Trend Micro™

Home Network Security 2020

Product Guide

V6.0

Trend Micro, Incorporated—US Headquarters
224 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900
Toll-free: (888) 762-8763

www.trendmicro.com

Trend Micro™ Home Network Security 2020 - Product Guide provides help for analysts, reviewers, potential customers, and users who are evaluating or using Trend Micro™ Home Network Security.

DOCUMENT PROFILE:

Product: Trend Micro™ Home Network Security 2020 – v6.00.1739

Document Title: Trend Micro™ Home Network Security 2020 - Product Guide v6.0

Document Filename: PG - TM Home Network Security 2020 - Product Guide v6.0

Document Release Date: November 20, 2020

Team: Consumer Technical Product Marketing

Table of Contents

Executive Summary

Figure 1. Trend Micro Home Network Security Station

The modern home is filled with connected devices that provide added convenience, entertainment, and safety for family members. But these new smart devices also open up homes to privacy and security risks, much of which require technical expertise to manage. Issues like hacking, privacy violations and harassment are quickly becoming commonly associated with smart devices. In addition, monitoring and managing their children's internet safety is an ongoing headache for parents. Most homeowners are not security or network experts and are unprepared when it comes to managing their devices or their kids' access to them.

Trend Micro™ Home Network Security (HNS) empowers consumers to manage the security and privacy risks of their smart devices and home network without requiring them to be experts. It equips the home network with an extra layer of protection and offers visibility into smart device security status including threats, vulnerabilities and suspicious behavior.

For parents, HNS provides powerful tools not just for monitoring and managing access to the internet and devices, but also a way to help their kids build up healthy digital habits. Parents are provided with the ability to set flexible limits on time, content and especially YouTube. In addition, they can turn on notifications to receive alerts when children are detecting using potentially inappropriate apps, use the internet for too long or even when they arrive home from school.

An easy-to-use **Home Network Security Smartphone App (HNS App)** for Android and iOS mobile devices lets the "home technology manager" make changes on the go and stay aware of important security events in the home network with timely and insightful notifications. When used with **Trend Micro™ Guardian**, a client app also available for Android and iOS, parental controls can extend to kids' devices outside the home.

For security conscious consumers who are concerned about their own home's cybersecurity risks but don't yet have an HNS Station, the **HNS App – Free Edition** now offers free device and network scanning to detect devices and vulnerabilities in the home network and offers guidance on ways to reduce the risks at home.

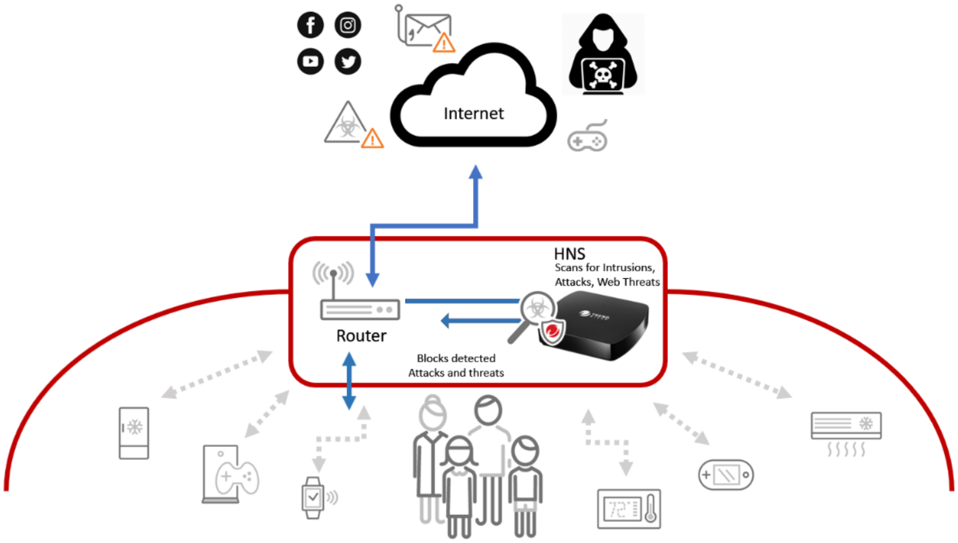

Internet
HNS
Scans for Intrusions, Attacks, Web Threats
Router
Blocks detected Attacks and threats

Figure 2. Protecting Your Smart Home. Trend Micro Home Network Security attaches to your gateway or router to detect and block network attacks, intrusions, and Web threats for all the networked devices in your smart home—and includes easy-to-use parental controls to protect your children.

Trend Micro Home Network Security Highlights

Trend Micro Home Network Security (HNS) provides an easy-to-use security solution to protect all the devices on your network.

- **Free Network and Device Scanner.** For security-conscious smart homeowners, use the HNS App's free scanner to check your network and devices for risks before deciding to purchase an HNS station.
- **Secure, Private Home Network.** Advanced, enterprise-grade Intrusion Prevention technology senses and blocks network attacks before they get to your devices. HNS scans your devices for vulnerabilities, to help you make sure that hackers can't get into your network.
- **Plug-n-Protect.** Unlike other security solutions requiring experts just to install it, our solution is a breeze to set up. Simply plug the HNS Station into your wireless router and a wall socket, download the mobile app, pair the app and the HNS Station—and your home network is immediately protected.
- **Home Device Management.** Check your security status in real-time and manage access for *all* the connected devices in your home—including your smart speakers, security cameras, smart TVs, mobile phones, and even smart home devices like lights and door locks.

- **Internet Safety for Kids and Family.** Set time limits on game consoles. Block access during homework and family time. Prevent mature content from making it to the screens of the immature. Know what they're doing online so you can teach them about using the Internet safely.
- **Extend Internet Safety to Any Network.** Install Trend Micro Guardian on your kid's mobile devices and pair with HNS to provide internet safety and time limits for kids, on any Wi-Fi or mobile network.
- **Anywhere, Anytime Visibility and Control.** Manage your network with our easy-to-use, real-time smartphone app. Customize the internet for family and guests at the touch of a button. Grant or block access to new computers, phones, tablets, or smart home devices entering your network. View Reports to see what's been happening recently on your network.
- **World-Class Protection.** Trend Micro Home Network Security taps into Trend Micro's World-Class AI security system, enabled by the Smart Protection Network (SPN). Your home network and all the devices on it are protected from wide range of threats, including network intrusions, malicious websites and files, default or weak passwords on your network devices, intranet or internet-based malicious behavior, system vulnerabilities, and privacy and network access violations.
- **Advanced Vulnerability Detection.** In HNS version 2.0, a Vulnerability Check was added to the Device Scan that assesses connected devices for high-severity vulnerabilities that have been exploited in the wild. Once a vulnerability is detected, HNS provides users with guidance on how to resolve the vulnerability.
- **Voice Control.** Use Amazon Alexa and Google Assistant voice control to execute commands through your smart speakers to perform specific functions on Trend Micro Home Network Security. See *Voice Control* for the lists of Google Assistant and Echo - Alexa voice commands.
- **Early Access Program.** HNS users now have the opportunity to try the very latest in security and protection for their network and devices. Early Access features include:
  - **Smart Alert.** HNS alerts you when any of your devices are behaving unusually. This new feature uses machine learning to first understand what behavior is normal for a device and then informs you if a device's behavior departs from the expected.
  - **Router Access Protection.** HNS helps prevent hackers from gaining control of your router and making changes to important settings that can leave your network and devices vulnerable. With Router Access Protection enabled, all attempts to login to your router will be blocked unless approved.
  - **Ad Block.** HNS helps you protect your family's privacy by blocking ads on all devices. It also brings the added benefit of faster load times for some sites.
  - **Cyberattack Shield.** HNS will deploy real-time emergency security policy to your network from the cloud in case of a global threat outbreak to prevent further spreading of threats like ransomware and botnets.

Section 1: Detailed Product Specifications

Key Features

Table 1. Trend Micro Home Network Security Key Features

TREND MICRO HOME NETWORK SECURITY		With Station	App Only
SECURITY			
THREAT BLOCKING	Internet (WAN) Traffic*	Yes	No
Intrusion Prevention (IPS)	Local (LAN) Traffic*	Yes	No
Web Threat Protection	Web Reputation Filtering	Yes	No
	Cloud File Scan	Yes	No
ACCESS CONTROL	New Device Approval	Yes	No
	Remote Access Protection	Yes	No
DEVICE SCAN	Password Check	Yes	No
	Vulnerability Check	Yes	Yes
PARENTAL CONTROLS			
WEB ACCESS CONTROL AND MONITORING	Daily Time Quota	Yes	No
	Customizable Schedule	Yes	No
	Pause Internet Access by Profile	Yes	No
	Online Connectivity Monitoring	Yes	No
WEBSITE & CONTENT FILTERING	Website Filtering	Yes	No
	Google Safe Search	Yes	No
	YouTube Restricted Mode	Yes	No
APP CONTROLS	YouTube Pause and Time Limits	Yes	No
	App Detection	Yes	No
TREND MICRO GUARDIAN	On-the-go Protection for Kids	Yes	No

TREND MICRO HOME NETWORK SECURITY		With Station	App Only
MANAGEMENT			
DEVICE MANAGEMENT	Profile-based Management	Yes	No
	Device Management	Yes	No
	Device Detection	Yes	Yes
	Device Approval	Yes	No
	Device Blocking	Yes	No
VISIBILITY	Notifications	Yes	No
	Dashboard	Yes	Yes
	View Report	Yes	No
	Timeline	Yes	No
	Network Usage	Yes	No
USER INTERFACE	Smartphone / Tablet	Yes	Yes
	Voice Control: Alexa, Google	Yes	No

Station Specifications

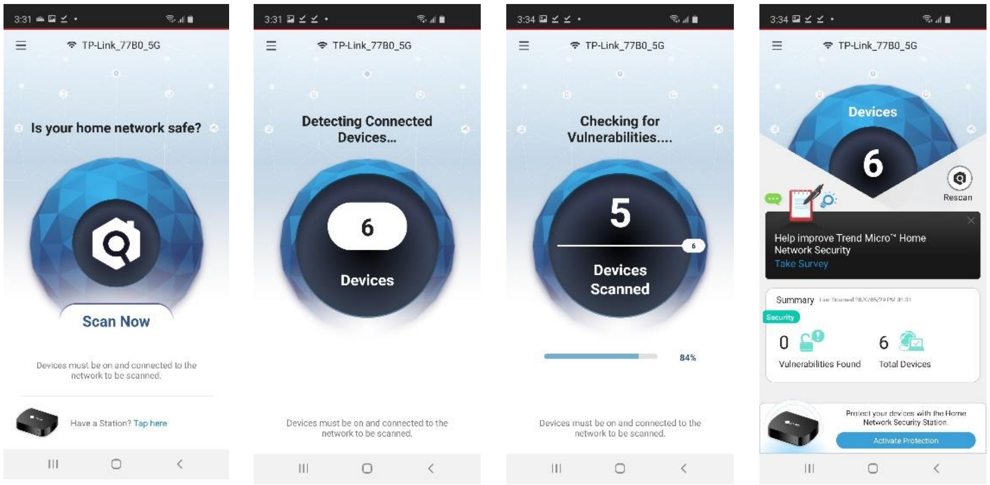
Table 2. Station Specifications

Trend Micro Home Network Security Station	
Dimensions	Length: 136.27 mm Width: 110.99 mm Height: 31.20 mm
Color	Black
Weight	0.5 lb. (226 g)
CPU	Dual Core 1.3 GHz
RAM	512 MB DDR3
Flash Memory	4 GB eMMC
Ports	1 Gbps Ethernet
Power Adaptor	AC Input: 90~260 VAC 47~63 Hz DC Output: 12V/1A Energy Star Version 2.0 Level VI efficiency requirements

Starting with the HNS App

The Trend Micro Home Network Security App (HNS App) is available for download on the Google Play Store and the Apple App Store. You can use the HNS App without the HNS Station to scan your network and discover vulnerabilities in your devices.

1. Ensure your phone is connected to the same network as the devices you wish to scan and that the devices are up and running.
2. Type "Trend Micro Home Network Security" into the app store search field. When you find the HNS App, download and install it on your Android or iOS smartphone.
3. Open the HNS App and tap **Scan Now** to conduct a free scan of your network. The HNS App will return the result and alert you if there are any issues on your network or your devices.
4. To address the issues highlighted by the scan, the user can purchase an HSN Station, then pair the HNS App to the Station.



Devices must be on and connected to the network to be scanned.

Help improve Trend Micro™ Home Network Security

Protect your devices with the Home Network Security Station.

Figure 3. HNS App - Scan Now – Activate Protection

Router Compatibility List

Before purchasing a Trend Micro Home Network Security Station (HNS Station), make sure your home Wi-Fi-capable router is compatible with the HNS Station and that it has an available Ethernet port to attach the HNS Station. You can check the Router Compatibility List on the Trend Micro Home Network Security Help pages to see if your router is on the list.

Pairing the HNS App and Station

The HNS App works with the HNS Station to address a wide range of security issues on your home network and its smart devices. With most routers, the installation flow is as follows:

1. Plug the HNS Station *directly into a free LAN port on your router* (do *not* plug into a switch) and then plug in the power.

2. If you haven't already done so (see the previous section), download and install the HNS app on your Android or iOS smartphone. Again, the smartphone should be on the same network you wish to protect.
3. Locate the link in the HNS App Console. If you haven't done a scan, click **Tap Here** to begin the pairing and activation process. If you have done a scan, click **Activate Protection** to begin the pairing and activation process.
4. Follow the prompts to pair the HNS Station and the HNS App on your smartphone to activate the service.

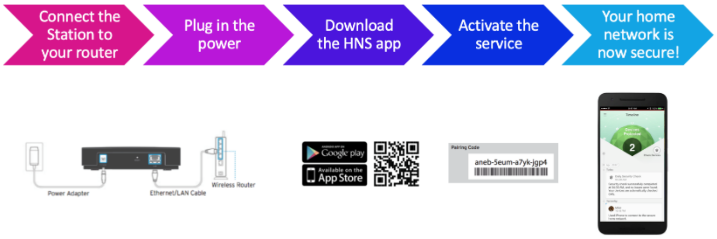


Figure 4. HNS Setup Flow

Minimum Requirements

The minimum requirements for using Trend Micro Home Network Security are:

- A working internet connection.
- A **compatible router** with a free LAN port. To ensure the optimal experience with Home Network Security make sure you are using a compatible router. Again, click here for the Router Compatibility List).
- A smartphone or tablet: Android 5.0+ or iOS 12.0+.

Target Audience

The primary users of Trend Micro Home Network Security are the "house geek" who's responsible for setting up the network and monitoring the smart devices in the home, while keeping them—and the family members who use them—safe from hackers and malware; and protective parents, who want to make sure their kids stay safe from threats and protected from unwanted content on the Internet.

Global Availability

Available now (2020) in the United States, Japan, Australia, New Zealand and Singapore.

Contacting Trend Micro

United States

Trend Micro Incorporated
225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900
Toll-free: (888) 762-8763
www.trendmicro.com

Japan

Shinjuku MAYNDS Tower
2-1-1 Yoyogi, Shibuya-ku
Tokyo, Japan ZIP 151-0053
Phone: +81.3.5334.3618
www.trendmicro.co.jp

Australia and New Zealand

Level 15, 1 Pacific Highway
North Sydney, NSW 2060
Australia
Toll-free: 1-800-642-421
www.trendmicro.com.au

Singapore

6 Temasek Boulevard #16-01 to 05 Suntec Tower Four
Singapore 038986
Phone: +65 6379 2060
www.trendmicro.com.sg

Free Phone, Email and Chat support

Trend Micro offers free phone, email, and chat support. For more info, go to Trend Micro Home and Home Office Support and more specifically to the Trend Micro Home Network Security support page.

You can also go to the Trend Micro Home Users Community to get your questions answered and problems solved.

Free ransomware-specific tech support is provided for all users, whether you are a customer or not, by calling 1-877-558-7363 between 5:00 a.m. to 9:00 p.m. PST, Monday through Friday.

Premium Support Services

Trend Micro provides users with Premium Support Services for a wide variety of technical issues including installation, virus and spyware removal, PC Tune-ups, etc. These services are offered as a bundle with a purchase of Trend Micro Security or as stand-alone and ad-hoc services.

Section 2: The Home Network Security Application and Station

The free **Home Network Security Application (HNS App)**, all on its own, allows you to scan your network to discover its devices and vulnerabilities.

However, the **HNS App** also provides setup, monitoring, and control of your **Home Network Security Station (HNS Station)** and all the devices it protects on your network. You can purchase the HNS Station online, from the Trend Micro Store; or from a retail outlet.

In the following screens, the **HNS App** version shown is v6.001739, taken from an Android device. The screens for the iOS version are identical.

Install the HNS App and Conduct a Network Scan

To install the HNS App:

1. Launch **Google Play** (or the Apple **App Store**) and search for **Trend Micro Home Network Security.**
2. When it appears, tap **Home Network Security,** then **Install**.

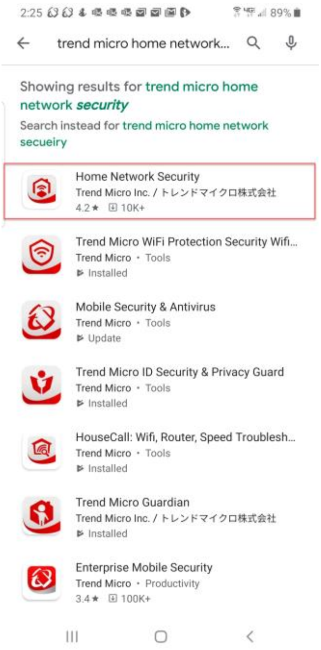

2:25
89%
trend micro home network...
Showing results for trend micro home network security
Search instead for trend micro home network secueiry
Home Network Security
Trend Micro Inc. / トレンドマイクロ株式会社
4.2★ 10K+
Trend Micro WiFi Protection Security Wifi...
Trend Micro • Tools
Installed
Mobile Security & Antivirus
Trend Micro • Tools
Update
Trend Micro ID Security & Privacy Guard
Trend Micro • Tools
Installed
HouseCall: Wifi, Router, Speed Troublesh...
Trend Micro • Tools
Installed
Trend Micro Guardian
Trend Micro Inc. / トレンドマイクロ株式会社
Installed
Enterprise Mobile Security
Trend Micro • Productivity
3.4★ 100K+

Figure 5. Home Network Security

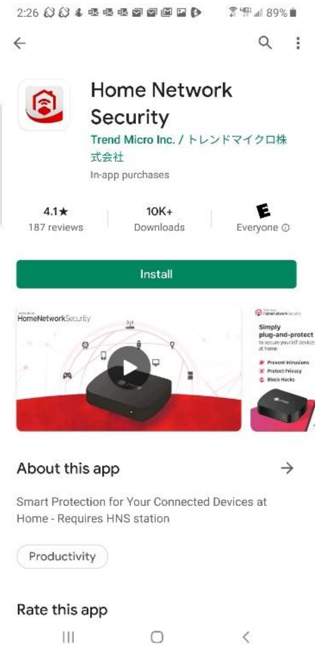
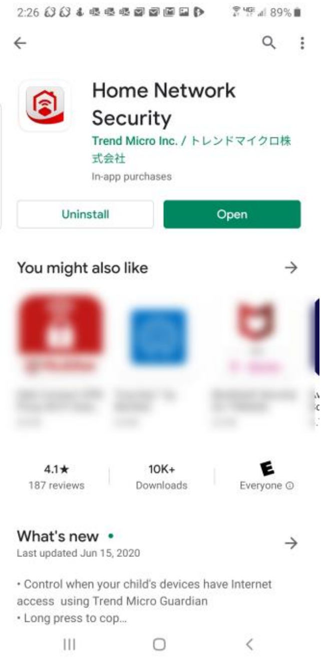


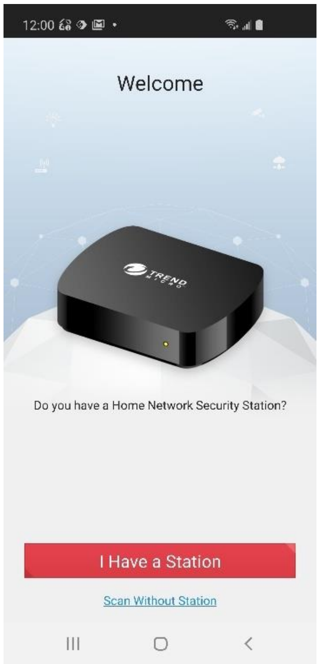
Figure 6. Install Home Network Security

3. When installation is complete, tap **Open** to launch the app.
4. The **Welcome** screen appears.
5. In this example, you do not yet have an **HNS Station** connected to the network, so click **Scan Without Station.**



• Control when your child's devices have Internet access using Trend Micro Guardian
• Long press to cop...

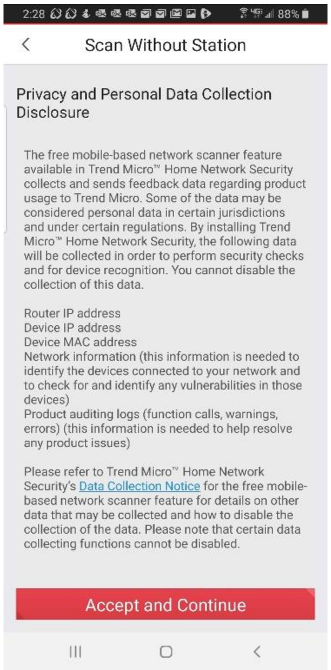
Figure 7. Open HNS App



Do you have a Home Network Security Station?

Figure 8. Scan Without Station

6. The **Privacy and Personal Data Collection Disclosure** appears.
7. Read the **Disclosure**. If you agree to the terms, tap **Accept and Continue.**
8. A screen appears, indicating you wish to scan your home network and its connected devices for risks. **Tap Trend Micro terms and conditions** to read the conditions.
9. If you agree to the conditions, click **Accept and Continue.**



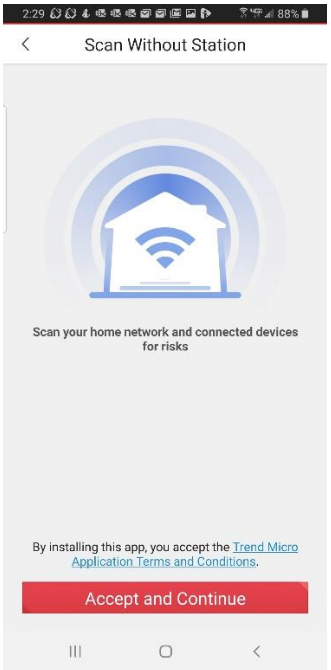
Privacy and Personal Data Collection Disclosure

The free mobile-based network scanner feature available in Trend Micro™ Home Network Security collects and sends feedback data regarding product usage to Trend Micro. Some of the data may be considered personal data in certain jurisdictions and under certain regulations. By installing Trend Micro™ Home Network Security, the following data will be collected in order to perform security checks and for device recognition. You cannot disable the collection of this data.

Router IP address
Device IP address
Device MAC address
Network information (this information is needed to identify the devices connected to your network and to check for and identify any vulnerabilities in those devices)
Product auditing logs (function calls, warnings, errors) (this information is needed to help resolve any product issues)

Please refer to Trend Micro™ Home Network Security's Data Collection Notice for the free mobile-based network scanner feature for details on other data that may be collected and how to disable the collection of the data. Please note that certain data collecting functions cannot be disabled.

Figure 9. Privacy and Personal Data Collection Disclosure

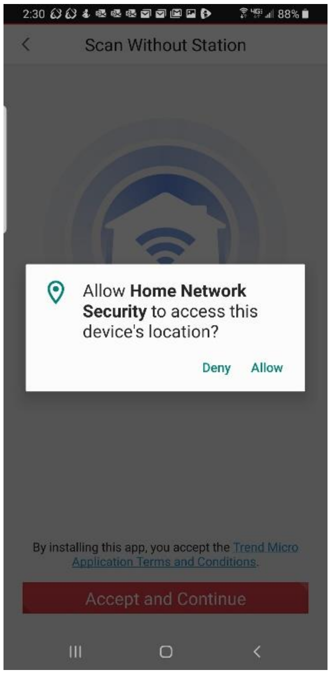


Scan your home network and connected devices for risks

By installing this app, you accept the Trend Micro Application Terms and Conditions.

Figure 10. Accept and Continue

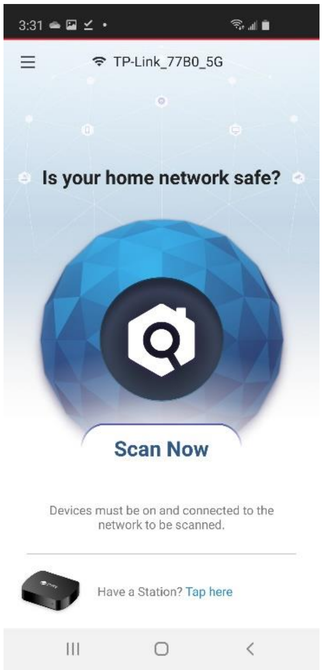
10. A popup appears, asking **Allow Home Network Security to access this device's location?**
11. If you agree, tap **Allow.**
12. The **Scan Now** screen appears, asking **Is your home network safe?**
13. Click **Scan Now** to conduct a scan and find out.



Allow **Home Network Security** to access this device's location?

By installing this app, you accept the Trend Micro Application Terms and Conditions.

Figure 11. Access Location



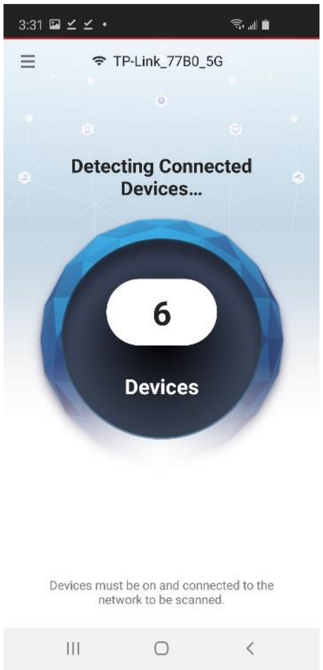
Is your home network safe?

Devices must be on and connected to the network to be scanned.

Have a Station? Tap here

Figure 12. Scan Now

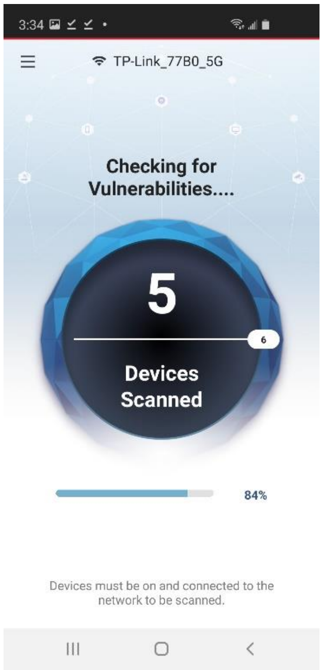
14. As the **HNS App** conducts the scan, it informs you it's **Detecting Connected Devices.**
15. It then informs you that it's **Checking for Vulnerabilities.**



Detecting Connected Devices...

Devices must be on and connected to the network to be scanned.

Figure 13. Detecting Network Devices



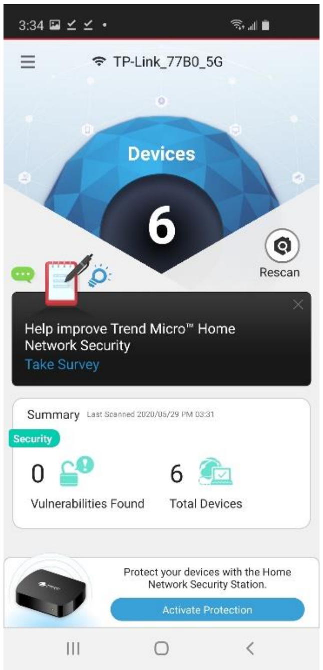
Checking for Vulnerabilities....

Devices must be on and connected to the network to be scanned.

Figure 14. Checking for Vulnerabilities

16. When the scan is complete, it informs you of the **Total Devices** and the number of **Vulnerabilities Found.**

17. Tap the various panels and screens to get an idea for what the full solution with the **Home Network Security Station** provides.



Help improve Trend Micro™ Home Network Security

Last Scanned 2020/05/29 PM 03:31

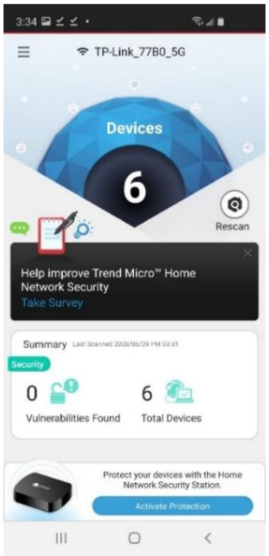
Protect your devices with the Home Network Security Station.

Figure 15. Total Devices and Vulnerabilities Found

To Learn More or Purchase a Home Network Security Station

To learn more or purchase a Home Network Security Station:

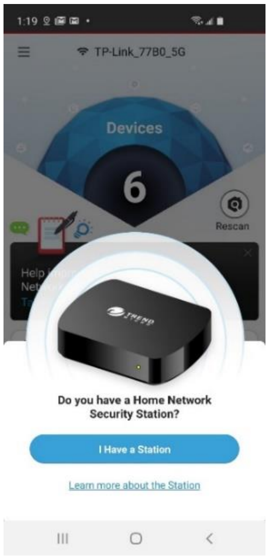
1. To find out about or to purchase the **Home Network Security Station**, click **Activate Protection**
2. A screen appears, asking **Do you have a Home Network Security Station?**
3. If you wish to purchase an HNS Station, click the link **Learn More About the Station.**



Help improve Trend Micro™ Home Network Security

Protect your devices with the Home Network Security Station.

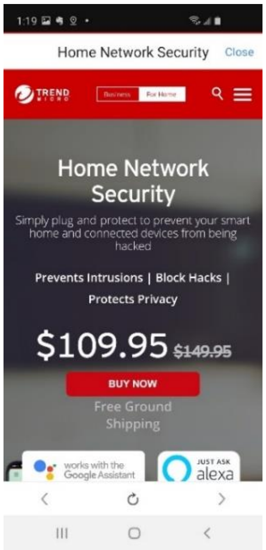
Figure 16. Activate Protection



Do you have a Home Network Security Station?

Figure 17. Learn More About the Station

4. Your browser loads and takes you to the **Home Network Security** webpage, where you can learn more or purchase an **HNS Station.**
5. Click **Buy Now** to purchase an **HNS Station**, then follow the prompts to complete your transaction.



Simply plug and protect to prevent your smart home and connected devices from being hacked

Figure 18. Home Network Security Webpage

Set Up the Station, Pair it with the HNS App, and Do a Network Scan

Once you receive your **Trend Micro Home Network Security Station (HNS Station)**, you need to set it up properly and pair it with the **Trend Micro Home Network Security App (HNS App)**, which you've already installed.

To set up the Station:

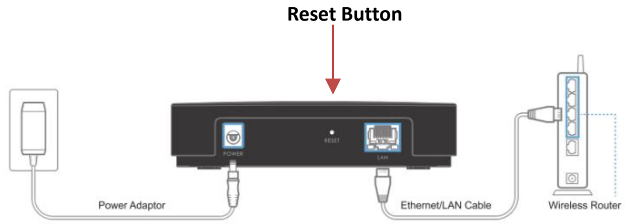


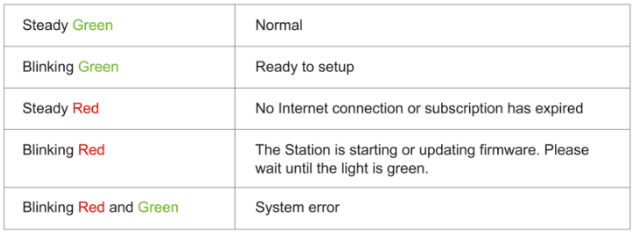
Figure 19. Back: Home Network Security – Power Adaptor, Reset Button, Router Ethernet Port Connection

1. Plug the power adaptor and the Ethernet/LAN cable into the **Station**.
2. Connect the **Station** *directly* to one of your wireless router's Ethernet/LAN ports and plug the power adapter into a power outlet.

   Important Note: There should be *no other device*, such as a switch, between your Router and the Station.

Figure 20. Front: Station Ready

3. When the light turns a **Blinking Green**, the **Station** is ready to set up.
4. If the light remains red for more than 1 minute, consult the **Light Status** table shown here.



Steady Green	Normal
Blinking Green	Ready to setup
Steady Red	No Internet connection or subscription has expired
Blinking Red	The Station is starting or updating firmware. Please wait until the light is green.
Blinking Red and Green	System error

Figure 21. Light Status

5. If the **Station** doesn't achieve a **Blinking Green**, you may need to reset the device by pushing a paperclip end into the **Reset** button for 5 seconds.

6. When the light on the **Station** is **Blinking Green**, connect your phone to the same Wi-Fi network as the **Station**.

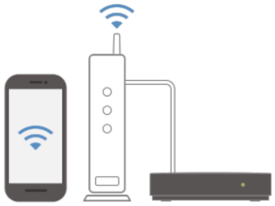
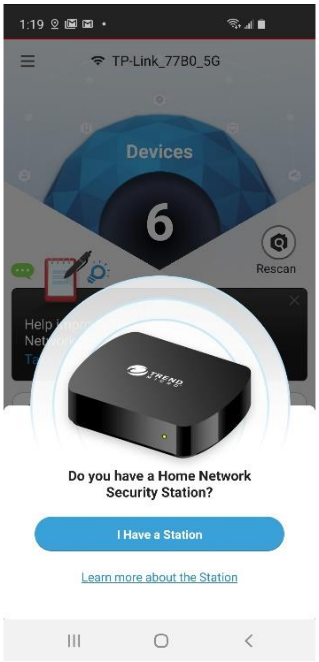


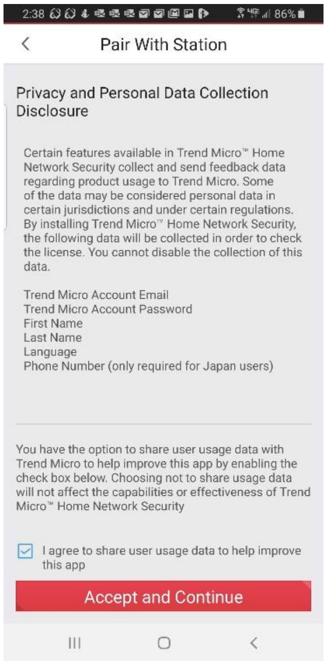
Figure 22. Connect to Same Wi-Fi Network

7. Since you've already installed the **HNS App** (see **HNS App Installation** section above), tap the **HNS App** icon on your smartphone to open the app.
8. Tap **I Have a Station.** The **Privacy and Personal Data Collection Disclosure** appears.
9. Read the **Disclosure**. If you accept, tap **I agree to share user usage data to help improve this app,** then tap **Accept and Continue.**



Do you have a Home Network Security Station?

Figure 23. I Have a Station



Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro™ Home Network Security collect and send feedback data regarding product usage to Trend Micro. Some of the data may be considered personal data in certain jurisdictions and under certain regulations. By installing Trend Micro™ Home Network Security, the following data will be collected in order to check the license. You cannot disable the collection of this data.

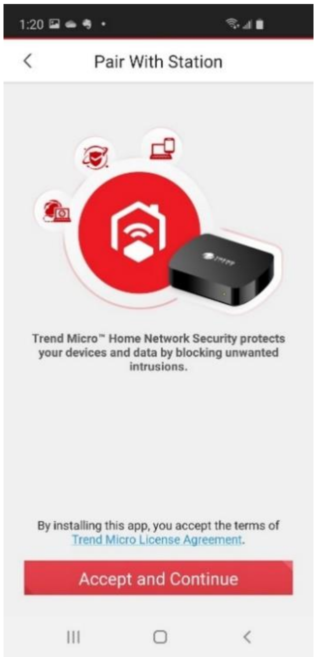
Trend Micro Account Email
Trend Micro Account Password
First Name
Last Name
Language
Phone Number (only required for Japan users)

You have the option to share user usage data with Trend Micro to help improve this app by enabling the check box below. Choosing not to share usage data will not affect the capabilities or effectiveness of Trend Micro™ Home Network Security

☑ I agree to share user usage data to help improve this app

Figure 24. Privacy and Personal Data Collection Disclosure

10. A screen appears, to start the pairing process. **Tap Accept and Continue.**
11. If you haven't already connected the **HNS Station** directly to your Router, do so now and make sure the **HNS Station** light is **Blinking Green**. Otherwise, click **Next**.



