



# StarHub Mobile Threat Defence User Guide

## Introduction

This documentation provides instructions and information on using the StarHub Mobile Threat Defence (MTD).

StarHub Mobile Threat Defence is a comprehensive security service that offers protection on a single device with a single subscription. It offers an Enterprise Grade Security solution for enterprises that is powered by Zimperium MTD. It provides continuous detection and mitigation of malicious events affecting devices running the iOS or Android platforms. This is accomplished through real-time forensic data analysis by a detection engine that has been enhanced by machine learning.

This section provides information on how to use the product to protect your own device.

Users do not need to interact with Zimperium MTD app for proper detection and prevention suspicious activities. However, users can access the app to determine the following:

- If the application is set up correctly
- If the application has found any suspicious activity
- To view recommendations on how to decrease the risk of device attacks

This guide contains information about:

- How the application is deployed and installed
- Setting runtime permissions
- Navigating the application
- Viewing events, risks, and threats
- The functionality provided by MTD



# Contents

<b>Installing StarHub Mobile Threat Defence</b>	<b>1</b>
<b>Runtime Permissions</b>	<b>3</b>
<b>Transferring of MTD Service to Another Device</b>	<b>4</b>
<b>MTD Functionality</b>	<b>5</b>
About the Dashboard .....	5
Viewing the Activity Report .....	6
Notifications .....	6
Options Menu .....	6
Full Event Log .....	7
Settings .....	8
Troubleshooting .....	9
The About Menu .....	9
<b>Threat Protection</b>	<b>10</b>
Apps .....	10
Web .....	14
Phishing and Content Policy .....	16
Device .....	18
Network .....	19

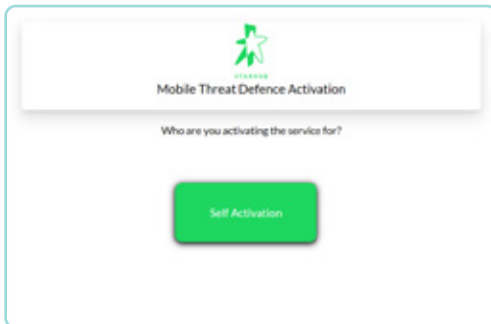
# Installing StarHub Mobile Threat Defence

To secure the mobile device, end users need to activate the StarHub MTD service at the activation portal and install the Zimperium MTD app on their device.

1

## Registration for QR Code Retrieval from the Mobile Threat Defence Activation Portal

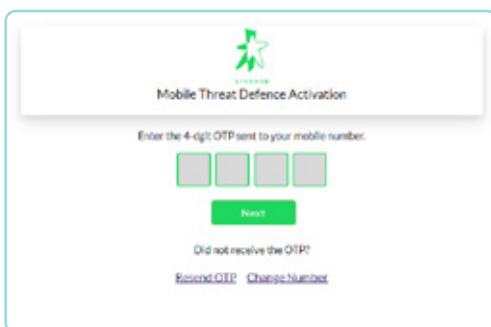
Self-Activation (self activation by end user):



1 Go to Activation Portal.



2 Enter your mobile number and company email address, a 4-digit OTP will be sent to your mobile number.



3 Enter the 4-digit OTP sent to your mobile number.



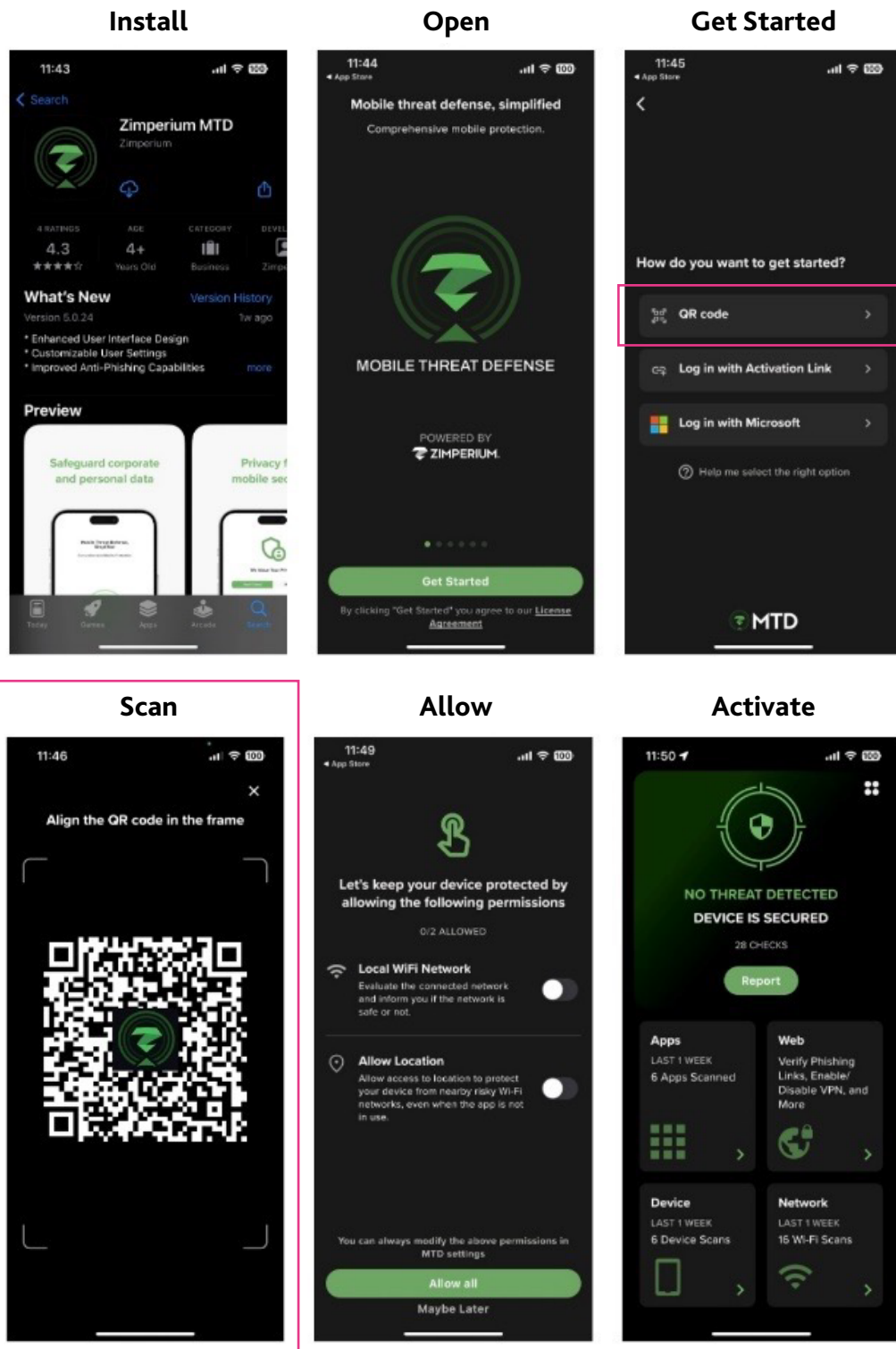
4 Follow the instructions on the screen to activate MTD on your mobile device.

