Trend Micro™
Home Network Security 2020
Product Guide

V5.0
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 Incorporated reserves the right to make changes to this document and to the service described herein without notice. Before implementing the service, please review the readme file and the latest version of the applicable user documentation.

Copyright © 2020 Trend Micro Inc., Consumer Technical Product Marketing. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and Trend Micro Security are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners. Android is a trademark of Google, Inc. Mac is a trademark of Apple, Inc.


DOCUMENT PROFILE:

Product: Trend Micro™ Home Network Security 2020 - v5.01.1664
Document Title: Trend Micro™ Home Network Security 2020 - Product Guide
Document Release Date: July 9, 2020
Team: Consumer Technical Product Marketing
Table of Contents

Executive Summary ............................................................................................................. 5
Trend Micro Home Network Security Highlights .................................................................6

Section 1: Detailed Product Specifications ........................................................................ 8
Key Features ..........................................................................................................................8
Station Specifications ..........................................................................................................9
Starting with the HNS App ..................................................................................................10
Router Compatibility List ...................................................................................................10
Pairing the HNS App and Station ......................................................................................10
Minimum Requirements .....................................................................................................11
Target Audience ................................................................................................................11
Global Availability .............................................................................................................11
Contacting Trend Micro ....................................................................................................12
United States ......................................................................................................................12
Japan ..................................................................................................................................12
Australia and New Zealand ...............................................................................................12
Singapore ............................................................................................................................12
Free Phone, Email and Chat support ................................................................................12
Premium Support Services ...............................................................................................13

Section 2: The Home Network Security Application and Station ....................................14
Install the HNS App and Conduct a Network Scan .............................................................14
To Learn More or Purchase a Home Network Security Station .........................................18
Set Up the Station, Pair it with the HNS App, and Do a Network Scan ...............................19
Dashboard ..........................................................................................................................25
Check Devices ....................................................................................................................25
Using the Dashboard ...........................................................................................................28
Timeline ..............................................................................................................................33
Devices ................................................................................................................................35
Family: Members, Devices, and Parental Controls ............................................................36
Add a Family Member and the Devices They Control .......................................................37
Install Trend Micro Guardian and Set Up Uninstall Protection ........................................ 39
Install Guardian on an iOS Device ................................................................................. 39
Set Up Guardian Uninstall Protection on an iOS Device ............................................... 48
Install Guardian on an Android Device ......................................................................... 55
Set Up Guardian Uninstall Protection on an Android Device ....................................... 62
Filtering ......................................................................................................................... 66
Inappropriate App Used ................................................................................................. 70
Time Limits .................................................................................................................... 71
Connection Alert ........................................................................................................... 74
Report ............................................................................................................................. 76
Devices ............................................................................................................................ 79
Network ........................................................................................................................... 80
Voice Control .................................................................................................................. 81
Help .................................................................................................................................. 87
Settings ........................................................................................................................... 88

Section 3: Core Technologies ......................................................................................... 95
Deep Packet Inspection (DPI) / Intrusion Prevention System (IPS) ............................... 95
Network Attacks ............................................................................................................. 96
Web Threats .................................................................................................................... 96
Device and Application Management ............................................................................ 97
Automatic Device Recognition ..................................................................................... 97
Automatic Vulnerability Scan ...................................................................................... 97
Web Threat Protection (SPN) ....................................................................................... 97
Anomaly Detection ........................................................................................................ 98
Network Attach Options ............................................................................................... 98

About Trend Micro ........................................................................................................ 100
Executive Summary

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.

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.

- **New! 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 for kids, on any Wi-Fi or mobile network. **New! Includes time limits in 5.0.**

- **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.

- **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.

- **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.

- **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.

- **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

<table>
<thead>
<tr>
<th>TREND MICRO HOME NETWORK SECURITY</th>
<th>With Station</th>
<th>App Only</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SECURITY</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>THREAT BLOCKING</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intrusion Prevention (IPS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet (WAN) Traffic*</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Local (LAN) Traffic*</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Web Threat Protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Reputation Filtering</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Cloud File Scan</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>ACCESS CONTROL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Device Approval</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Remote Access Protection</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>DEVICE SCAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password Check</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Vulnerability Check</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>PARENTAL CONTROLS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WEB ACCESS CONTROL AND MONITORING</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Daily Time Quota</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Customizable Schedule</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Pause Internet Access by Profile</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Online Connectivity Monitoring</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>WEBSITE &amp; CONTENT FILTERING</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Website Filtering</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Google Safe Search</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>YouTube Restricted Mode</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>APP CONTROLS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>YouTube Pause and Time Limits</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>App Detection</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>TREND MICRO GUARDIAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>On-the-go Protection for Kids</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
### Trend Micro Home Network Security 2020 - Product Guide

**GLOBAL 5.0**

#### TREND MICRO HOME NETWORK SECURITY

<table>
<thead>
<tr>
<th>MANAGEMENT</th>
<th>With Station</th>
<th>App Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEVICE MANAGEMENT</td>
<td>Profile-based Management</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Device Management</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Device Detection</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Device Approval</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Device Blocking</td>
<td>Yes</td>
</tr>
<tr>
<td>VISIBILITY</td>
<td>Notifications</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Dashboard</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Timeline</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Network Usage</td>
<td>Yes</td>
</tr>
<tr>
<td>USER INTERFACE</td>
<td>Smartphone / Tablet</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Voice Control: Alexa, Google</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Station Specifications

**Table 2. Station Specifications**

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

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 v5.01.1664, 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.
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**.

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**.
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.

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.**
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.