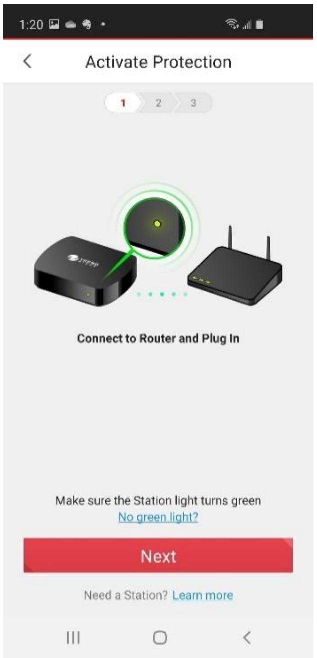
1:20

Pair With Station

Trend Micro™ Home Network Security protects your devices and data by blocking unwanted intrusions.

By installing this app, you accept the terms of Trend Micro License Agreement.

Figure 25. Accept and Continue



1:20

Activate Protection

Connect to Router and Plug In

Make sure the Station light turns green

No green light?

Need a Station? Learn more

Figure 26. Next

12. Type the **Pairing Code** without dashes into the **Pair with the Station** field. The code is on the bottom of the **HNS Station** or in the card provided in your HNS box. Then click **Next**.
13. A **Connecting** screen appears showing that the **HNS App** is pairing with the **Station**.

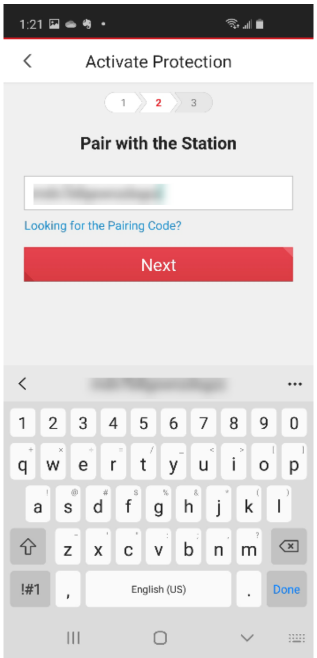
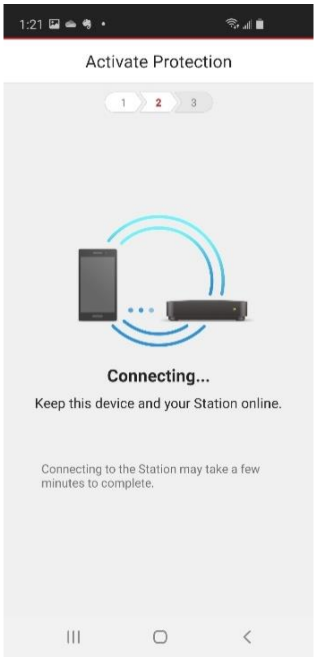


Figure 27. Pair with the Station



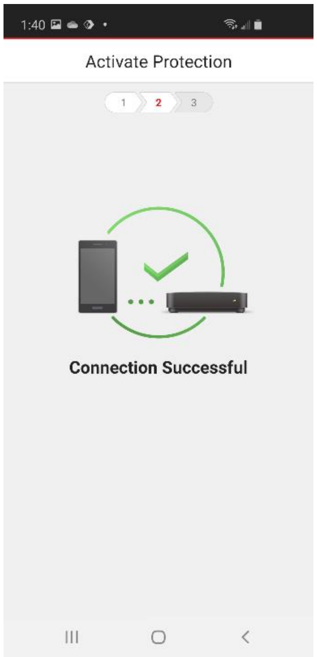
Connecting...

Keep this device and your Station online.

Connecting to the Station may take a few minutes to complete.

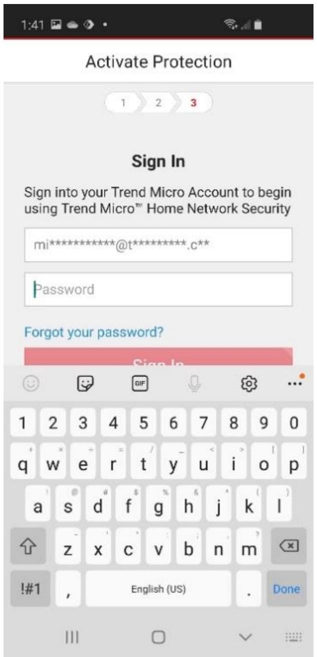
Figure 28. Connecting

14. When the pairing completes, a screen appears saying **Connection Successful.**
15. Another screen appears, prompting you to **Sign In** to your Trend Micro Account. Type the username and password you used to create your account during purchase, then click **Sign In.**



Connection Successful

Figure 29. Connection Successful



Sign In

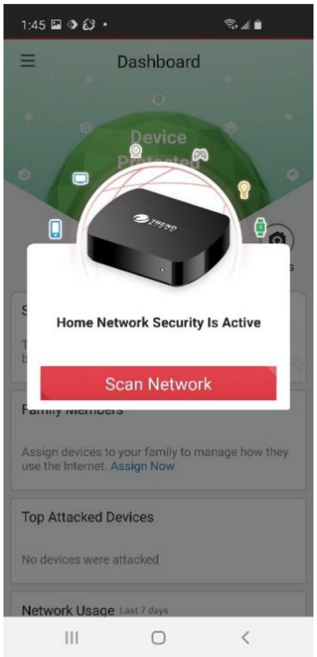
Sign into your Trend Micro Account to begin using Trend Micro™ Home Network Security

mi***********@t*********.c**

Password

Figure 30. Sign In

16. Once you’re signed in, the **HNS Station** activates and the **Dashboard** prompts you to **Scan Network.**
17. Tap **Scan Network.** A screen appears showing you that its **Starting Network Check.**

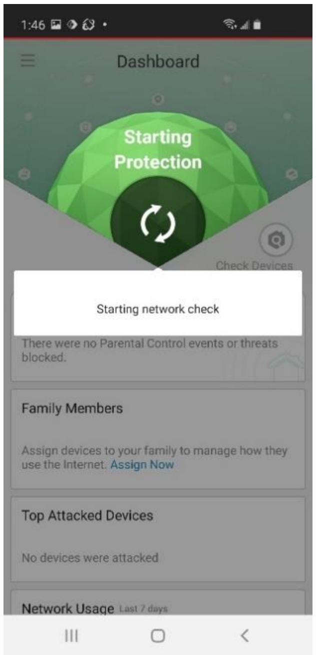


Home Network Security Is Active

Assign devices to your family to manage how they use the Internet. Assign Now

No devices were attacked

Figure 31. Scan Network



Starting network check

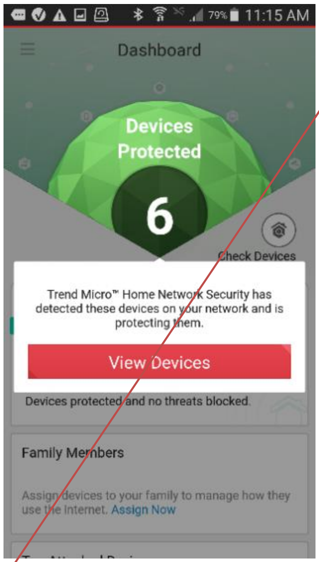
There were no Parental Control events or threats blocked.

Assign devices to your family to manage how they use the Internet. Assign Now

No devices were attacked

Figure 32. Starting Network Check

18. When the scan is complete, it shows the number of devices it has found on your network and prompts you to **View Devices.**
19. Tap the **View Devices** button to view your network devices.
20. **Home Network Security** provides you with a list of **All Devices** on the network.
21. Return to the **Dashboard** by tapping the three-bar **Command Menu Icon** in the upper left corner.

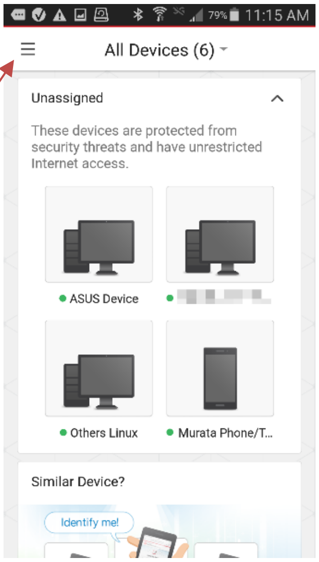


Trend Micro™ Home Network Security has detected these devices on your network and is protecting them.

Devices protected and no threats blocked.

Assign devices to your family to manage how they use the Internet. Assign Now

Figure 33. View Devices



These devices are protected from security threats and have unrestricted Internet access.

Figure 34. All Devices

22. Then tap **Dashboard** item in the menu.
23. View the **Dashboard** items by scrolling down the **Dashboard** screen.

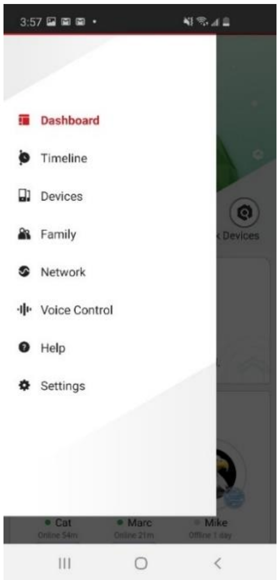
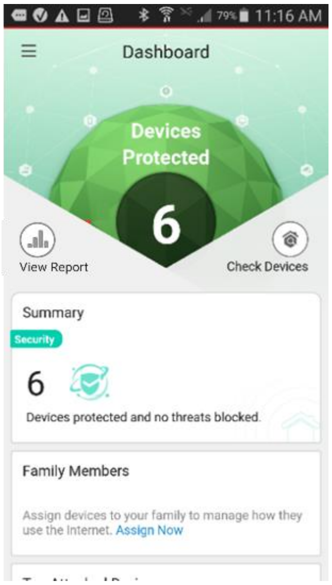


Figure 35. Command Menu

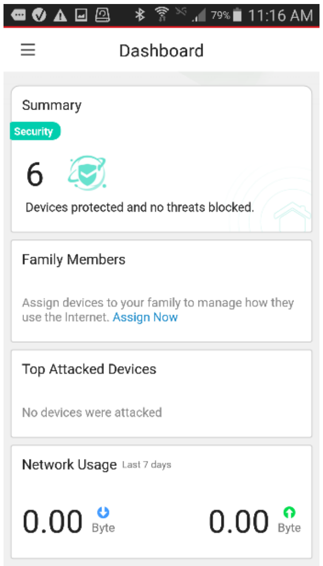


Devices protected and no threats blocked.

Assign devices to your family to manage how they use the Internet. Assign Now

Figure 36. Dashboard

24. Tap **Family Members: Assign Now**, then **Add Someone** to begin to creating family members and assigning devices to them. (See the **Family** section below to learn how to do this.)
25. Congratulations! You're all set up! You may now begin using **Trend Micro Home Network Security** to monitor and manage all the smart devices on your network.



Devices protected and no threats blocked.

Assign devices to your family to manage how they use the Internet. Assign Now

No devices were attacked

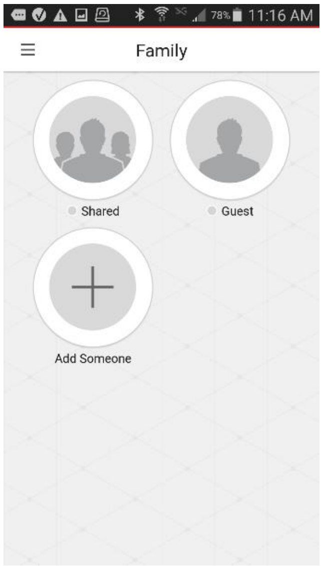


Figure 37. Dashboard Scrolled Down

Figure 38. Family

Dashboard

The HNS App's **Dashboard** provides a quick overview of all the monitoring and security functions of Home Network Security, with easy-to-use screens showing the security status of all the connected devices on your network.

Check Devices

To check devices and actions required:

1. Tap the **Home Network Security (HNS)** icon on your home screen of your mobile device to open the **HNS App Console**. The **Console** opens and displays the **Dashboard**.
2. You can access any screen in the **Console** by tapping the **Command Menu** icon in the upper left-hand corner. The **Command Menu** displays, with menu items for all the main functions of the **HNS App.**

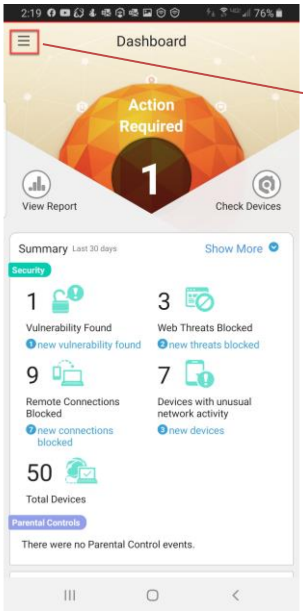


Figure 39. Dashboard | Command Menu

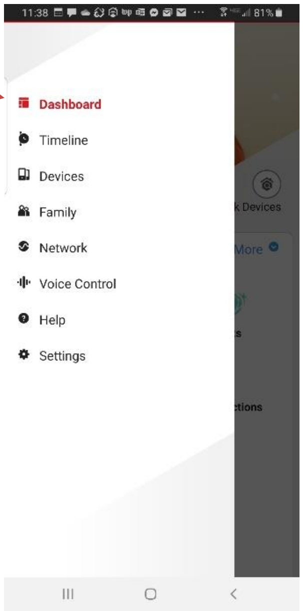
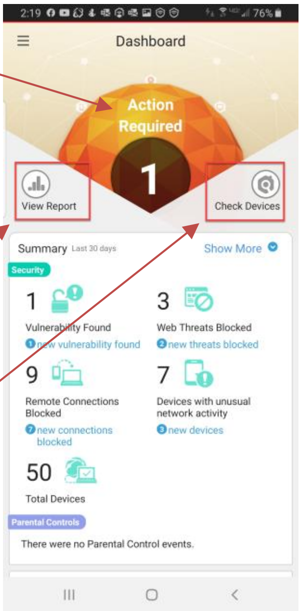


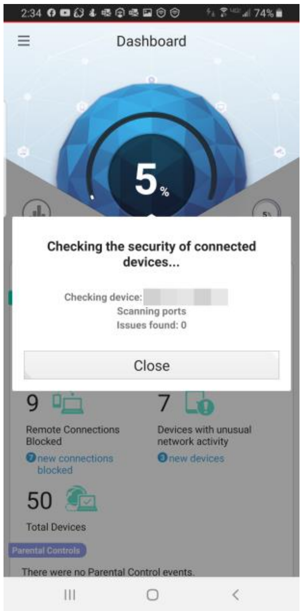
Figure 40. Command Menu > Dashboard Menu Item

3. If there are any past **Action Required** items, they'll display in the **Dashboard** indicator at the top; just tap to review them.
4. To view the report on your network, tap **View Report.**
5. To find all the connected devices on your network and to check their security, tap **Check Devices**.
6. **HNS** conducts a network scan to determine what devices are connected to your network and to check their security status, providing a **Progress Indicator** and a popup showing the progress of the scan.



There were no Parental Control events.

Figure 41. Dashboard > Action Required > View Report > Check Devices


2:34 74%
Dashboard
5%
Close
9 Remote Connections Blocked
7 new connections blocked
7 Devices with unusual network activity
3 new devices
50 Total Devices
Parental Controls

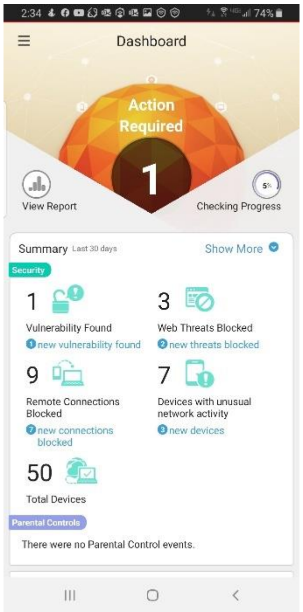
Checking the security of connected devices...

Checking device:
Scanning ports
Issues found: 0

There were no Parental Control events.

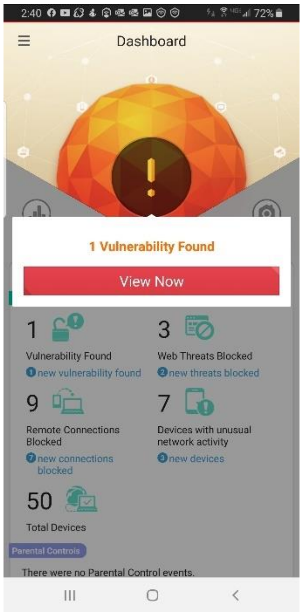
Figure 42. Device Scan Progress Indicator

7. While the scan is being conducted, you can tap the **Back-Arrow** on your device to go back to the **Dashboard**.
8. The **Check Devices** button now shows **Checking Progress.**
9. When the scan is done it returns the result. In this example, **1 Vulnerability Found**.
10. Tap **View Now** to view the issue it has found.



There were no Parental Control events.

Figure 43. Checking Progress

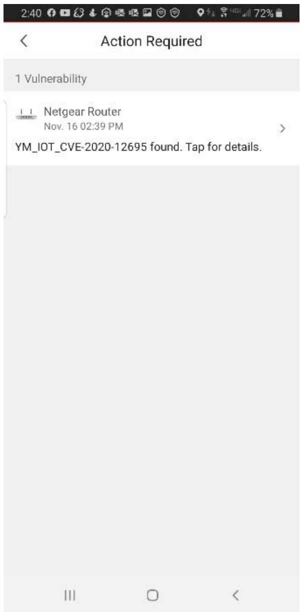


1 Vulnerability Found

There were no Parental Control events.

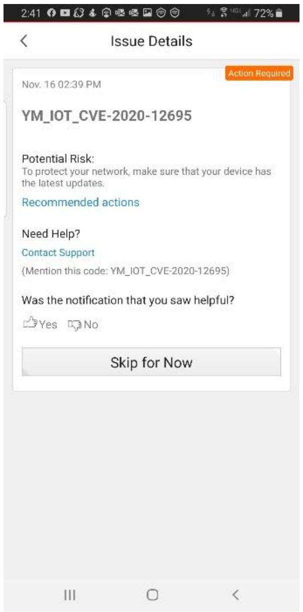
Figure 44. 1 Vulnerability Found

11. In this example, the **Action Required** screen indicates that the router has been discovered with a vulnerability**.**
12. Tap the panel to obtain the **Issue Details.** Read the **Potential Risk** description to understand the issue.
13. Tap **Recommended Actions** to see what **you can** do to resolve the issue. (You can also tap **Skip for Now** to skip the remediation process.)



YM_IOT_CVE-2020-12695 found. Tap for details.

Figure 45. Action Required



YM_IOT_CVE-2020-12695

Potential Risk:
To protect your network, make sure that your device has the latest updates.

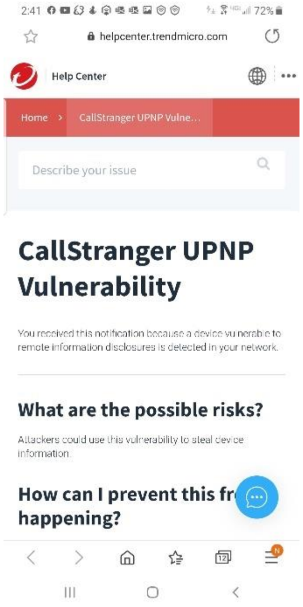
Recommended actions

Need Help?
Contact Support
(Mention this code: YM_IOT_CVE-2020-12695)

Was the notification that you saw helpful?

Figure 46. Issue Details

14. The **HNS App** loads your mobile browser and takes you to the **Trend Micro eSupport** site, which provides more details on the issue and recommended actions.
15. Scroll through the page to learn more about the possible risks, what you can do to prevent the problem from happening in the future, and places to go for more answers to any questions you may have about the issue.



CallStranger UPNP Vulnerability

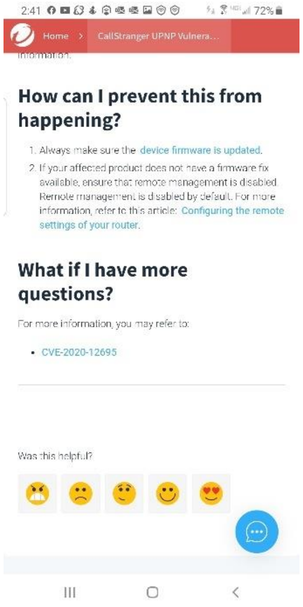
You received this notification because a device vulnerable to remote information disclosures is detected in your network.

What are the possible risks?

Attackers could use this vulnerability to steal device information.

How can I prevent this fr
happening?

Figure 47. eSupport Page



information.

How can I prevent this from happening?

1. Always make sure the device firmware is updated.
2. If your affected product does not have a firmware fix available, ensure that remote management is disabled. Remote management is disabled by default. For more information, refer to this article: Configuring the remote settings of your router.

What if I have more questions?

For more information, you may refer to:

- CVE-2020-12695

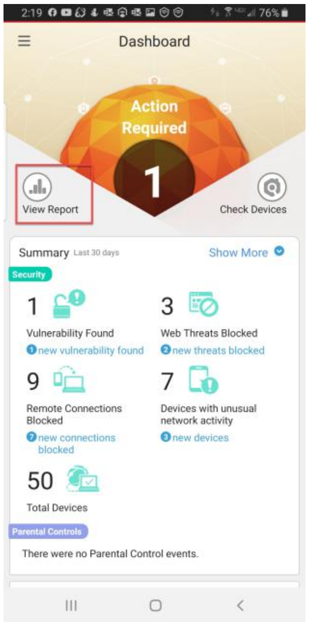
Was this helpful?

Figure 48. eSupport Page (2)

View Report

To View Report:

1. Back in the **Dashboard**, you can tap **View Report** to view a network report. The **Report** screen appears.
2. In the first tab, you can view **Security Events** by the **Past 14 Days: Previous Week** and **This Week,** and **Most Active - By Family Member.**
3. Scroll the **By Family Member** panel left and right, then tap the relevant icon to select the family member you wish to examine.



There were no Parental Control events.

Figure 49. View Report

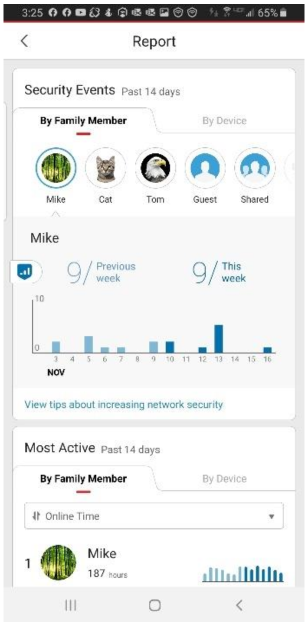
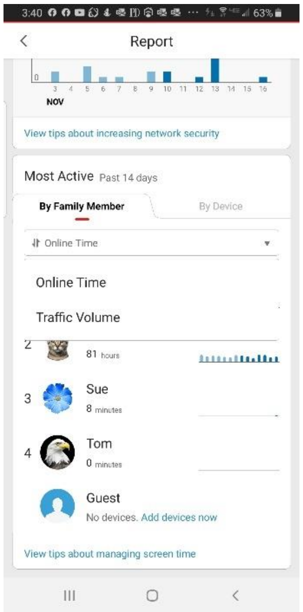


Figure 50. Security Events - By Family Member

4. Scroll down to view **Most Active** members of your network by **Online Time** and **Traffic Volume.**
5. Similarly, view **Security Events - By Device** for the **Past 14 Days** by tapping the device you wish to examine in the scrollbar.



View tips about increasing network security

Most Active Past 14 days

By Family Member | By Device

Online Time ▾

Online Time

Traffic Volume

2 81 hours

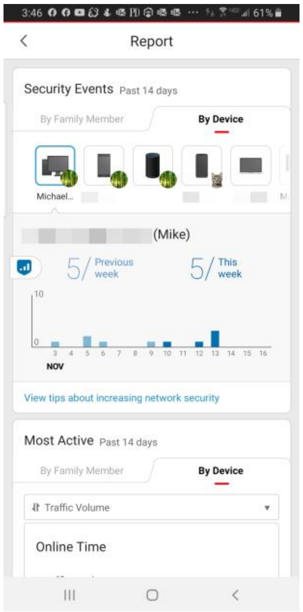
3 Sue 8 minutes

4 Tom 0 minutes

Guest No devices. Add devices now

View tips about managing screen time

Figure 51. Most Active | Online Time | Traffic Volume - By Family Member



Security Events Past 14 days

By Family Member | By Device

[redacted] (Mike)

5/ Previous week 5/ This week

View tips about increasing network security

Most Active Past 14 days

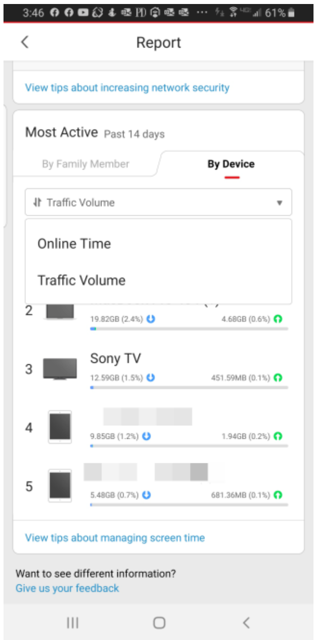
By Family Member | By Device

Traffic Volume ▾

Online Time

Figure 52. Security Events - By Device

6. Or scroll down to view **Most Active** for the **Past 14 Days - By Device**, either for **Online Time** or **Traffic Volume.**
7. Click the blue links to **View tips** about **increasing network security** or **managing screen time.**



View tips about increasing network security

Most Active Past 14 days

By Family Member | By Device

Traffic Volume ▾

Online Time

Traffic Volume

2 19.82GB (2.4%) 4.68GB (0.6%)

3 Sony TV 12.59GB (1.5%) 451.59MB (0.1%)

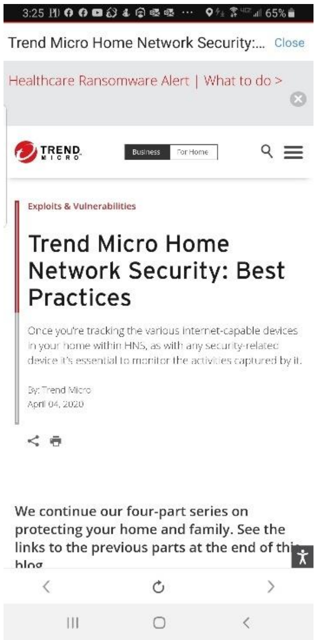
4 [redacted] 9.85GB (1.2%) 1.94GB (0.2%)

5 [redacted] 5.48GB (0.7%) 681.36MB (0.1%)

View tips about managing screen time

Want to see different information?
Give us your feedback

Figure 53. Most Active | Online Time | Traffic Volume – By Device



Trend Micro Home Network Security:... Close

Healthcare Ransomware Alert | What to do >

Exploits & Vulnerabilities

Trend Micro Home Network Security: Best Practices

Once you're tracking the various Internet-capable devices in your home within HNS, as with any security-related device it's essential to monitor the activities captured by it.

By: Trend Micro
April 04, 2020

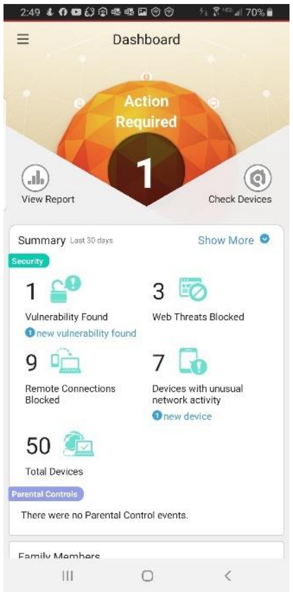
We continue our four-part series on protecting your home and family. See the links to the previous parts at the end of thi
blog

Figure 54. Tips - Best Practices

Using the Dashboard

To review Dashboard items:

1. Back in the **Dashboard**, you can review HNS **Summary** protection results in the **Security, Parental Controls, Family Members, Top Attacked Devices**, and **Network Usage** panels.
2. Tap the link **Show More/Show Less** to show more or less detail respectively.



There were no Parental Control events.

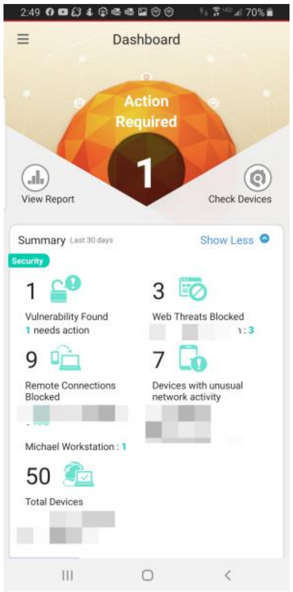
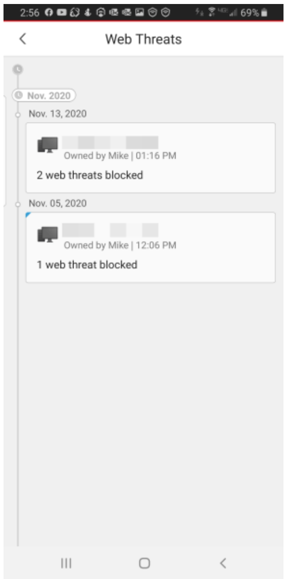


Figure 55. Summary Items > Showing Less

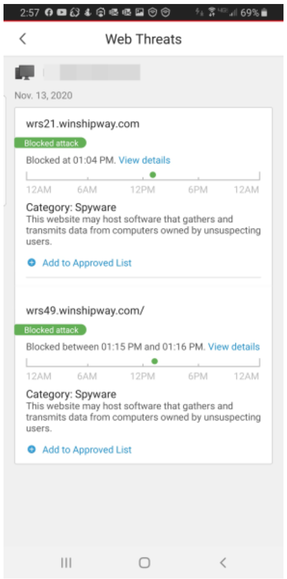
Figure 56. Summary Items > Showing More

3. Tap individual items, e.g., **Vulnerability Found, Web Threats Blocked, Remote Connections Blocked, etc.,** to reveal information on the various threats by device.
4. Tap individual panels to show additional details about particular attacks or threats.



[redacted]
Owned by Mike | 01:16 PM
2 web threats blocked

[redacted]
Owned by Mike | 12:06 PM
1 web threat blocked



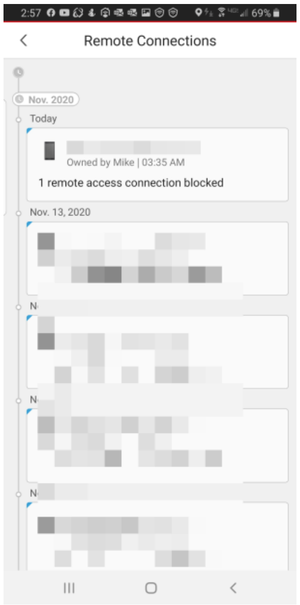
wrs21.winshipway.com
Blocked attack
Blocked at 01:04 PM. View details
Category: Spyware
This website may host software that gathers and transmits data from computers owned by unsuspecting users.
Add to Approved List

wrs49.winshipway.com/
Blocked attack
Blocked between 01:15 PM and 01:16 PM. View details
Category: Spyware
This website may host software that gathers and transmits data from computers owned by unsuspecting users.
Add to Approved List

Figure 57. Network Attacks

Figure 58. Network Attacks Detail

5. Do the same for **Remote Connections, Total Devices Protected.**
6. Again, tap individual panels to show details about the particular security issue: e.g. the **Remote Access** application blocked.



Nov. 2020

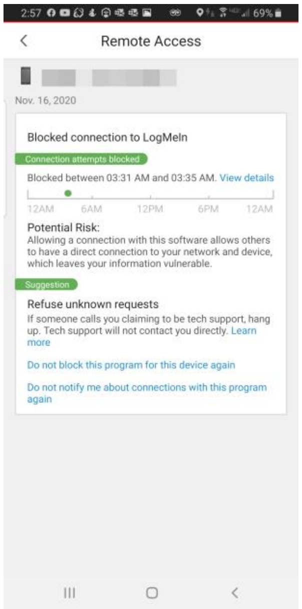
Today

Owned by Mike | 03:35 AM

1 remote access connection blocked

Nov. 13, 2020

Figure 59. Remote Connections



Nov. 16, 2020

Blocked connection to LogMeIn

Connection attempts blocked

Blocked between 03:31 AM and 03:35 AM. View details

Potential Risk:
Allowing a connection with this software allows others to have a direct connection to your network and device, which leaves your information vulnerable.

Suggestion

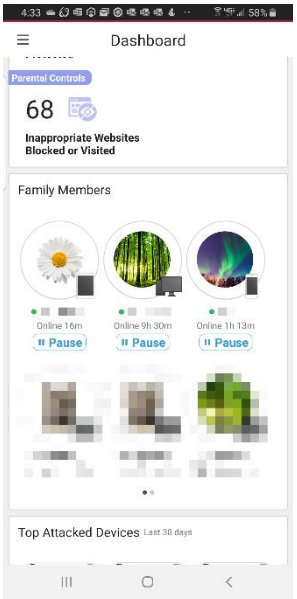
Refuse unknown requests
If someone calls you claiming to be tech support, hang up. Tech support will not contact you directly. Learn more

Do not block this program for this device again

Do not notify me about connections with this program again

Figure 60. Remote Access App Blocked

7. Tap the **Parental Controls** panel to view **Inappropriate Websites Blocked** or **Visited**.
8. Tap the panels for the individual instances to get more details on the violation.
9. In the **Family Members** panel, tap an individual family member to access the **Report, Settings,** and **Device(s)** controlled by the member.



68

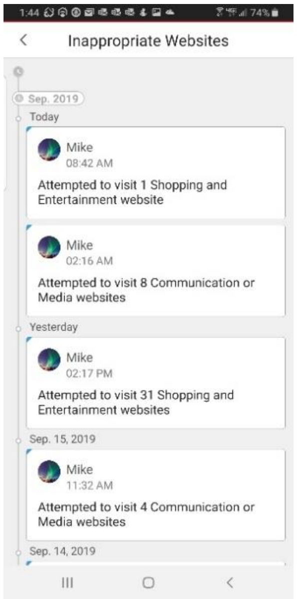
Inappropriate Websites Blocked or Visited

Online 16m

Online 9h 30m

Online 1h 13m

Figure 61. Family Members



Sep. 2019

Today

Mike
08:42 AM
Attempted to visit 1 Shopping and Entertainment website

Mike
02:16 AM
Attempted to visit 8 Communication or Media websites

Yesterday

Mike
02:17 PM
Attempted to visit 31 Shopping and Entertainment websites

Sep. 15, 2019

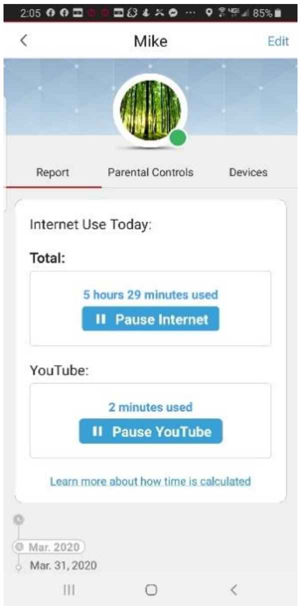
Mike
11:32 AM
Attempted to visit 4 Communication or Media websites

Sep. 14, 2019

Figure 62. Inappropriate Websites

10. The family member’s **Report** informs you about their **Internet Use Today,** including the **Total** number of hours and minutes used, and the total amount of time they spent watching **YouTube.**
11. Tap the **Pause** buttons to **Pause Internet** or **Pause YouTube** for that family member. Tap it again to **Resume** the usage.
12. Tap **Parental Controls** for that person. Here you can set up **Trend Micro Guardian** to protect your kids away from home, **Filtering, Inappropriate App(s) Used, Time Limits,** and **Connection Alert(s).**

    (See the **Family** section in this guide for setup details.