(this step can be combined with the next page on "Activate the Zimperium MTD App on the mobile device")

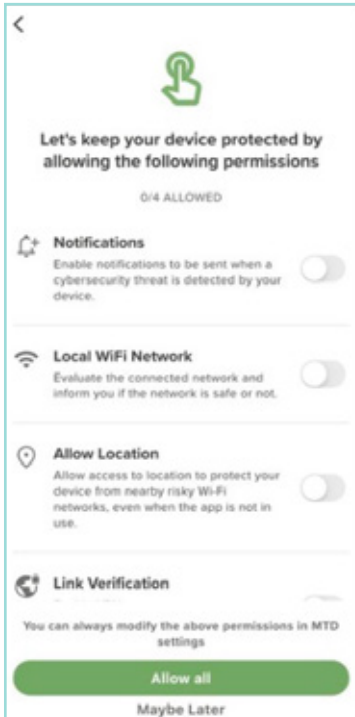
## 2

### Activate the Zimperium MTD App on the mobile device

1. Visit the **Apple App Store** or **Google Play Store** to download and install the app on your device.
2. Launch MTD app and activate by scanning the QR Code.



## Runtime Permissions



When you first log into the MTD app, you are prompted to select the permissions you want to allow.

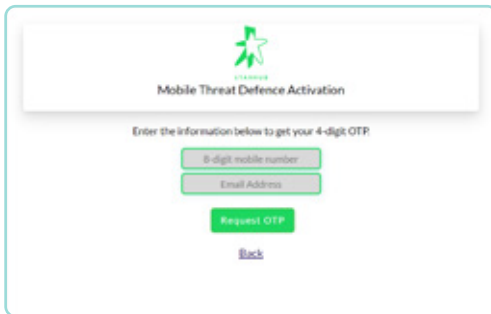
*Note: To modify permissions at any time while using MTD, tap the options **☰** menu icon and press **Settings**. Scroll down to the **Permissions** section and make your changes.*

Users receive runtime permission requests for these topics:

- **Notifications**
- **Local WiFi Network (iOS only)**
- **Allow Location**
- **Link Verification**

# Transferring of MTD Service to Another Device

Follow these steps to transfer your MTD service residing on the current device to another device.



Mobile Threat Defence Activation

Enter the information below to get your 4-digit OTP

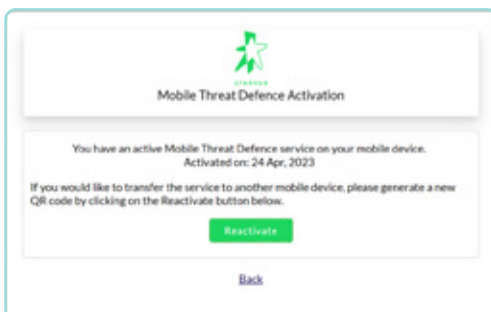
8-digit mobile number

Email Address

Request OTP

[Back](#)

1 Go to Activation Portal.



Mobile Threat Defence Activation

You have an active Mobile Threat Defence service on your mobile device.  
Activated on: 24 Apr, 2023

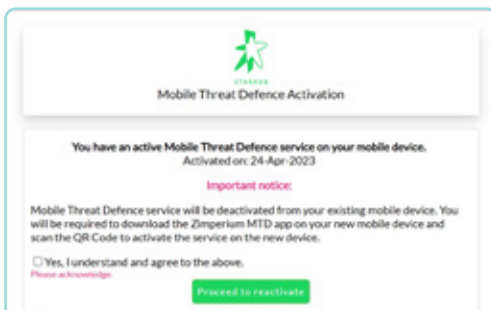
If you would like to transfer the service to another mobile device, please generate a new QR code by clicking on the Reactivate button below.

Reactivate

[Back](#)

2 Enter your mobile number and company email address.

3 You will see a notice that you already have an active MTD service on another device. Click on "Reactivate" if you wish to transfer the MTD service to another mobile device.



Mobile Threat Defence Activation

You have an active Mobile Threat Defence service on your mobile device.  
Activated on: 24 Apr, 2023

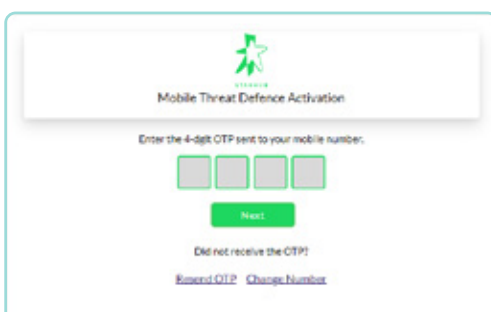
**Important notice:**

Mobile Threat Defence service will be deactivated from your existing mobile device. You will be required to download the Zimperium MTD app on your new mobile device and scan the QR Code to activate the service on the new device.

Yes, I understand and agree to the above.  
Please acknowledge.

Proceed to reactivate

4 By clicking on "Reactivate", the MTD service will be deactivated from your existing mobile device. Check "Yes, I understand and agree" and click on "Proceed to reactivate" to confirm.



Mobile Threat Defence Activation

Enter the 4-digit OTP sent to your mobile number:

Next

Did not receive the OTP?

