



CTM SAFE

User Guide

(Android / iOS)

March 2022

Table of contents

Introduction	3
First time login to CTM SAFE and secure your mobile device.....	4
Forget password.....	6
Safety Butler Service (Management portal)	7
<i>Download and Install CTM SAFE.....</i>	<i>8</i>
<i>Install CTM SAFE on a different device</i>	<i>9</i>
Sharing protection with family or friends via CTM SAFE “People”	10
Making browsing Internet safe for children with Family Rules	11
<i>Adding a new device for children via CTM SAFE “People”</i>	<i>12</i>
<i>Setting up Family Rules for children.....</i>	<i>14</i>
Browsing Internet Safely	20
<i>CTM SAFE Browser.....</i>	<i>20</i>
<i>Disabling Safari on children's devices (For iOS Only).....</i>	<i>21</i>
<i>Removing other browsers (For iOS Only).....</i>	<i>21</i>
Protecting Online Banking.....	22
Returning from or entering a blocked website.....	23
Protecting your device against Virus & Threats	24
App notifications (For Android Only).....	25
Technical Support	26
CTM SAFE features per platform	27

Introduction

CTM SAFE is a comprehensive security service that offers award-winning protection on multiple devices with a single subscription. With CTM SAFE, you can protect yourself and your loved ones against all threats on a computer, smartphone, or tablet.

The Safety Butler Service management website and the in-app Peoples & Devices view gives an overview of the people and their devices that you, as the subscription owner, have protected with your subscription. To see detailed information about a user, just select the user and a user-specific view will open, giving you an overview of the protection of the user.

CTM SAFE applications

Install the CTM SAFE application on all your devices to protect your security and privacy. SAFE supports devices running on Windows, Mac, Android, and iOS operating systems. CTM SAFE also protects you and your loved ones while browsing the Internet with technology like:

- Browsing Protection (referred to as Safe browsing on mobile platforms), which uses advanced cloud-based web reputation checking to verify the web pages and make sure only safe web sites can be accessed.
- Banking Protection, which protects your online banking activities by securing your connection when you access an online banking portal.