Internet Use Today:

Total:

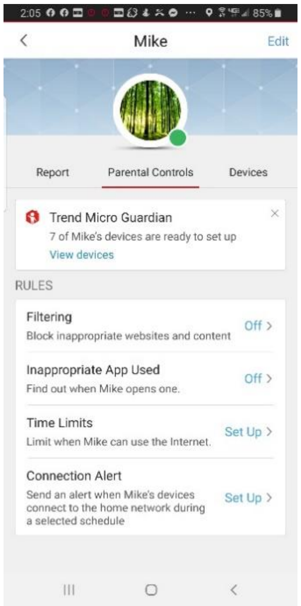
5 hours 29 minutes used

YouTube:

2 minutes used

Mar. 31, 2020

Figure 63. Pause Internet or YouTube



Trend Micro Guardian
7 of Mike's devices are ready to set up

Filtering
Block inappropriate websites and content

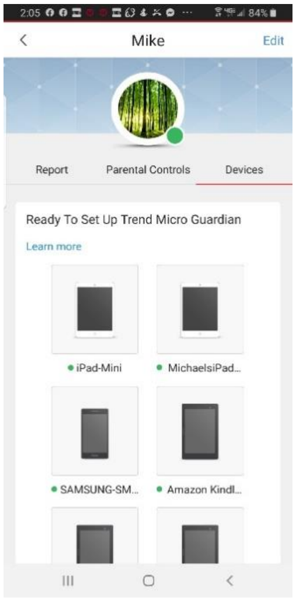
Inappropriate App Used
Find out when Mike opens one.

Time Limits
Limit when Mike can use the Internet.

Connection Alert
Send an alert when Mike's devices connect to the home network during a selected schedule

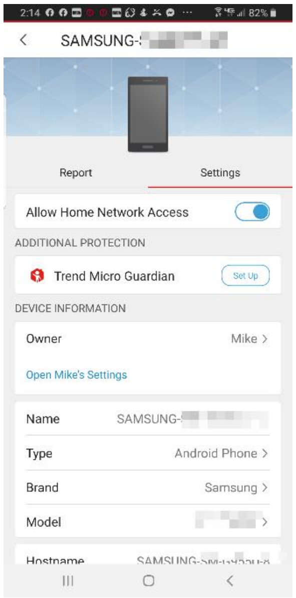
Figure 64. Parental Controls Setup

13. Tap the **Devices** tab to see a list of the devices controlled by the family member, then tap any individual device icon for more details about it.
14. In the device's **Settings** tab, toggle **Allow Home Network Access On** or **Off**, to control the device's access to the network.
15. Tap **Trend Micro Guardian Set Up** to set up the device for **Additional Protection** for a child's device outside the home network.
16. Tap the specific device information, e.g., **Owner, Name, Type**, etc., to assign new ownership or to view or edit the item, using the relevant menu or editor.



Ready To Set Up Trend Micro Guardian

Figure 65. Device List by Owner



Allow Home Network Access ●

ADDITIONAL PROTECTION

Trend Micro Guardian

DEVICE INFORMATION

Owner Mike

Name SAMSUNG-[redacted]

Type Android Phone

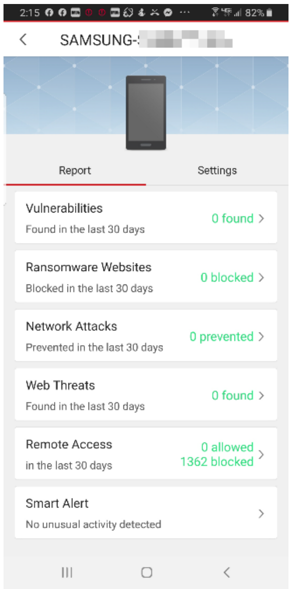
Brand Samsung

Model [redacted]

Hostname SAMSUNG-[redacted]

Figure 66. Device Settings

17. Tap the **Report** tab to obtain a **Protection Report** for the various categories of protection; then tap individual panels for more details on that section of the report.



2:15 82%

SAMSUNG-[redacted]

Report | Settings

Vulnerabilities
Found in the last 30 days
0 found

Ransomware Websites
Blocked in the last 30 days
0 blocked

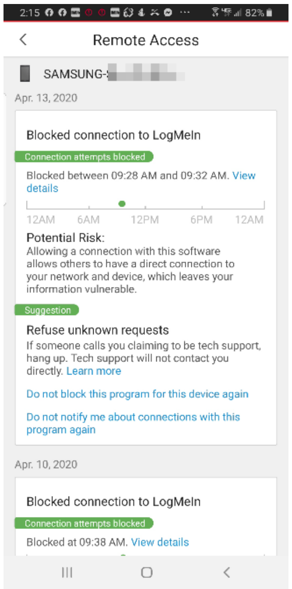
Network Attacks
Prevented in the last 30 days
0 prevented

Web Threats
Found in the last 30 days
0 found

Remote Access
in the last 30 days
0 allowed
1362 blocked

Smart Alert
No unusual activity detected

Figure 67. Device Report



2:15 82%

Remote Access

SAMSUNG-[redacted]

Apr. 13, 2020

Blocked connection to LogMeIn

Connection attempts blocked

Blocked between 09:28 AM and 09:32 AM. View details

Potential Risk:
Allowing a connection with this software allows others to have a direct connection to your network and device, which leaves your information vulnerable.

Suggestion

Refuse unknown requests
If someone calls you claiming to be tech support, hang up. Tech support will not contact you directly. Learn more

Do not block this program for this device again

Do not notify me about connections with this program again

Apr. 10, 2020

Blocked connection to LogMeIn

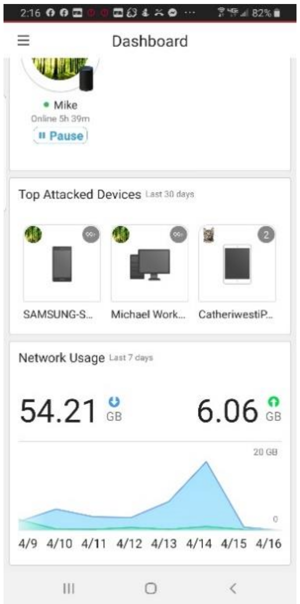
Connection attempts blocked

Blocked at 09:38 AM. View details

Figure 68. Remote Access Risk Blocked

18. The **Report** and **Settings** tabs for devices are also available by tapping a device icon in the **Top Attacked Devices** section of the **Dashboard**.

19. Back in the bottom of the main **Dashboard** screen, tap **Network Usage** to obtain **Download** and **Upload** network consumption for the **Last 7** or **30 Days,** with a graph showing overall consumption and a list of **Download/Upload** consumption by device.



2:16 82%

Dashboard

Mike
Online 5h 39m
Pause

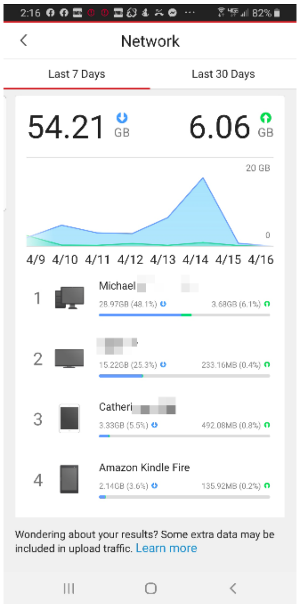
Top Attacked Devices Last 30 days

SAMSUNG-S...
Michael Work...
CatheriwestiP...

Network Usage Last 7 days

54.21 GB
6.06 GB

Figure 69. Network Usage



2:16 82%

Network

Last 7 Days | Last 30 Days

54.21 GB
6.06 GB

1	Michael[redacted]	28.97GB (48.1%)	3.68GB (6.1%)
2	[redacted]	15.22GB (25.3%)	233.16MB (0.4%)
3	Catheri[redacted]	3.33GB (5.5%)	492.08MB (0.8%)
4	Amazon Kindle Fire	2.14GB (3.6%)	135.92MB (0.2%)

Wondering about your results? Some extra data may be included in upload traffic. Learn more

Figure 70. Network Usage > Last 30 Days

Timeline

The **Timeline** provides a handy list by date of all issues discovered by Home Network Security, letting you monitor or take action to address them.

To use the Timeline:

1. Tap **Timeline** in the **Command Menu.** The **Timeline** displays.
2. Review all items in the **Timeline** by tap-holding and scrolling down the screen.

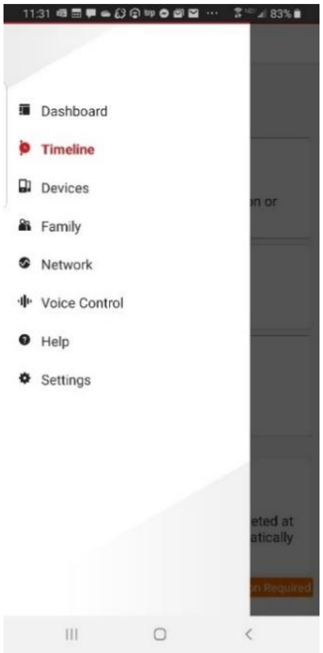
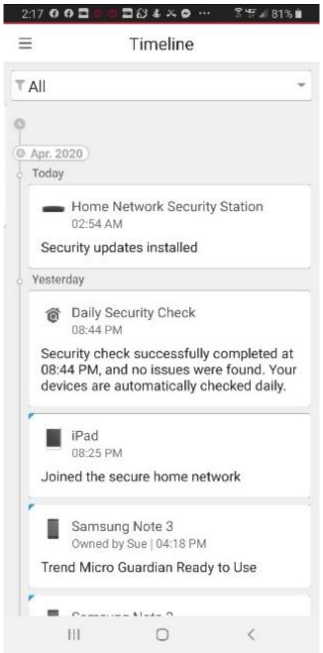


Figure 71. Timeline Menu Item



Home Network Security Station
02:54 AM
Security updates installed

Daily Security Check
08:44 PM
Security check successfully completed at 08:44 PM, and no issues were found. Your devices are automatically checked daily.

iPad
08:25 PM
Joined the secure home network

Samsung Note 3
Owned by Sue | 04:18 PM
Trend Micro Guardian Ready to Use

Figure 72. Timeline > Scroll Down

3. Use the **Filter** menu to filter issues by **Show All, Security, Parental Controls, Connections, Action Required,** or **System.**
4. Tap individual items to display the **Issue Details.**
5. As previously noted, tap **Recommended Actions**, if available, to obtain instructions for what you can do to address the problem.

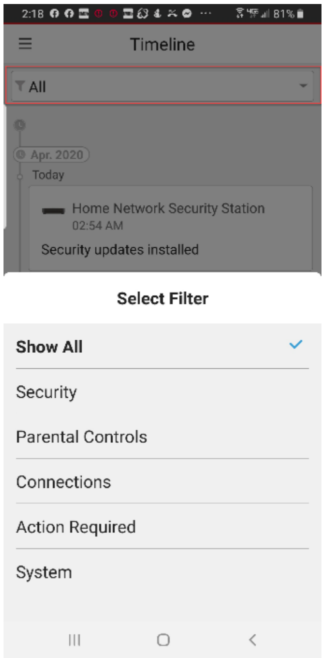
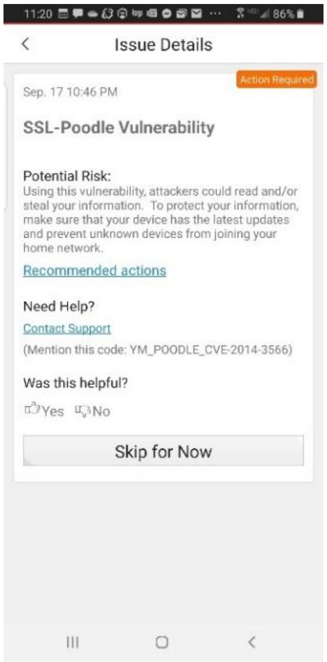


Figure 73. Timeline > Scrolled Down



Sep. 17 10:46 PM

SSL-Poodle Vulnerability

Potential Risk:
Using this vulnerability, attackers could read and/or steal your information. To protect your information, make sure that your device has the latest updates and prevent unknown devices from joining your home network.

Recommended actions

Need Help?
Contact Support
(Mention this code: YM_POODLE_CVE-2014-3566)

Was this helpful?

Figure 74. Issue Details

Devices

The **Devices** function lets you view **All Devices** or **Online Devices** assigned or unassigned to family members.

To use Devices:

1. Tap **Devices** in the **Command Menu.** The **Devices** screen appears.
2. Use the drop-down menu at the top to filter the **Devices** list by **All Devices** or **Online Devices.**
3. Tap the icon for an individual device to display the **Settings** screen for the device.

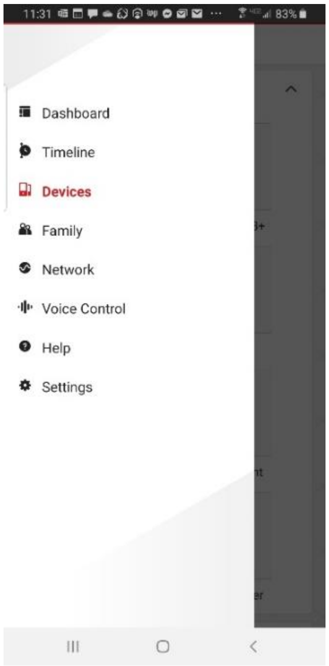


Figure 75. Devices Menu Item

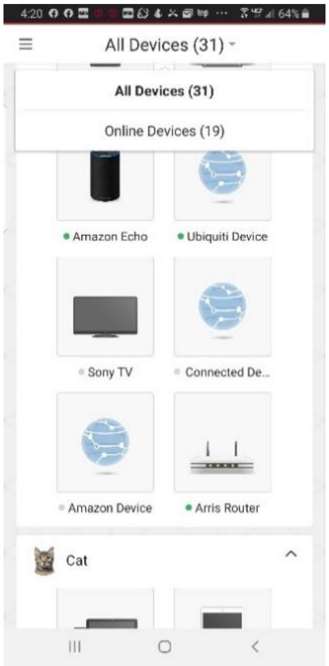
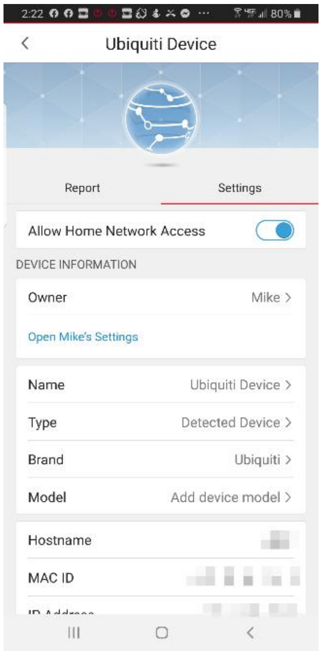


Figure 76. Online Devices > All Devices

4. Tap **Owner** to change the owner to another family member, guest, or to move the device back to the unassigned list by tapping **Move to Unassigned.**
5. Edit fields or selection menus allow you to edit/change items in the other settings.
6. As previously indicated, the **Report** tab provides details on security issues pertaining to the device.



Allow Home Network Access

DEVICE INFORMATION

Owner: Mike

Open Mike's Settings

Name: Ubiquiti Device

Type: Detected Device

Brand: Ubiquiti

Model: Add device model

Hostname: [redacted]

MAC ID: [redacted]

IP Address: [redacted]

Figure 77. Access Point Device

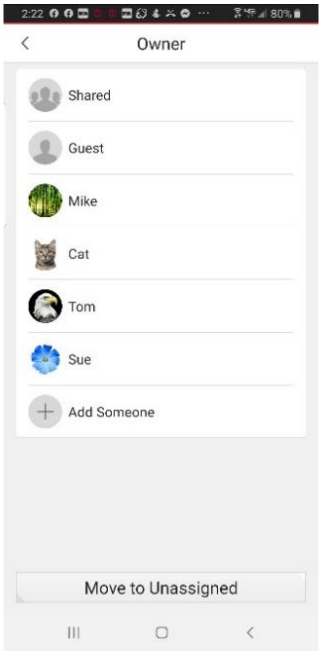


Figure 78. Owner > Move to Unassigned

Family: Members, Devices, and Parental Controls

You can add new family **Members** and the **Devices** they control. You can also set up **Parental Controls** for any family member and their devices, using the **Filtering** function to block **Inappropriate Websites and Content**. You can also block **Inappropriate Apps**, set **Time Limits** for internet use, and get a **Connection Alert** in your device's pull-down **Notification** menu whenever the family member's devices try to connect within the preset monitoring period.

To extend **Parental Controls** beyond your home network, you can install **Trend Micro Guardian** on your child's mobile devices and pair with HNS. Once set up, the supported **Parental Control** rules will apply to your child's device on any Wi-Fi or mobile network, at home or out in the world.

Add a Family Member and the Devices They Control

To add a family member:

1. Tap **Family** in the **Command Menu**. The **Family** member list appears.
2. In the **Family** member list, scroll down the list if you need to, then tap the **Plus (+)** button to **Add Someone.**

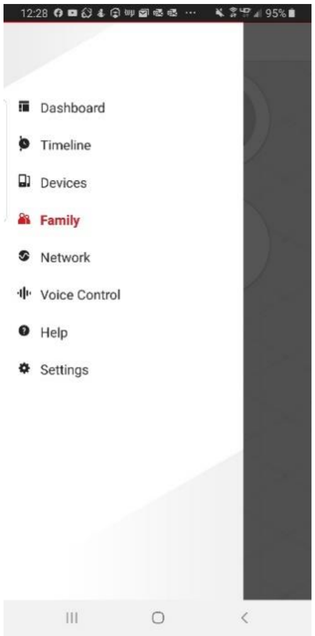


Figure 79. Family Menu Item

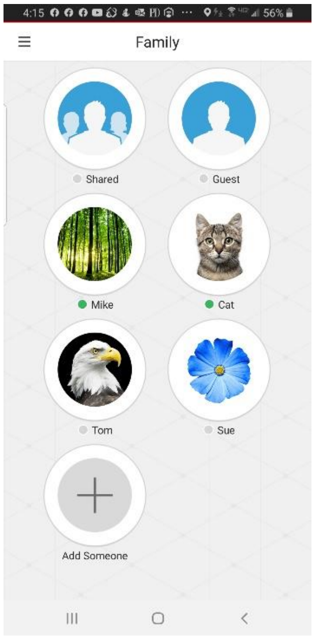
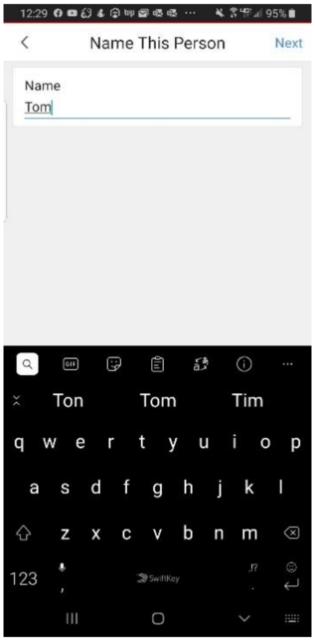


Figure 80. Family Member List > Add Someone (+)

3. In the **Name** field of the **Name This Person** screen, type a name, then tap **Next**.
4. **Choose a Picture** to help you identify the family member in your **Family Member** list, then tap **Next**.



Name
Tom

Figure 81. Name This Person

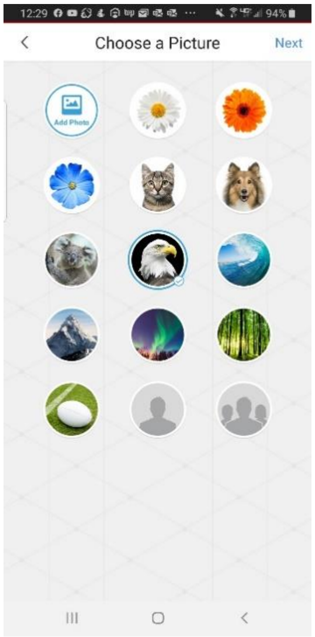


Figure 82. Choose a Picture

5. **Assign Devices** to the person by tapping the device(s) in the **Unassigned** panel. The devices you select will move into the ownership panel for that person.
6. Tap **Done**. You're then presented with the **Parental Controls** screen for that person, where you can apply **Parental Control Rules** as you see fit. (See below.)

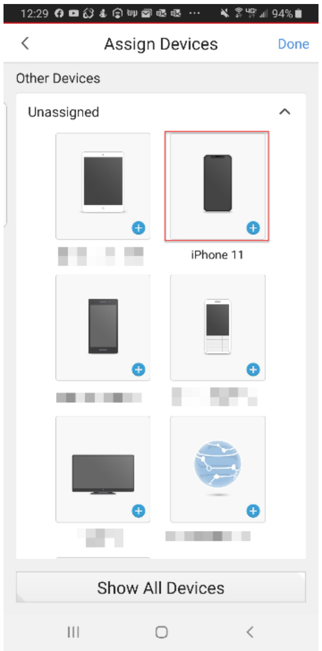


Figure 83. Assign Devices (1)

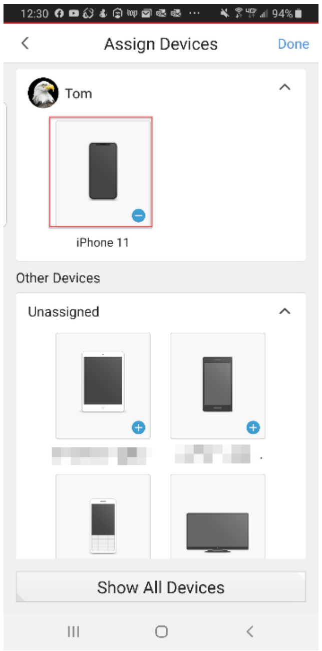


Figure 84. Assign Devices (2)

Install Trend Micro Guardian and Set Up Uninstall Protection

Once you've assigned a device to a child, it's recommended that you install **Trend Micro Guardian** on the child's device before setting up **Parental Controls**, because **Guardian** will extend those controls to the child's smartphone or tablet to protect them when they go beyond your network. Once installed, you need to protect it from uninstallation.

You may also conduct the **Trend Micro Guardian** setup process *after* you've defined the **Parental Controls** rules for your child. Once installed, **Guardian** accepts the rules already defined and applies them to the child's device when they're outside the home.

Both processes—**Guardian Installation** and **Uninstall Protection**—are set up slightly differently on an iOS or Android device. See the relevant sections below.

Install Guardian on an iOS Device

The install example below uses an Apple iPhone 11 assigned to the child "Tom."

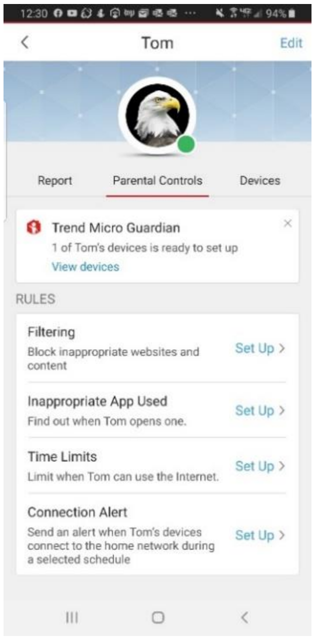
To Install Trend Micro Guardian on an iOS Device:

1. Once the iOS device is assigned to a family member, e.g., "Tom," you can install **Trend Micro Guardian** on it.
2. Tap the **Trend Micro Guardian** popup panel in **Parental Controls** to begin the installation.
3. An **Introducing Trend Micro Guardian** popup appears, where you can read about the protection **Trend Micro Guardian** provides:

   >Mobile devices use the same rules as inside your home network.

   >Your child is protected online, on all networks.

   >Set Time Limits and block access, both inside and outside the home.
4. Tap **Set Up Now**.



Trend Micro Guardian
1 of Tom's devices is ready to set up
View devices

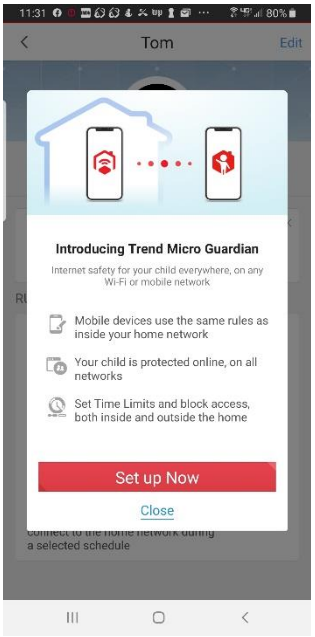
Filtering
Block inappropriate websites and content

Inappropriate App Used
Find out when Tom opens one.

Time Limits
Limit when Tom can use the Internet.

Connection Alert
Send an alert when Tom's devices connect to the home network during a selected schedule

Figure 85. Trend Micro Guardian Popup Panel

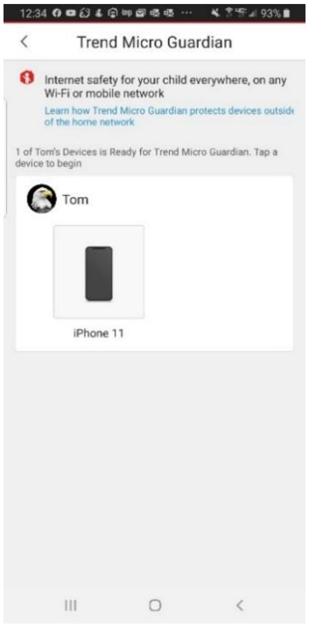


Introducing Trend Micro Guardian
Internet safety for your child everywhere, on any Wi-Fi or mobile network

Mobile devices use the same rules as inside your home network
Your child is protected online, on all networks
Set Time Limits and block access, both inside and outside the home

Figure 86. Introducing Trend Micro Guardian

5. A device list appears with device(s) ready for **Trend Micro Guardian.**
6. Tap a device to begin. A screen appears for you to install **Trend Micro Guardian** on your child's device.
7. Using the child's device, search for **Trend Micro Guardian** in the Apple App Store, or scan the **QR Code** with a QR Code Scanner to get the link to the app.

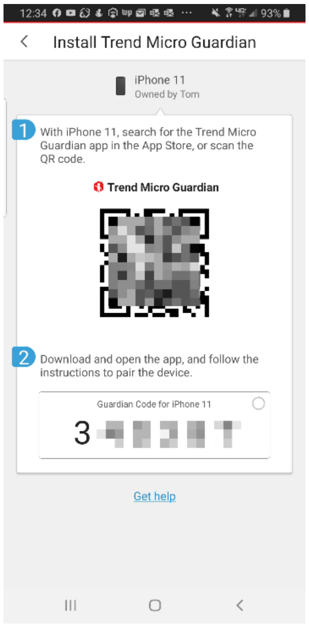


Internet safety for your child everywhere, on any Wi-Fi or mobile network

Learn how Trend Micro Guardian protects devices outside of the home network

1 of Tom's Devices is Ready for Trend Micro Guardian. Tap a device to begin

Figure 87. Device List for Child



1 With iPhone 11, search for the Trend Micro Guardian app in the App Store, or scan the QR code.

2 Download and open the app, and follow the instructions to pair the device.

Guardian Code for iPhone 11: 3[redacted]

Figure 88. Install Trend Micro Guardian

8. **Trend Micro Guardian** appears in the Apple App Store on the child's device.
9. Tap the **Get** or **Cloud Download** icon or to get the app. If needed, the **App Store Account** screen appears for your approval.
10. If you approve the install, tap **Install.**

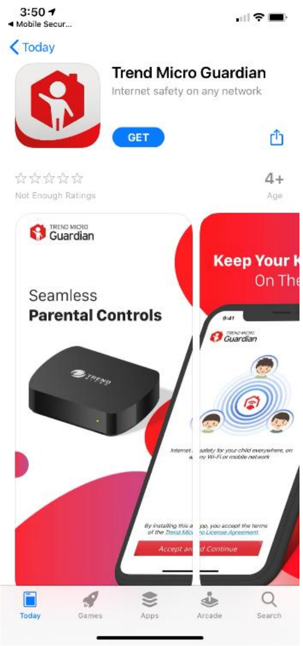
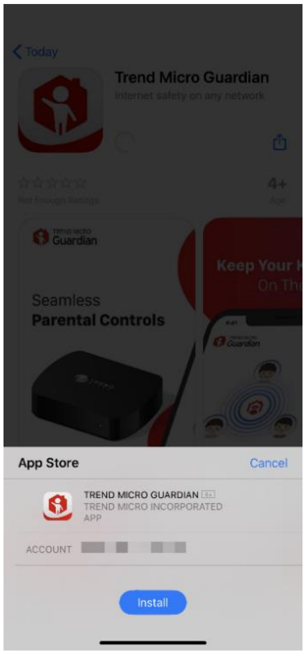


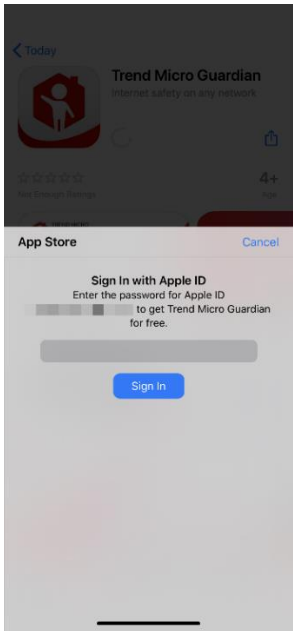
Figure 89. Trend Micro Guardian on Apple App Store



ACCOUNT [redacted]

Figure 90. App Store Account Popup

11. If you're not signed in, the App Store asks you to **Sign In with Apple ID** password.
12. Enter your password and tap **Sign In. Trend Micro Guardian** downloads and installs
13. Tap **Open** to open the app.



App Store Cancel

Sign In with Apple ID
Enter the password for Apple ID [redacted] to get Trend Micro Guardian for free.

Figure 91. Sign in with Apple ID

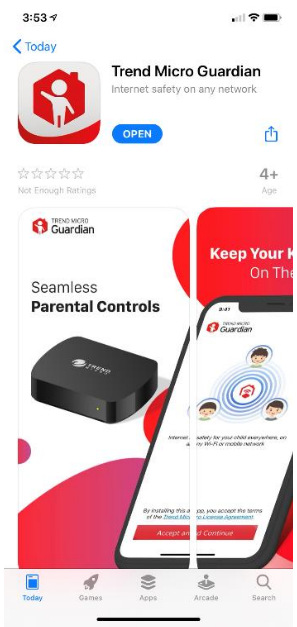
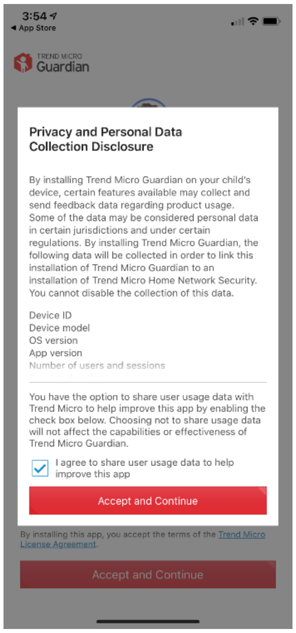


Figure 92. Trend Micro Guardian Installed

14. The **Privacy and Personal Data Collection Disclosure** screen appears.
15. Read the disclosure, which outlines what kind of data **Trend Micro Guardian** collects.
16. If you agree, check **"I agree to share user usage data to help improve this app"** and tap **Accept and Continue**.
17. An instructional screen appears describing the Internet Security it provides for your child. Tap **Accept and Continue.**



Privacy and Personal Data Collection Disclosure

By installing Trend Micro Guardian on your child's device, certain features available may collect and send feedback data regarding product usage. Some of the data may be considered personal data in certain jurisdictions and under certain regulations. By installing Trend Micro Guardian, the following data will be collected in order to link this installation of Trend Micro Guardian to an installation of Trend Micro Home Network Security. You cannot disable the collection of this data.

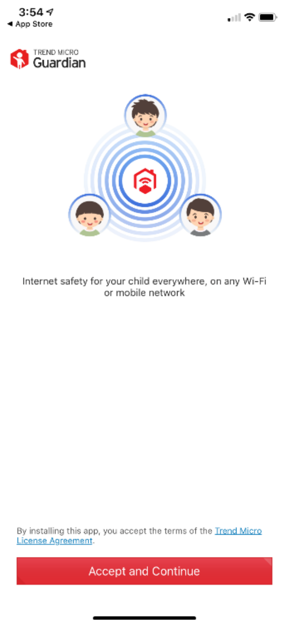
Device ID
Device model
OS version
App version
Number of users and sessions

You have the option to share user usage data with Trend Micro to help improve this app by enabling the check box below. Choosing not to share usage data will not affect the capabilities or effectiveness of Trend Micro Guardian.

☑ I agree to share user usage data to help improve this app

By installing this app, you accept the terms of the Trend Micro License Agreement.

Figure 93. Privacy and Personal Data Collection Disclosure

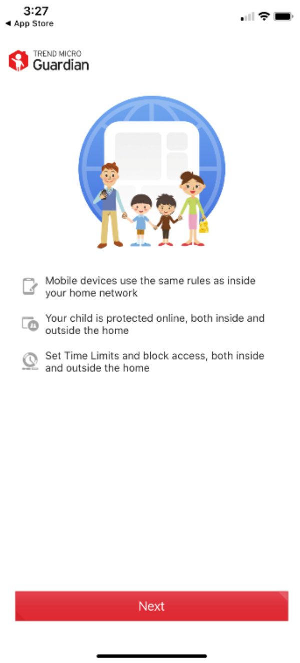


Internet safety for your child everywhere, on any Wi-Fi or mobile network

By installing this app, you accept the terms of the Trend Micro License Agreement.

Figure 94. Instructional Screen (1) - Accept and Continue

18. A second instructional screen appears describing how mobile devices use the same rules inside and outside the home network.
19. Tap **Next**. The **Pair Now** screen appears.
20. Tap **Pair Now.**


3:27
◂ App Store

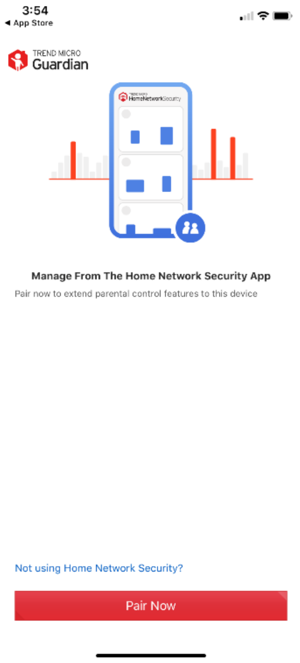
TREND MICRO Guardian

Mobile devices use the same rules as inside your home network

Your child is protected online, both inside and outside the home

Set Time Limits and block access, both inside and outside the home

Figure 95. Instructional Screen (2) - Next


3:54
◂ App Store

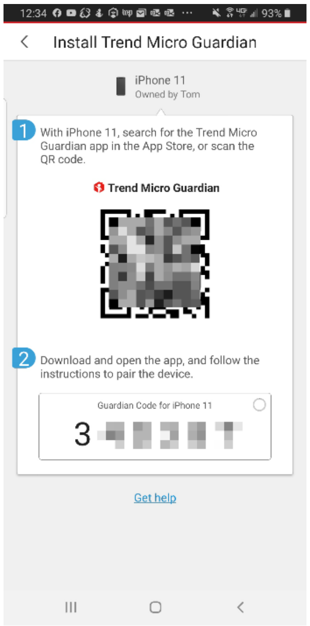
TREND MICRO Guardian

Manage From The Home Network Security App

Pair now to extend parental control features to this device

Figure 96. Pair Now

21. Back on the managing device, view the **Pairing Code** in the **Trend Micro Home Network Security** application.
22. On the child's device, enter the **Pairing Code** that's currently showing on the managing device into the **Trend Micro Guardian** app.