[Reset OTP](#) [Change Number](#)

5 Enter the 4-digit OTP sent to your mobile number.



Mobile Threat Defence Activation

1 Download the Zimperium MTD app from your mobile device's app store.

2 Launch the app, select "QR Code" and scan the QR code below.

Home

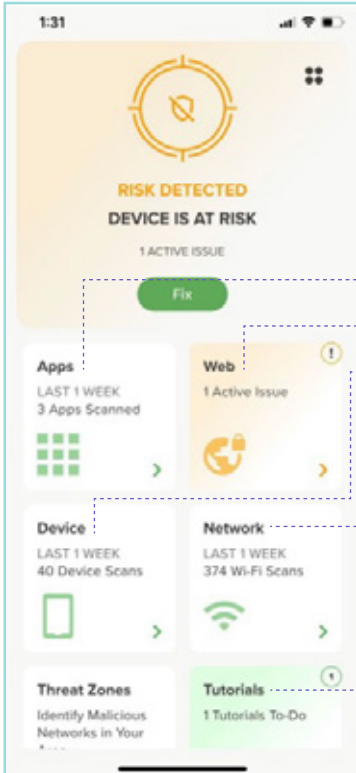
6 Follow the instructions on the screen to activate MTD on your mobile device.

# MTD Functionality

## About the Dashboard

The first screen that is displayed after the activation is the Dashboard. The area at the top of the **dashboard** provides a summary of the status.

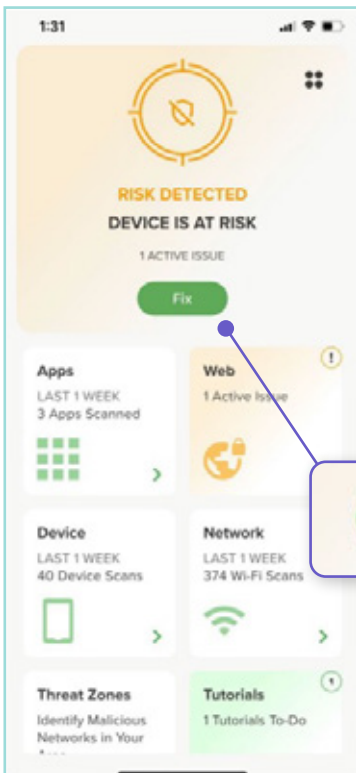
Each tile represents a specific category for threat detection:



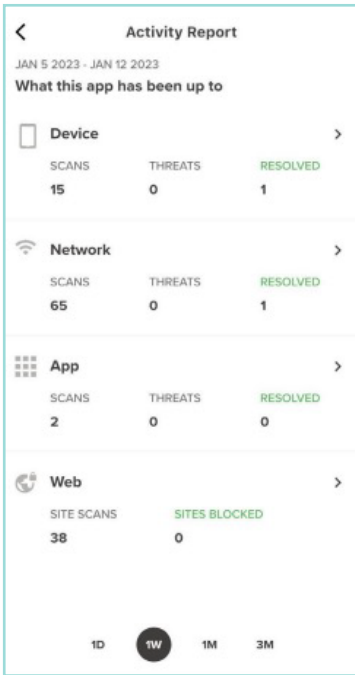
- **Apps** scans for potentially harmful applications
- **Web** checks for phishing links and enables and disables VPN
- **Device** scans for potential threats or risks to the device, such as outdated OS version or update required
- **Network** identifies and protects from threats to the networks
- **Tutorials** contains links to helpful information on various topics

Each tile is colour-coded based on the status of that category, as shown in this example.

Colour	Description
Green	Verifications have been made and there are no issues found
Yellow	Threats have been detected during this timeframe, but none are critical
Red	Critical threats have been detected during this timeframe



You can press any tile to display the list of the active issues detected and view the risks or threats for that category. If, as shown in the prior screenshot, there is an issue to fix, you can press **Fix** to display the Full Event Log.



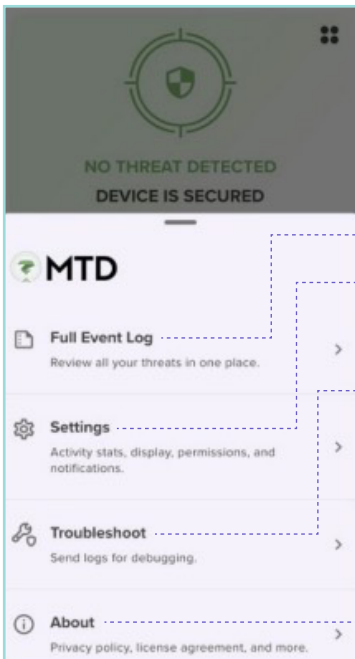
## Viewing the Activity Report

From the dashboard, press the **Report** button to display the Activity Report shown here. This report displays statistics for the Device, Network, App, and Web categories, including the number of security scans, threats, and issues resolved or websites blocked during the specified time range shown at the bottom of the screen.

You can tap on a row to display the corresponding log page for that threat category and view the events in more detail as shown in this example.

## Notifications

There are two types of notifications: banners and popups. Tapping the notification launches the MTD app and provides the user with additional information. It also includes recommended actions for the event.

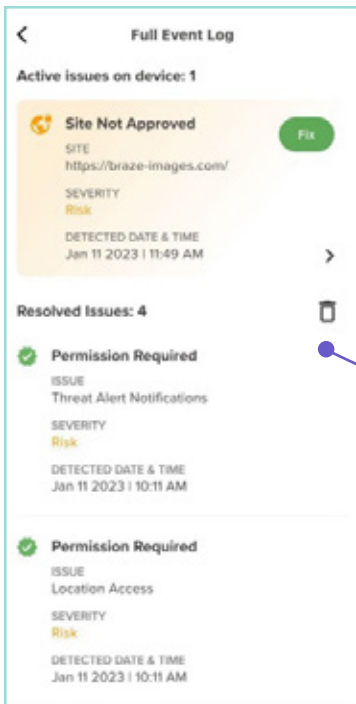


## Options Menu

Tap the **☰** icon in the upper-right corner of the dashboard to display these options.

- **Full Event Log:** A comprehensive list of the threat log items.
- **Settings:** These are settings for the user's device display, such as the number of days for statistics, and dark or light appearance.
- **Troubleshoot:** Allows you to send log and debugging information. You can also access the Advanced Details screen from the Advanced Troubleshooting screen that displays when you long press the **Troubleshoot** option.
- **About:** Displays information about the current version of MTD, including the privacy policy and the license agreement.



