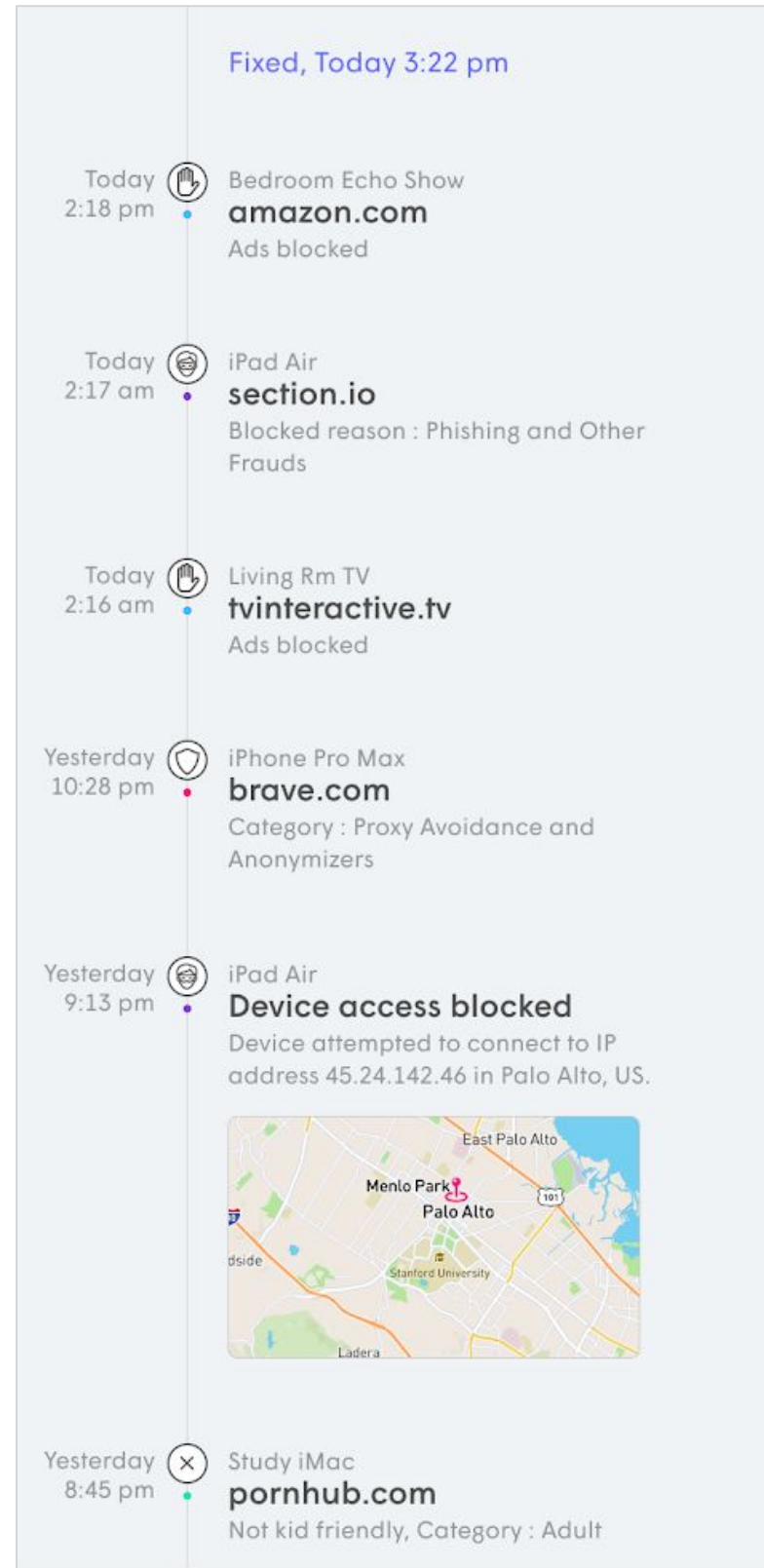
Manually Approving Content

Admins can approve (whitelist) domains or IP Addresses* that have been blocked by Content Access, Online Protection or Adblocking.

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

Device level settings supersede person and network level settings.