12:34 93%

Install Trend Micro Guardian

iPhone 11
Owned by Tom

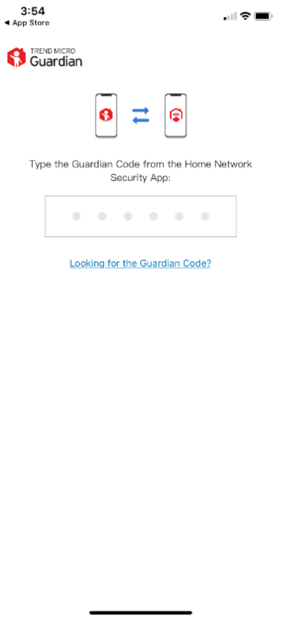
1 With iPhone 11, search for the Trend Micro Guardian app in the App Store, or scan the QR code.

Trend Micro Guardian

2 Download and open the app, and follow the instructions to pair the device.

Guardian Code for iPhone 11
3[redacted]

Figure 97. Get Pairing Code


3:54
◂ App Store

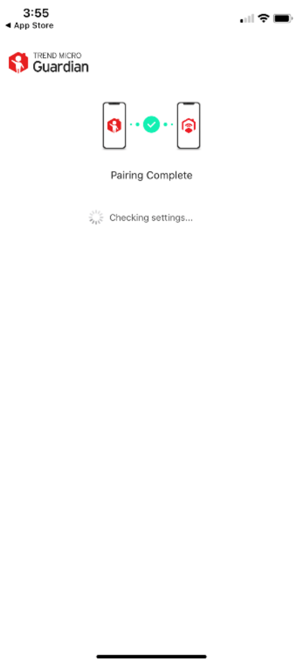
TREND MICRO Guardian

Type the Guardian Code from the Home Network Security App:

● ● ● ● ● ●

Figure 98. Type in Guardian Pairing Code

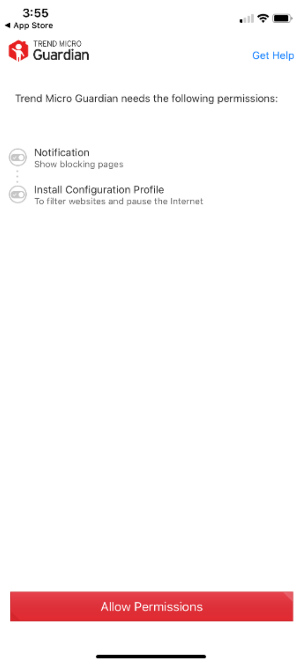
23. The **Pairing Complete** screen appears, showing the process of pairing as it checks the settings and pairs.
24. When the pairing process has finished, a screen appears indicating that **Trend Micro Guardian** needs the following permissions: **Notification** and **Install the Configuration Profile.**
25. Tap **Allow Permissions.**



Pairing Complete

Checking settings...

Figure 99. Pairing Process



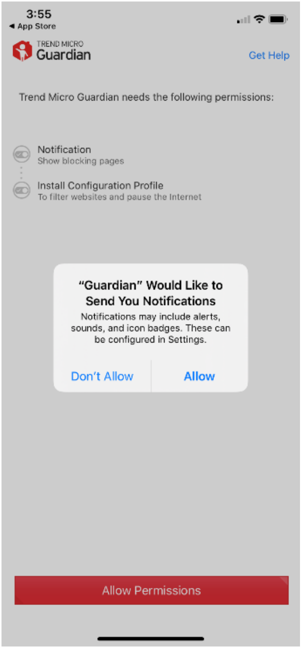
Trend Micro Guardian needs the following permissions:

Notification
Show blocking pages

Install Configuration Profile
To filter websites and pause the Internet

Figure 100. Allow Permissions

26. A popup appears, asking **"Guardian" Would Like to Send You Notifications.**
27. Tap **Allow**. The **Profile installation** screen appears.
28. Tap **Download Profile** to download and install the profile.



Trend Micro Guardian needs the following permissions:

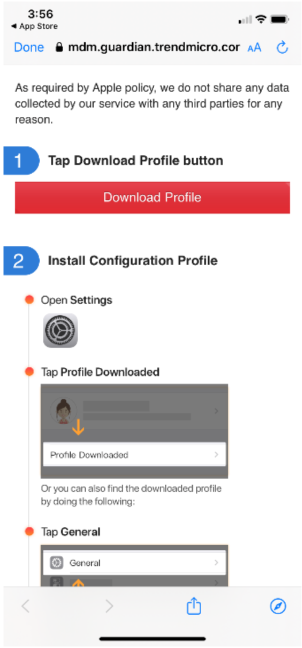
Notification
Show blocking pages

Install Configuration Profile
To filter websites and pause the Internet

"Guardian" Would Like to Send You Notifications

Notifications may include alerts, sounds, and icon badges. These can be configured in Settings.

Figure 101. Notifications



As required by Apple policy, we do not share any data collected by our service with any third parties for any reason.

1 Tap Download Profile button

2 Install Configuration Profile

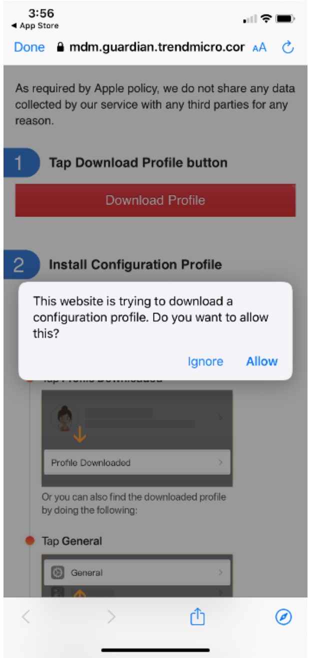
- Open Settings
- Tap Profile Downloaded

Or you can also find the downloaded profile by doing the following:

- Tap General

Figure 102. Download Profile

29. A popup appears, indicating **"This website is trying to download a configuration profile. Do you want to allow this?"**
30. Tap **Allow**. A popup appears, indicating **Profile Downloaded.**
31. Tap **Close**, then go to your device **Settings** screen.

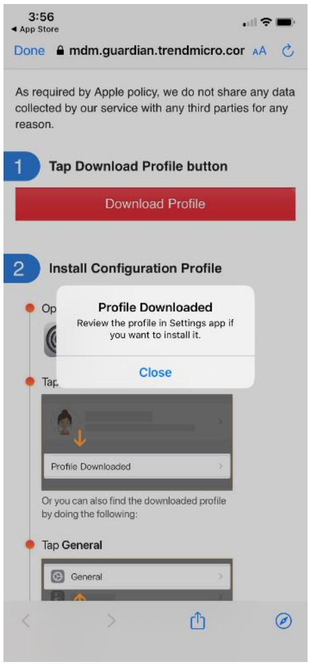

3:56
◂ App Store
Done
mdm.guardian.trendmicro.cor
AA
1 Tap Download Profile button
Download Profile
2 Install Configuration Profile
Ignore
Allow
Profile Downloaded
Tap General
General

As required by Apple policy, we do not share any data collected by our service with any third parties for any reason.

This website is trying to download a configuration profile. Do you want to allow this?

Or you can also find the downloaded profile by doing the following:

Figure 103. Allow Download of Profile


3:56
◂ App Store
Done
mdm.guardian.trendmicro.cor
AA
1 Tap Download Profile button
Download Profile
2 Install Configuration Profile
Close
Profile Downloaded
Tap General
General

As required by Apple policy, we do not share any data collected by our service with any third parties for any reason.

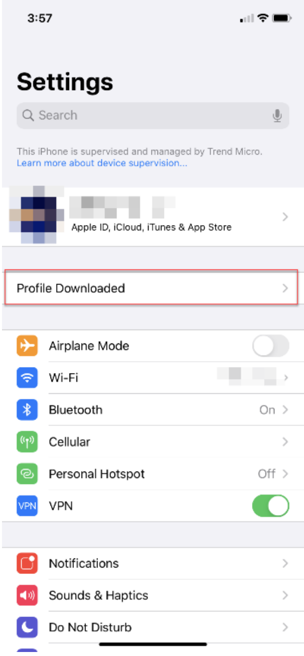
Profile Downloaded

Review the profile in Settings app if you want to install it.

Or you can also find the downloaded profile by doing the following:

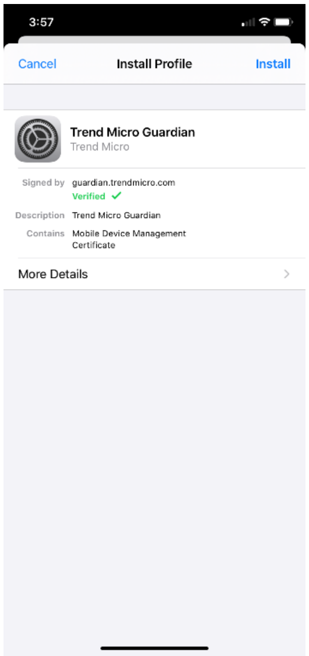
Figure 104. Profile Download

32. In the **Settings** screen, tap **Profile Downloaded.** A screen appears for you to **Install Profile.**
33. Tap **Install**.



This iPhone is supervised and managed by Trend Micro. Learn more about device supervision...

Figure 105. Profile Downloaded



Signed by guardian.trendmicro.com Verified ✓

Description Trend Micro Guardian

Contains Mobile Device Management Certificate

Figure 106. Install Profile

34. The **Enter Passcode** screen appears.
35. Enter the passcode you use to access your Apple device.
36. A **Warning** screen appears, indicating the **Mobile Device Management** (MDM) controls and data collection processes that will allow the administrator to remotely manage the phone.
37. Read the warning and if you agree, tap **Install**.

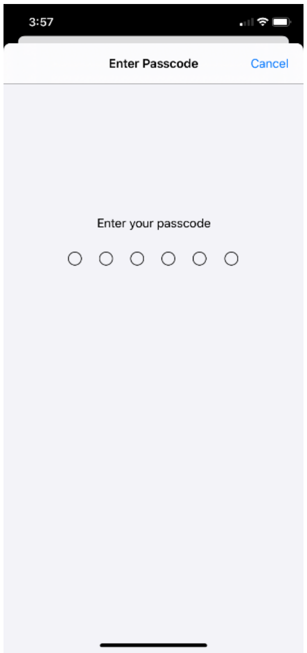
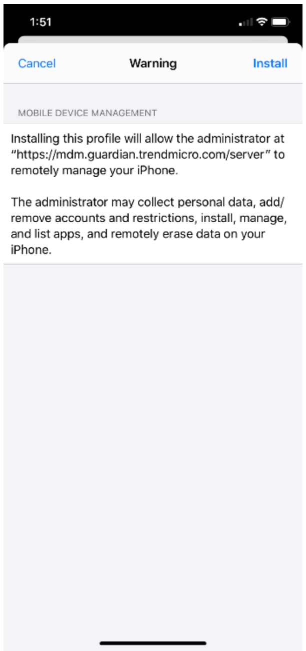


Figure 107. Enter Passcode



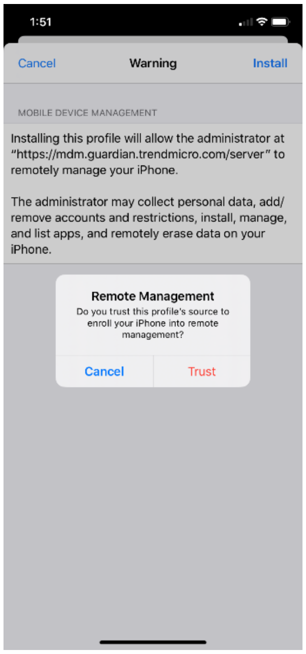
MOBILE DEVICE MANAGEMENT

Installing this profile will allow the administrator at "https://mdm.guardian.trendmicro.com/server" to remotely manage your iPhone.

The administrator may collect personal data, add/remove accounts and restrictions, install, manage, and list apps, and remotely erase data on your iPhone.

Figure 108. Warning

38. A popup appears, asking if you trust this profile's source to enroll your phone into **Remote Management.**
39. If you agree, tap **Trust, then Done.**
40. The **Trend Micro Guardian Profile** installs and displays the **Trend Micro Guardian Device Management** screen (MDM). The **MDM Profile** is now installed.



MOBILE DEVICE MANAGEMENT

Installing this profile will allow the administrator at "https://mdm.guardian.trendmicro.com/server" to remotely manage your iPhone.

The administrator may collect personal data, add/remove accounts and restrictions, install, manage, and list apps, and remotely erase data on your iPhone.

Remote Management

Do you trust this profile's source to enroll your iPhone into remote management?

Figure 109. Trust Remote Management

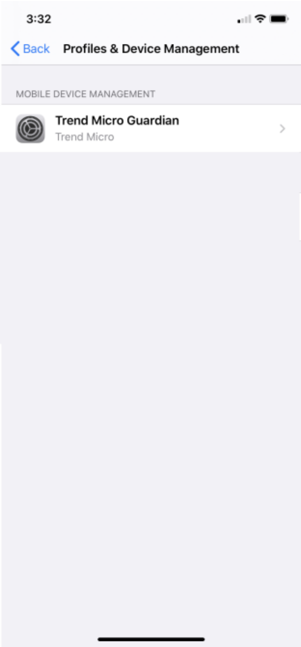
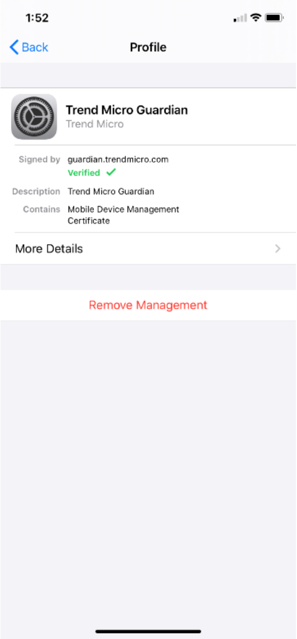


Figure 110. Trend Micro Guardian MDM Installed

41. Tap **Trend Micro Guardian** to view the **Profile**.
42. In the future, if you need to remove the profile for **Trend Micro Guardian** you'll return to this screen and tap **Remove Management.**
43. For now, exit **Settings** and tap the **Guardian** icon on your child's device.



Trend Micro Guardian
Trend Micro

Signed by guardian.trendmicro.com
Verified ✓
Description Trend Micro Guardian
Contains Mobile Device Management Certificate

Figure 111. Profile - Remove Management

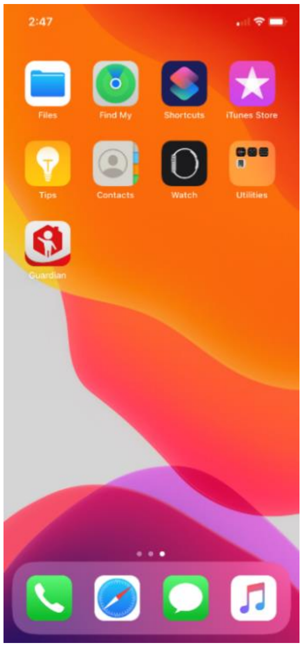
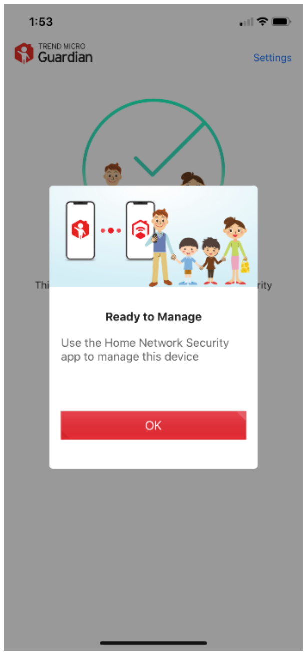


Figure 112. Guardian Icon

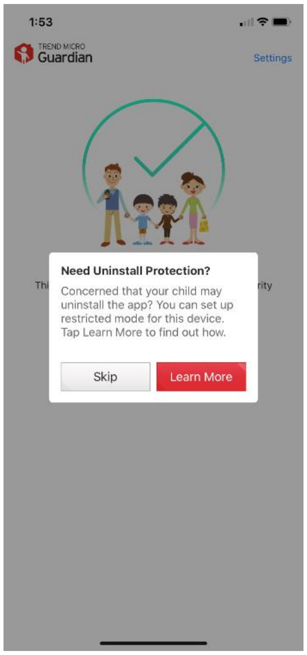
44. **Guardian** loads and a popup indicates **Ready to Manage.**
45. Tap **OK**. A popup appears, asking if you **Need Uninstall Protection?** This lets you set up **Restricted Mode** to prevent your child from uninstalling **Guardian**.
46. Tap **Learn More** to learn how to set up **Restricted Mode** for the **Guardian** app. An **Instructional** screen appears.



Ready to Manage

Use the Home Network Security app to manage this device

Figure 113. Ready to Manage

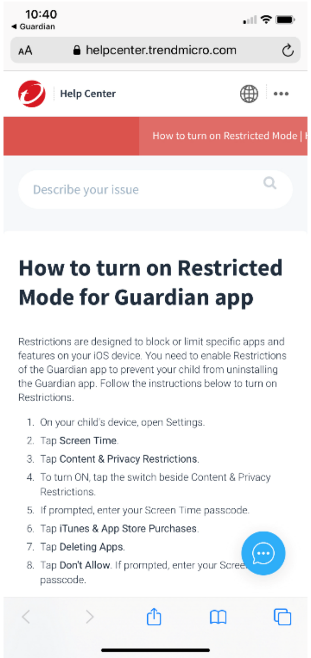


Need Uninstall Protection?

Concerned that your child may uninstall the app? You can set up restricted mode for this device. Tap Learn More to find out how.

Figure 114. Need Uninstall Protection?

47. Follow the instructions for your child’s device to set up **Restricted Mode.** (See the section **Restricted Mode** following for more detailed instructions.)
48. Back in **Guardian**, the main screen shows **Trend Micro Guardian is Active.**

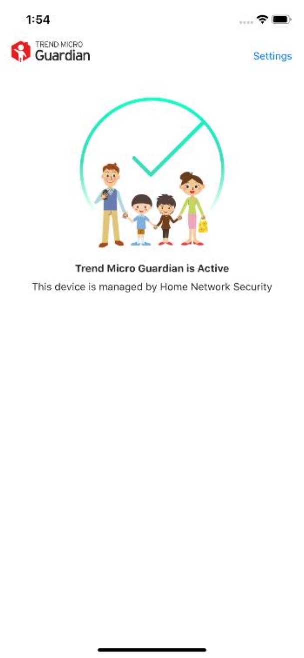


How to turn on Restricted Mode for Guardian app

Restrictions are designed to block or limit specific apps and features on your iOS device. You need to enable Restrictions of the Guardian app to prevent your child from uninstalling the Guardian app. Follow the instructions below to turn on Restrictions.

1. On your child's device, open Settings.
2. Tap Screen Time.
3. Tap Content & Privacy Restrictions.
4. To turn ON, tap the switch beside Content & Privacy Restrictions.
5. If prompted, enter your Screen Time passcode.
6. Tap iTunes & App Store Purchases.
7. Tap Deleting Apps.
8. Tap Don't Allow. If prompted, enter your Scree passcode.

Figure 115. Restricted Mode

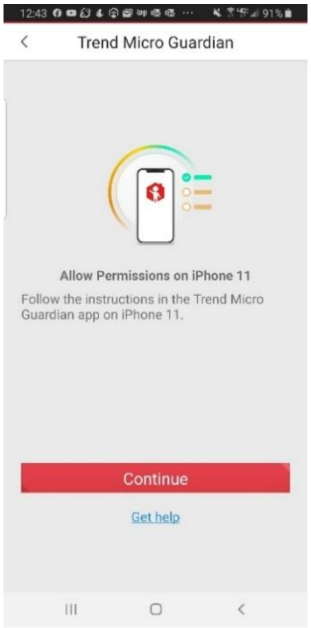


Trend Micro Guardian is Active

This device is managed by Home Network Security

Figure 116. Trend Micro Guardian is Active

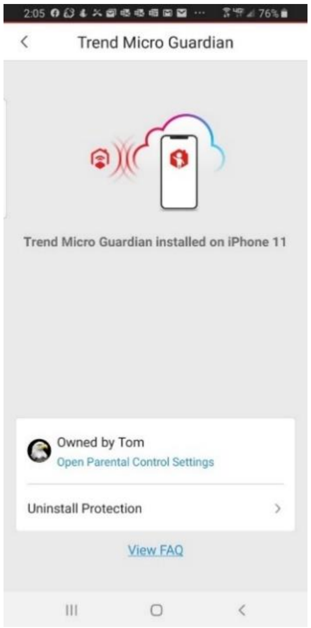
49. Back on your managing device, click **Continue**.
50. A screen appears, showing that **Trend Micro Guardian** is now installed on the child’s phone.
51. You may tap the panel **Owned by “Child”** to open the **Parental Control Settings**, or tap **Uninstall Protection** panel to learn more about activating uninstall protection.



Allow Permissions on iPhone 11

Follow the instructions in the Trend Micro Guardian app on iPhone 11.

Figure 117. HNS Managing Device: Continue



Trend Micro Guardian installed on iPhone 11

Owned by Tom

Figure 118. Guardian Installed on Child’s Device

52. In the future, you'll tap a **Family Member** to access the **Report** panel, **Parental Controls**, and **Devices** controlled by that member.

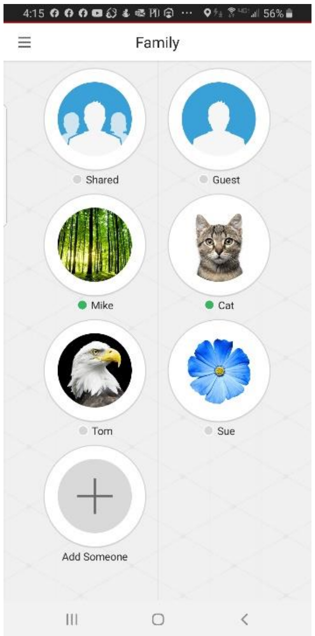
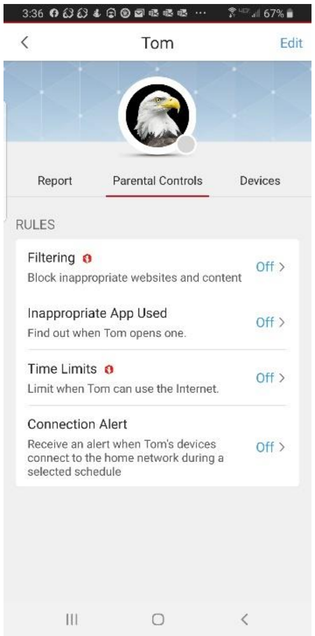


Figure 119. Family Member List



RULES

Filtering — Block inappropriate websites and content — Off

Inappropriate App Used — Find out when Tom opens one. — Off

Time Limits — Limit when Tom can use the Internet. — Off

Connection Alert — Receive an alert when Tom's devices connect to the home network during a selected schedule — Off

Figure 120. Family Member: Report, Parental Controls, Devices

Set Up Guardian Uninstall Protection on an iOS Device

On your child's device, turn on **Restricted Mode** to prevent the child from uninstalling **Trend Micro Guardian.** While you're at it, turn on **Always Allowed** to make sure you can manage your child's device at all times using the **Home Network Security** management app with **Guardian**.

The instructions below use an iPhone 11 and provide the fastest route to turning on **Uninstall Protection** and **Always Allowing Guardian** within the **Screen Time** settings. Your choices may differ depending on the age of your child. You can enable/disable additional **Screen Time** functions later at any time.

To turn on Restricted Mode:

1. On your child's device, tap **Settings**. The **Settings** screen appears.
2. In the **Settings** screen, tap **Screen Time**. The **Turn On Screen Time** screen appears.

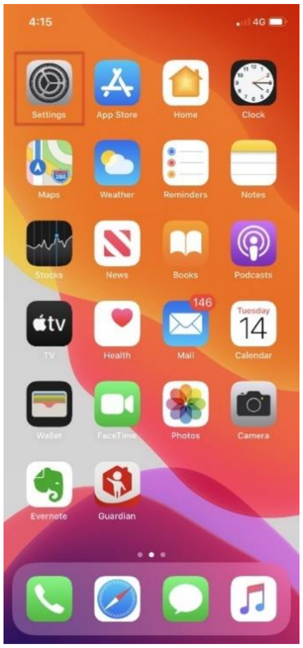


Figure 121. Settings

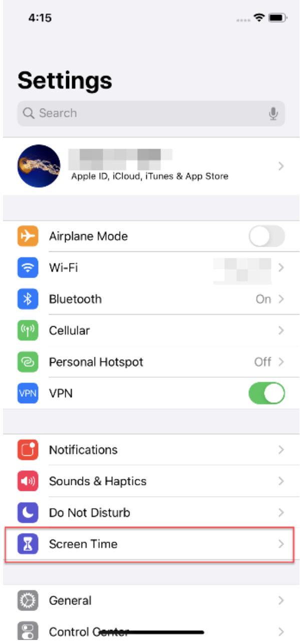
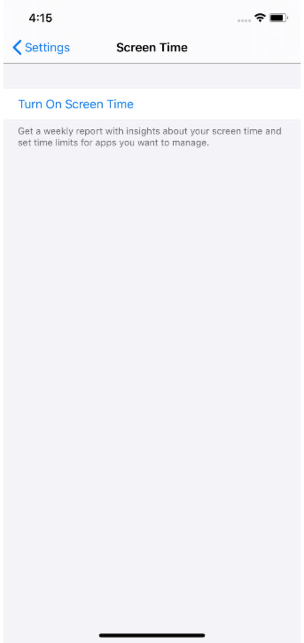


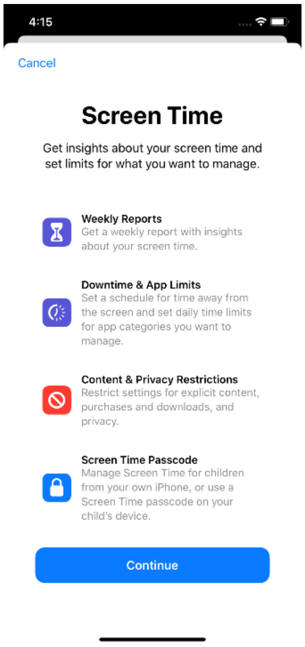
Figure 122. Screen Time

3. Tap **Turn On Screen Time.** An overview screen appears.
4. Tap **Continue**.



Get a weekly report with insights about your screen time and set time limits for apps you want to manage.

Figure 123. Turn On Screen Time



Get insights about your screen time and set limits for what you want to manage.

Weekly Reports
Get a weekly report with insights about your screen time.

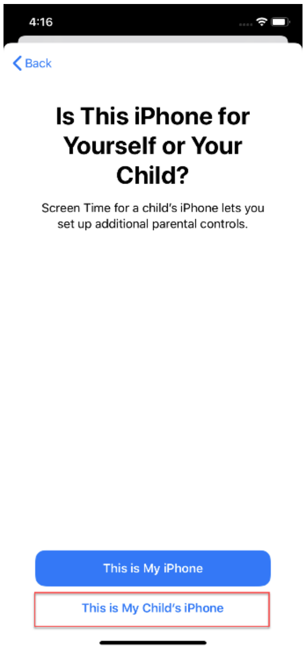
Downtime & App Limits
Set a schedule for time away from the screen and set daily time limits for app categories you want to manage.

Content & Privacy Restrictions
Restrict settings for explicit content, purchases and downloads, and privacy.

Screen Time Passcode
Manage Screen Time for children from your own iPhone, or use a Screen Time passcode on your child's device.

Figure 124. Screen Time Overview

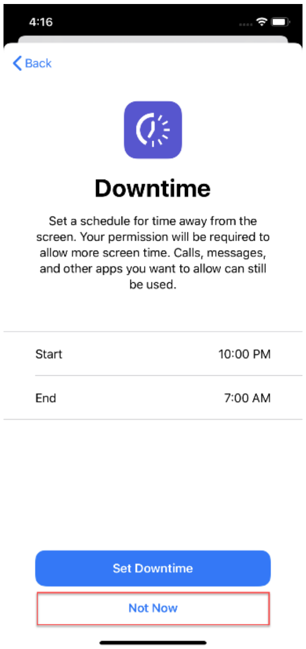
5. The resulting **Screen Time** screen asks: **Is This iPhone for Yourself or Your Child?** Tap **This is My Child's iPhone.**
6. In the **Downtime** screen, tap **Not Now.** This setting will be managed by **Home Network Security.**



Is This iPhone for Yourself or Your Child?

Screen Time for a child's iPhone lets you set up additional parental controls.

Figure 125. This is My Child's Phone



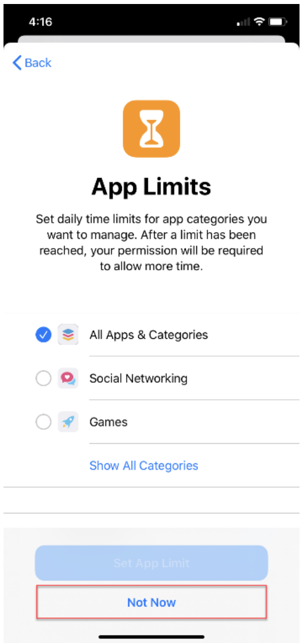
Downtime

Set a schedule for time away from the screen. Your permission will be required to allow more screen time. Calls, messages, and other apps you want to allow can still be used.

Start 10:00 PM
End 7:00 AM

Figure 126. Downtime > Not Now

7. In the **App Limits** screen (a future item), tap **Not Now.** This also will be managed by **Home Network Security** when it's available.
8. In the **Content & Privacy** screen, tap **Continue**.

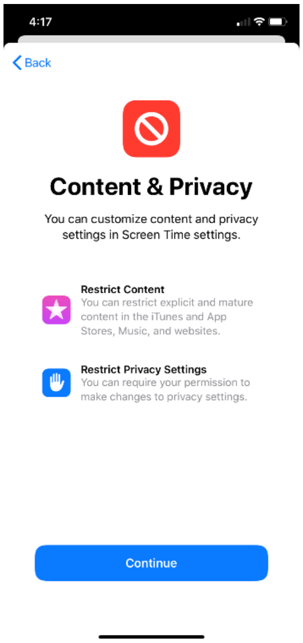


App Limits

Set daily time limits for app categories you want to manage. After a limit has been reached, your permission will be required to allow more time.

☑ All Apps & Categories
○ Social Networking
○ Games

Figure 127. App Limits > Not Now



Content & Privacy

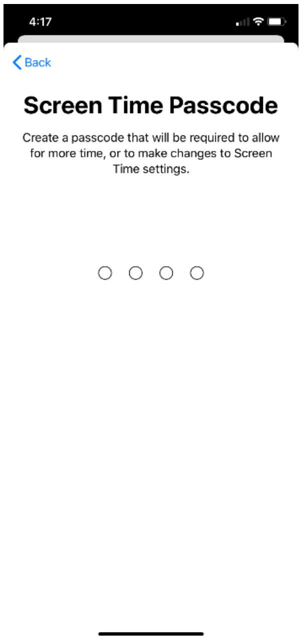
You can customize content and privacy settings in Screen Time settings.

Restrict Content
You can restrict explicit and mature content in the iTunes and App Stores, Music, and websites.

Restrict Privacy Settings
You can require your permission to make changes to privacy settings.

Figure 128. Content & Privacy > Continue

9. Enter a **Screen Time Passcode** in the first screen. A second screen appears for validation of the passcode.
10. **Re-enter your Passcode** in the second **Screen Time Passcode** screen. The **Screen Time Passcode Recovery** screen appears, to save your passcode in your Apple account, so you can recover it should you forget it.

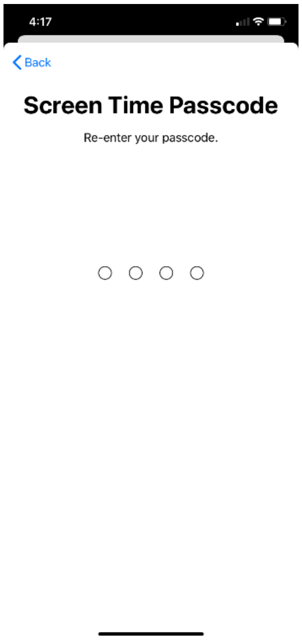


Screen Time Passcode

Create a passcode that will be required to allow for more time, or to make changes to Screen Time settings.

○ ○ ○ ○

Figure 129. Screen Time Passcode (1)



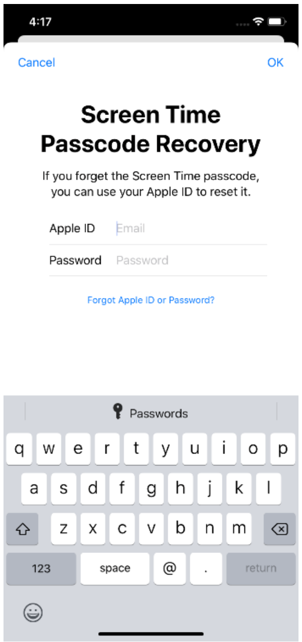
Screen Time Passcode

Re-enter your passcode.

○ ○ ○ ○

Figure 130. Screen Time Passcode (2)

11. In the **Screen Time Passcode Recovery screen**, enter your **Apple ID and Password.** Make sure the credentials you enter are your own—not the same ones you used to register the child's device.
12. The **Screen Time** screen appears. Tap **Always Allowed.**



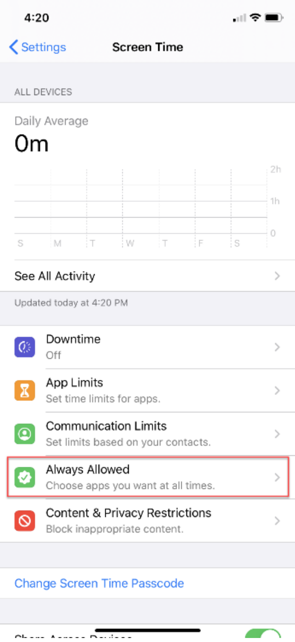
Screen Time Passcode Recovery

If you forget the Screen Time passcode, you can use your Apple ID to reset it.

Apple ID Email

Password Password

Figure 131. Screen Time Passcode Recovery



Daily Average
0m

Updated today at 4:20 PM

Downtime
Off

App Limits
Set time limits for apps.

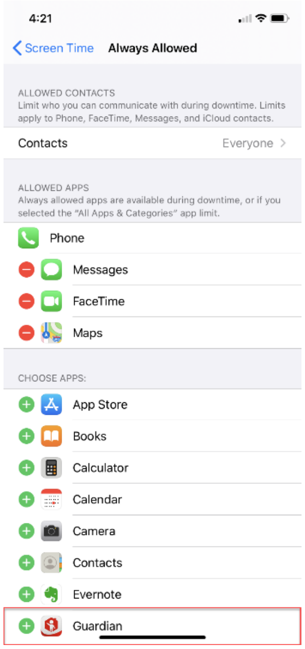
Communication Limits
Set limits based on your contacts.

Always Allowed
Choose apps you want at all times.

Content & Privacy Restrictions
Block inappropriate content.

Figure 132. Screen Time > Always Allowed

13. In the **Always Allowed** screen, tap the **Guardian** Add (**+**) sign to add it to **Allowed Apps.**
14. Enter your **Screen Time Passcode** again, to ensure **Guardian's Always Allowed** status cannot be changed without the passcode.



Limit who you can communicate with during downtime. Limits apply to Phone, FaceTime, Messages, and iCloud contacts.

Contacts: Everyone

Always allowed apps are available during downtime, or if you selected the "All Apps & Categories" app limit.