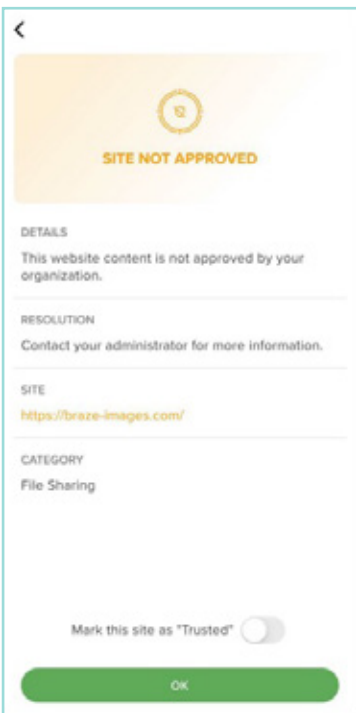


## Full Event Log

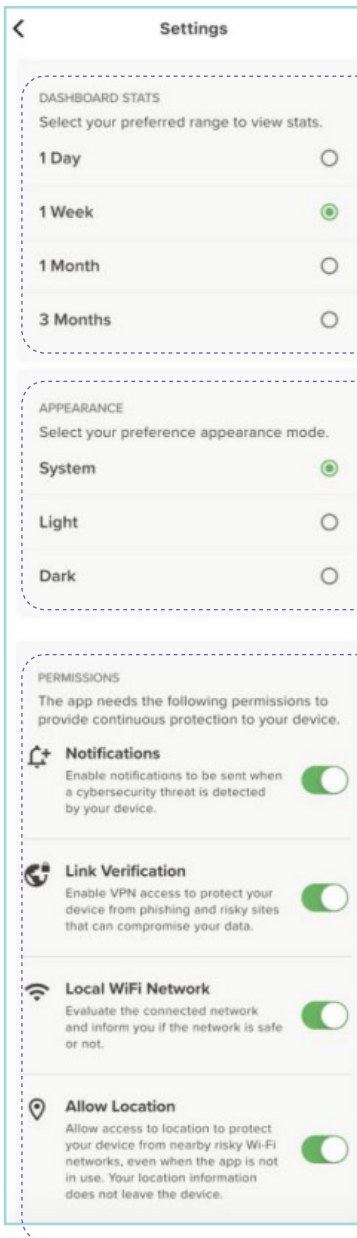
The **Full Event Log** is available from the options menu ☰ and provides a list of all threats detected on the device. If a risky site is detected, you will see a message that the site is blocked. The event log also displays a description of the threat and the date/time that it was detected. You can scroll through this log.



The active issues display at the top of the threat list. Once a threat is mitigated, it moves to the bottom of the list under **Resolved Issues**. You can press the trash can icon to remove all the resolved threats.



You can click **Fix** for any active issue to view details, resolution recommendations, and the URL and category for the site. You can enable the option to **Mark this site as "Trusted"** if you deem this site as safe and wish to turn off the alerts related to it. Click **OK** when you are finished.



## Settings

If you select **Settings** from the options menu ☰, you can view and edit new settings for these topics:

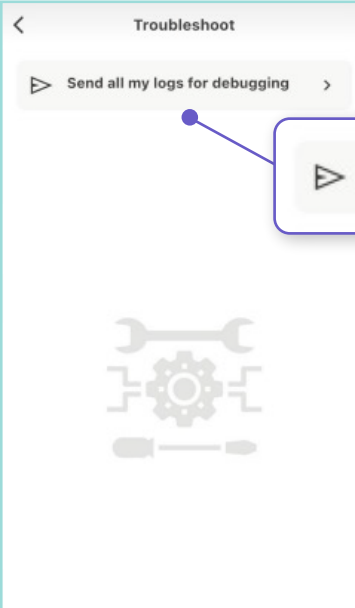
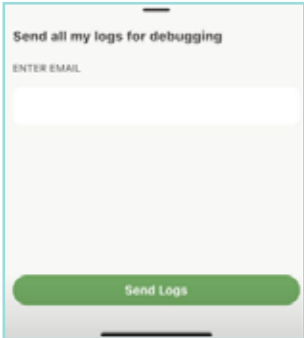
- **Dashboard Stats** – Allows you to select the preferred day range to view statistics for the MTD app dashboard.
- **Appearance** – Allows you to select the display for the app, such as light, dark, or the system appearance mode.
- **Permissions** – Allows you to review and reset the permissions that MTD requests to provide continuous protection. Permissions include Notifications, Link Verification, Local WiFi Network, and Allow Location.

## Troubleshooting

When you select Troubleshooting from the options menu ☰, this is where you can select to have debug logs sent to an email address.

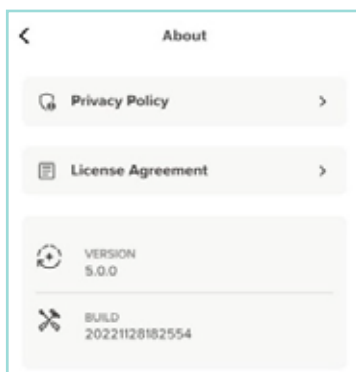
### Send Logs for Debugging

Troubleshooting allows the user to view and share the MTD application log information. Perform these steps to set this up:

1. From the Troubleshoot screen, press **Send all my logs for debugging** to display this screen.
2. Enter your email address and press **Send Logs**. A confirmation message indicates that your logs have been sent.

## The About Menu

To view information about the current version of MTD, such as the Privacy Policy and the License Agreement, tap **About** in the options menu ☰ to display this screen.



# Threat Protection

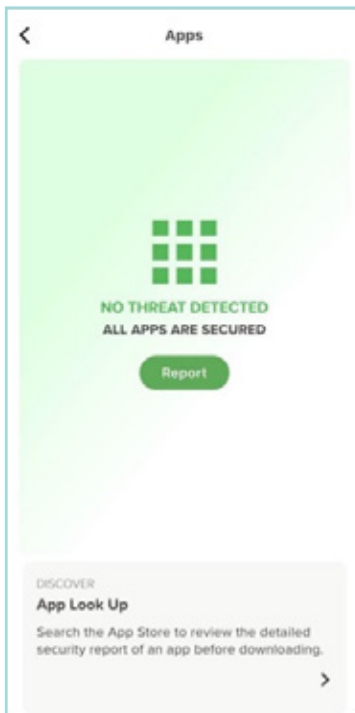
MTD scans specific categories for threats to your security. These categories are displayed in tiles on the dashboard:

- Apps
- Tutorials
- Web
- Device
- Network

Each of these categories is explained in this section, along with ways to access and interpret the information reported by MTD.