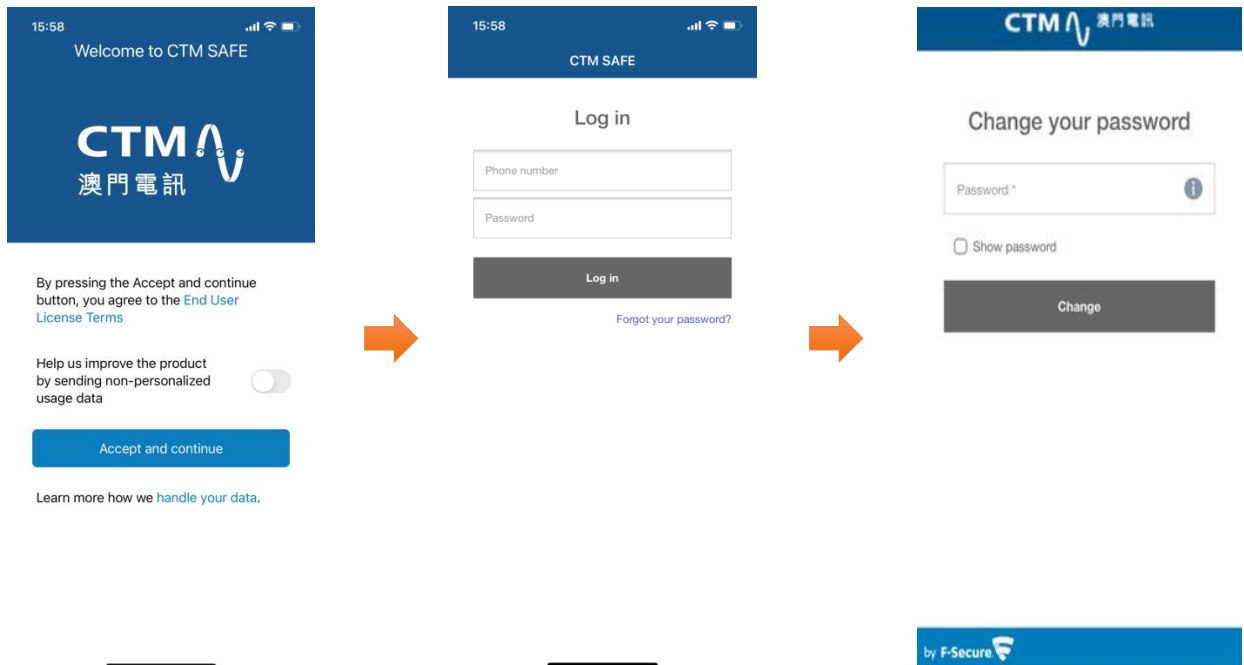
System requirements

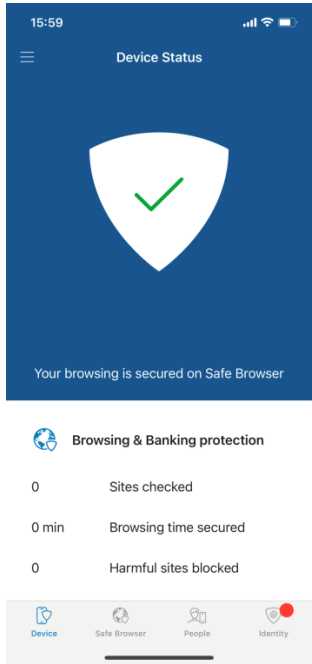
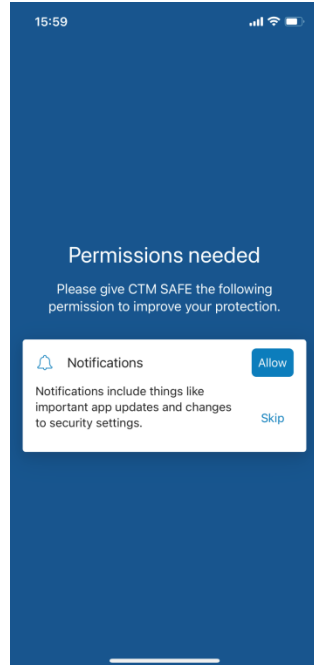
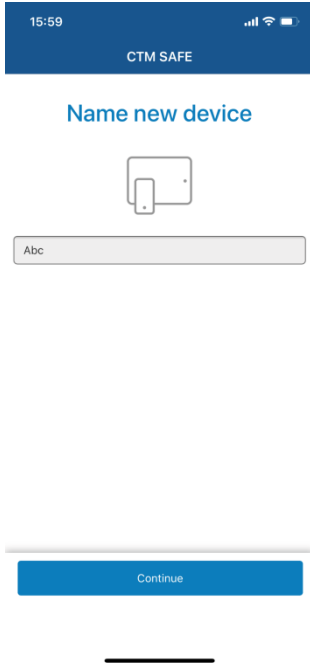
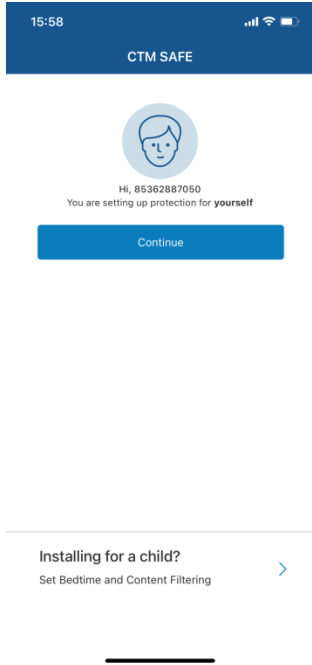
CTM SAFE supports smartphones and tablets that are running:

- Android OS 6.0 and greater. The installation of the application requires about 75 MB of free storage. The application can only be installed in device's internal memory. Activation and updates require a working Internet connection.
- iOS 13.0 and greater. The installation of the client application requires about 20-30 MB of free space.

First time login to CTM SAFE and secure your mobile device

1. Once the activation SMS is received successfully;
2. Click the link in the SMS to download and install CTM SAFE;
3. Open CTM SAFE, and click **Accept and continue**;
4. Enter the phone number registered when applying for the service (**+853 is required**) and the temporary password in the SMS, and then click **Login**;
5. The app will request a password change for first time login. Enter a new password.
6. To protect this mobile device, click **Continue**; to set parental control rules on this mobile device, click **Installing for a children?**;
7. Name the new device, click **Continue**;
8. After clicking **Allow**, this mobile device is protected.