Figure 133. Guardian

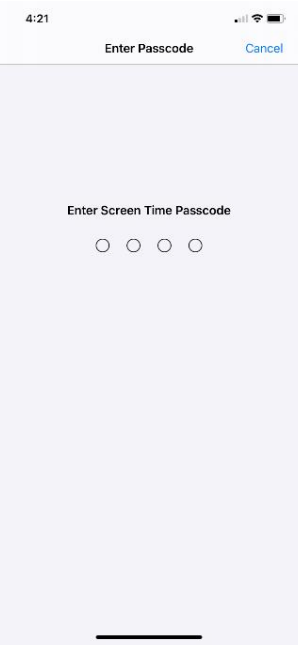
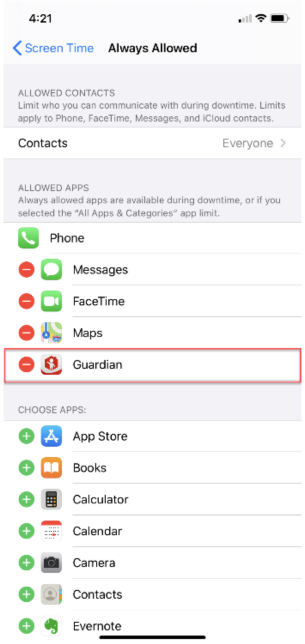


Figure 134. Enter Screen Time Passcode

15. **Guardian** is now listed in **Allowed Apps** list.
16. Back in the **Screen Time Settings**, tap **Content & Privacy Restrictions.**

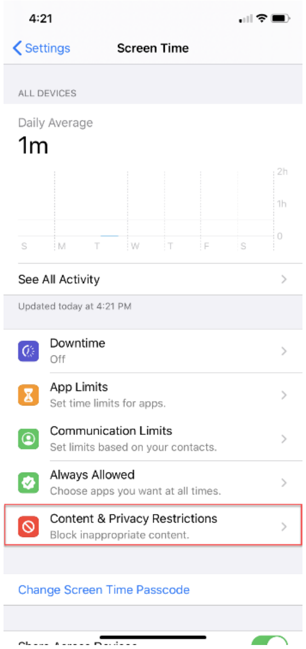


Limit who you can communicate with during downtime. Limits apply to Phone, FaceTime, Messages, and iCloud contacts.

Contacts: Everyone

Always allowed apps are available during downtime, or if you selected the "All Apps & Categories" app limit.

Figure 135. Guardian Always Allowed



Daily Average: 1m

Updated today at 4:21 PM

Downtime: Off

Set time limits for apps.

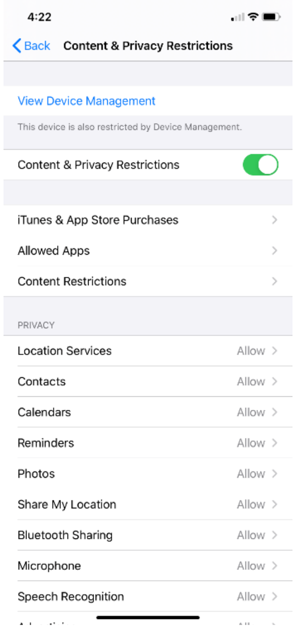
Set limits based on your contacts.

Choose apps you want at all times.

Block inappropriate content.

Figure 136. Content & Privacy Restrictions

17. Toggle **Content & Privacy Restrictions** to **On**.
18. Tap **iTunes & App Store Purchases**.
19. The settings for **Installing, Deleting,** and **In-app Purchases** are shown in the **iTunes & App Store Purchases** screen as **Allow** by default.
20. Change the settings as you see fit, appropriate to the age and app options you give to your child, but ensure you tap **Don’t Allow** for **Deleting Apps.**

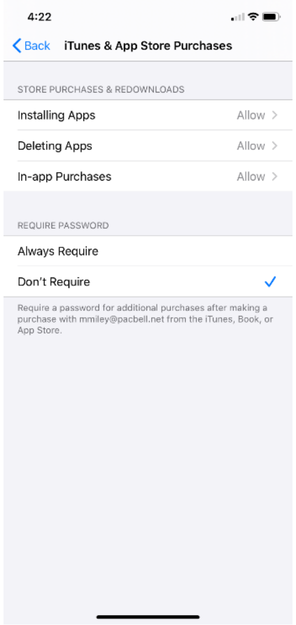


This device is also restricted by Device Management.

Content & Privacy Restrictions ●

Location Services Allow
Contacts Allow
Calendars Allow
Reminders Allow
Photos Allow
Share My Location Allow
Bluetooth Sharing Allow
Microphone Allow
Speech Recognition Allow

Figure 137. Content & Privacy Restrictions On



Installing Apps Allow
Deleting Apps Allow
In-app Purchases Allow

Don’t Require ✓

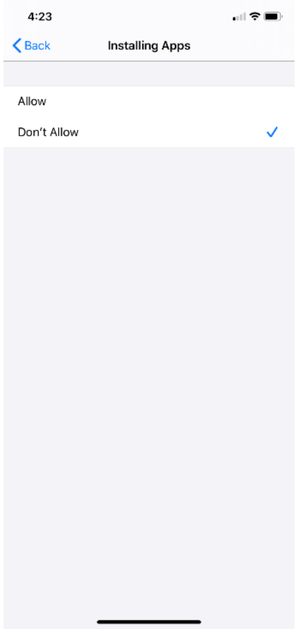
Require a password for additional purchases after making a purchase with mmiley@pacbell.net from the iTunes, Book, or App Store.

Figure 138. Store Purchases & Downloads - Change to Don't Allow

21. In our example, in **Store Purchases & Redownloads** we check **Don’t Allow**

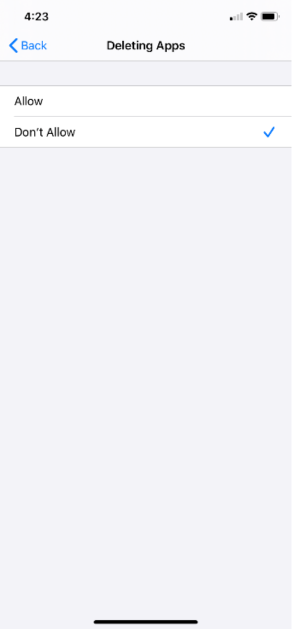
    for **Installing Apps…**

    for **Deleting apps…**



Don’t Allow ✓

Figure 139. Installing Apps > Don't Allow

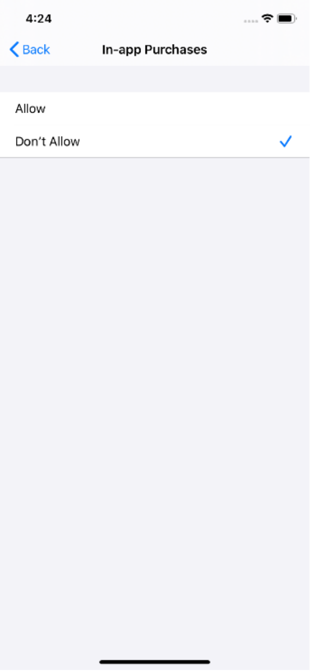


Don’t Allow ✓

Figure 140. Deleting Apps > Don't Allow

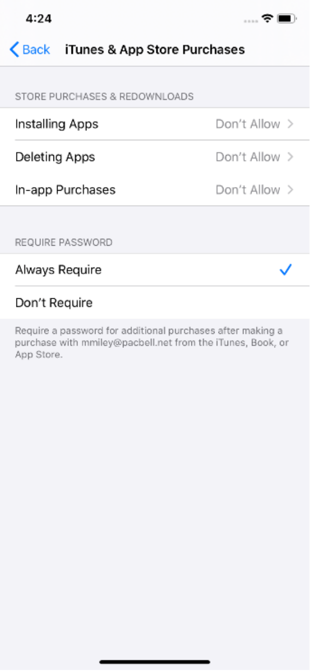
and for **In-App Purchases.**

22. Tap **Always Require** to require the passcode anytime an attempt is made to change these settings.
23. In summary, your child will now be restricted from **Installing apps, Deleting apps,** and making **In-app Purchases** and the password is required to change the settings.
24. Also, **Trend Micro Guardian** cannot be uninstalled without first entering the **Screen Time Passcode/Password.**



Allow
Don't Allow ✓

Figure 141. In-app Purchases > Don't Allow



STORE PURCHASES & REDOWNLOADS

Installing Apps: Don't Allow
Deleting Apps: Don't Allow
In-app Purchases: Don't Allow

REQUIRE PASSWORD

Always Require ✓
Don't Require

Require a password for additional purchases after making a purchase with mmiley@pacbell.net from the iTunes, Book, or App Store.

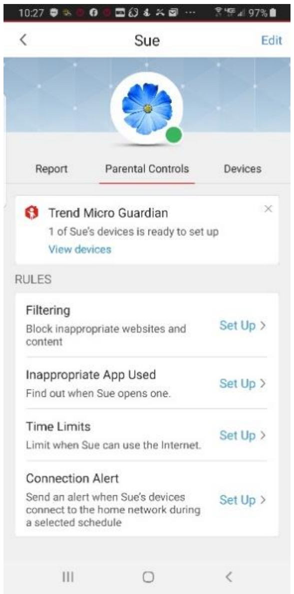
Figure 142. Always Require Password for Changes

Install Guardian on an Android Device

The install example below uses a Samsung Galaxy Note 3 assigned to the child “Sue.”

To install Guardian on an Android Device:

1. Once you’ve assigned the Android device to a family member, e.g., “Sue,” you can install **Trend Micro Guardian** on it.
2. Tap **View Devices** in the **Trend Micro Guardian** popup panel in **Parental Controls** to begin the installation.
3. An **Introducing Trend Micro Guardian** popup appears, where you can read about the protection **Trend Micro Guardian** provides.
4. Tap **Next**.



Trend Micro Guardian
1 of Sue’s devices is ready to set up

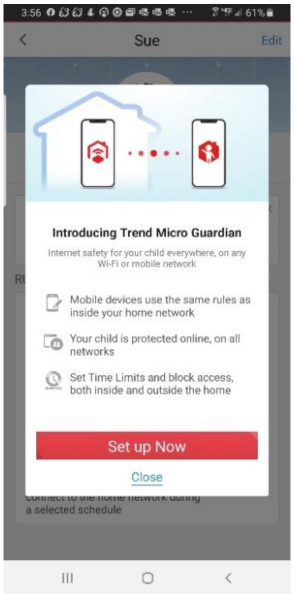
Filtering
Block inappropriate websites and content

Inappropriate App Used
Find out when Sue opens one.

Time Limits
Limit when Sue can use the Internet.

Connection Alert
Send an alert when Sue’s devices connect to the home network during a selected schedule

Figure 143. Parental Controls



Introducing Trend Micro Guardian
Internet safety for your child everywhere, on any Wi-Fi or mobile network

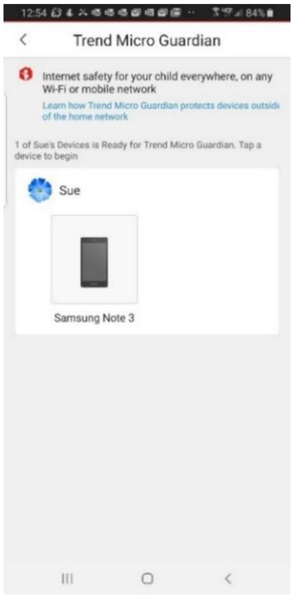
Mobile devices use the same rules as inside your home network

Your child is protected online, on all networks

Set Time Limits and block access, both inside and outside the home

Figure 144. Introducing Trend Micro Guardian

5. A device list appears with device(s) ready for **Trend Micro Guardian.**
6. Tap a device to begin. A screen appears for you to install **Trend Micro Guardian.**
7. Using the child's device, search for **Trend Micro Guardian** in **Google Play**, or scan the **QR Code** with a QR Code Scanner to get the link to the app.

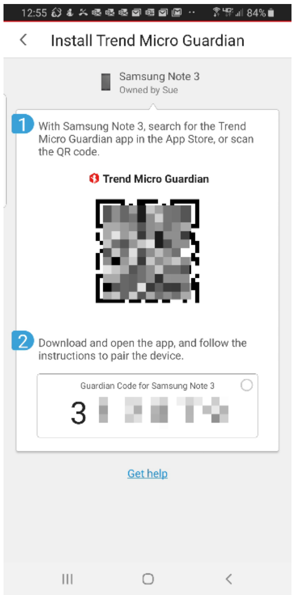


Internet safety for your child everywhere, on any Wi-Fi or mobile network

Learn how Trend Micro Guardian protects devices outside of the home network

1 of Sue's Devices is Ready for Trend Micro Guardian. Tap a device to begin

Figure 145. Tap a Device to Begin



1 With Samsung Note 3, search for the Trend Micro Guardian app in the App Store, or scan the QR code.

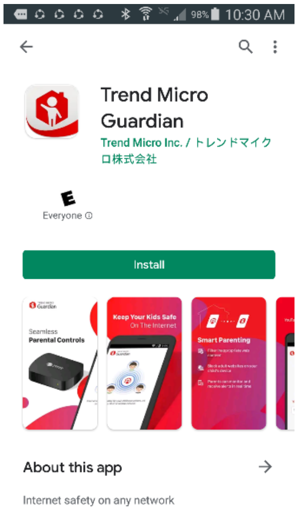
2 Download and open the app, and follow the instructions to pair the device.

Guardian Code for Samsung Note 3

3 [redacted]

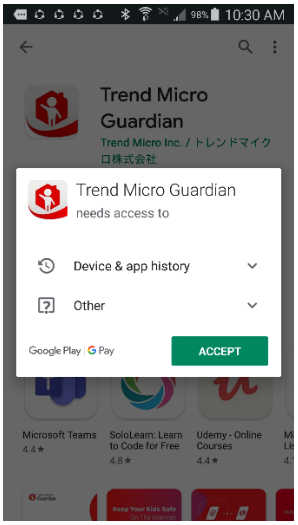
Figure 146. Install Trend Micro Guardian

8. **Trend Micro Guardian** appears in **Google Play** on the child's device. (Or you may pick it from a list if you searched for it, and the **Install** screen shows.)
9. Tap **Install.** The **App Manifest** appears, showing what data on your device **Trend Micro Guardian** has access to. Tap the down-arrows for details.
10. If you approve the install, tap **Accept.**


98%
10:30 AM
Trend Micro Guardian
Trend Micro Inc. / トレンドマイクロ株式会社
E
Everyone
Install
Seamless Parental Controls
Keep Your Kids Safe On The Internet
Smart Parenting
About this app

Internet safety on any network

Figure 147. Google Play > Trend Micro Guardian

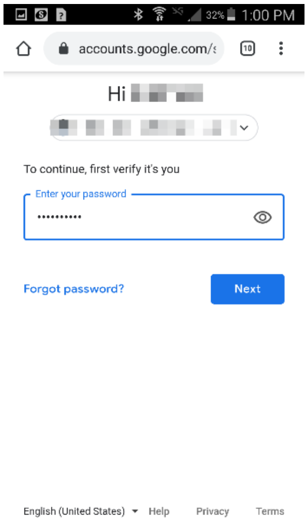

98%
10:30 AM
Trend Micro Guardian
Trend Micro Inc. / トレンドマイクロ株式会社

Trend Micro Guardian needs access to

Device & app history
Other
Google Play | G Pay
ACCEPT
Microsoft Teams 4.4★
SoloLearn: Learn to Code for Free 4.8★
Udemy - Online Courses 4.4★
Keep Your Kids Safe On The Internet

Figure 148. Continue

11. If you're not signed into **Google Play**, it asks you to sign in with your **Account** credentials.
12. Enter your Account ID and Password and tap **Next**. **Trend Micro Guardian** downloads and installs.
13. Tap **Open** to open the app.



To continue, first verify it's you

Figure 149. Enter Google Account Credentials

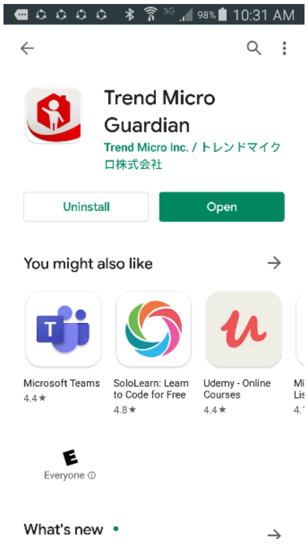
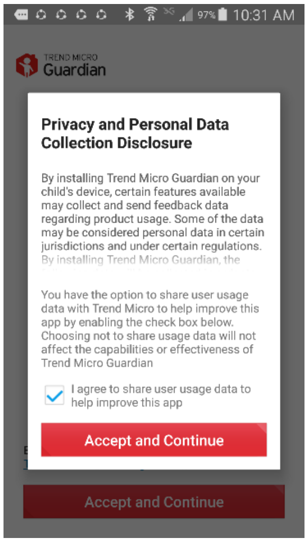


Figure 150. Trend Micro Guardian Installed

53. The **Privacy and Personal Data Collection Disclosure** screen appears.
54. Read the disclosure, which outlines what kind of data **Trend Micro Guardian** collects.
55. If you agree, check **"I agree to share user usage data to help improve this app"** and tap **Accept and Continue**.
14. An instructional screen appears describing the Internet Security it provides for your child.
15. Tap **Accept and Continue.**



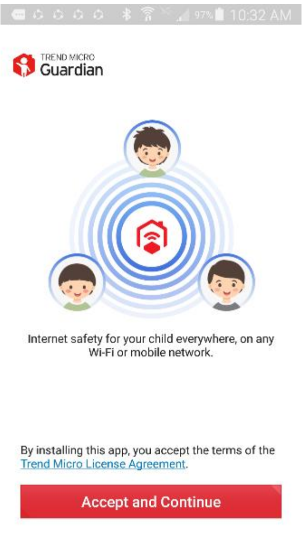
Privacy and Personal Data Collection Disclosure

By installing Trend Micro Guardian on your child's device, certain features available may collect and send feedback data regarding product usage. Some of the data may be considered personal data in certain jurisdictions and under certain regulations. By installing Trend Micro Guardian, the

You have the option to share user usage data with Trend Micro to help improve this app by enabling the check box below. Choosing not to share usage data will not affect the capabilities or effectiveness of Trend Micro Guardian

☑ I agree to share user usage data to help improve this app

Figure 151. Privacy and Personal Data Collection Disclosure

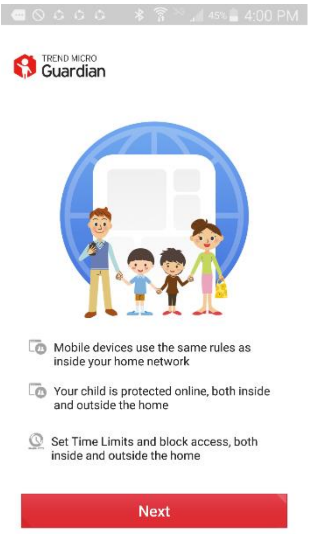


Internet safety for your child everywhere, on any Wi-Fi or mobile network.

By installing this app, you accept the terms of the Trend Micro License Agreement.

Figure 152. Accept and Continue

16. A second instructional screen appears describing how mobile devices use the same rules inside and outside the home network.
17. Tap **Next**. The **Pair Now** screen appears.
18. Tap **Pair Now.**

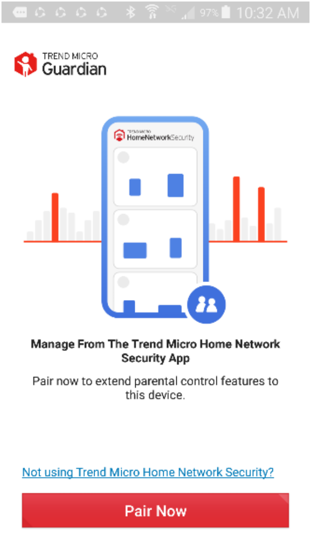


Mobile devices use the same rules as inside your home network

Your child is protected online, both inside and outside the home

Set Time Limits and block access, both inside and outside the home

Figure 153. Next

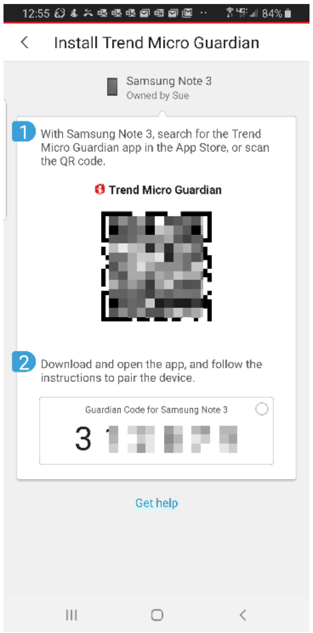


Manage From The Trend Micro Home Network Security App

Pair now to extend parental control features to this device.

Figure 154. Pair Now

19. Back on the managing device, view the **Pairing Code** in the **Trend Micro Home Network Security** application.
20. On the child's device, enter the **Pairing Code** that's currently showing on the managing device into the **Trend Micro Guardian** app.



Samsung Note 3
Owned by Sue

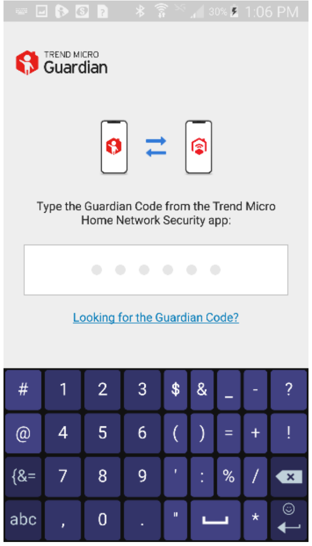
1 With Samsung Note 3, search for the Trend Micro Guardian app in the App Store, or scan the QR code.

2 Download and open the app, and follow the instructions to pair the device.

Guardian Code for Samsung Note 3

3 [redacted]

Figure 155. Managing Device > View Pairing Code



Type the Guardian Code from the Trend Micro Home Network Security app:

● ● ● ● ● ●

Figure 156. Child's Device > Enter Pairing Code

21. The **Pairing Complete** screen appears, showing the process of pairing as it checks the settings and pairs.
22. When the pairing process has finished, a screen appears indicating that **Trend Micro Guardian** needs the following permissions: **Install VPN Profile, Accessibility, Notification Access, and Display Over Other Apps,** and **Device Administrators** (for uninstallation protection).

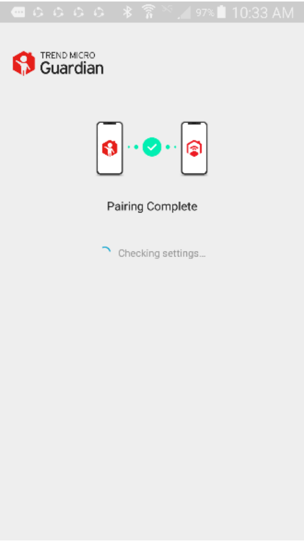
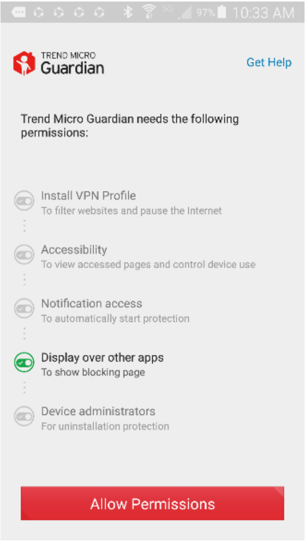


Figure 157. Pairing in Process



Trend Micro Guardian needs the following permissions:

Install VPN Profile
To filter websites and pause the Internet

Accessibility
To view accessed pages and control device use

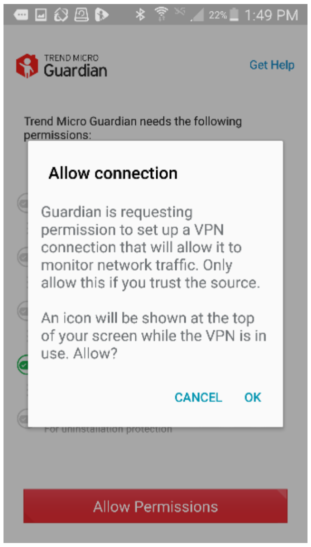
Notification access
To automatically start protection

Display over other apps
To show blocking page

Device administrators
For uninstallation protection

Figure 158. Allow Permissions

23. Tap **Allow Permissions.** An **Allow Connection** screen appears, indicating Guardian wants to set up a VPN. Tap **OK**.
24. An **Accessibility Permission** screen appears. Tap **OK**.



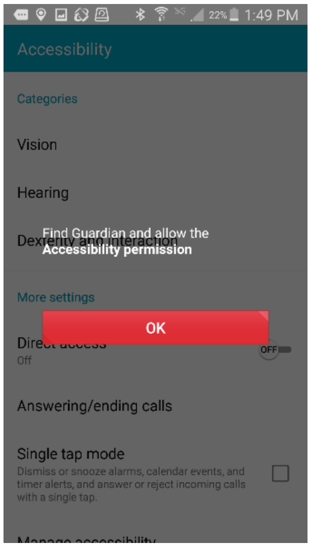
Trend Micro Guardian needs the following permissions:

Allow connection

Guardian is requesting permission to set up a VPN connection that will allow it to monitor network traffic. Only allow this if you trust the source.

An icon will be shown at the top of your screen while the VPN is in use. Allow?

Figure 159. Allow Connection

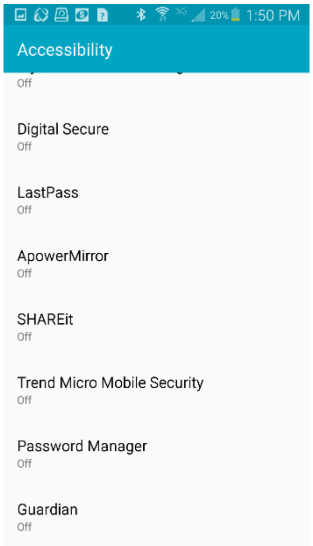


Find Guardian and allow the **Accessibility permission**

Dismiss or snooze alarms, calendar events, and timer alerts, and answer or reject incoming calls with a single tap.

Figure 160. Allow Accessibility Permission

25. The **Accessibility** screen appears.
26. Scroll down and tap **Guardian** to enable it. A **Guardian** screen appears.
27. Tap **Guardian** to Toggle **Accessibility On** for it.



Accessibility

Off

Digital Secure
Off

LastPass
Off

ApowerMirror
Off

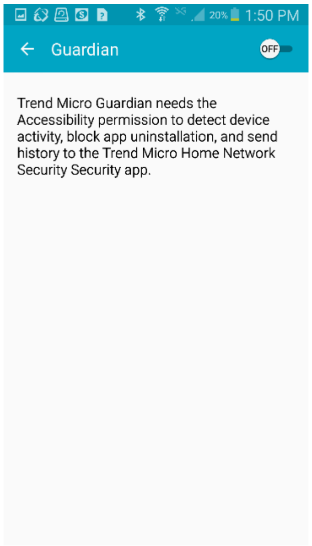
SHAREit
Off

Trend Micro Mobile Security
Off

Password Manager
Off

Guardian
Off

Figure 161. Accessibility > Guardian

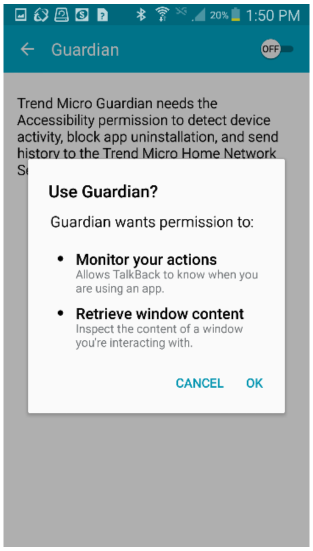


Guardian

Trend Micro Guardian needs the Accessibility permission to detect device activity, block app uninstallation, and send history to the Trend Micro Home Network Security Security app.

Figure 162. Guardian > Toggle Accessibility Permission On

28. A **Use Guardian** popup appears, asking if you want to grant Guardian the ability to **Monitor your actions** and **Retrieve window content.**
29. Tap **OK**.
30. A **Notification Access** popup appears. Tap **OK** to close it.



Guardian

Trend Micro Guardian needs the Accessibility permission to detect device activity, block app uninstallation, and send history to the Trend Micro Home Network

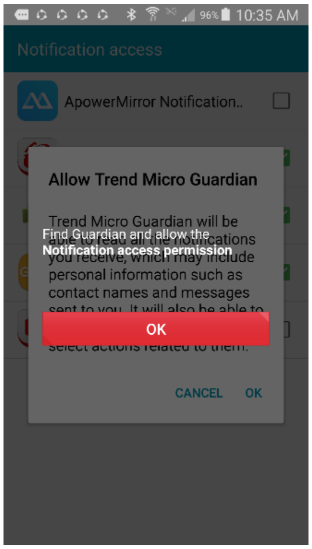
Use Guardian?

Guardian wants permission to:

- **Monitor your actions**
  Allows TalkBack to know when you are using an app.
- **Retrieve window content**
  Inspect the content of a window you're interacting with.

CANCEL OK

Figure 163. Use Guardian?



Notification access

ApowerMirror Notification.. ☐

Allow Trend Micro Guardian

Trend Micro Guardian will be able to read all the notifications you receive, which may include personal information such as contact names and messages sent to you. It will also be able to select actions related to them.

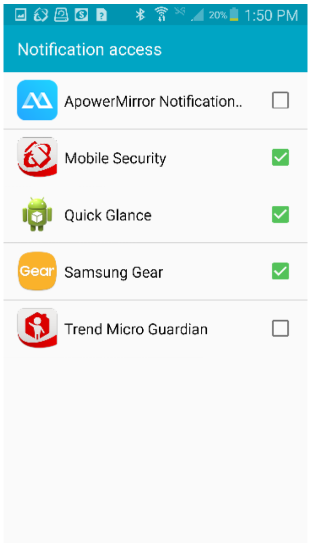
CANCEL OK

Find Guardian and allow the **Notification access permission**

OK

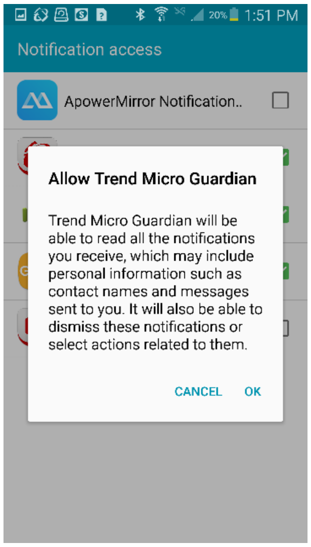
Figure 164. Notification Access Popup

31. Locate **Trend Micro Guardian** in the list and tap the checkbox to check it.
32. A popup appears, asking if you wish to **Allow Trend Micro Guardian** the ability to read all the notifications you receive.
33. Tap **OK**.



ApowerMirror Notification.. ☐
Mobile Security ☑
Quick Glance ☑
Samsung Gear ☑
Trend Micro Guardian ☐

Figure 165. Notification Access > Trend Micro Guardian

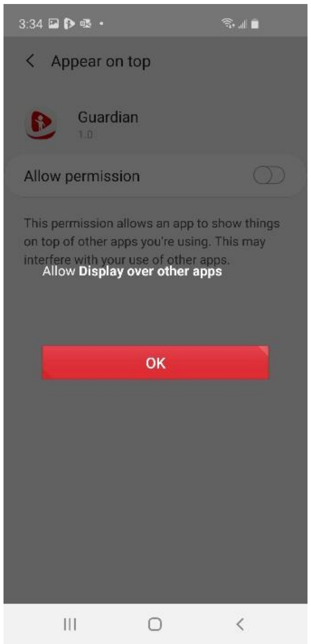


Allow Trend Micro Guardian

Trend Micro Guardian will be able to read all the notifications you receive, which may include personal information such as contact names and messages sent to you. It will also be able to dismiss these notifications or select actions related to them.

Figure 166. Allow Trend Micro Guardian

34. **Trend Micro Guardian** now has the ability to receive notifications.
35. An **Allow Display over other apps** popup appears, which lets **Guardian** show blocking pages.
36. Tap **Allow Permission** to let **Guardian** appear on top of other apps.
37. You'll now set up **Device Administration,** for **Uninstall Protection.** See the section following.

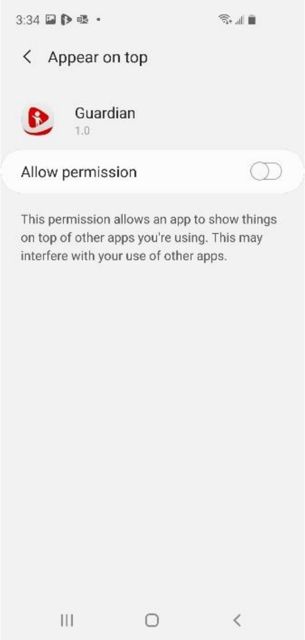


Allow permission ○

This permission allows an app to show things on top of other apps you're using. This may interfere with your use of other apps.

Allow **Display over other apps**

Figure 167. Allow Display Over Other Apps



Allow permission ○

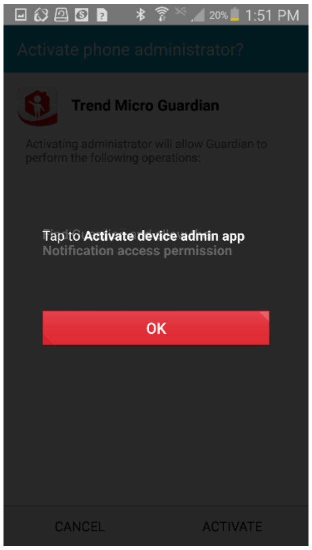
This permission allows an app to show things on top of other apps you're using. This may interfere with your use of other apps.

Figure 168. Allow Guardian to Appear on Top of Other Apps

Set Up Guardian Uninstall Protection on an Android Device

To set up Device Administration for Uninstallation Protection:

38. Continuing from the instructions above, a popup appears to instruct you to **Activate device admin app**.
39. Tap **OK.** A screen appears to **Activate Device Administrator?**
40. Tap **Activate**. **Uninstallation Protection** is now active on the Android device.

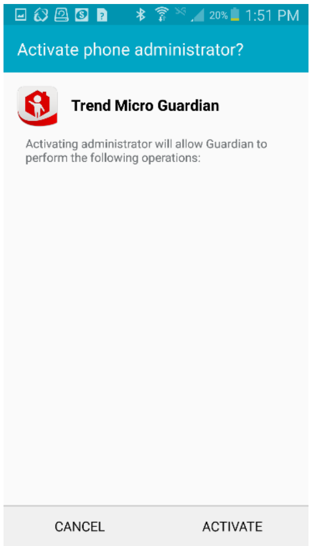


Activate phone administrator?

Activating administrator will allow Guardian to perform the following operations:

Tap to **Activate device admin app**
Notification access permission

Figure 169. Activate Device Admin

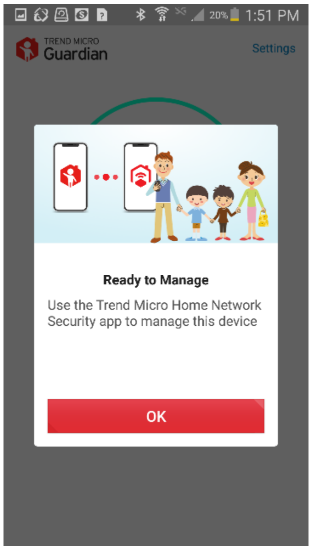


Activate phone administrator?

Activating administrator will allow Guardian to perform the following operations:

Figure 170. Activate Phone Administrator for Trend Micro Guardian

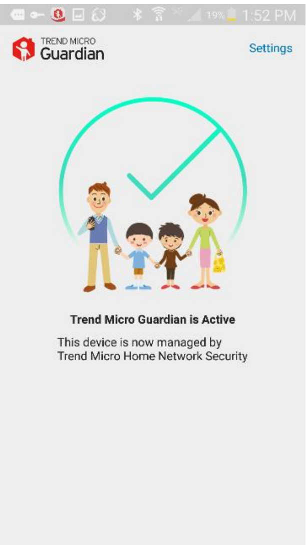
41. A popup appears, indicating **Guardian** is **Ready to Manage** your child's phone.
42. Tap **OK.** A screen appears indicating **Trend Micro Guardian Is Active.**
43. Tap **Settings** to review the settings.