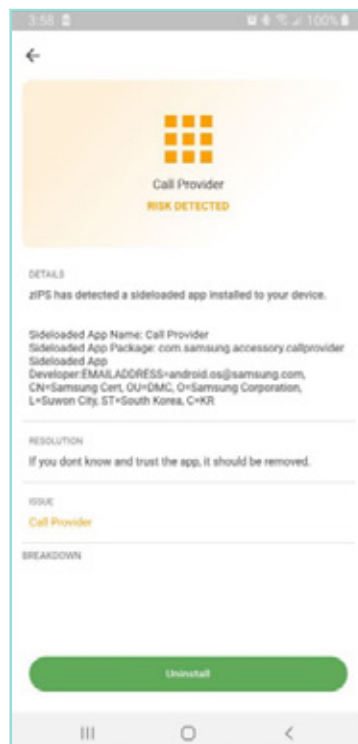
## Apps

In the dashboard, the **Apps** tile displays the status with green, yellow, or red indicating respectively if no threats are detected, if risks are detected, or if threats are detected. Tapping on this tile takes the user to the **Apps** screen.



If a risky app is found, the screen provides the user with information on the application and a recommendation on how to proceed. Categories for risky apps include:

- **Suspicious apps** are apps installed that are high-risk. They have the potential to compromise the device.  
*Note: This is only applicable to Android.*
- **Sideloaded apps** are apps installed outside of the Google Play Store or App Store. They have not been officially validated and are considered risky.
- **Out of Compliance (OOC) apps** are apps that have characteristics that do not comply with the organisation's privacy and security policies.



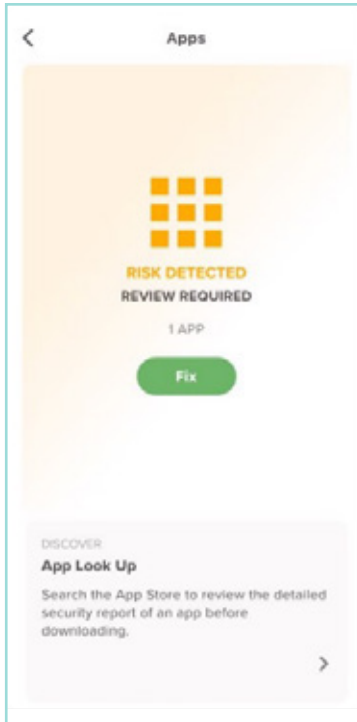
This screen shows an Android example with a sideloaded threat.

## Application Scanning

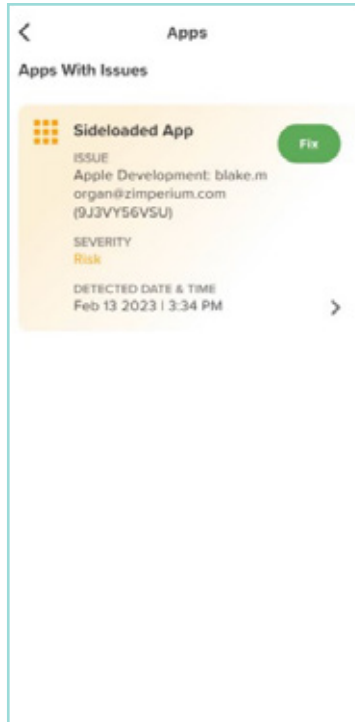
MTD automatically scans the device for risky apps when it is initially installed. Apps are also scanned when they are downloaded and installed.

*Note: This is only applicable to Android.*

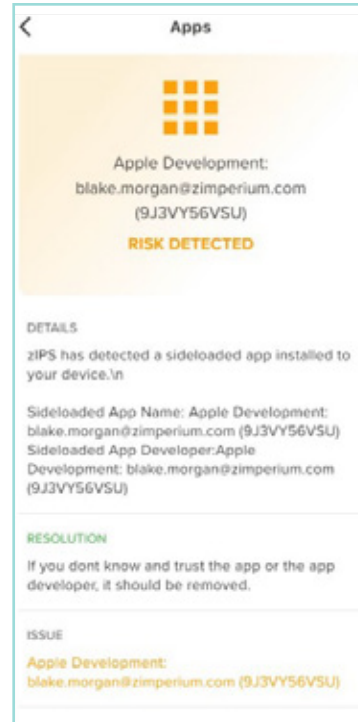
Here is a screen where a risky app has been detected.



Press the screen to display a list of the apps with issues.



You can press **Fix** if you want to display the details and recommendations.

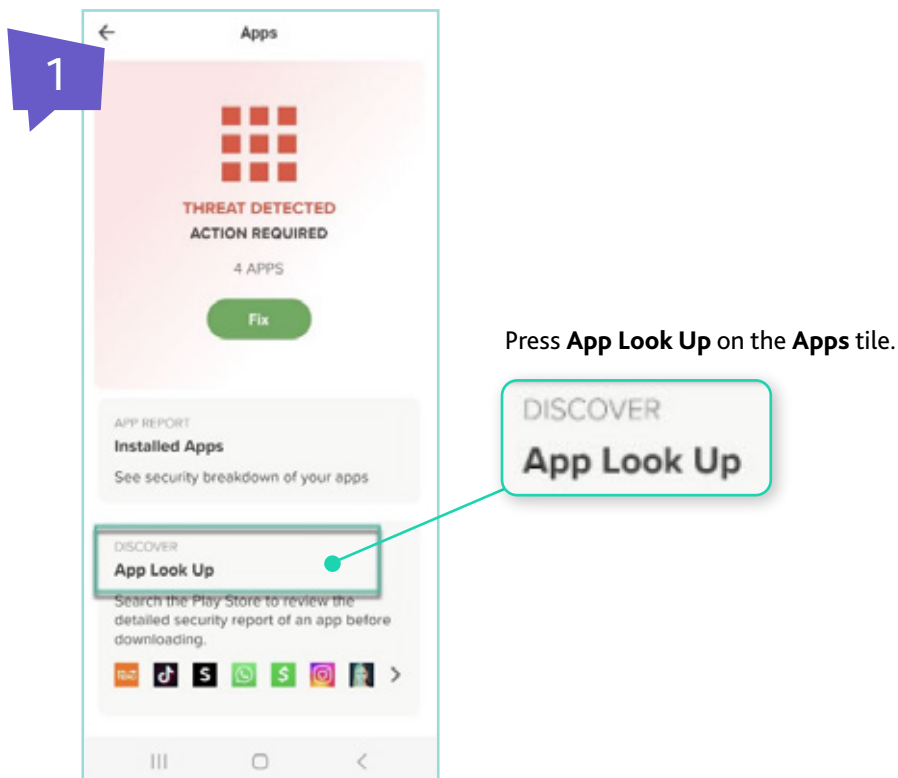


## Searching Installed Apps to Determine Risk

When users want to install an app on their device, but want assurance that the app is safe, they can search for the app from a comprehensive database. This displays the summarised privacy and security rating of the app, which helps users determine if it poses a threat to the device. Searches can be performed for non-English languages as well.