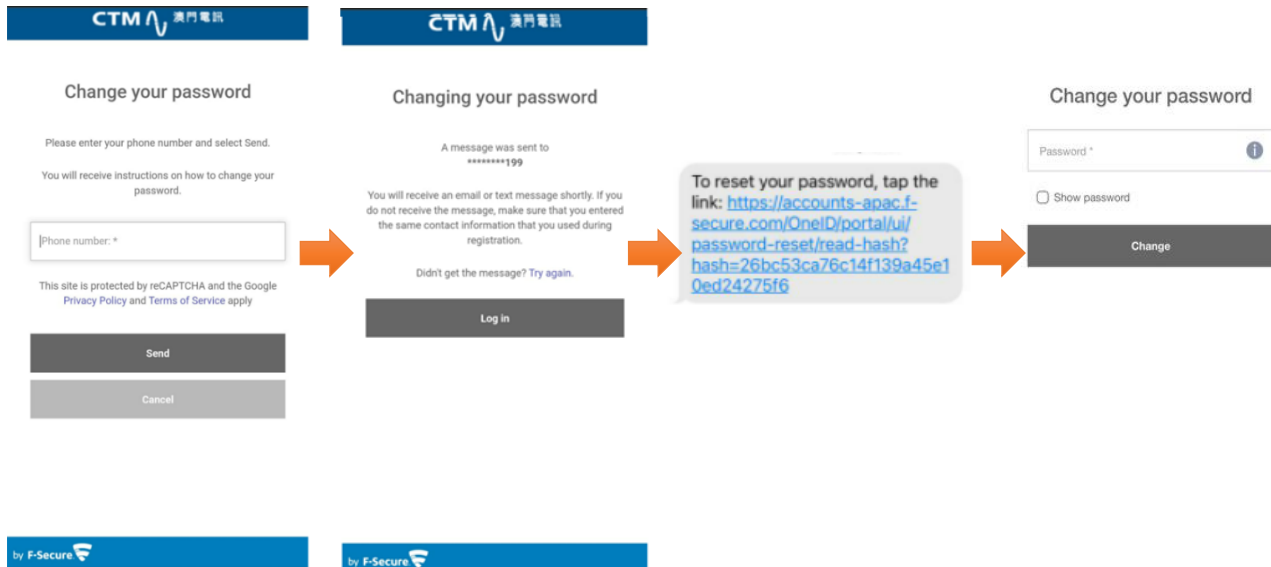




Forget password

If you forget your account password for the Safety Butler Service, you can create a new password through the process of forget password:

1. Click **Forget Password** on the Login page.
2. Enter your phone number and click **Send**. A change password SMS will be sent to the device.
3. Open the password reset link in the SMS.
4. Set new password.



Safety Butler Service (Management portal)

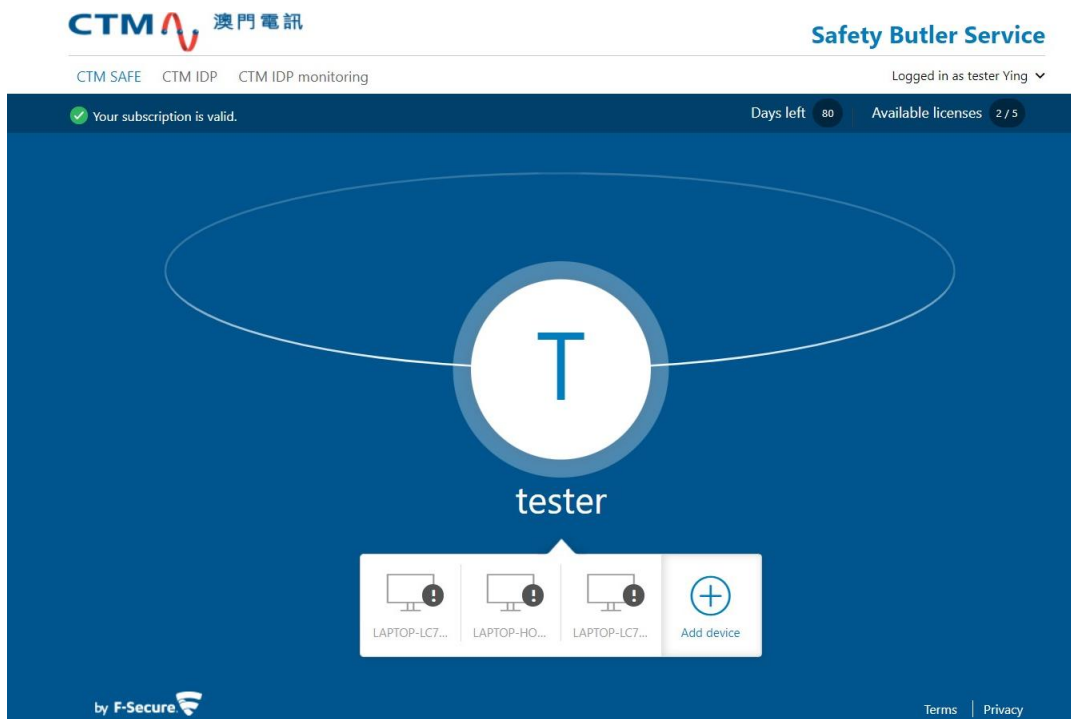
Safety Butler Service Management Portal is an easy-to-use online service that you can use to install the CTM SAFE app onto your selected device remotely and manage your subscription.

Upon logging into the Safety Butler Service Management Portal, you can manage your device, view your subscription status, and add family members to share your Safety Butler Service with.

You can use Safety Butler Service Management Portal to easily transfer a CTM SAFE product from one device to another, whenever you choose to do so. If you need additional licenses to protect more devices, you can subscribe to the Safety Butler SAFE Value-added Service via CTM.