Ready to Manage

Use the Trend Micro Home Network Security app to manage this device

Figure 171. Ready to Manage

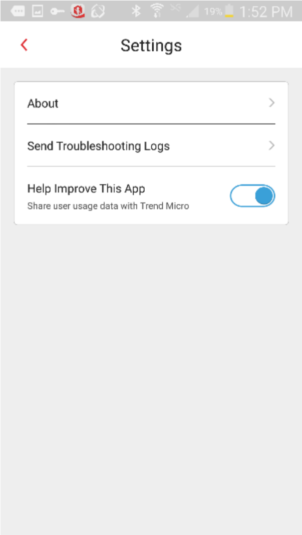


Trend Micro Guardian is Active

This device is now managed by Trend Micro Home Network Security

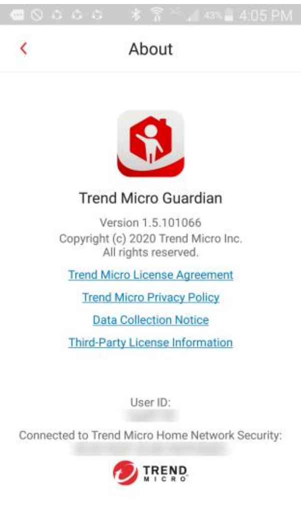
Figure 172. Trend Micro Guardian is Active

44. Here you'll view **About** to learn more about the Guardian app, to **Send Troubleshooting Logs**, and to toggle **On/Off** the **Help improve this App** function, which shares usage data with Trend Micro.
45. Tap **About** to get information about the app. Here you'll view the **Trend Micro Guardian** app details, along with **User ID** and Guardian's connection to your **Trend Micro Home Network Security Station** and its ID.



Share user usage data with Trend Micro

Figure 173. Settings



Trend Micro Guardian

Version 1.5.101066
Copyright (c) 2020 Trend Micro Inc.
All rights reserved.

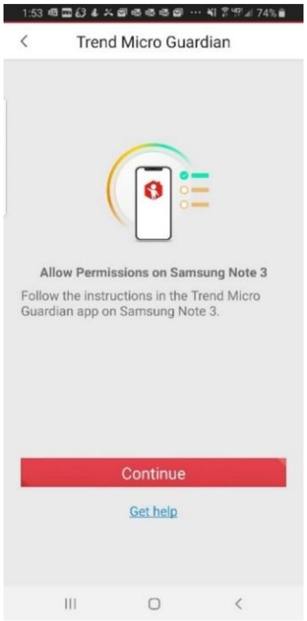
Trend Micro License Agreement
Trend Micro Privacy Policy
Data Collection Notice
Third-Party License Information

User ID:
[redacted]

Connected to Trend Micro Home Network Security:
[redacted]

Figure 174. About > Trend Micro Guardian

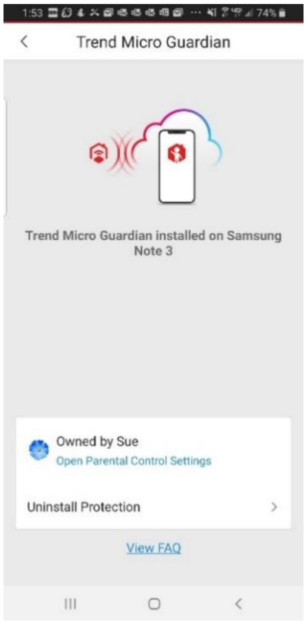
46. Back in the **Home Network Security** app on your managing device, complete the **Trend Micro Guardian** permissions process by tapping **Continue**.
47. A screen appears, showing **Trend Micro Guardian** is now installed on the device, e.g., the Samsung Note 3; and that the device is **Owned by Sue.**
48. Tap **Uninstall Protection** to view the protection.



Allow Permissions on Samsung Note 3

Follow the instructions in the Trend Micro Guardian app on Samsung Note 3.

Figure 175. Allow Permissions on Samsung Note 3 > Continue



Trend Micro Guardian installed on Samsung Note 3

Owned by Sue

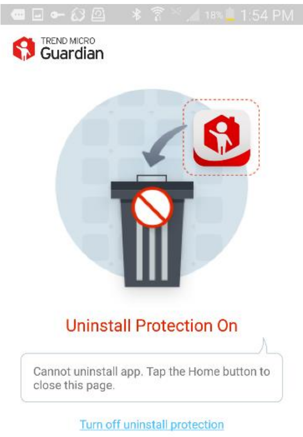
Figure 176. Owned by Sue > Uninstall Protection

49. A screen appears, indicating that **Uninstall Protection** is **On** for the child's device.
50. Tap **Turn Off Uninstall Protection** to view the **Uninstall Protection** screen
51. To remove **Trend Micro Guardian** from the child's device at any time, follow the steps shown in the screen. On the child's device

    >Deactivate **Device Administrator**, using the **Guardian Code** shown here

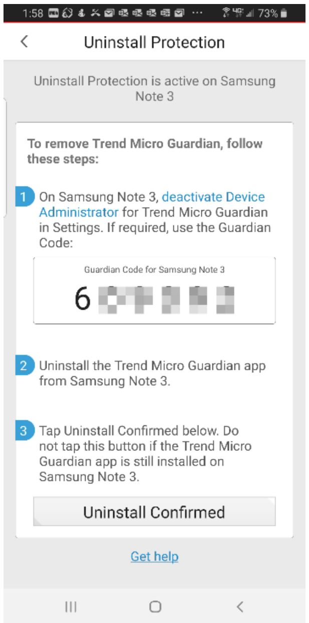
    >**Uninstall Guardian** on the child's device

    >Return to the managing device and tap **Uninstall Confirmed.**



Cannot uninstall app. Tap the Home button to close this page.

Figure 177. Child's Device > Uninstall Protection On



Uninstall Protection is active on Samsung Note 3

To remove Trend Micro Guardian, follow these steps:

1 On Samsung Note 3, deactivate Device Administrator for Trend Micro Guardian in Settings. If required, use the Guardian Code:

Guardian Code for Samsung Note 3

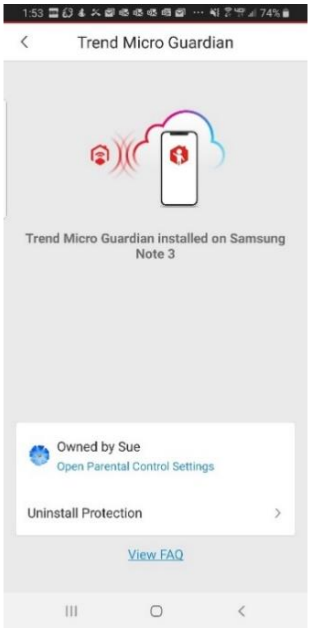
6[redacted]

2 Uninstall the Trend Micro Guardian app from Samsung Note 3.

3 Tap Uninstall Confirmed below. Do not tap this button if the Trend Micro Guardian app is still installed on Samsung Note 3.

Figure 178. Managing Device > Uninstall Procedure

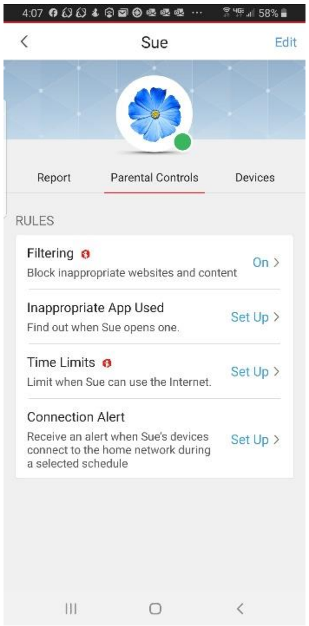
52. Tap the back-arrow to return to **Trend Micro Guardian** screen for the device.
53. Tap the **Open Parental Controls Settings** link in the panel **Owned by "Child".**
54. You may now begin setting up **Parental Controls** for this child.



Trend Micro Guardian installed on Samsung Note 3

Owned by Sue

Figure 179. Trend Micro Guardian Installed on Device



Filtering — Block inappropriate websites and content — On

Inappropriate App Used — Find out when Sue opens one. — Set Up

Time Limits — Limit when Sue can use the Internet. — Set Up

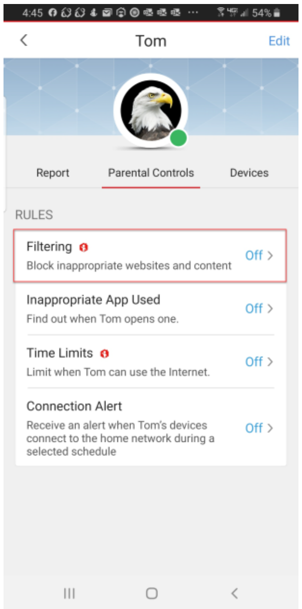
Connection Alert — Receive an alert when Sue's devices connect to the home network during a selected schedule — Set Up

Figure 180. Parental Controls

Filtering

To set up Filtering:

1. To begin setting up **Parental Controls** for a family member's devices, tap their icon from the **Family Members List.** The **Parental Controls** screen appears.
2. Note the red icon in the **Filtering** panel. This indicates remote **Filtering** can be enabled via **Guardian**.
3. Tap **Filtering** to set it up to block inappropriate websites and content. The **Filtering** screen appears.



RULES

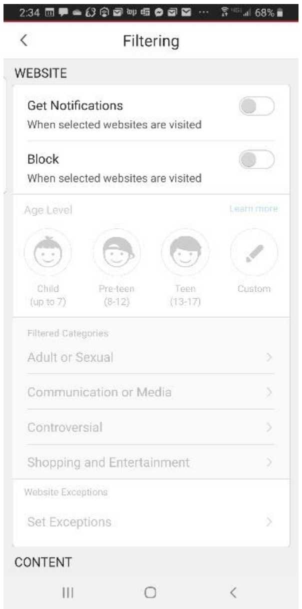
Filtering — Block inappropriate websites and content — Off

Inappropriate App Used — Find out when Tom opens one. — Off

Time Limits — Limit when Tom can use the Internet. — Off

Connection Alert — Receive an alert when Tom's devices connect to the home network during a selected schedule — Off

Figure 181. Filtering



WEBSITE

Get Notifications — When selected websites are visited

Block — When selected websites are visited

Age Level — Learn more

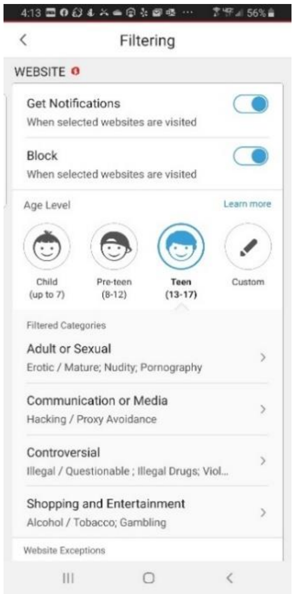
Filtered Categories
Adult or Sexual
Communication or Media
Controversial
Shopping and Entertainment

Website Exceptions
Set Exceptions

CONTENT

Figure 182. Filtering Setup

4. Toggle on **Get Notifications** for this family member when selected websites are visited.
5. Toggle on **Block** to block selected websites for this family member.
6. Tap the **Age Level** for this child, or tap **Custom** to manually select categories and subcategories to block.
7. You may begin with an **Age Level** filter and customize it.



WEBSITE

Get Notifications — When selected websites are visited

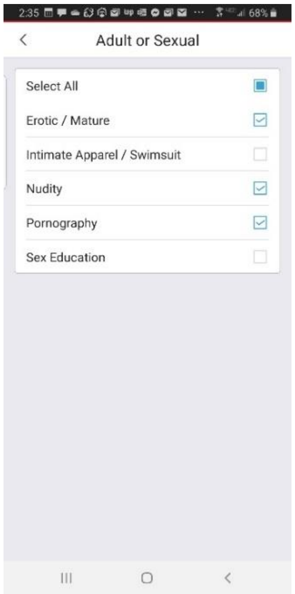
Block — When selected websites are visited

Age Level — Learn more

Filtered Categories
Adult or Sexual — Erotic / Mature; Nudity; Pornography
Communication or Media — Hacking / Proxy Avoidance
Controversial — Illegal / Questionable ; Illegal Drugs; Viol...
Shopping and Entertainment — Alcohol / Tobacco; Gambling

Website Exceptions

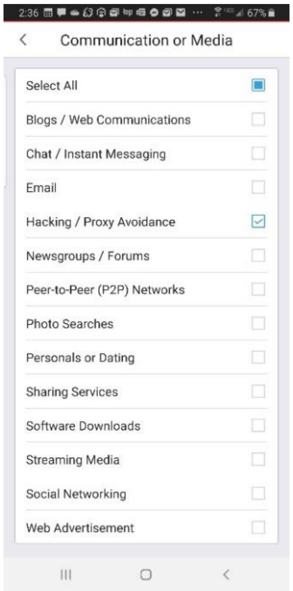
Figure 183. Toggle On Filtering



Select All ■
Erotic / Mature ☑
Intimate Apparel / Swimsuit ☐
Nudity ☑
Pornography ☑
Sex Education ☐

Figure 184. Adult or Sexual Category

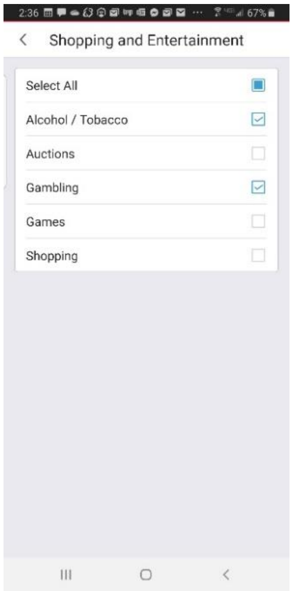
8. Add items in the **Adult or Sexual** category by tapping the checkbox(es).
9. Check items in the **Communication or Media** list.
10. Do the same for **Controversial** or **Shopping and Entertainment.**



Communication or Media

- ☑ Select All
- ☐ Blogs / Web Communications
- ☐ Chat / Instant Messaging
- ☐ Email
- ☑ Hacking / Proxy Avoidance
- ☐ Newsgroups / Forums
- ☐ Peer-to-Peer (P2P) Networks
- ☐ Photo Searches
- ☐ Personals or Dating
- ☐ Sharing Services
- ☐ Software Downloads
- ☐ Streaming Media
- ☐ Social Networking
- ☐ Web Advertisement

Figure 185. Communications or Media

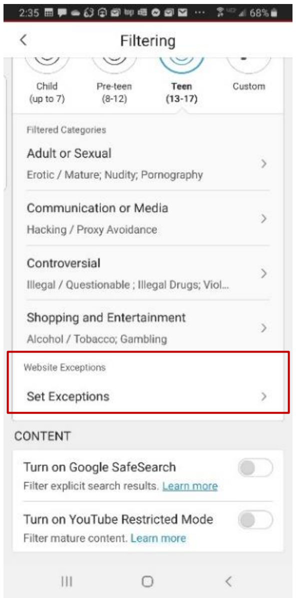


Shopping and Entertainment

- ☑ Select All
- ☑ Alcohol / Tobacco
- ☐ Auctions
- ☑ Gambling
- ☐ Games
- ☐ Shopping

Figure 186. Shopping and Entertainment

11. Back in the **Filtering** screen, tap **Set Exceptions** to set them.
12. Tap **Allowed List** or **Denied List** to add exceptions to that list.



Filtering

Child (up to 7) Pre-teen (8-12) **Teen (13-17)** Custom

Filtered Categories

Adult or Sexual
Erotic / Mature; Nudity; Pornography

Communication or Media
Hacking / Proxy Avoidance

Controversial
Illegal / Questionable ; Illegal Drugs; Viol...

Shopping and Entertainment
Alcohol / Tobacco; Gambling

Website Exceptions

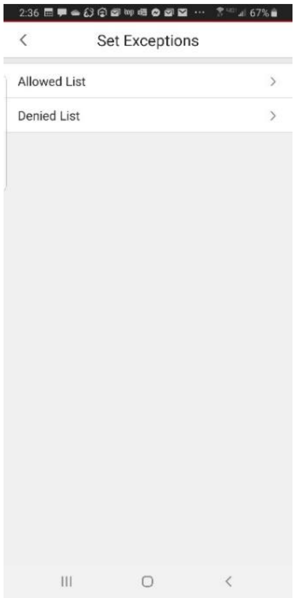
Set Exceptions

CONTENT

Turn on Google SafeSearch ○
Filter explicit search results. Learn more

Turn on YouTube Restricted Mode ○
Filter mature content. Learn more

Figure 187. Set Exceptions



Set Exceptions

Allowed List

Denied List

Figure 188. Allowed/Denied Lists

13. Tap **Add a new website** to add the exception to the list.
14. Type in the URL for the website you wish to add, then tap **Done**.

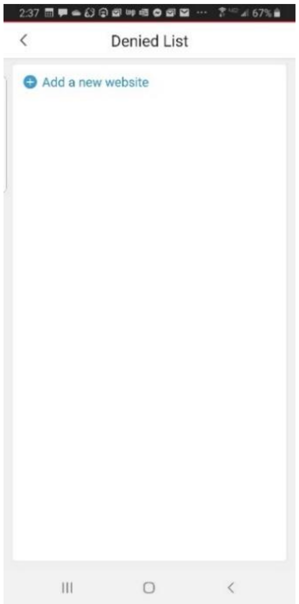
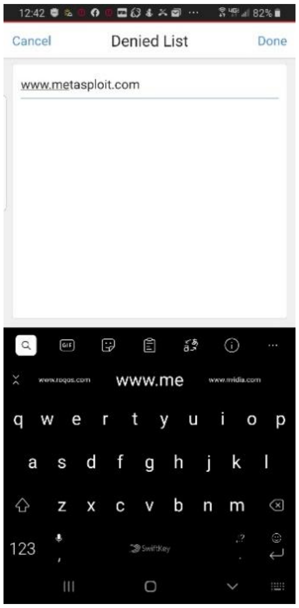


Figure 189. Denied List

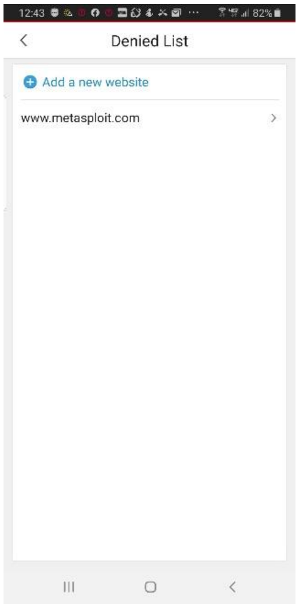


www.metasploit.com

Figure 190. Add Denied Website

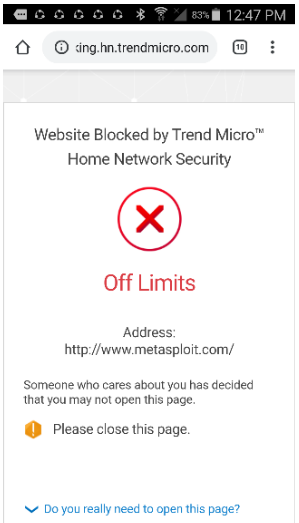
15. The website is added to the list.

    Test the site on the child's device by typing the URL in its browser. HNS blocks you from going to the website, providing an **Off Limits** notice. This is the notice child will see when they attempt to go to this website. You (as the parent) will also be notified that they attempted to access it.



www.metasploit.com

Figure 191. Denied List > Website Added



Website Blocked by Trend Micro™ Home Network Security

Off Limits

Address:
http://www.metasploit.com/

Someone who cares about you has decided that you may not open this page.

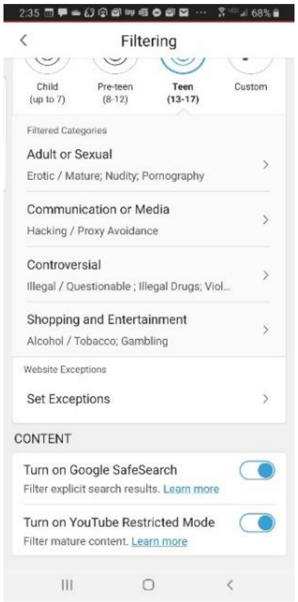
Please close this page.

Do you really need to open this page?

Figure 192. Child's Device > Off Limits

16. Toggle on **Google SafeSearch** to filter explicit search results in the family member's mobile browser and **YouTube Restricted Mode** to filter out mature content on YouTube.

17. Back in the **Parental Controls** screen for Tom, **Filtering** is now **On**, blocking inappropriate websites and content.



Adult or Sexual: Erotic / Mature; Nudity; Pornography

Communication or Media: Hacking / Proxy Avoidance

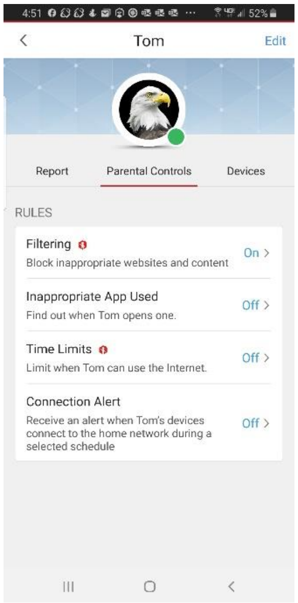
Controversial: Illegal / Questionable ; Illegal Drugs; Viol...

Shopping and Entertainment: Alcohol / Tobacco; Gambling

Turn on Google SafeSearch — Filter explicit search results. (on)

Turn on YouTube Restricted Mode — Filter mature content. (on)

Figure 193. Content Toggles



Filtering — Block inappropriate websites and content — On

Inappropriate App Used — Find out when Tom opens one. — Off

Time Limits — Limit when Tom can use the Internet. — Off

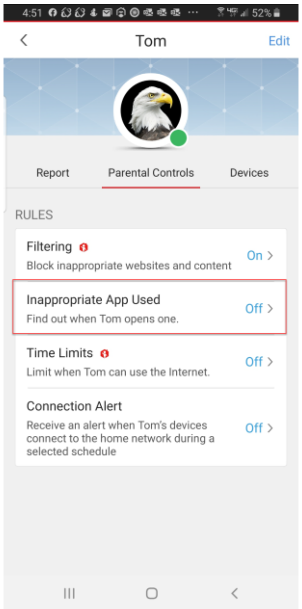
Connection Alert — Receive an alert when Tom's devices connect to the home network during a selected schedule — Off

Figure 194. Filtering On

Inappropriate App Used

To set up Inappropriate App Used:

1. Tap **Inappropriate App Used** panel to set it up. The **Inappropriate App Used** screen appears.
2. Tap **Get Notifications** to toggle the feature **On**.



RULES

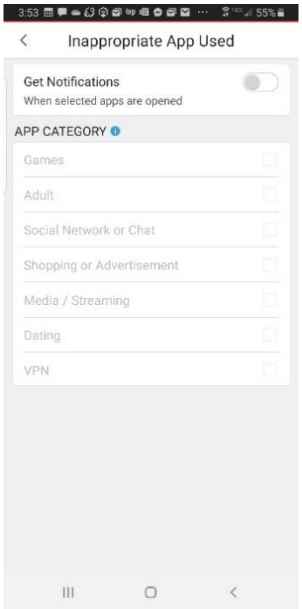
Filtering — Block inappropriate websites and content — On

Inappropriate App Used — Find out when Tom opens one. — Off

Time Limits — Limit when Tom can use the Internet. — Off

Connection Alert — Receive an alert when Tom's devices connect to the home network during a selected schedule — Off

Figure 195. Inappropriate App Used



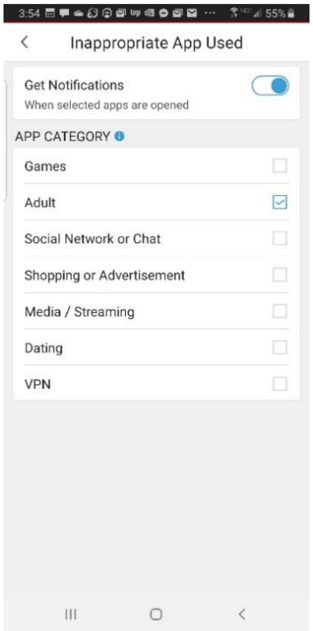
Get Notifications — When selected apps are opened

APP CATEGORY

- ☐ Games
- ☐ Adult
- ☐ Social Network or Chat
- ☐ Shopping or Advertisement
- ☐ Media / Streaming
- ☐ Dating
- ☐ VPN

Figure 196. Toggle On Notifications

3. Tap the checkboxes for **App Categories** you wish to receive notifications for.



Get Notifications — When selected apps are opened

APP CATEGORY

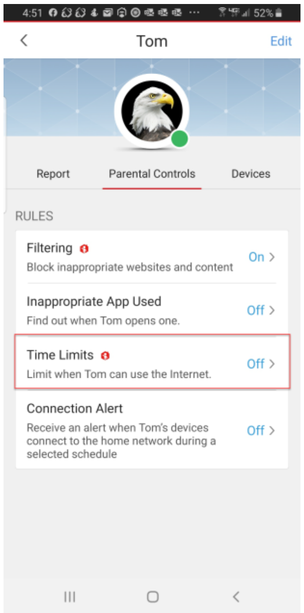
- ☐ Games
- ☑ Adult
- ☐ Social Network or Chat
- ☐ Shopping or Advertisement
- ☐ Media / Streaming
- ☐ Dating
- ☐ VPN

Figure 197. App Categories

Time Limits

To set up Time Limits:

1. Tap the **Time Limits** panel to set it up The **Time Limits** screen appears
2. Tap **Add First Rule** to add it.



Tom Edit

RULES

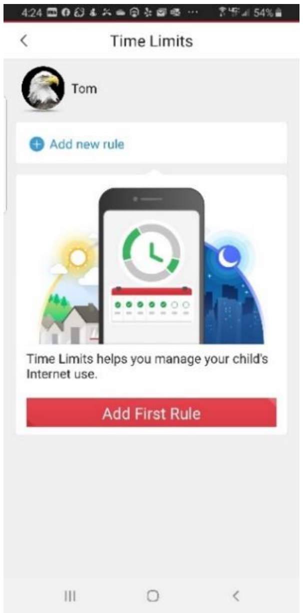
Filtering — Block inappropriate websites and content — On

Inappropriate App Used — Find out when Tom opens one. — Off

Time Limits — Limit when Tom can use the Internet. — Off

Connection Alert — Receive an alert when Tom's devices connect to the home network during a selected schedule — Off

Figure 198. Set Up Time Limits



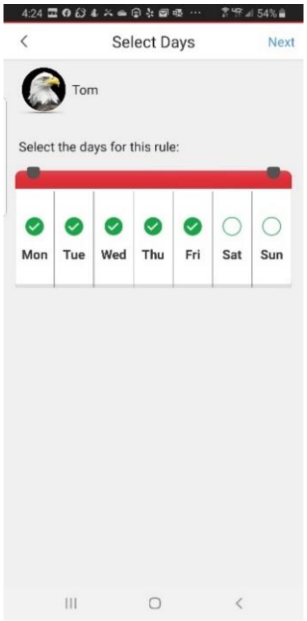
Time Limits

Tom

Time Limits helps you manage your child's Internet use.

Figure 199. Add First Rule

3. **Select the Days** for this rule; e.g., **Mon-Fri**, and tap **Next**.
4. Set the **Internet Time Limit** and **Time on YouTube** by scrolling back and forth to see the limits available, then tap the limits you want to set them.
5. Toggle on **Get Notifications.**



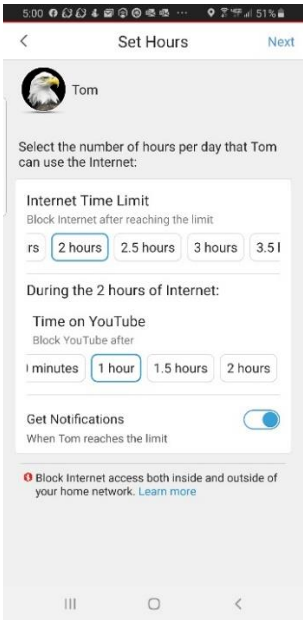
Select Days Next

Tom

Select the days for this rule:

☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ○ Sat ○ Sun

Figure 200. Select Days



Set Hours Next

Tom

Select the number of hours per day that Tom can use the Internet:

Internet Time Limit
Block Internet after reaching the limit
rs | 2 hours | 2.5 hours | 3 hours | 3.5 l

During the 2 hours of Internet:

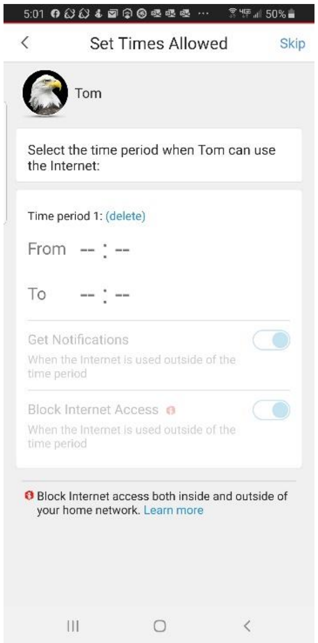
Time on YouTube
Block YouTube after
l minutes | 1 hour | 1.5 hours | 2 hours

Get Notifications
When Tom reaches the limit

Block Internet access both inside and outside of your home network. Learn more

Figure 201. Set Hours

6. Set the time period when the family member can use the Internet by tapping the **From** field, then move the **Time Clock** to the beginning time.
7. When the **Time Clock** sets the time, tap **AM** or **PM** to set it, then **OK**.



Tom

Select the time period when Tom can use the Internet:

Time period 1: (delete)

From -- : --

To -- : --

Get Notifications

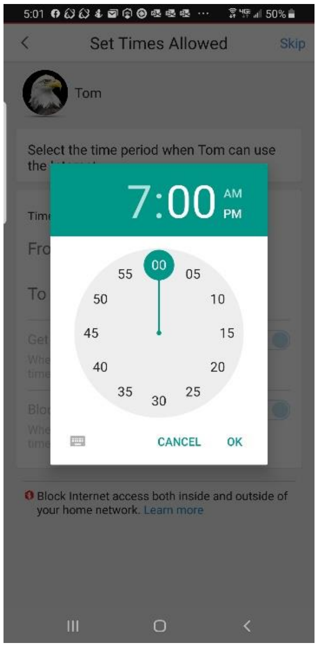
When the Internet is used outside of the time period

Block Internet Access

When the Internet is used outside of the time period

Block Internet access both inside and outside of your home network. Learn more

Figure 202. Set Times Allowed

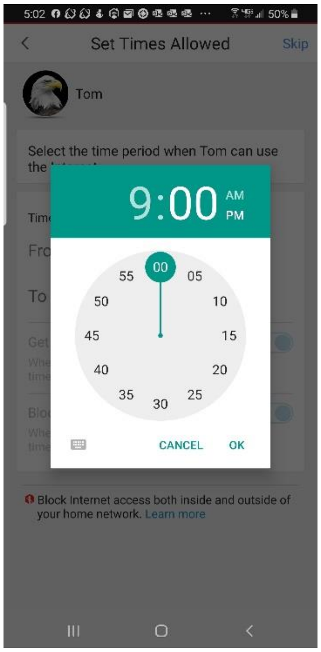


Tom

Block Internet access both inside and outside of your home network. Learn more

Figure 203. Set Beginning Time

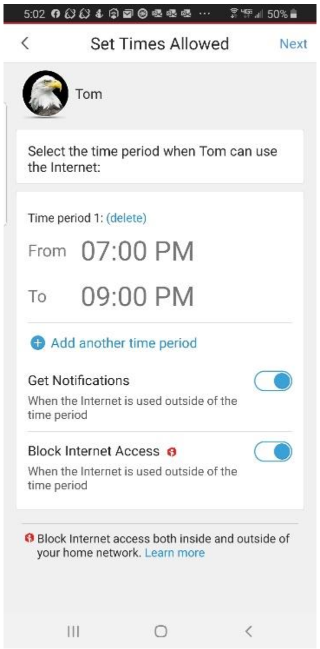
8. Do the same operations for the **Ending** time and tap **OK**.
9. Toggle on **Get Notifications** and **Block Internet Access**, for when the Internet is used outside of the time period.
10. Tap **Add another time period** if you wish and repeat the processes outlined above.
11. Tap **Next** to complete the rule setup



Tom

Block Internet access both inside and outside of your home network. Learn more

Figure 204. Set Ending Time



Tom

Select the time period when Tom can use the Internet:

Time period 1: (delete)

From 07:00 PM

To 09:00 PM

Add another time period

Get Notifications

When the Internet is used outside of the time period

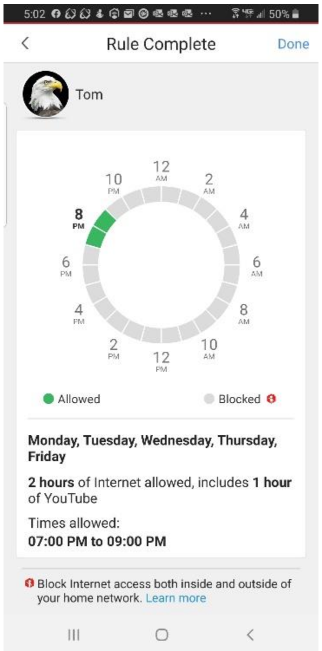
Block Internet Access

When the Internet is used outside of the time period

Block Internet access both inside and outside of your home network. Learn more

Figure 205. Time Period, Get Notifications, Block Internet

12. When you have finished setting the rule(s), the **Rule Complete** screen shows a summary of the rule you set, providing a clock to show the **Allowed Time**, the **Days** for which the rule is set, the **Hours** of Internet allowed, including any time allowed for **YouTube** viewing, and the **Times** allowed.
13. Tap **Done** to finalize the rule. The Time Limits screen shows you the rule for the family member. Toggle the rule **Off** if you wish, or **Add new rule** to set a new rule.



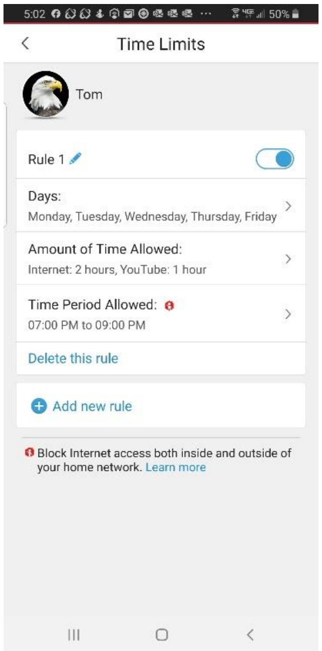
Monday, Tuesday, Wednesday, Thursday, Friday

2 hours of Internet allowed, includes **1 hour** of YouTube

Times allowed:
07:00 PM to 09:00 PM

Block Internet access both inside and outside of your home network. Learn more

Figure 206. Rule Complete



Days:
Monday, Tuesday, Wednesday, Thursday, Friday

Amount of Time Allowed:
Internet: 2 hours, YouTube: 1 hour

Time Period Allowed:
07:00 PM to 09:00 PM

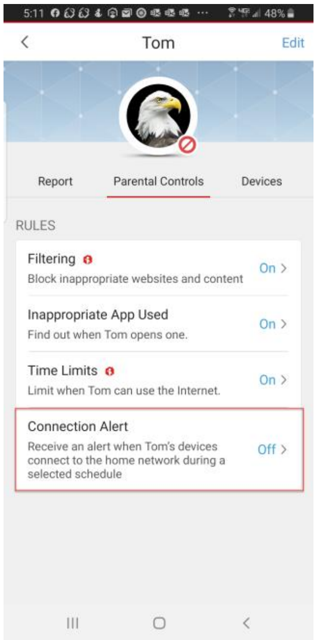
Block Internet access both inside and outside of your home network. Learn more

Figure 207. Family Member Rule

Connection Alert

To set up Connection Alert:

1. Tap **Set Up** to set up **Connection Alert and the screen appears**
2. Tap the **Get Notifications** toggle to **On**, then set the **Schedule** for the **Connection Alert** as you did for the **Time Limits,** by using the **Time Clock**. In this example, we'll leave the default.
3. The checkboxes for the Child's device(s) should be automatically checked in the **Select Devices** panel to enable the **Connection Alert** for those devices.
4. Uncheck to remove the device(s) for the monitoring period (e.g., when they connect to the internet between 12 and 10pm.)