Within the **Apps** tile, you can press the **App Look Up** link.

Follow these steps to search for an app risk report:



2 Search an app name.

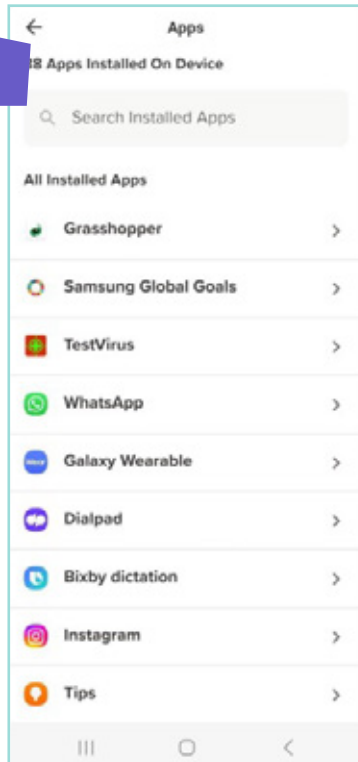
3 Tap the app name to view the privacy and security risk report for the app.

Follow these steps to view the app risk report for your installed apps (Android only):

1

Press **Installed Apps** on the **Apps** tile.  
This displays a list of apps installed on the device.

2



Search for and select an app.

3

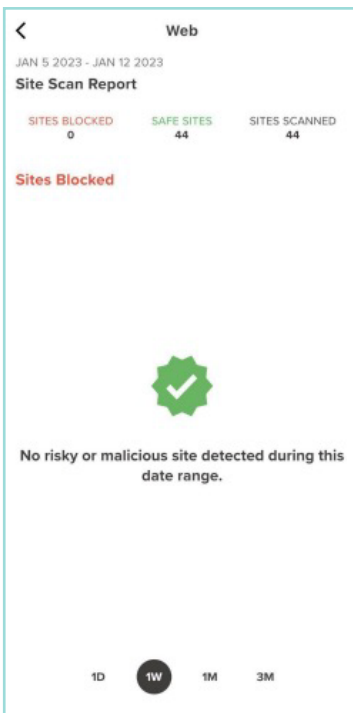
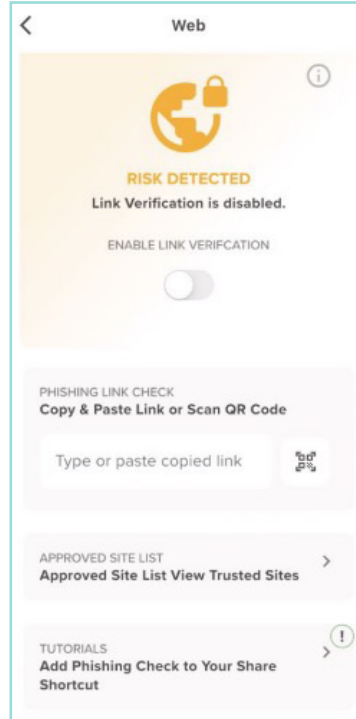
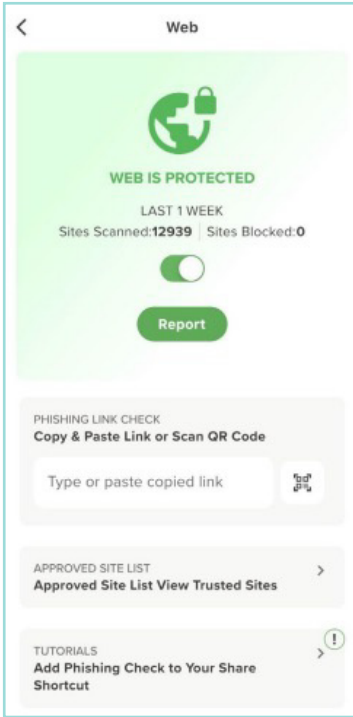
Tap the app name to view the privacy and security risk report for the app.

### Uninstalling Apps (iOS only)

To uninstall an app on your iOS device, long press the app icon and select **Remove App**. Or, you can long press the background and a minus (-) icon displays beside each app. Click that icon to uninstall the app.

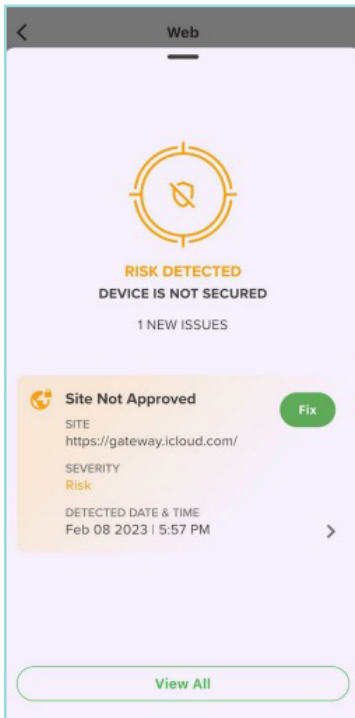
## Web

In the dashboard, the **Web** tile displays the status of threat detection (red, yellow, or green). Tapping on this tile takes you to the **Web** screen.