Tap the link to enter Safety Butler Service Management Portal:

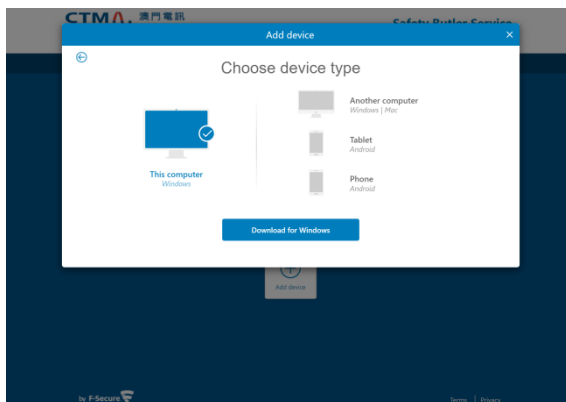
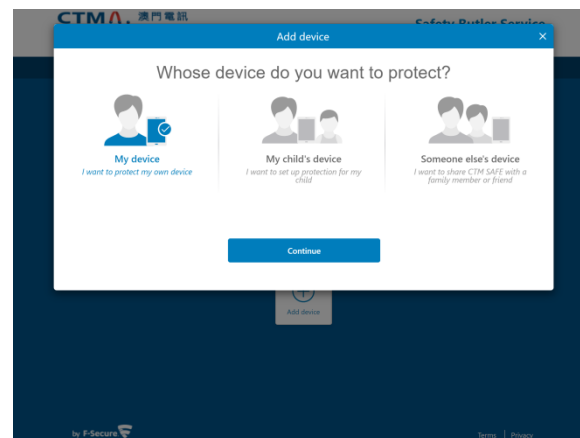
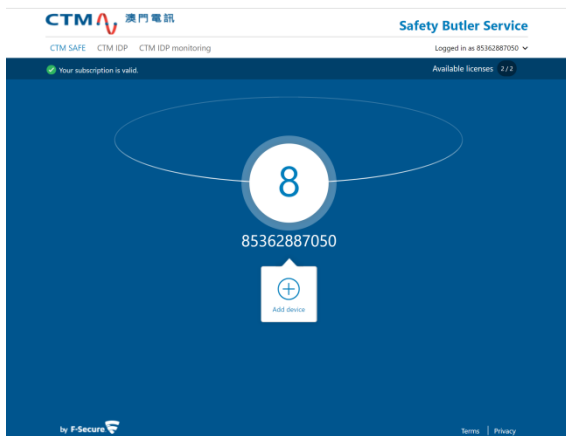
<https://safeavenue-jp.f-secure.com/iframe/-sso/ctm/>



Download and Install CTM SAFE

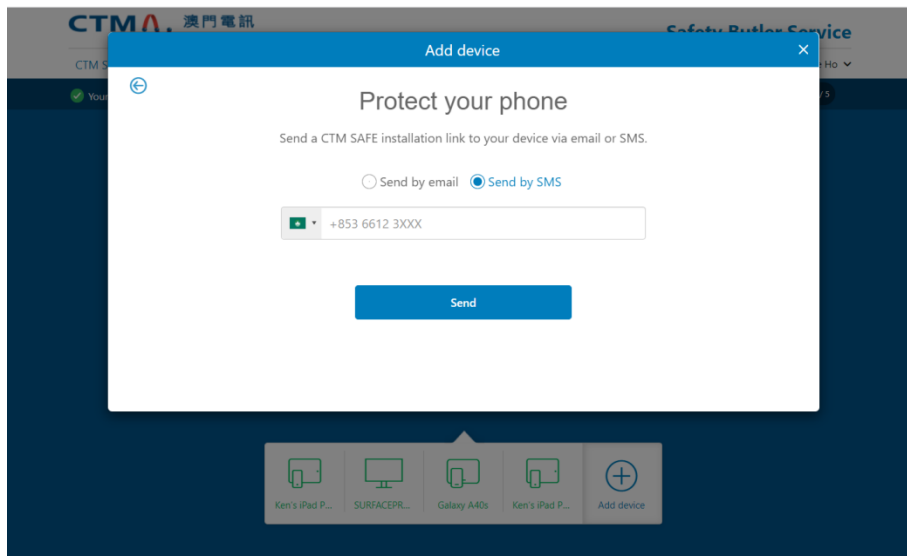
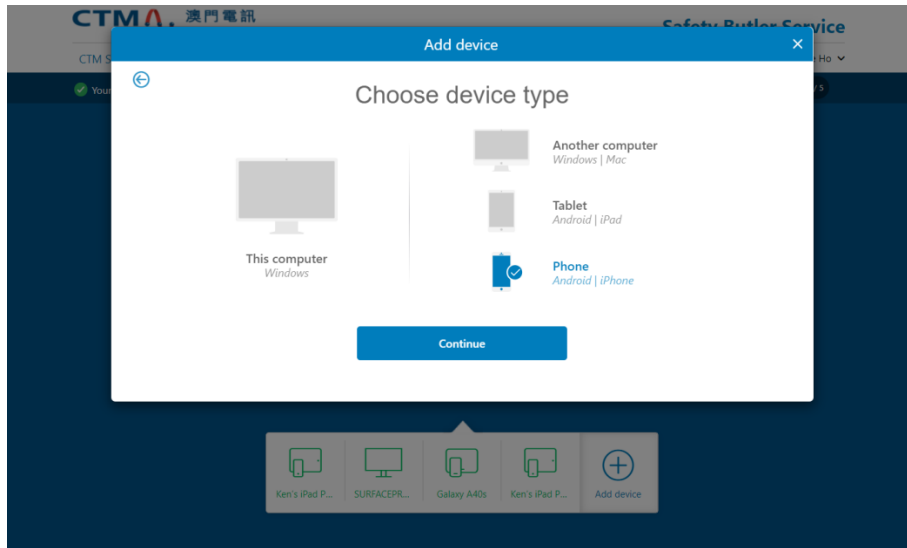
Through Safety Butler Service Management Portal, you can download and install CTM SAFE on a computer by email or mobile by SMS, making it easy for you to deliver CTM SAFE to a device that you want to protect.