RULES

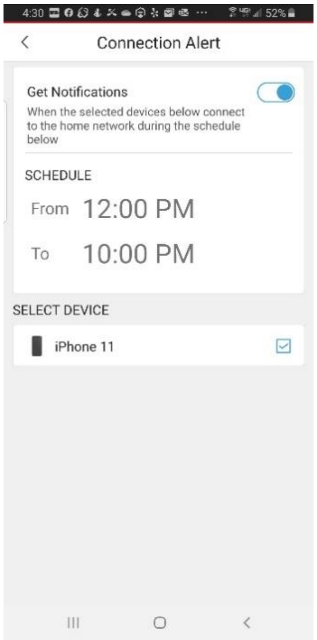
Filtering — On
Block inappropriate websites and content

Inappropriate App Used — On
Find out when Tom opens one.

Time Limits — On
Limit when Tom can use the Internet.

Connection Alert — Off
Receive an alert when Tom's devices connect to the home network during a selected schedule

Figure 208. Set Up Connection Alert



Get Notifications
When the selected devices below connect to the home network during the schedule below

SCHEDULE

From 12:00 PM

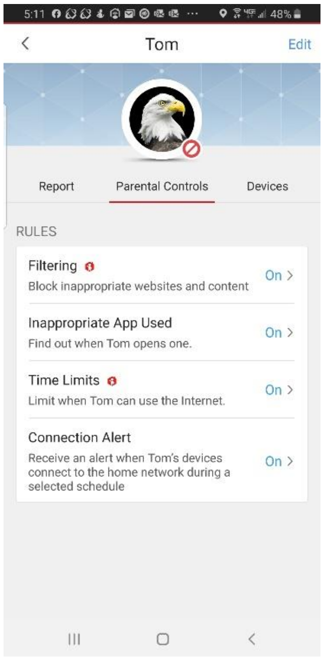
To 10:00 PM

SELECT DEVICE

iPhone 11 ☑

Figure 209. Get Notifications for Devices Connecting to Network

5. Tap the back arrow to return to the main screen for the family member.
6. All **Parental Controls** for the family member have now been set to **On**.



RULES

Filtering — Block inappropriate websites and content — On

Inappropriate App Used — Find out when Tom opens one. — On

Time Limits — Limit when Tom can use the Internet. — On

Connection Alert — Receive an alert when Tom's devices connect to the home network during a selected schedule — On

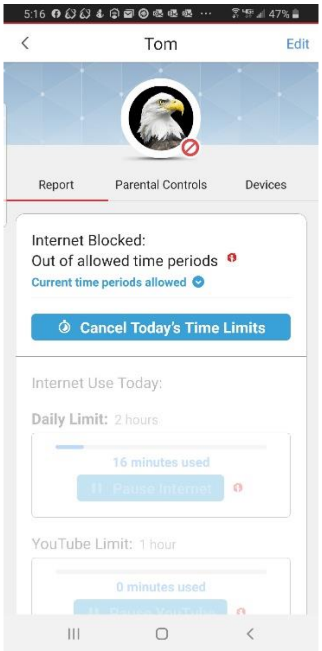
Figure 210. Parental Controls Set for Family Member

Report

The **Report** tab for a family member shows details on **Internet** and **YouTube** usage, plus information on **Filtering** rules that are enabled; e.g., blocking of inappropriate sites.

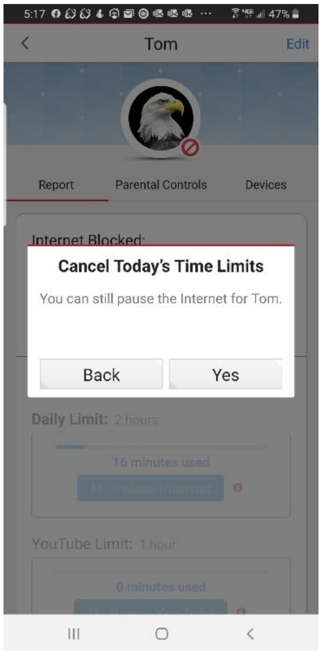
To view the Report:

1. Tap the **Report** tab in the family member's screen. The **Report** screen appears.
2. In this instance, the screen shows **Internet Blocked: Out of allowed time periods.**
3. Tap **Cancel Today's Time Limits**, if you choose to do so for the child.
4. A popup appears, asking if you truly wish to cancel the time limits. Tap **Yes**.



Internet Blocked:
Out of allowed time periods
Current time periods allowed
Internet Use Today:
Daily Limit: 2 hours
16 minutes used
YouTube Limit: 1 hour
0 minutes used

Figure 211. Cancel Today's Time Limits (1)



Cancel Today's Time Limits
You can still pause the Internet for Tom.

Figure 212. Cancel Today's Time Limits (2)

5. View **Internet Use Today** in the **Daily Limit** and **YouTube Limit** panels.
6. Tap **Pause Internet** to pause it for the family member.
7. Tap **Resume Internet** to resume it for the family member.

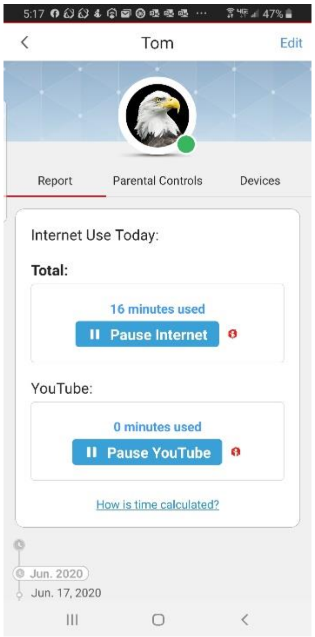


Figure 213. Pause Internet

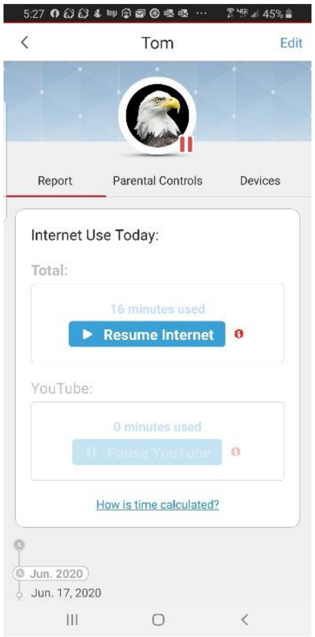


Figure 214. Resume Internet

8. Tap **Pause YouTube** to pause it for the family member.
9. Tap **Resume YouTube** to resume it for the family member.

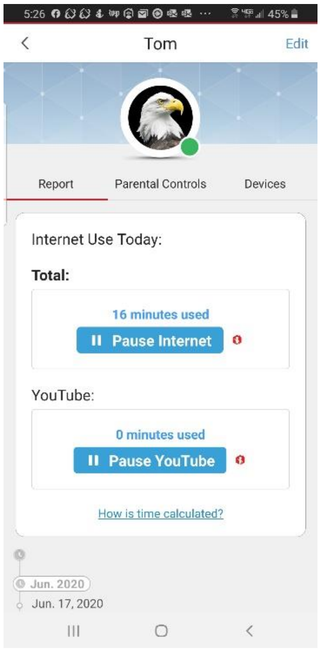


Figure 215. Pause YouTube

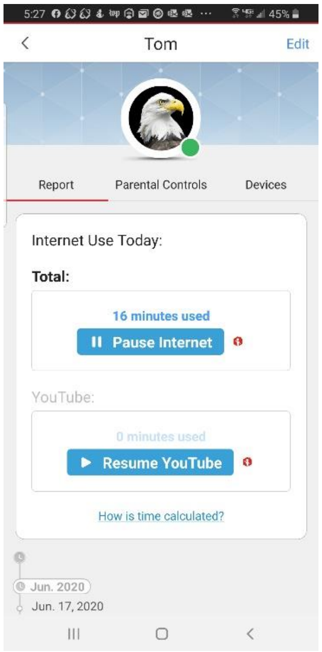
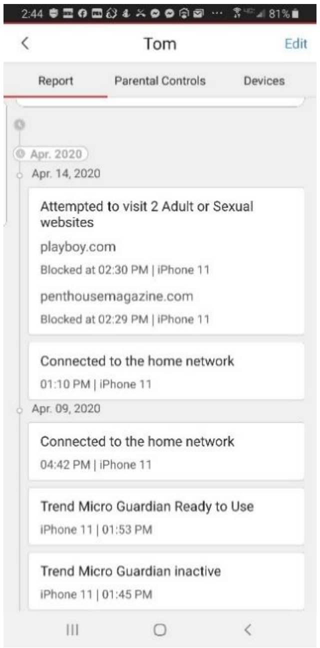


Figure 216. Resume YouTube

10. Scroll down to provide usage details for the family member, including reports on **Filters** that have been triggered.



Apr. 14, 2020

Attempted to visit 2 Adult or Sexual websites

playboy.com

Blocked at 02:30 PM | iPhone 11

penthousemagazine.com

Blocked at 02:29 PM | iPhone 11

Connected to the home network

01:10 PM | iPhone 11

Apr. 09, 2020

Connected to the home network

04:42 PM | iPhone 11

Trend Micro Guardian Ready to Use

iPhone 11 | 01:53 PM

Trend Micro Guardian inactive

iPhone 11 | 01:45 PM

Figure 217. Report Details

Devices

The **Devices** tab for the family member shows the devices under their control and allows you to add devices to their list.

To view the devices under control of the family member:

1. Tap the **Devices** tab to view the devices under control of the family member.
2. Tap **Manage Devices** to view the list **Assigned** and **Unassigned / Show All Devices**; then simply tap an **Unassigned** device to moved it into the **Managed** panel.

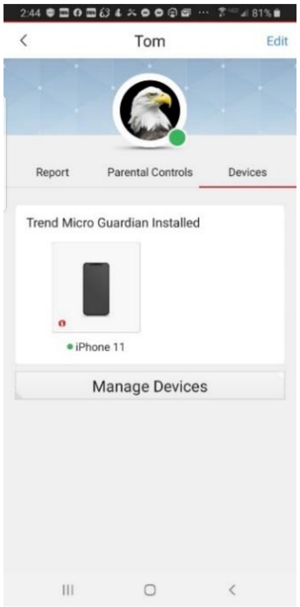


Figure 218. Devices

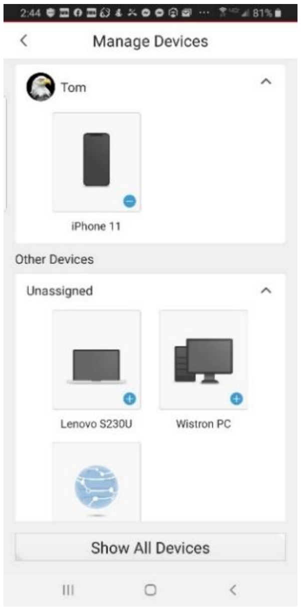
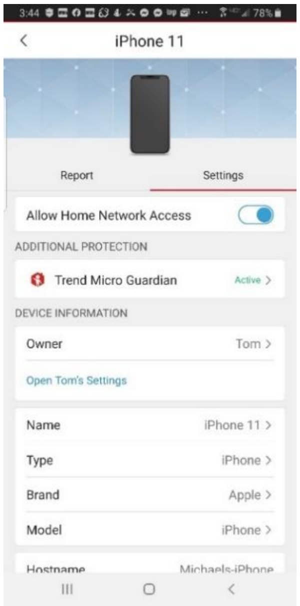


Figure 219. Manage Devices

3. In the first screen, tap the **Managed** device to obtain details about the **Settings** on the device.
4. Toggle **Allow Home Network Access Off** or **On** to disable/enable it.
5. Note the **Additional Protection** installed on this device: **Trend Micro Guardian.**
6. View **Device** Information, including the **Owner**, **Settings**, and other details about the device.



Allow Home Network Access ●

Trend Micro Guardian Active

Owner Tom

Name iPhone 11

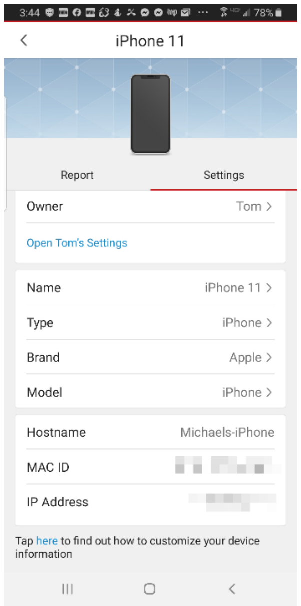
Type iPhone

Brand Apple

Model iPhone

Hostname Michaels-iPhone

Figure 220. Device Settings (1)



Owner Tom

Name iPhone 11

Type iPhone

Brand Apple

Model iPhone

Hostname Michaels-iPhone

MAC ID [redacted]

IP Address [redacted]

Tap here to find out how to customize your device information

Figure 221. Device Settings (2)

Network

The **Network** control allows you to view the total amount of data you've downloaded and uploaded over your network for the Last 7 or 30 Days. It also provides individual upload and download amounts per device.

1. Tap **Network** in the **Command Menu** to display the **Network** screen.
2. View the graph by date for the total amount downloaded and uploaded over the network for the **Last 7 Days**, as well as the amounts downloaded and uploaded per device.

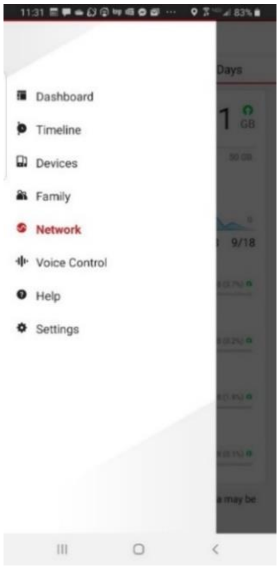
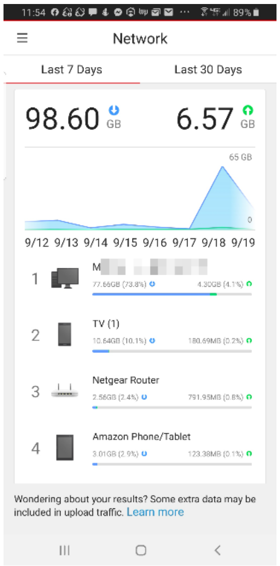


Figure 222. Network



98.60 GB 6.57 GB

1 M[redacted] 77.66GB (73.8%) 4.30GB (4.1%)

2 TV (1) 10.64GB (10.1%) 180.69MB (0.2%)

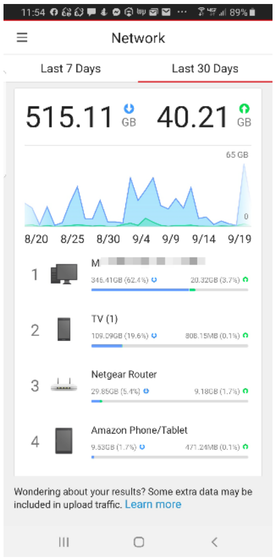
3 Netgear Router 2.56GB (2.4%) 791.95MB (0.8%)

4 Amazon Phone/Tablet 3.01GB (2.9%) 123.38MB (0.1%)

Wondering about your results? Some extra data may be included in upload traffic. Learn more

Figure 223. Network > Last 7 Days

3. Tap **Last 30 Days** to view the graph and data for the past 30 days.



1 M[redacted] 346.41GB (62.4%) 20.32GB (3.7%)

2 TV (1) 109.09GB (19.6%) 808.15MB (0.1%)

3 Netgear Router 29.85GB (5.4%) 9.18GB (1.7%)

4 Amazon Phone/Tablet 9.53GB (1.7%) 471.24MB (0.1%)

Wondering about your results? Some extra data may be included in upload traffic. Learn more

Figure 224. Network > Last 30 Days

Voice Control

Voice Control lets you give voice commands through **Google Assistant**- or the **Alexa**-enabled device or smart speakers to conduct a scan and obtain security data from Home Network Security. To use **Voice Control** you need a Google Assistant- or Alexa -enabled device and a valid Google or Amazon account. The example below uses Amazon Echo and Alexa, but the same controls are available through Google Assistant for Google smart devices.

To use Voice Control:

1. Tap **Voice Control** in the **Command Menu**. The **Voice Control** demo page appears.
2. Tap **View on Google Assistant** or **View on Amazon** to enable **Voice Control** for your **HNS Station** via your **Google Assistant or Alexa-enabled device** (e.g., an Echo).
3. In this example, we tap on **View on Amazon.**

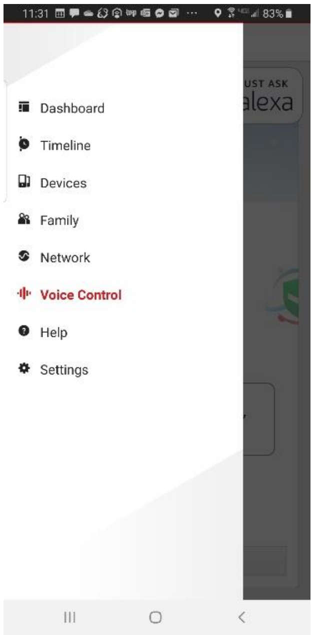
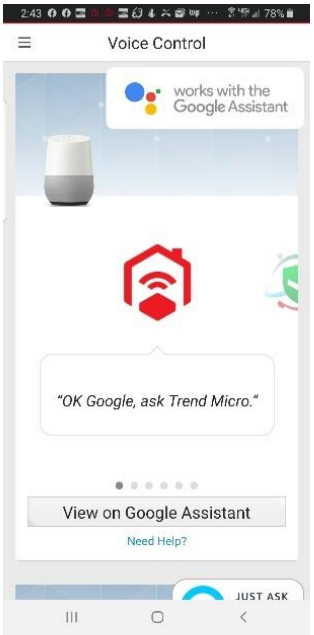
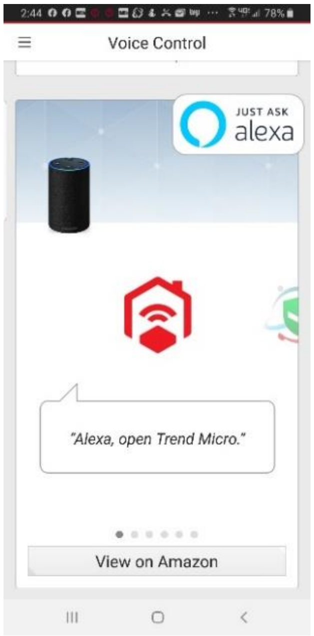


Figure 225. Voice Control



"OK Google, ask Trend Micro."

Figure 226. View on Google Assistant



"Alexa, open Trend Micro."

Figure 227. View on Amazon

4. The **HNS App** loads your browser and takes you to the **Amazon** login page to enable you to **Sign In** to your Amazon account to enable **Voice Control.**
5. Here we assume you've already created your **Amazon** account. Simply add your email address and password to the entry fields and tap **Sign In.**

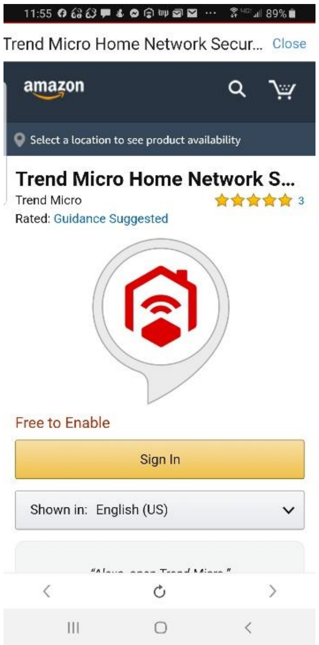
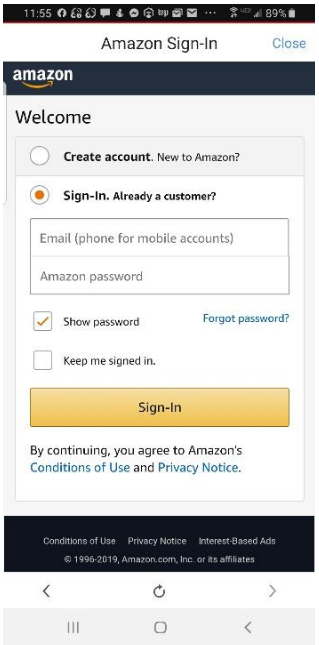

11:55
89%
Trend Micro Home Network Secur... Close
amazon
Select a location to see product availability
Trend Micro Home Network S...
Trend Micro
3
Rated: Guidance Suggested
Free to Enable
Sign In
Shown in: English (US)

Figure 228. Amazon Sign In



By continuing, you agree to Amazon's Conditions of Use and Privacy Notice.

Figure 229. Enter Email and Password

6. In the **Trend Micro Home Network Security** enabling page, tap **Enable** to enable Voice Control.
7. You're taken to the **Home Network Security Trend Micro Account** page to sign in with your **Trend Micro Account** to connect to Alexa.
8. Enter the email address and password you used to create your account and tap **Sign In.**

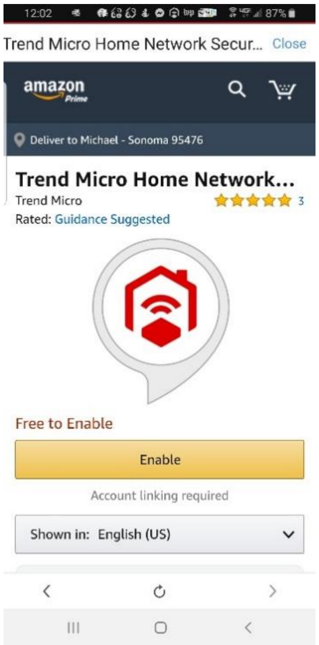
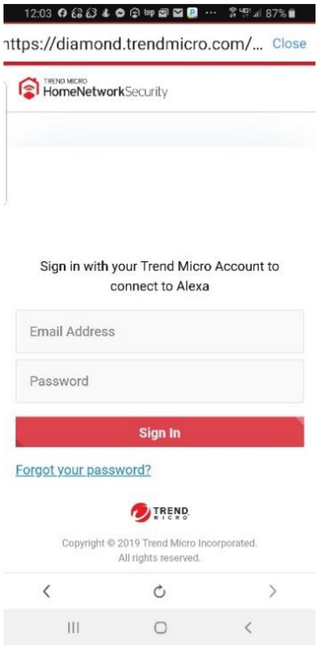

12:02
87%
Trend Micro Home Network Secur... Close
amazon Prime
Deliver to Michael - Sonoma 95476
Trend Micro Home Network...
Trend Micro
3
Rated: Guidance Suggested
Free to Enable
Enable
Account linking required
Shown in: English (US)

Figure 230. Enable Alexa Voice Commands


12:03
87%
https://diamond.trendmicro.com/... Close
TREND MICRO HomeNetworkSecurity

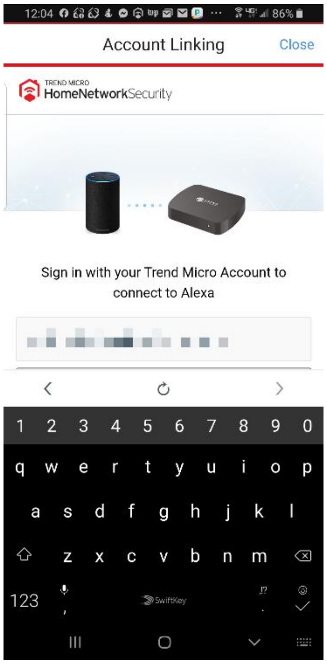
Sign in with your Trend Micro Account to connect to Alexa

Email Address
Password
Sign In
Forgot your password?
TREND MICRO

Copyright © 2019 Trend Micro Incorporated. All rights reserved.

Figure 231. Sign In to Trend Micro Account

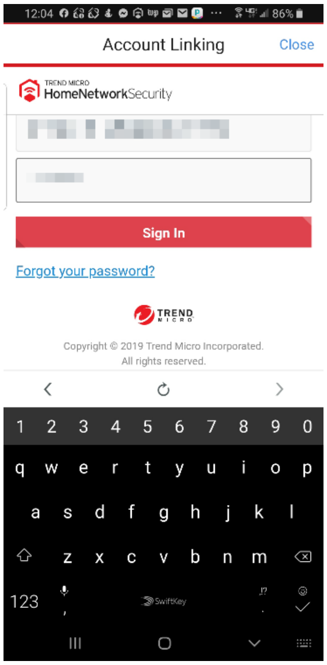
9. As you proceed through the **Account Linking** process, you're notified as you go along.



Sign in with your Trend Micro Account to connect to Alexa

[redacted]

Figure 232. Account Linking (1)



[redacted]

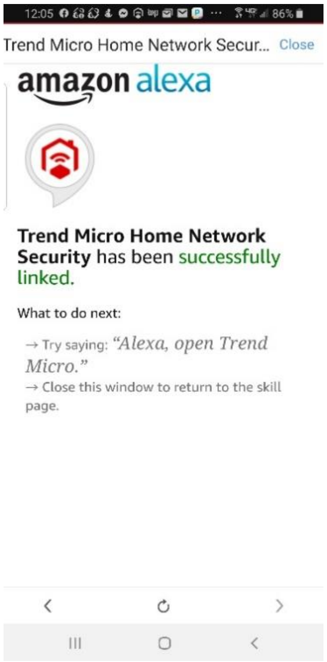
[redacted]

Copyright © 2019 Trend Micro Incorporated.
All rights reserved.

Figure 233. Account Linking (2)

10. Once completed, you're informed that **Trend Micro Home Network Security** has been successfully linked in your **Amazon Alexa** skill page.
11. Tap **Close** to close the linking page.
12. You now have five **Voice Control Commands** ("intents") you may now use via Alexa to control your **HNS Station.**
13. The following launch request opens a skill *without* an intent:

    "Alexa, open Trend Micro."

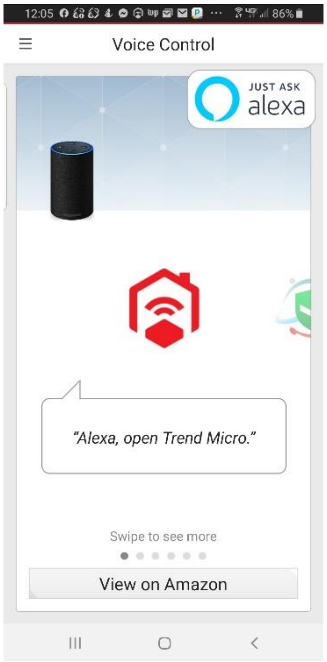


Trend Micro Home Network Security has been successfully linked.

What to do next:

→ Try saying: *"Alexa, open Trend Micro."*
→ Close this window to return to the skill page.

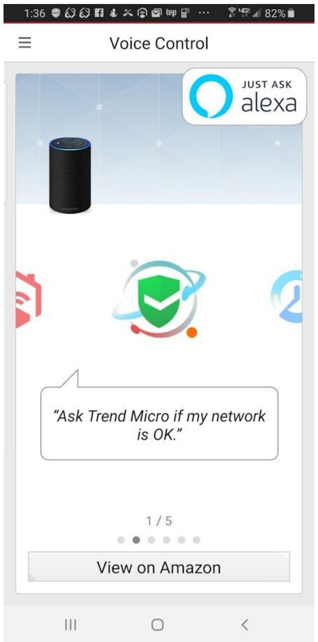
Figure 234. HNS Linked



"Alexa, open Trend Micro."

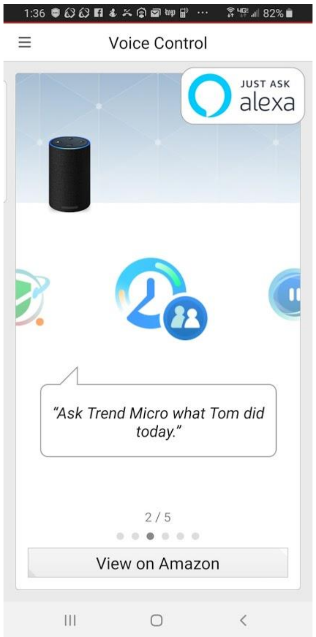
Figure 235. Open Command

14. The following commands open a skill *with* an intent.
15. **“Alexa, ask Trend Micro if my network is OK.”**
16. **“Alex, ask Trend Micro what Tom (or other name) did today.”**



“Ask Trend Micro if my network is OK.”

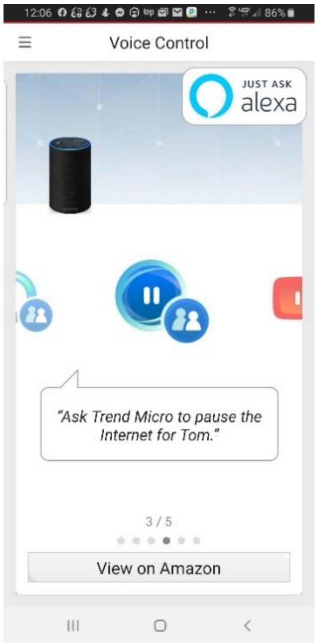
Figure 236. Network OK?



“Ask Trend Micro what Tom did today.”

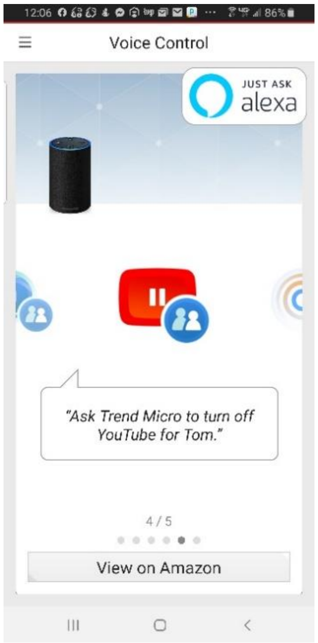
Figure 237. What did Tom do Today?

17. **“Alexa, ask Trend Micro to pause the Internet for Tom (or other name).”**
18. **“Alexa, ask Trend Micro to turn off YouTube for Tom (or other name).”**



“Ask Trend Micro to pause the Internet for Tom.”

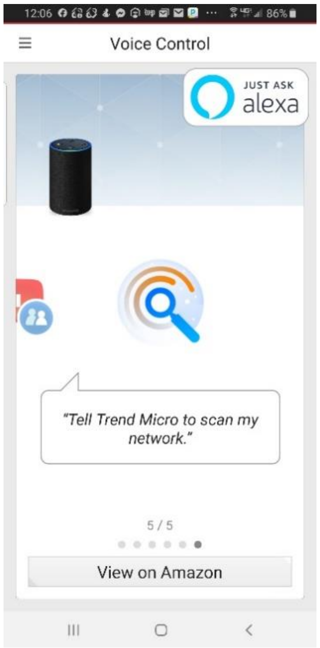
Figure 238. Pause Internet for Tom



“Ask Trend Micro to turn off YouTube for Tom.”

Figure 239. Turn Off YouTube for Tom

19. **“Alexa, tell Trend Micro to scan my network.”**
20. At any time, if you wish to disable **Voice Commands** via Alexa, simply log into your Amazon account by tapping **View on Amazon**, log in, then tap **Disable Skill.**
21. **Voice Commands** will be disabled on your **HNS Station.**



"Tell Trend Micro to scan my network."

Figure 240. Scan Network

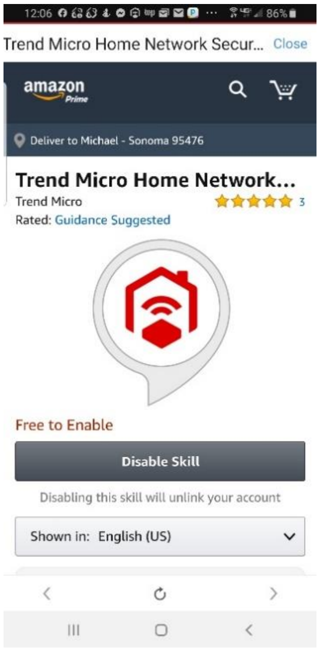

12:06
86%
Trend Micro Home Network Secur...
Close
amazon
Prime
Deliver to Michael - Sonoma 95476
Trend Micro Home Network...
Trend Micro
3
Rated: Guidance Suggested
Free to Enable
Disable Skill
Disabling this skill will unlink your account
Shown in: English (US)

Figure 241. Disable Skill

Help

Home Network Security provides various kinds of **Help**, to facilitate the smooth operation of the **HNS Station.**

To obtain Help:

1. Tap **Help** in the **Command Menu.** The **Help** screen appears.
2. Here you'll find a phone number to **Contact Support.**
3. You can also tap **Request a call from Support**; enter your phone number in the form provided.
4. If need be, scroll down the screen to reveal more items.

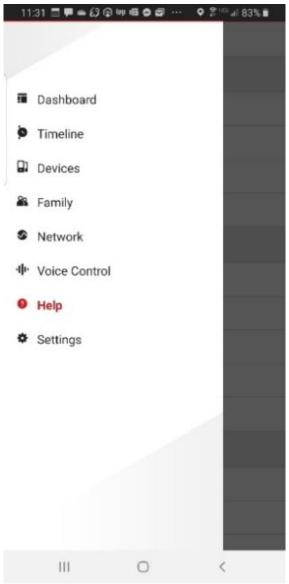
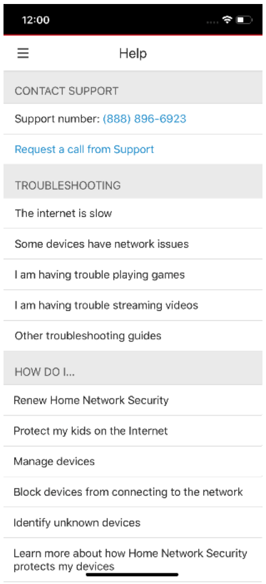


Figure 242. Help Menu



CONTACT SUPPORT

Support number: (888) 896-6923

Request a call from Support

TROUBLESHOOTING

The internet is slow

Some devices have network issues

I am having trouble playing games

I am having trouble streaming videos

Other troubleshooting guides

HOW DO I...

Renew Home Network Security

Protect my kids on the Internet

Manage devices

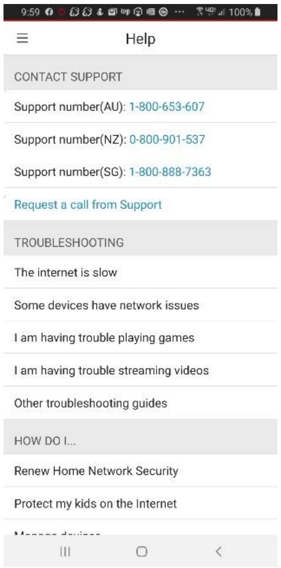
Block devices from connecting to the network

Identify unknown devices

Learn more about how Home Network Security protects my devices

Figure 243. Help (US)

5. Tap the items in the **Troubleshooting** section, or the **How Do I** section to take you to individual **Help** pages.



CONTACT SUPPORT

Support number(AU): 1-800-653-607

Support number(NZ): 0-800-901-537

Support number(SG): 1-800-888-7363

Request a call from Support

TROUBLESHOOTING

The internet is slow

Some devices have network issues

I am having trouble playing games

I am having trouble streaming videos

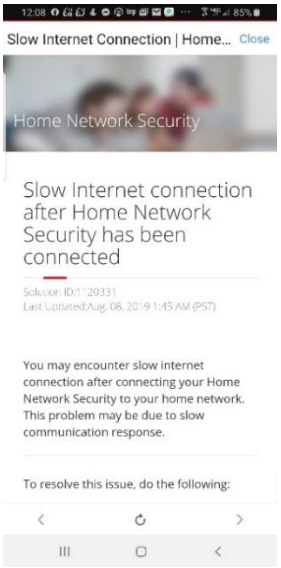
Other troubleshooting guides

HOW DO I...