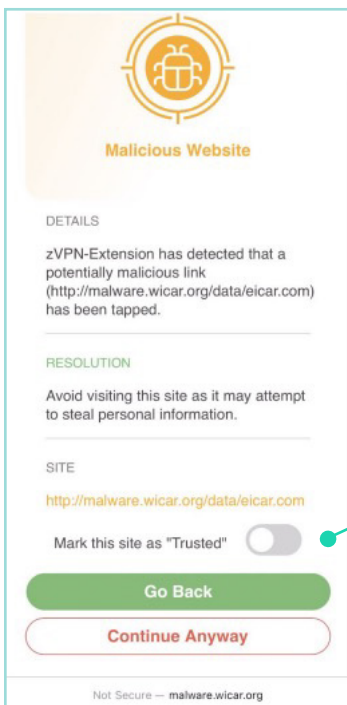


If you press the **Report** button, a **Site Scan** report displays. This report shows the number of sites that are blocked and their URLs, along with the number of safe sites and sites scanned.

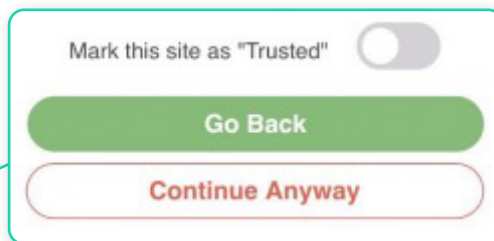




This screen displays when a risky site is detected.



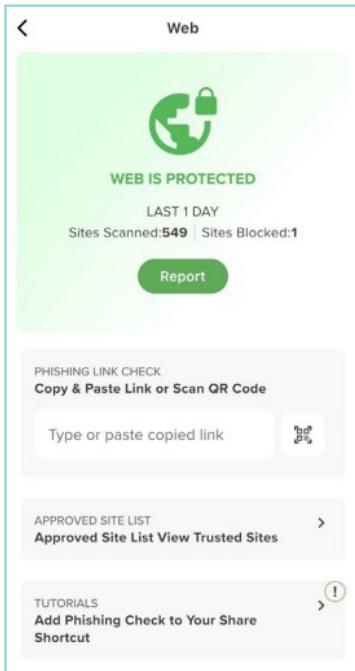
When you click on the threat, the following screen displays. Users will have an option to **Continue Anyway** and **Mark this site as "Trusted"** appear for the user to select if they choose to bypass the warnings in the future.



## Phishing and Content Policy


The phishing and web content filtering policy protect users from accessing any harmful websites and links (such as malware, phishing, botnets, and suspected domains) that contain content that might be risky.

When a user is alerted about a website or queries a website to see if it is safe, MTD provides the category of that site, such as gambling or illegal drugs. This guidance helps the user determine what action to take next.



### Checking for Phishing Risk

If this feature is enabled, when you press the **Web** dashboard tile, the screen shows the protection available for insecure (HTTP) connections. To check a link for phishing risk, you can:

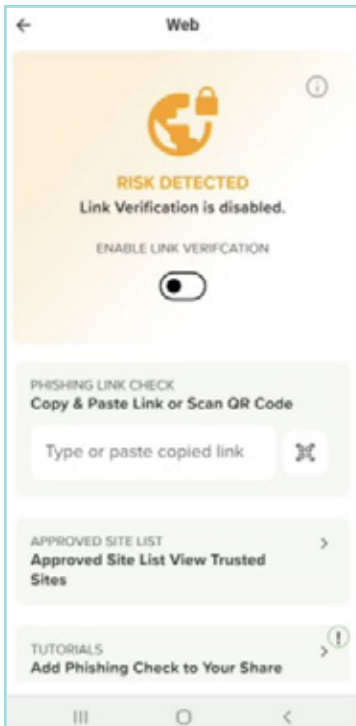
- Type or paste a copied link.
- Press  and scan a QR code. You will be prompted to allow MTD to use the camera.

The screen shows the **Phishing Link Check** field, where you can copy and paste a link or scan a QR code.

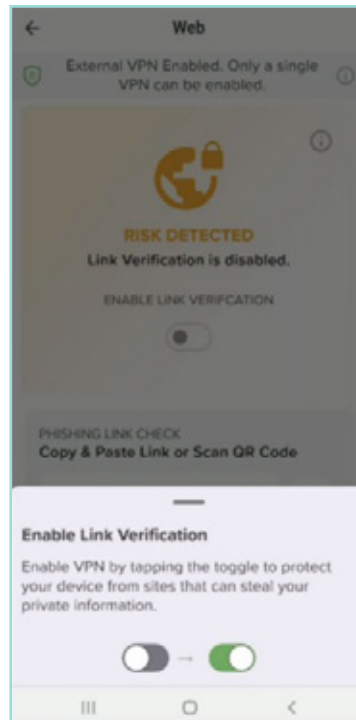
## VPN Protection

Once the VPN configuration is set up on the device, an alert displays when the device encounters an attempt to access an unsecured WiFi network. MTD automatically connects the device to a secured VPN to tunnel the insecure (HTTP) traffic over the unsecured WiFi connection.

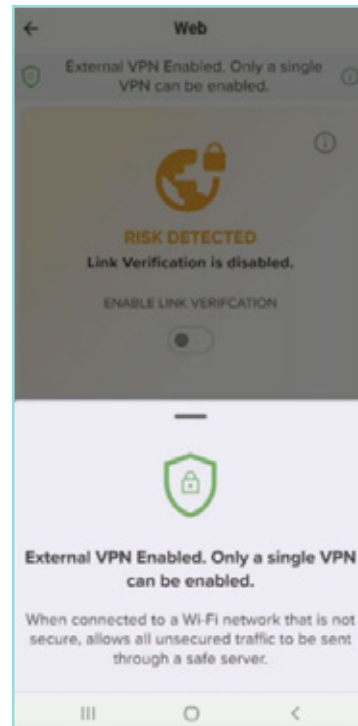
An example of an alert is shown here.



If you toggle **Enable Link Verification on**, this popup displays.



The following message displays as confirmation that Link Verification is enabled.