1. Login to Safety Butler Service Management Portal with your phone number (**+853 is required**) and password.
2. Select **CTM SAFE**, and click **Add device**.
3. Choose whose device you want to add, select **My Device** (If installing on your own devices) and then click **Continue**.
4. Select **This device** to install CTM SAFE on your current device, then select **Install from app store** to go to the app store and start the installation.
5. After the installation is completed, open and login to activate the product. The product will not protect your device before you activate it.



Install CTM SAFE on a different device

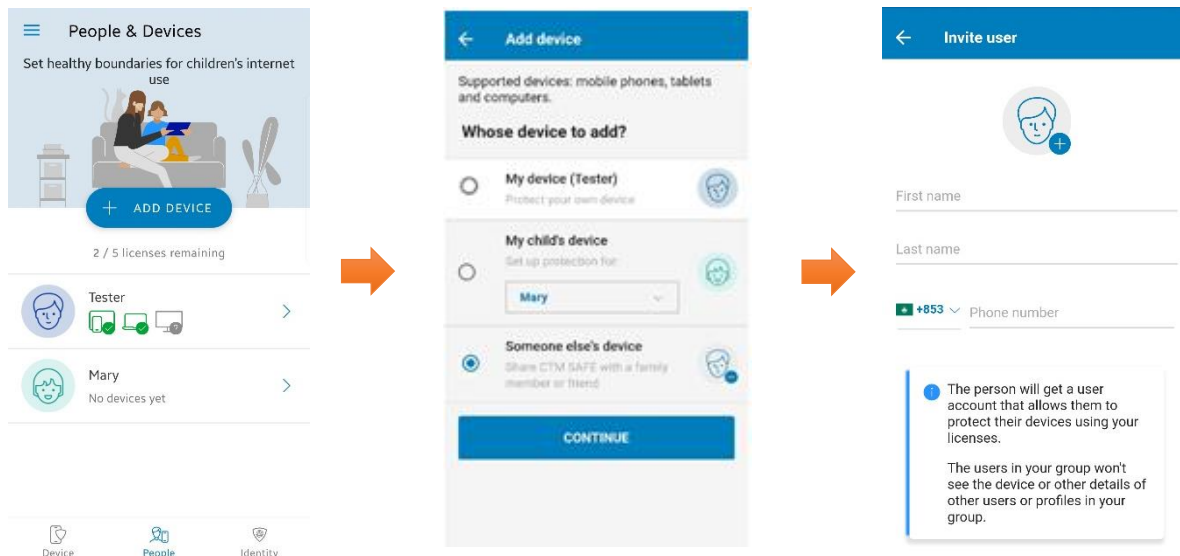
- Select the device type and then select **Continue**.
- Select **Send by SMS** and enter the phone number for the device.
If the device does not have a phone number, select **Send by email** and enter an email address that you can access on the device.
- Select **Send**.
- Follow the installation instructions that are sent to the device.



Sharing protection with family or friends via CTM SAFE “People”

When you invite family members or friends to your group, the invited persons get their own user account that will allow them to protect their devices using your licenses. To share Safety Butler Service with someone else:

1. Open the CTM SAFE app and select the **People** tab.
The **People & Devices** view will open.
2. In the **People & Devices** view, select **+ ADD DEVICE**.
3. Select **Someone else's device** > **CONTINUE**.
4. To invite a user to your group:
 - Enter the first name of the user.
 - Enter the last name of the user.
 - Enter the email address of the user.
5. Select **SEND INVITATION**. The invitee will receive an invitation SMS to join your Safety Butler Service group.
6. The invitee will own an account after receiving the invitation SMS which will allow them to protect their devices using your licenses. The users in your group won't see the devices or other details of other users or profiles in the group.



Note: If the person you want to invite to your group has already been added to your group or belongs to another My F-Secure group, you will see a message in the invitation dialog saying that the person already belongs to your group or to another group. This means that the email address used in the invitation has already been activated for an account. You can solve this either by using another email address, if any, to invite the user to your group or you can ask this user to delete the existing account after which you can then use the email address in the invitation.