Renew Home Network Security

Protect my kids on the Internet

Figure 244. Help (Other Regions)



Slow Internet connection after Home Network Security has been connected

Solution ID:1120331
Last Updated:Aug. 08, 2019 1:45 AM (PST)

You may encounter slow internet connection after connecting your Home Network Security to your home network. This problem may be due to slow communication response.

To resolve this issue, do the following:

Figure 245. Item Tapped

Settings

The **Settings** in the **HNS App** help you set up and configure **Home Network Security** to fit your needs.

To configure Settings:

1. Tap **Settings** in the **Command Menu** to open the **Settings** screen.
2. In the **NETWORK AND SECURITY** section, tap **Threat Blocking** to configure the settings that block threats.

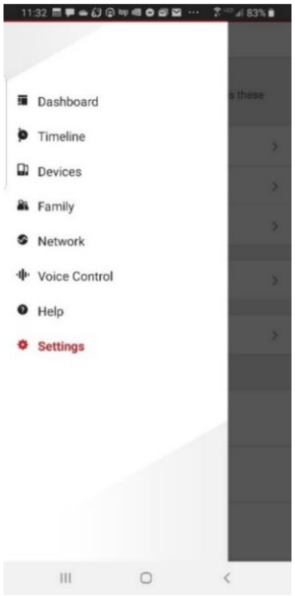
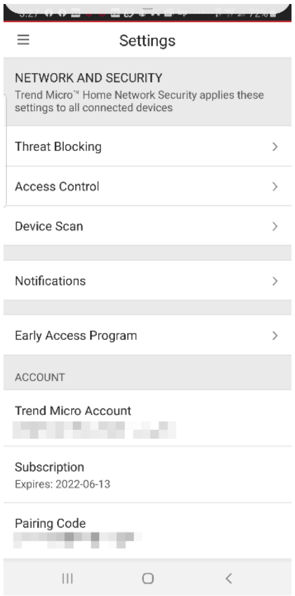


Figure 246. Settings Menu



Trend Micro™ Home Network Security applies these settings to all connected devices

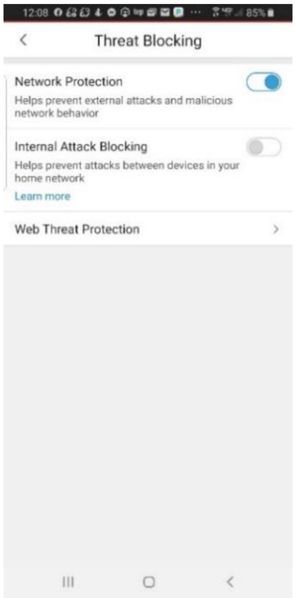
[redacted]

Expires: 2022-06-13

[redacted]

Figure 247. Settings

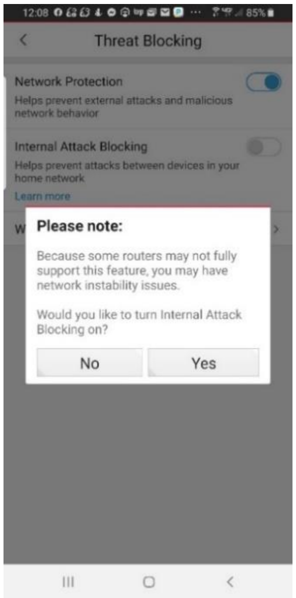
3. Toggle On/Off **Network Protection**. When this protection is **On**, HNS helps prevent external attacks and malicious network behavior using IPS protection.
4. To help prevent attacks between devices in your home network, tap **Internal Attack Blocking.**
5. A popup appears because some routers may not support this feature and you may have network instability issues.



Helps prevent external attacks and malicious network behavior

Helps prevent attacks between devices in your home network

Figure 248. Threat Blocking



Because some routers may not fully support this feature, you may have network instability issues.

Would you like to turn Internal Attack Blocking on?

Figure 249. Internal Attack Blocking Popup

6. Tap **Web Threat Protection** on the **Threat Blocking** screen to open the settings.
7. Toggle **On/Off Dangerous Websites Blocked** and **Dangerous Files Blocked.**
8. Tap **Approved List** to add websites to the list.
9. Tap **Add a new website** to add a new website by entering the URL in the entry field provided.

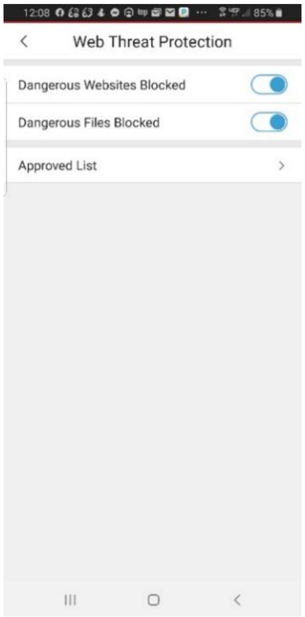


Figure 250. Web Threat Protection

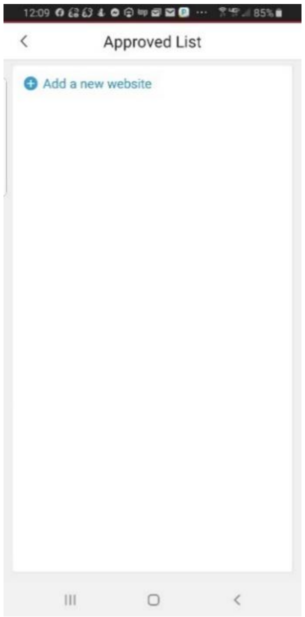


Figure 251. Add a new website

10. Back in the main **Settings** page, tap **Access Control** to access the settings.
11. Tap **Remote Access Protection** to limit remote access to your devices, or toggle **New Device Approval On**/Off to require permission when a new device joins the network.
12. In **Remote Access Protection**, toggle **Block Remote Access On/Off** to control the function.
13. Tap **Approved List** to add an approved remote access program to the list.

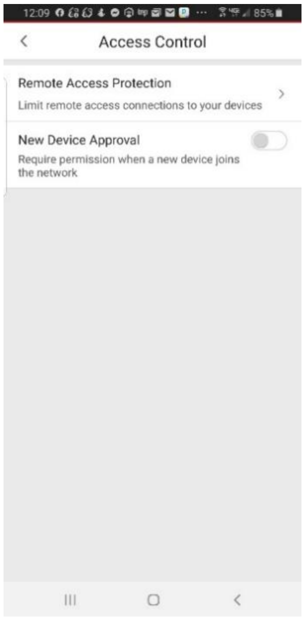

12:09
Access Control
Remote Access Protection
Limit remote access connections to your devices
New Device Approval
Require permission when a new device joins the network

Figure 252. Access Control

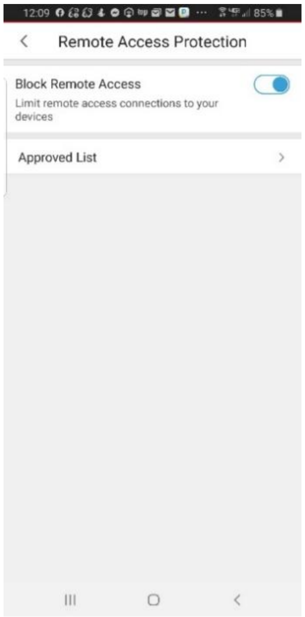
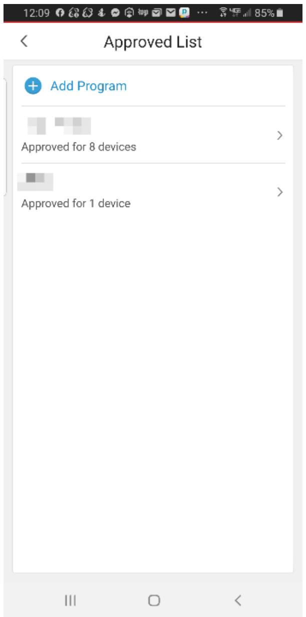


Figure 253. Remote Access Protection

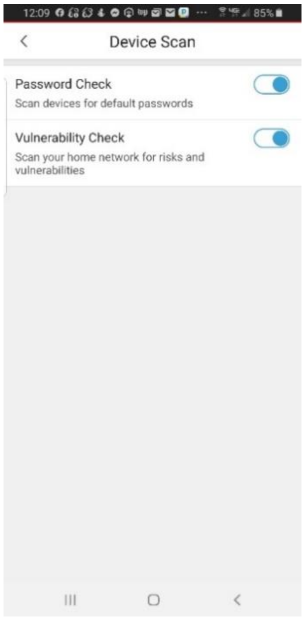
14. Tap **Add Program** to add programs or tap existing apps to remove them from the list.
15. Back in the main **Settings** screen, tap **Device Scan** to access the **Device Scan** settings.
16. Toggle **Password Check** and **Vulnerability Check On/Off** to control the settings.



Approved for 8 devices

Approved for 1 device

Figure 254. Approved List



Password Check — On
Scan devices for default passwords

Vulnerability Check — On
Scan your home network for risks and vulnerabilities

Figure 255. Device Scan

17. Back in the main **Settings** screen, tap **Notifications** to access the settings for notifications.

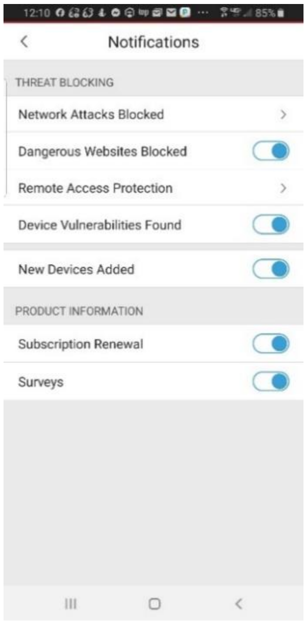
    NOTE: **Notifications** show up in the drop-down menu of your device.

18. Tap **Network Attacks Blocked** to choose the notifications options:

    >No Notifications

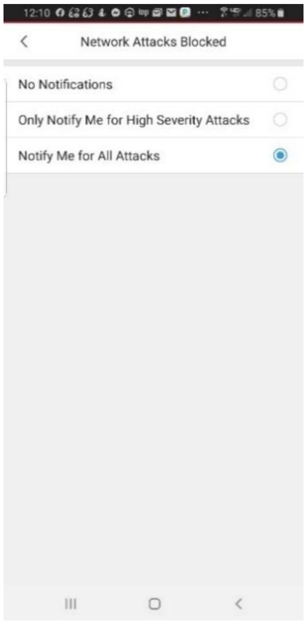
    >Only Notify Me for High Severity Attacks

    >Notify Me for All Attacks



Dangerous Websites Blocked — On
Device Vulnerabilities Found — On
New Devices Added — On
Subscription Renewal — On
Surveys — On

Figure 256. Notifications



No Notifications ○
Only Notify Me for High Severity Attacks ○
Notify Me for All Attacks ●

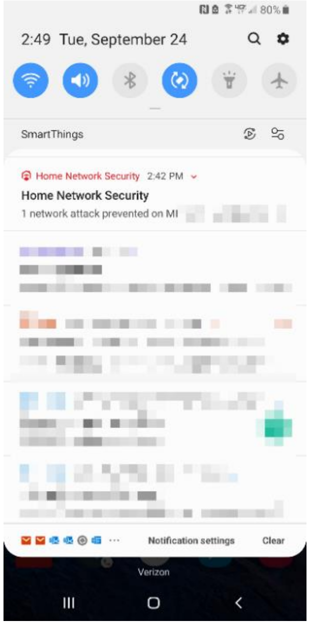
Figure 257. Network Attacks Blocked

19. Toggle the various other options **On/Off** to **Enable/Disable** the respective setting.
20. Continuing in the **Notifications** screen, tap **Remote Access Protection** to access the various options:

    >No notifications

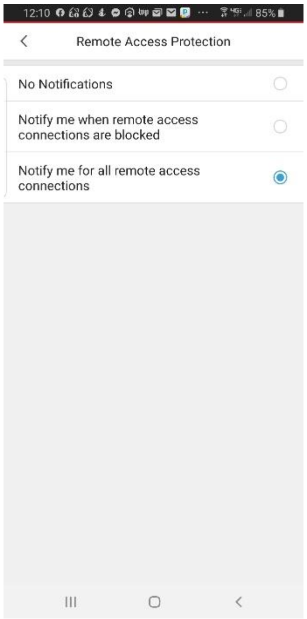
    >Notify me when remote access connections are blocked

    >Notify me for all remote access connections



Home Network Security 2:42 PM
Home Network Security
1 network attack prevented on MI

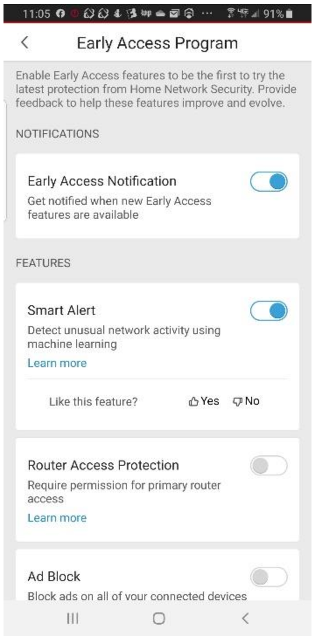
Figure 258. Network Attack Notification



○ No Notifications
○ Notify me when remote access connections are blocked
● Notify me for all remote access connections

Figure 259. Remote Access Protection

21. Back in the main **Settings** screen, tap **Early Access Program** to access the settings.
22. Enable the **Early Access** features to be the first to try the latest protections and give feedback
23. Toggle the **Early Access Notification On/Off** to Enable/Disable the notification.
24. Toggle on **Smart Alert, Router Access Protection**, **Ad Block**, and **Cyberattack Shield** to test and give feedback on these features.



Enable Early Access features to be the first to try the latest protection from Home Network Security. Provide feedback to help these features improve and evolve.

NOTIFICATIONS

Early Access Notification (On)
Get notified when new Early Access features are available

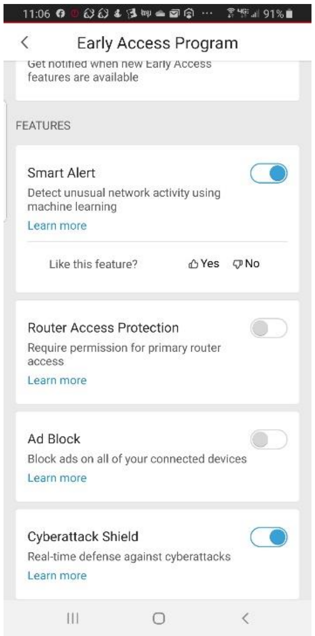
FEATURES

Smart Alert (On)
Detect unusual network activity using machine learning

Router Access Protection (Off)
Require permission for primary router access

Ad Block (Off)
Block ads on all of your connected devices

Figure 260. Early Access Program (1)



Get notified when new Early Access features are available

FEATURES

Smart Alert (On)
Detect unusual network activity using machine learning

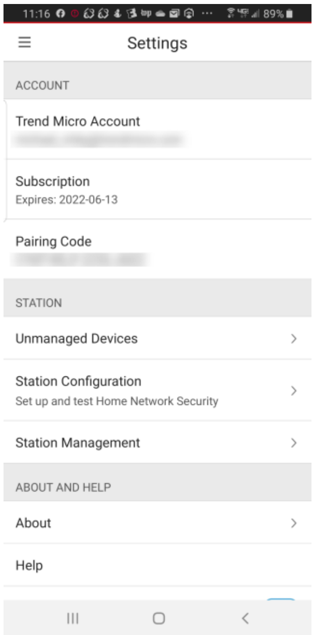
Router Access Protection (Off)
Require permission for primary router access

Ad Block (Off)
Block ads on all of your connected devices

Cyberattack Shield (On)
Real-time defense against cyberattacks

Figure 261. Early Access Program (2)

25. Back in the main **Settings** screen under **ACCOUNT**, view your **Trend Micro Account**, **Subscription Expiration Date**, and 16-character **Pairing Code.**
26. Tap **Unmanaged Devices** to add such devices or to remove them from the **Managed Devices** list.



Trend Micro Account
[redacted]

Subscription
Expires: 2022-06-13

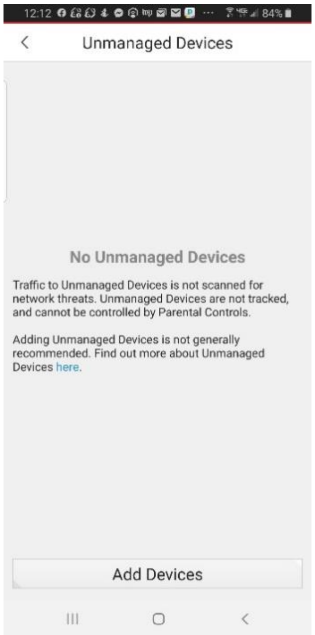
Pairing Code
[redacted]

Unmanaged Devices

Station Configuration
Set up and test Home Network Security

Station Management

Figure 262. Pairing Code



No Unmanaged Devices

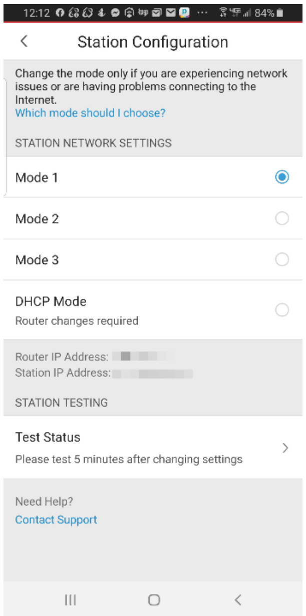
Traffic to Unmanaged Devices is not scanned for network threats. Unmanaged Devices are not tracked, and cannot be controlled by Parental Controls.

Adding Unmanaged Devices is not generally recommended. Find out more about Unmanaged Devices here.

Figure 263. Unmanaged Devices

27. Tap **Station Configuration** to change the **Mode** to optimize the connection to your router, or to enable **DHCP Mode**.

    (See **Network Attach Options** in the following section).
28. Once you've made your change, tap **Test Status** to ensure the change has taken effect and the HNS Station is functioning well.



Change the mode only if you are experiencing network issues or are having problems connecting to the Internet.
Which mode should I choose?

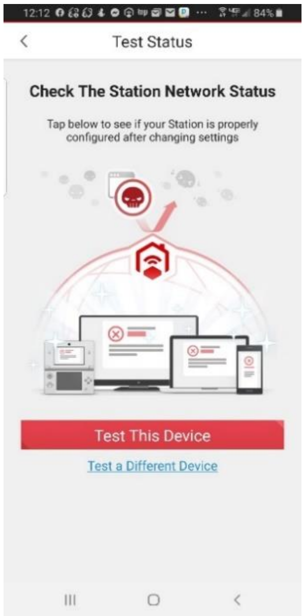
Mode 1 ●
Mode 2 ○
Mode 3 ○
DHCP Mode ○
Router changes required

Router IP Address: [redacted]
Station IP Address: [redacted]

Test Status
Please test 5 minutes after changing settings

Need Help?

Figure 264. Station Configuration > Mode Settings

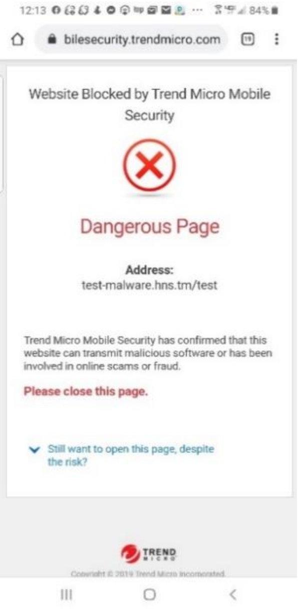


Check The Station Network Status

Tap below to see if your Station is properly configured after changing settings

Figure 265. Check Station Network Status

29. If it's functioning correctly, you'll see a **Dangerous Page** alert showing the test website has been blocked.
30. In the main **Settings** screen, tap **Station Management** to access the settings.
31. If you wish to **End Station Management**, tap the setting.


12:13 84%
bilesecurity.trendmicro.com
TREND MICRO
Copyright © 2019 Trend Micro Incorporated.

Website Blocked by Trend Micro Mobile Security

Dangerous Page

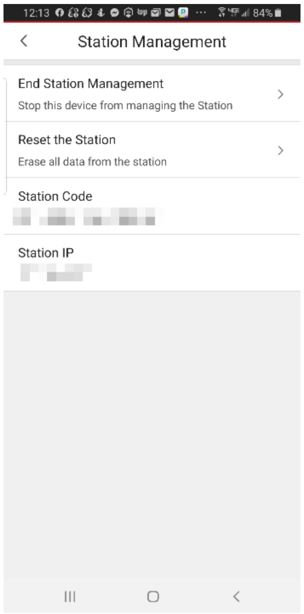
Address: test-malware.hns.tm/test

Trend Micro Mobile Security has confirmed that this website can transmit malicious software or has been involved in online scams or fraud.

Please close this page.

Still want to open this page, despite the risk?

Figure 266. Dangerous Page

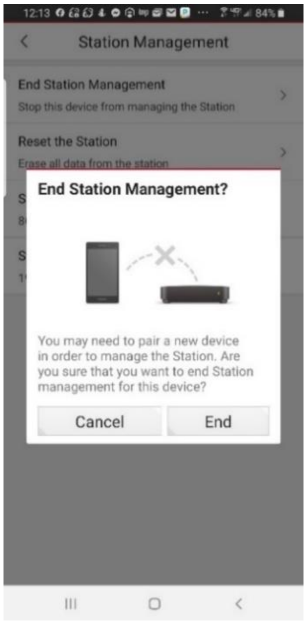


[redacted]

[redacted]

Figure 267. Station Management

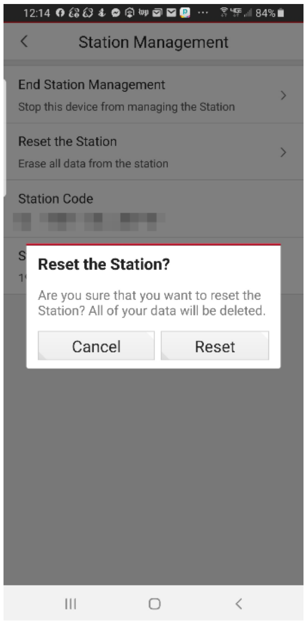
32. A popup appears, asking if you really wish to **End Station Management?**
33. Tap **Cancel** to abort the process, or **End** to **End Station Management.**
34. To **Reset the Station**, tap the setting.
35. A popup appears, asking if you sure you wish to **Reset the Station?** All of your data will be deleted.
36. Tap **Cancel** to abort the process or **Reset** to complete it.


12:13 84%
Station Management
End Station Management
Stop this device from managing the Station
Reset the Station
Erase all data from the station

End Station Management?

You may need to pair a new device in order to manage the Station. Are you sure that you want to end Station management for this device?

Figure 268. End Station Management?



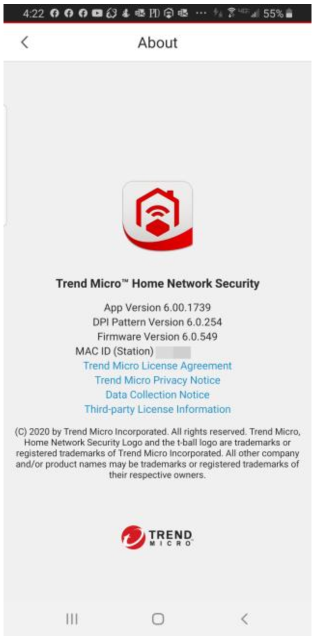
Reset the Station?

Are you sure that you want to reset the Station? All of your data will be deleted.

Figure 269. Reset the Station?

37. Back in the main **Settings** screen, tap **About** to obtain information about Trend Micro Home Network Security, including **App Version, DPI Pattern Version, Firmware Version,** and the **Mac ID** for the **Station**. The screen also provides the various agreements policies, and notices.

38. Back in the main **Settings** screen, tap **Help** to obtain help using **Home Network Security.** You're taken to the **Help** pages in eSupport.

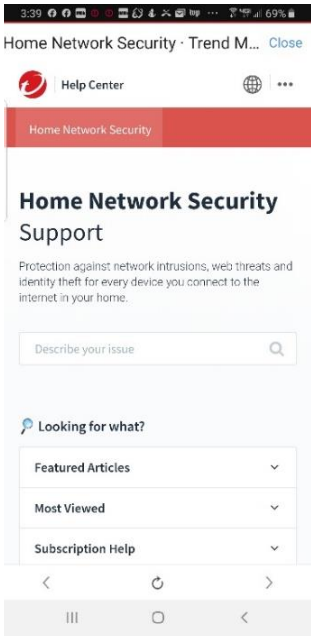


Trend Micro™ Home Network Security

App Version 6.00.1739
DPI Pattern Version 6.0.254
Firmware Version 6.0.549
MAC ID (Station) [redacted]
Trend Micro License Agreement
Trend Micro Privacy Notice
Data Collection Notice
Third-party License Information

(C) 2020 by Trend Micro Incorporated. All rights reserved. Trend Micro, Home Network Security Logo and the t-ball logo are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their respective owners.

Figure 270. About



Home Network Security Support

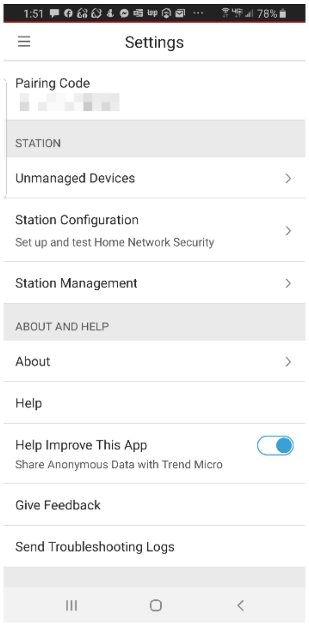
Protection against network intrusions, web threats and identity theft for every device you connect to the internet in your home.

Figure 271. Home Network Security Support

39. Back in the main **Settings** page, toggle **Help Improve This App On** or **Off**, to share/not share anonymous data with Trend Micro.

40. Tap **Give Feedback** to send feedback to Trend Micro about Home Network Security.

41. During a troubleshooting session with a Trend Micro Support Technician, you may be asked to **Send Troubleshooting Logs** to help solve your problem. Simply tap this function when asked.

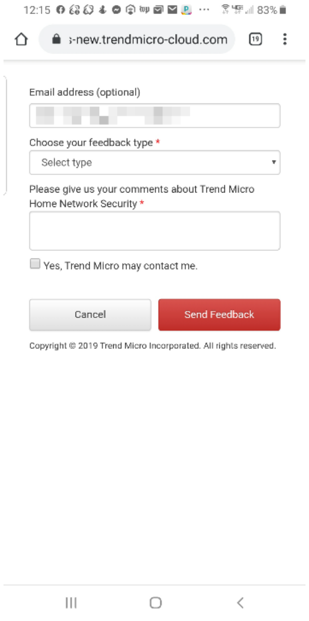


Pairing Code [redacted]

STATION
Unmanaged Devices
Station Configuration
Set up and test Home Network Security
Station Management

ABOUT AND HELP
About
Help
Help Improve This App
Share Anonymous Data with Trend Micro
Give Feedback
Send Troubleshooting Logs

Figure 272. Help Improve This App, Give Feedback, Send Troubleshooting Logs



Email address (optional)
[redacted]
Choose your feedback type *
Select type
Please give us your comments about Trend Micro Home Network Security *
☐ Yes, Trend Micro may contact me.

Copyright © 2019 Trend Micro Incorporated. All rights reserved.

Figure 273. Give Feedback

Section 3: Core Technologies

Trend Micro Home Network Security provides an array of technologies that enable the key functions of the solution. These include:

- A Deep Packet Inspection (DPI) engine / Intrusion Prevention System (IPS)
- Automatic Device Recognition
- Automatic Vulnerability Scan
- Web Threat Protection
- Anomaly Detection
- Network Attach Options

Deep Packet Inspection (DPI) / Intrusion Prevention System (IPS)

HNS's Intrusion Prevention System (IPS) security technology covers a broad spectrum of threats and vulnerabilities that home networks face today. Behind HNS's IPS is the Deep Packet Inspection (DPI) engine, an advanced technology for analyzing and managing network traffic.

DPI goes beyond packet filtering, which only analyzes packet headers, by inspecting the data and payload of the traffic. This scan returns multiple results for security and management applications in a performant, single-pass process. This approach allows HNS to protect you and your devices against sophisticated network intrusion and device compromise attempts while minimizing impact on network throughput.

The threat coverage of IPS far exceeds the protection provided by DNS-based security implementations in a number of important areas, including device compromise through inbound attacks that use techniques like brute force logins and exploit system vulnerabilities.

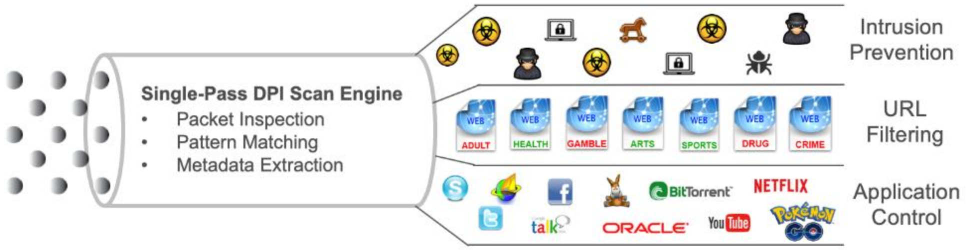


Figure 274. HNS Single-Pass DPI Scan Engine

Network Attacks

Where HNS's IPS protection really shines is detecting and blocking network attacks. Because it scans traffic coming in and going out of a network, HNS's IPS is able to protect consumer home networks against inbound device compromise attempts, remote device control (botnets) and even cryptocurrency mining. Recent and well-known examples of these types of threats include WannaCry, Heartbleed and Shellshock. DNS-based solutions aren't able to see or analyze these attack attempts, let alone block them from reaching their targeted victims.

Web Threats

By forwarding URL requests to Trend Micro's Smart Protection Network (SPN), HNS's IPS is able to provide granular and accurate web-threat protection to consumers. DNS-based solutions are limited when it comes to URL filtering because the precision of their reputation systems only cover the domain of a requested URL. In addition, any requests which directly use an IP address are not covered by a DNS-based solution. Trend Micro's own data shows that two-thirds of all web threats are matched at the directory or URL level, not the domain level, indicating that a majority of web threats could be missed by DNS-based solutions.

Trend Micro's SPN also dynamically scans potentially executable files, including .EXE and .PDF files, *in the cloud and in real-time* to ensure that those files are not malware.

Table 5. Threat coverage of DPI-based IPS vs DNS-based security

Threat Category	HNS (DPI-based IPS)	DNS-based Solution
Web Threats		
DNS Reputation	Yes	Yes
URL Reputation	Yes	Partial (domain-level only)
Dynamic Cloud-based File Scan	Yes	No
Inbound Device Compromise		
Brute Force Login	Yes	No
Default Credential Exploitation	Yes	No
Vulnerability Exploitation	Yes	No
Remote Device Control		
Botnet Participation via DoS / DDoS	Yes	No
Others		
Cryptocurrency Mining	Yes	No

Device and Application Management

Additional benefits of DPI include the identification and management of devices and applications. Metadata picked up during traffic inspection allows Trend Micro to show consumers the devices that are connected to their network as well as the applications that are in use. Beyond visibility, DPI allows for the management of those devices and applications, including allowing or blocking devices and applications and setting time limits.

Trend Micro Guardian, which integrates with HNS's parental control rules, utilizes Mobile Device Management technology to enforce those rules on any network, Wi-Fi or mobile.

Automatic Device Recognition

Automatic Device Recognition takes the output of an active network scan, which analyzes the response metadata to assess a device's brand, model and category. Metadata from scanned network traffic offers additional input used in recognition.

In cases where the recognition is incomplete or inaccurate, users can modify the recognition result generated by HNS. That learning is fed back into the system to improve recognition going forward.

Automatic Vulnerability Scan

HNS's Automatic Vulnerability Scan probes for default/weak password settings on devices that have administrative consoles like routers, IP cameras and network attached storage (NAS) units.

After version 2.0 has been released (Fall 2019), high severity vulnerabilities like Heartbleed and Poodle will be tested for in connected devices. If found, users will be provided with a notice giving advice on how to mitigate the vulnerability (like updating their device's firmware).

Web Threat Protection (SPN)

Trend Micro maintains one of the world's largest web reputation databases—a key component of the Trend Micro Smart Protection Network (SPN), which also includes world-class file and email reputation databases, as well as other advanced technologies including Trend Micro™ XGen machine learning, the artificial intelligence powering Trend Micro Home Network Security.

With its Web Threat Protection (WTP) technology, websites are scored on age, location changes, and suspicious behavior. Through a two-tier system, Trend Micro examines both single and multi-component testing of web sites, sandboxing and testing of new components on existing sites, and monitoring of cyber-criminal activity. Real-time page analysis, using script analyzers and browser exploit prevention technology, identifies new malicious URLs at the time of access. The result is industry-leading blocking of both existing and evolving web threats to Trend Micro's customers.

In short, Trend Micro Home Network Security's Web Threat Protection (WTP) feature taps into the SPN's web reputation database as soon as it's installed, ensuring the safety of your home users whenever they access the web on any device that's part of your network. If a user clicks a bad link in a browser, an email or instant message, or on a social networking site, they're instantly notified and blocked from going to the malicious website—and the home network administrator is notified of the blocking action, by user and device, as part of HNS's normal reporting mechanism.

Anomaly Detection

Anomaly Detection has been introduced into HNS as a forward-looking intelligent monitoring capability. HNS's Smart Alert is an Early Access feature that uses machine learning to build patterns from smart devices' network behavior so that it can identify anomalies, particularly behavior that indicates device compromise or privacy violations.

When an anomaly is detected, users are alerted with more details and potential further actions they can take to confirm their device's health.

Network Attach Options

HNS acts as the gateway when attached to the network router in the following ways:

- **Automatically**. Setup occurs without user configuration, by utilizing ARP Spoofing. This technique is important for helping get even the least tech-savvy customer up and running and their network and devices secured. No decision-making or networking knowledge is required on the part of the user when using this mode.

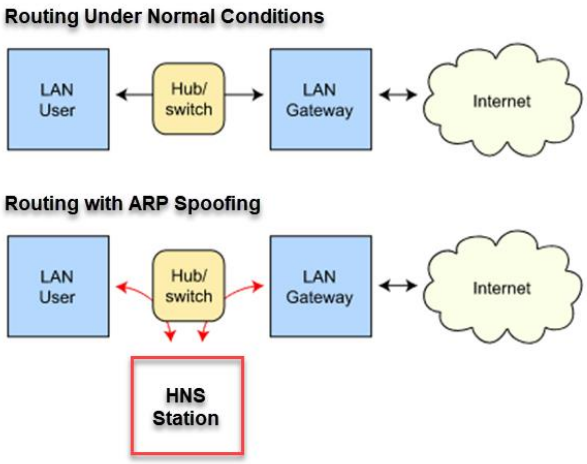


Figure 275. HNS ARP Spoofing for MITM Security

- **Mode 1, Mode 2, Mode 3.** Mode 1 is the default setting. Mode 2 or Mode 3, which are also ARP Spoofing modes, may be triggered automatically or can be used manually (just tap the option) if you are experiencing network issues or are having problems connecting to the Internet. If you change the mode, run a **Test Status** check 5 minutes after changing the settings.

- **DHCP Mode.** Using DHCP Mode you can configure Home Network Security as a DHCP Server. Enabling DHCP Mode requires you to first disable the router's DHCP server. With a small number of routers, this configuration is required so HNS can secure the network and devices. Also, some more technical customers who are willing and able may feel more comfortable with this setup and make the changes themselves.

HNS will attempt to determine the correct method during the setup process based on the router it is connected to. Most routers support the automatic method, though a very small number do require manual setup. An even smaller number are not compatible with HNS.

To ensure the optimal experience with Home Network Security, make sure you are using a compatible router. Click here for a List of Compatible Routers.

About Trend Micro

Trend Micro Incorporated, a global leader in cyber security solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables users to enjoy their digital lives safely.

For more information, visit Trend Micro Security for Home or Home Network Security.