![Figure 15. Total Devices and Vulnerabilities Found](image)
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.

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.
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:

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.

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.
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.

<table>
<thead>
<tr>
<th>Light Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steady Green</td>
<td>Normal</td>
</tr>
<tr>
<td>Blinking Green</td>
<td>Ready to setup</td>
</tr>
<tr>
<td>Steady Red</td>
<td>No Internet connection or subscription has expired</td>
</tr>
<tr>
<td>Blinking Red</td>
<td>The Station is starting or updating firmware. Please wait until the light is green</td>
</tr>
<tr>
<td>Blinking Red and Green</td>
<td>System error</td>
</tr>
</tbody>
</table>
6. When the light on the Station is Blinking Green, connect your phone to the same Wi-Fi network as the Station.

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.
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.
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**.

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**.

---

![Figure 27. Pair with the Station](image1)

![Figure 28. Connecting](image2)

![Figure 29. Connection Successful](image3)

![Figure 30. Sign In](image4)
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**.

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.
22. Then tap Dashboard item in the menu.

23. View the Dashboard items by scrolling down the Dashboard screen.

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.
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 find all the connected devices on your network and to check their security, tap Check Devices.

5. 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.

6. While the scan is being conducted, you can tap the Back-Arrow on your device to go back to the Dashboard.

7. The Check Devices button now shows Checking Progress.

8. When the scan is done it returns the result. In this example, 1 Vulnerability Found.

9. Tap View Now to view the issue it has found.
10. In this example, the **Action Required** screen indicates that a network printer has been discovered with an **SSL-Poodle Vulnerability**.

11. Tap the panel to obtain the **Issue Details**. Read the **Potential Risk** description to understand the issue.

12. 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.)

13. 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.

14. 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.
Using the Dashboard

To review Dashboard items:


2. Tap the link Show More/Show Less to show more or less detail respectively.

3. Tap individual items, e.g., Vulnerability Found, Network Attacks, Web Threats Blocked, etc., to reveal information on the various threats by device.

4. Tap individual panels to show additional details about particular attacks or threats.
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.

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.
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.)
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.
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.

![Figure 61. Device Report](image)

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.

![Figure 62. Remote Access Risk Blocked](image)

![Figure 63. Network Usage](image)

![Figure 64. Network Usage > Last 30 Days](image)
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 tapping and scrolling down the screen.
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.
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 69. Devices Menu Item

Figure 70. 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.

**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.
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**.

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.)
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.
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.

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.
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.


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.
18. A second instructional screen appears describing how mobile devices use the same rules inside and outside the home network.


20. Tap Pair Now.


22. On the child’s device, enter the Pairing Code that’s currently showing on the managing device into the Trend Micro Guardian app.
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.

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.
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.

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

33. Tap Install.
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**.

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.
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.

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.
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**.

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

![Family Member List](image)

![Family Member: Report, Parental Controls, Devices](image)

**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.

3. Tap Turn On Screen Time. An overview screen appears.

4. Tap Continue.
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.**

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.**
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.

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**.
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.

15. Guardian is now listed in Allowed Apps list.

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.

21. In our example, in Store Purchases & Redownloads we check Don’t Allow for Installing Apps... for Deleting apps...

Figure 131. Content & Privacy Restrictions On

Figure 132. Store Purchases & Downloads - Change to Don’t Allow

Figure 133. Installing Apps > Don’t Allow

Figure 134. 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**.

Figure 135. In-app Purchases > Don’t Allow

Figure 136. 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.
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.

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.
11. If you’re not signed into Google Play, it asks you to sign in with your Account credentials.


13. Tap Open to open the app.

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.


15. Tap 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.


20. On the child’s device, enter the Pairing Code that’s currently showing on the managing device into the Trend Micro Guardian app.
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).

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**.
25. The Accessibility screen appears.


27. Tap **Guardian** to Toggle Accessibility On for it.

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.
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.

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.

Figure 159. Notification Access > Trend Micro Guardian

Figure 160. 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 display these notifications on top of other apps you’re using. This may interfere with your use of other apps.

Figure 161. Allow Display Over Other Apps

Figure 162. 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.

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.
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.

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.
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**.
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.
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.

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.
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.

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.
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.

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.
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.

![Figure 187. Content Toggles](image1.png)

![Figure 188. Filtering On](image2.png)
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.

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

**Figure 192. Set Up Time Limits**

**Figure 193. Add First Rule**

**Figure 194. Select Days**

**Figure 195. 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.

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.
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.
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.)

---

Figure 202. Set Up Connection Alert

Figure 203. 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.
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.

Figure 205. Cancel Today’s Time Limits (1)

Figure 206. 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.

8. Tap Pause YouTube to pause it for the family member.

9. Tap Resume YouTube to resume it for the family member.
10. Scroll down to provide usage details for the family member, including reports on **Filters** that have been triggered.

*Figure 211. 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 212. Devices](image1.png)

![Figure 213. Manage Devices](image2.png)
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.

Figure 214. Device Settings (1)  
Figure 215. 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 216. Network  
Figure 217. Network > Last 7 Days
3. Tap **Last 30 Days** to view the graph and data for the past 30 days.

![Network Last 30 Days Graph](image)

**Figure 218. 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.
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.


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

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.”
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.”

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

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.
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.

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.


13. Tap **Approved List** to add an approved remote access program to the list.
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.

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

---

![Figure 248. Approved List](image1)

![Figure 249. Device Scan](image2)

![Figure 250. Notifications](image3)

![Figure 251. Network Attacks Blocked](image4)
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

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.
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.

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.
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.

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.


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.
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 268. 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

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

- **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.