Making browsing Internet safe for children with Family Rules

The Internet is full of interesting web sites, but there are also many risks for children who use the Internet. Children are at risk when they browse the web with their mobile devices unsupervised.

Many web sites contain material that you might consider inappropriate for your children. They can be exposed to inappropriate material, may accidentally download malware that could damage the mobile device, or may receive harassing messages after browsing in unsafe web sites.

Family Rules helps you keep your children safe from unsuitable content when on the internet. With Family Rules, there are different ways that you can restrict your child's internet usage as follows:

- You can set time limits for daily use,
- You can set a bedtime,
- You can restrict the apps that your child has access to, and (For Android only)
- You can block certain types of content.

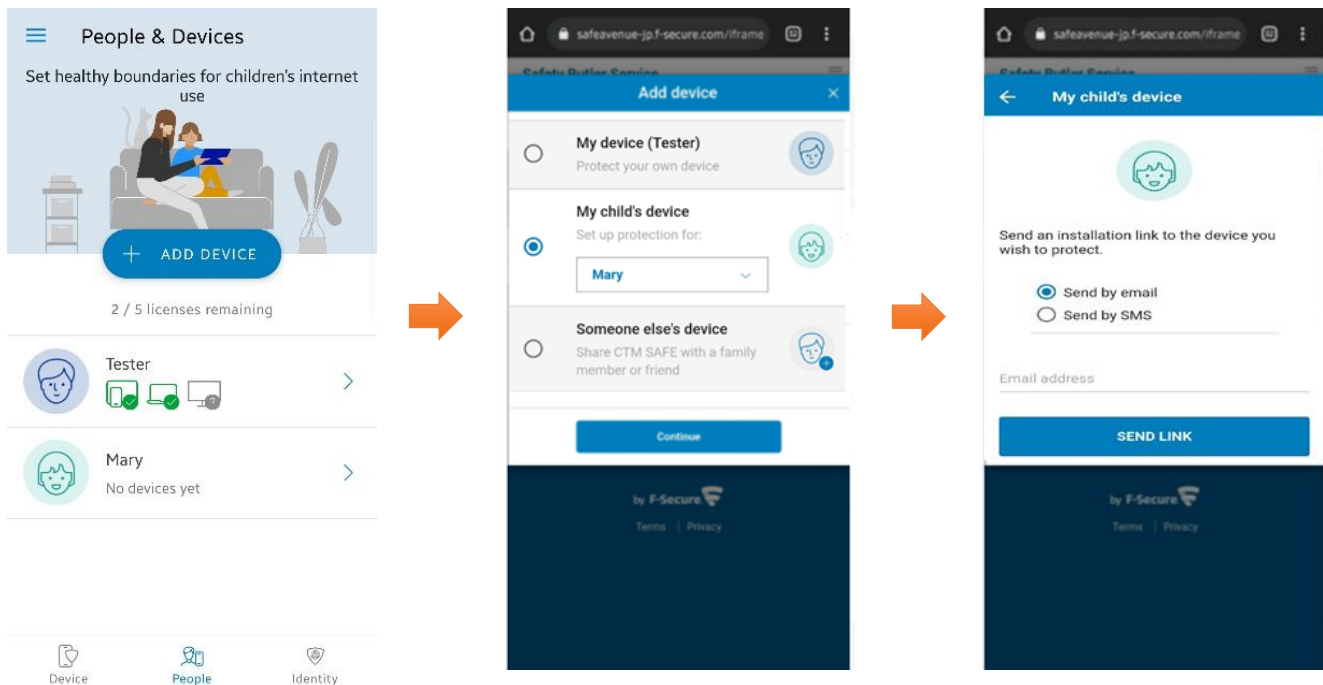
For ease of use, you can manage your child's online activity on your own device. This is a versatile way to make changes and add or remove restrictions on the fly without having your child's device physically with you.

Note: The Family Rules settings can be edited only in the parent's People & Devices view or by logging in to the Safety Butler Service.

Adding a new device for children via CTM SAFE “People”