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



* IP Addresses can only be blocked if Outbound IP Protection and Intrusion Prevention has been enabled

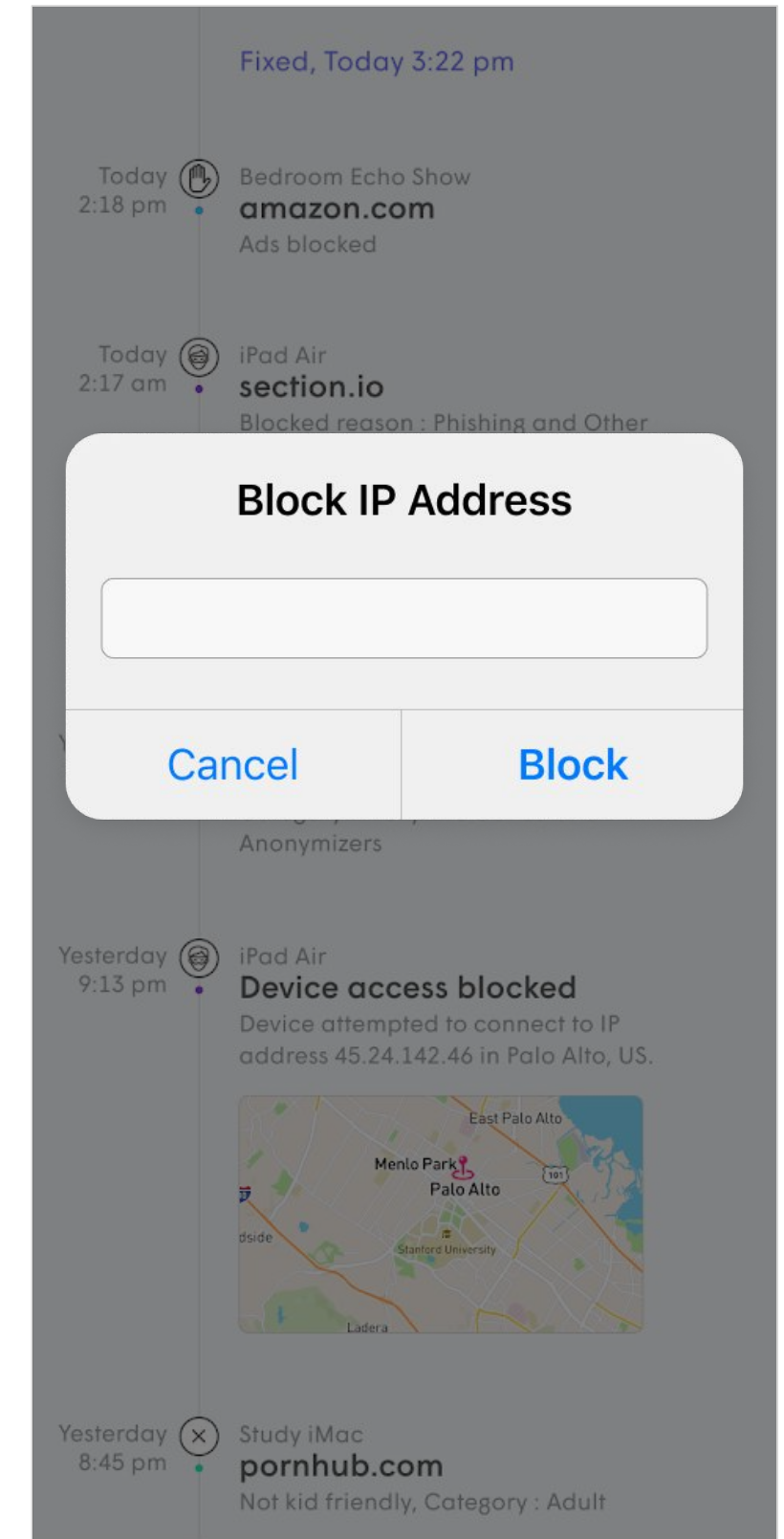