## Device

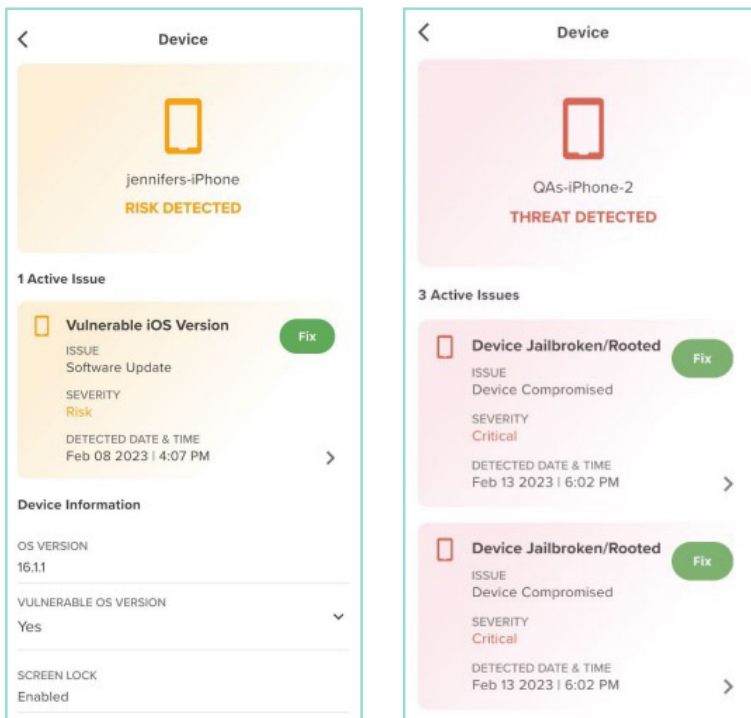
In the dashboard, the **Device** tile displays the current state of the device itself. Examples of threats that show up in this category include:

- **App Tampering**
- **Device Jailbroken / Rooted**
- **File System Changed**
- **MITM (Man in the Middle)**

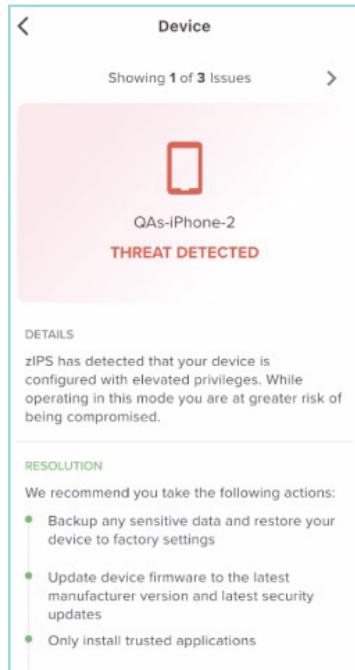
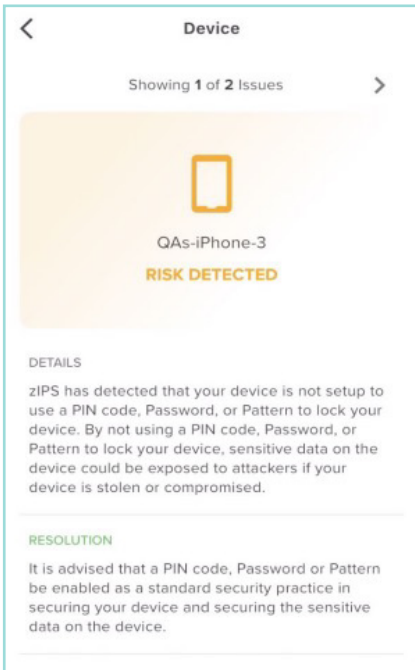
Tapping on this category takes the user to the **Device** page. If there are any critical events or risks detected, the details and Yes/No values show the items that are issues.

MTD colour-codes the screens to help you quickly identify the severity of issues. If a critical threat is detected, the title bar changes to red. A yellow title bar indicates that a risk was detected. Green indicates that no risks or threats were detected.

If any of the detections show 'Yes', you can tap the down arrow to get recommendations and more information on the item.



These screens show the **Device** screen with risk detected (yellow) and threat detected (red).



If you press **Fix**, the threat details and recommended resolutions will show.

## Network

In the dashboard, the **Network** tile displays the current state of the network or Wi-Fi connection. Examples of threats that show up in this category include:

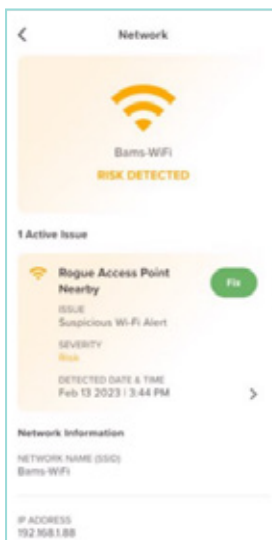
- Compromised Network
- Danger Zone Connected
- MITM - Fake SSL Certificate
- Rogue Access Point
- SSL/TLS Downgrade

Once a critical threat is detected, the title bar changes to red. A yellow title bar indicates that a risk has been detected.

Tapping on this category takes you to the **Network** screen, which displays an overview of the device network configuration, including the device's IP address along with the currently connected SSID and its BSSID.

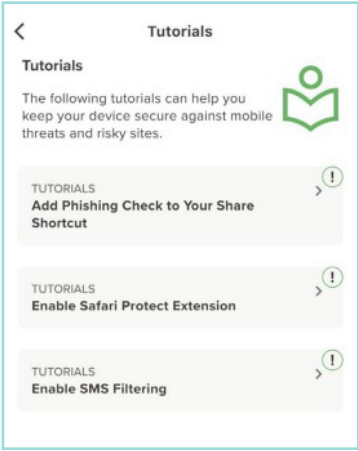
If there are any critical events, the title bar will be yellow and the display title changes to **Risk Detected**. Recommendations for the user to stay safe are displayed as appropriate for the critical event detected.

*Note: If a device is connected to an unsecured WiFi and MTD is installed and activated afterward, sometimes no threat is detected for that existing WiFi connection. If this WiFi connection is dropped and a reconnection is performed, you will be notified of the threat.*



Here are some examples of the **Network** screens: one with threats (yellow) and the other without them (green).

# Using the MTD Tutorials



MTD provides tutorials to walk you through certain features. These are available from the Tutorials tile on the dashboard and are shown below.

The tutorials that are currently available within the app are listed below for each OS type:

**iOS:**

- Add Phishing Check to Your Share Shortcut
- Enable Safari Protect Extension
- Enable SMS Filtering

**Android:**

- Add Phishing Check to Your Share Shortcut

For more information on StarHub Mobile Threat Defence, please visit [starhub.com/mtd-basic](http://starhub.com/mtd-basic), or refer to our Frequently Asked Questions.

For technical enquiries, please contact the StarHub Service Support Operations at [ssops@starhub.com](mailto:ssops@starhub.com).