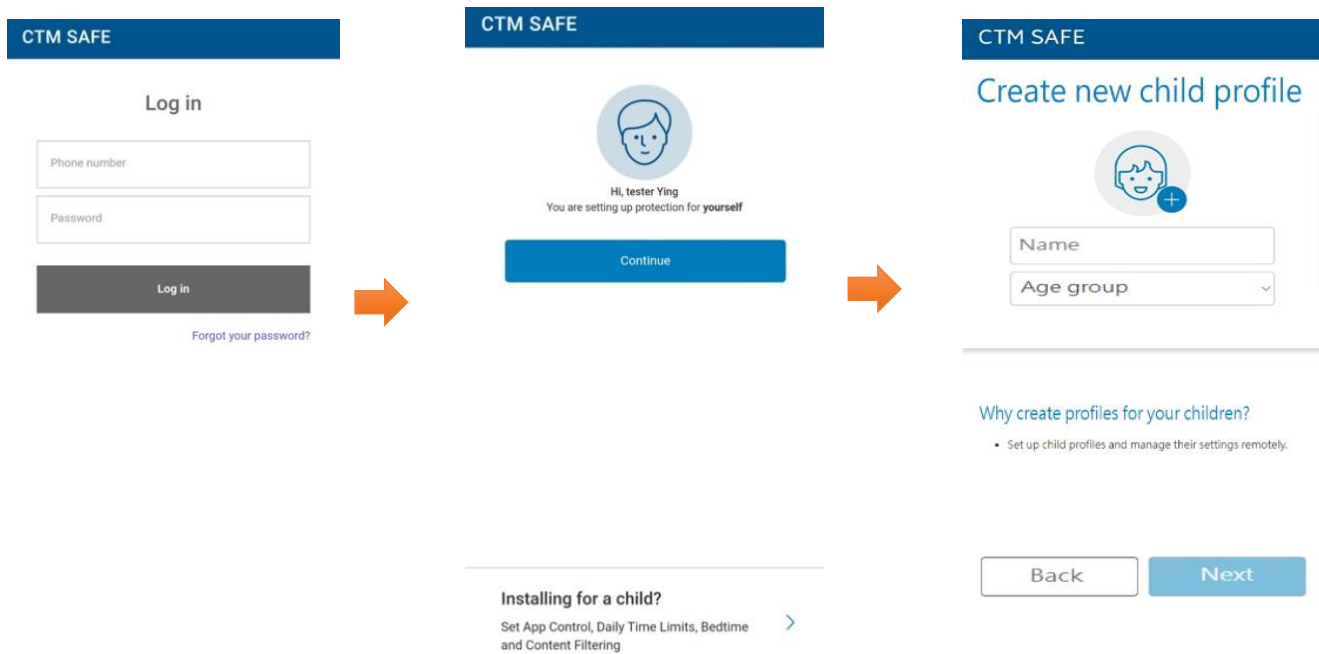
To start using Family Rules, install CTM SAFE on your child's device and set up a child profile. You can set up Family Rules when installing the CTM SAFE app or any time afterwards. Once that's done, you can start protecting your child's online activity.

1. Open **CTM SAFE** on your device and select **People**.
2. In **People**, select **Add Devices**
3. Select **My Child’s Device** and then click **Continue**.
4. Select **Send by SMS** and enter the phone number for the device. If the device does not have a phone number, select **Send by email** and enter an email address that you can access on the device. Select **Send**.
5. Follow the installation instructions that are sent to the device.



6. After the installation is complete, choose **Installing for a child?** You are prompted to set up Family Rules. Select from existing profile listed or create new child profile, then follow the instructions shown onscreen to set up Family Rules.
- Enter the name of your child.
 - Select the age group your child belongs to.
 - Select Next.

Before you start setting up the Family Rules settings, discuss the family rules together with your child first.



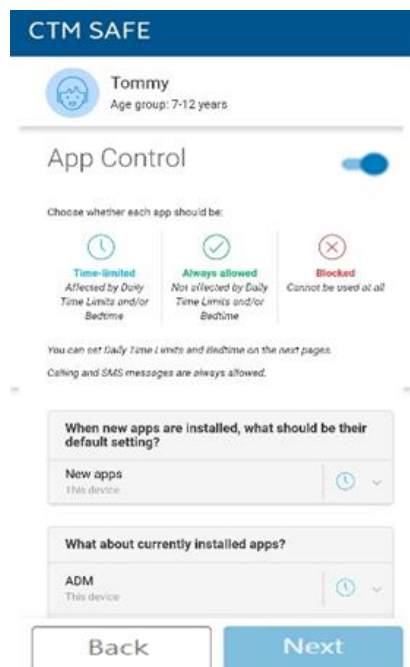
Setting up Family Rules for children

Under **FAMILY RULES**, check the different settings and edit them if need be:

a. App Control (for Android only)

With App Control, you can select which apps are allowed when you set daily time limits and bedtimes.

- Under **DEFAULT SETTING**, you can define how a newly installed app is treated by App Control:
 - ✓ Time-limited – This means that the app use is restricted by daily time limits and bedtime limits.
 - ✓ Always blocked – This means that the app cannot be used at all.
- Under **ALL CURRENT APPS**, you can see the apps that have already been installed on the device. For each app, you can select individually how it is treated by App Control:
 - ✓ Time-limited – This means that the app use is restricted by daily time limits and bedtime limits.
 - ✓ Always allowed – This means that the app use is not restricted by daily time limits nor bedtime limits.
 - ✓ Always blocked – This means that the app cannot be used at all.