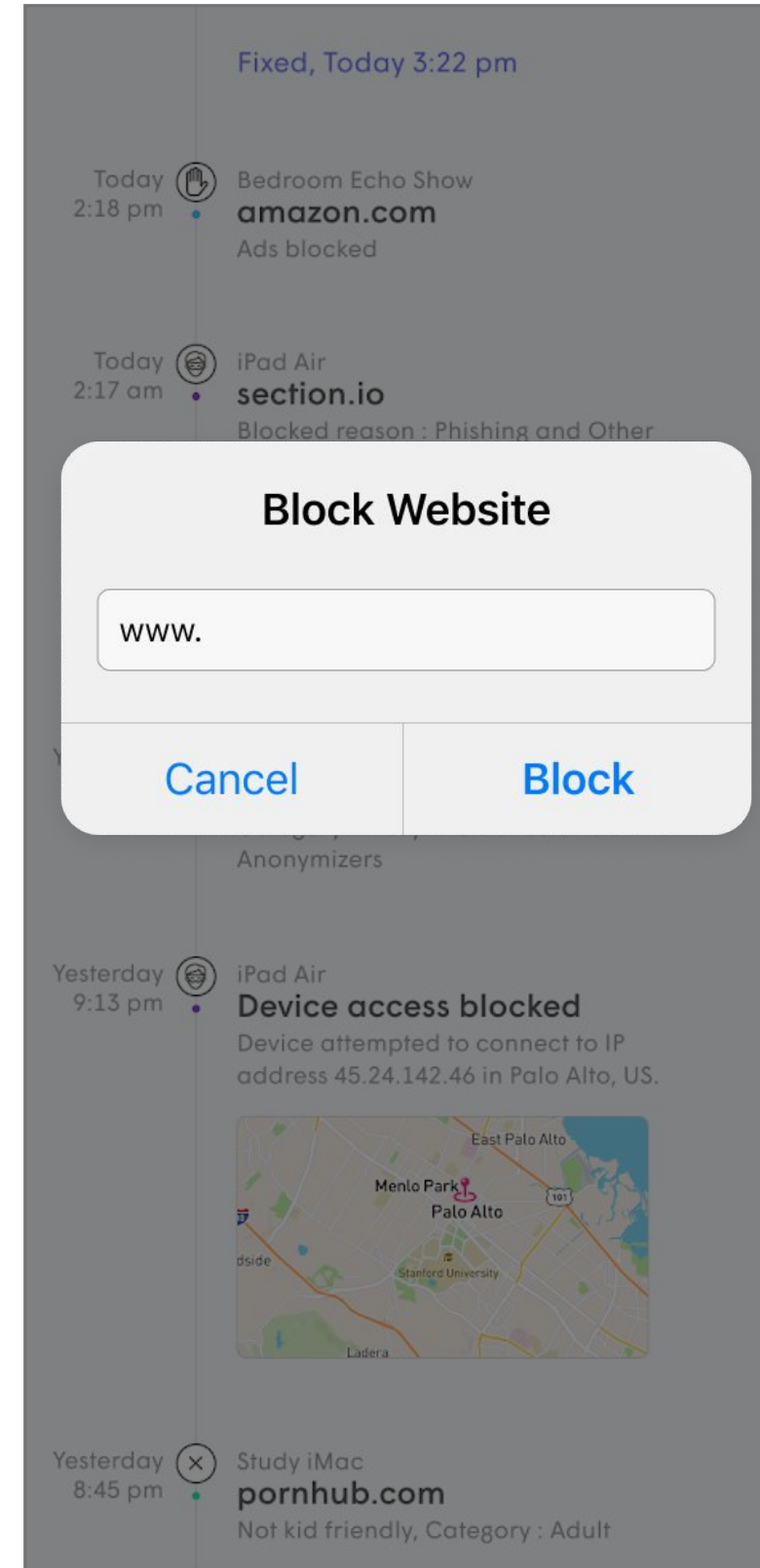
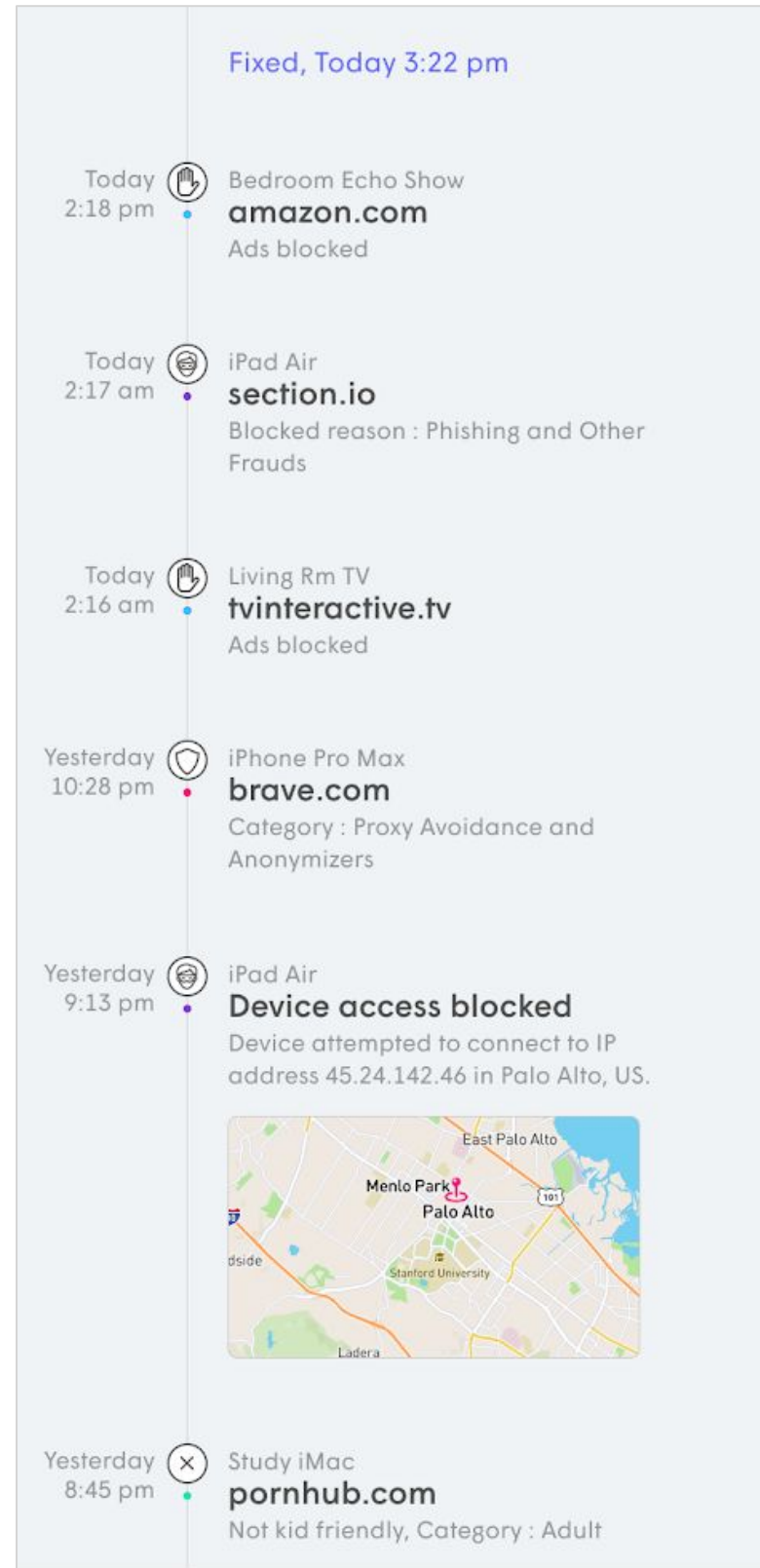
Manually Blocking Content

Admins can manually block (blacklist) domains or IP Addresses* that have not been blocked by Content Access, Online Protection or Adblocking.

Up to 20 entries can be manually blocked.

Device level settings supersede person settings which supersede network level settings.

Tapping on a **security event** in the person, device or Shield pages, lets you manually block a specific domain or IP address* by entering it in the **Block** list.



* IP Addresses can only be blocked if Outbound IP Protection and Intrusion Prevention has been enabled

Managing the Account

Managing the Account

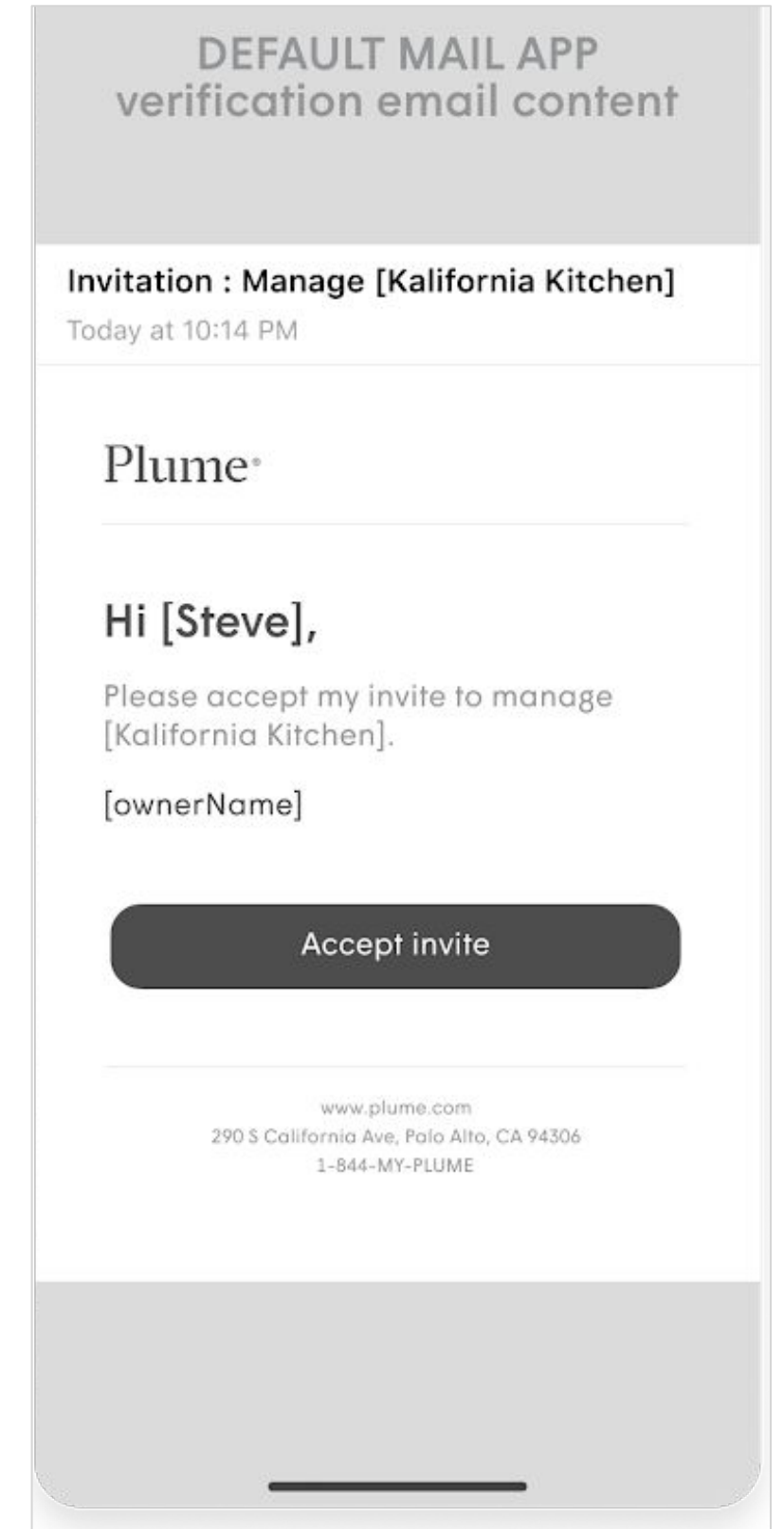
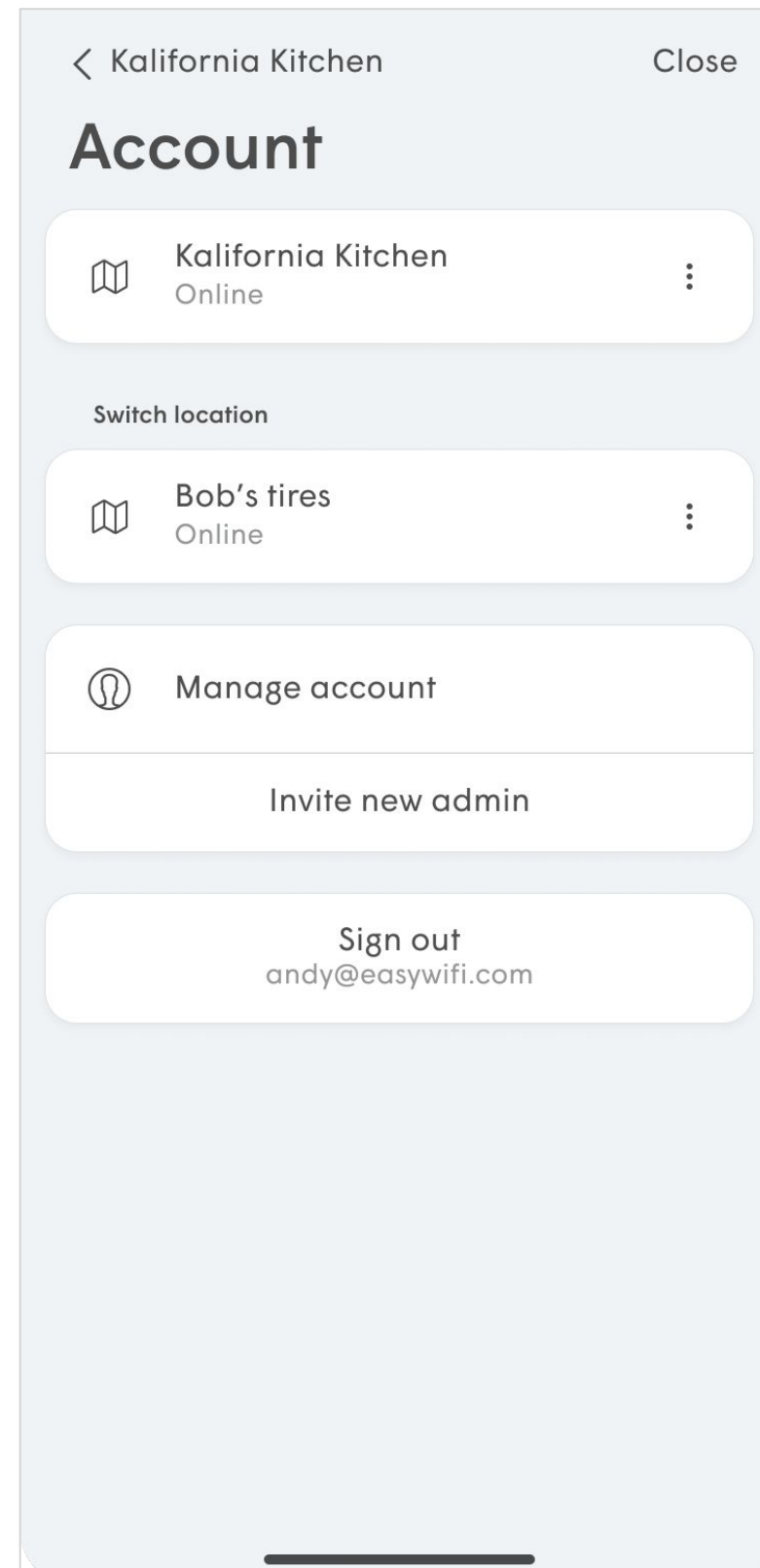
Logging out

Closing the WorkPass app does not log the user out of the account.

The Admin can log out of the WorkPass app from the Account menu.

Once logged out, the user will be prompted to log in the next time they launch the app.

The user will either need to request the magic link again or enter their password, depending on the option they chose during initial setup.



Speed Tests

Speed Tests

ISP Speed Tests

The ISP Speed Test is actually running on the Gateway pod itself, measuring the speed being delivered by the ISP.

This test is run automatically once every 6 hours, but only when there is no traffic on the network.

The most recent speed tests for both **upload** and **download** is displayed at the bottom of the Home tab.

ISP Speed tests can be disabled in **Settings** under the **More** screen.