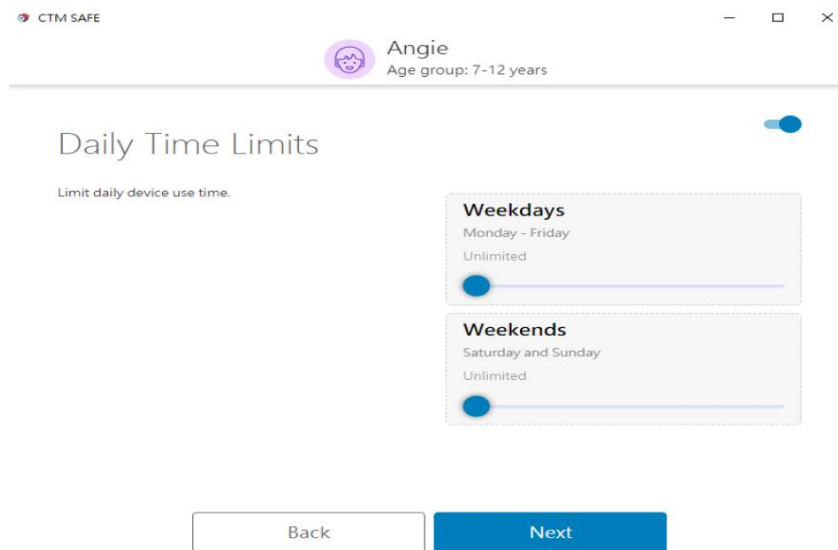


b. **Daily Time Limits**

You can control how long the child is allowed to use the Internet every day. For example, you can allow access for only one hour per day. You can set different limits for weekdays and weekends.

To set the allowed times, open the **Daily time limits** pane to set the maximum number of hours that the child is allowed to use the device each day.

If you do not want to limit the amount of time that the child spends on the device each day, make sure that the allowed number of hours is set to **Unlimited**.



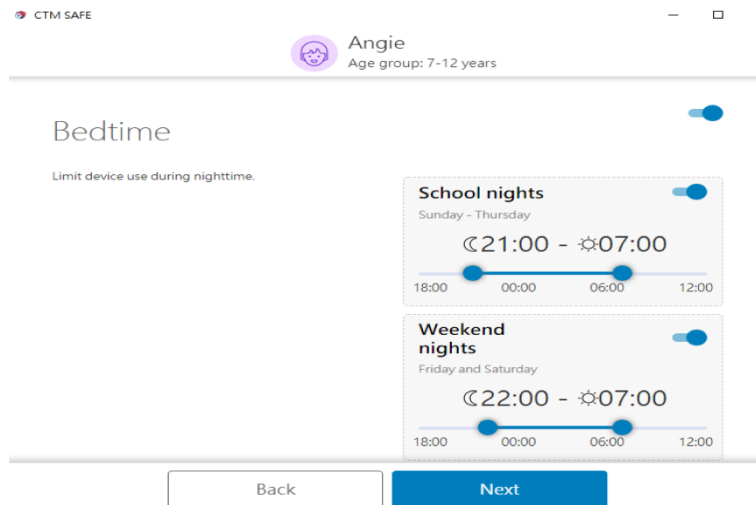
c. **Bedtime**

You can control when the child is allowed to use the Internet. For example, you can allow access only until 8 o'clock in the evening.

Select **Edit** in the **Bedtime** pane to prevent the use of the device during night-time. You can set a different bedtime for weekdays and weekends.

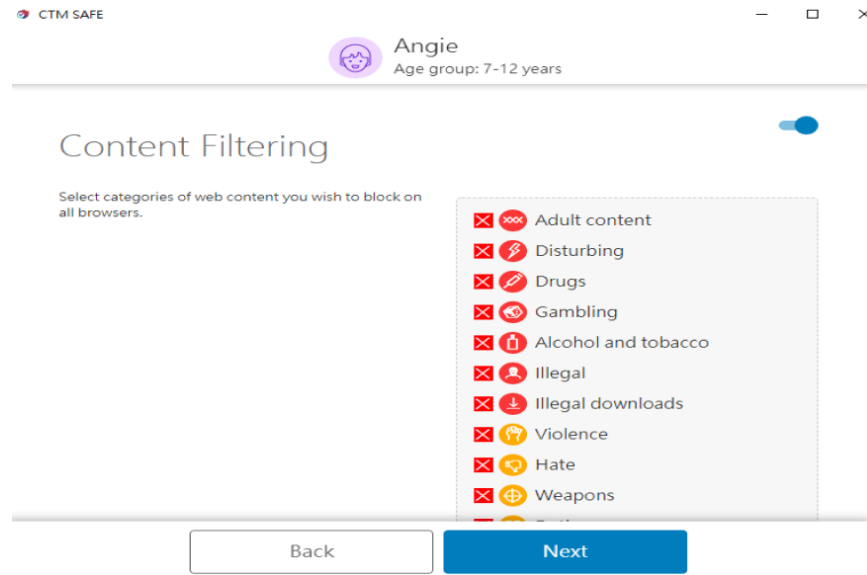
- To set the bedtime on weekdays, turn on **School Nights** and set the time when the bedtime starts and ends.
- To set the bedtime on weekends, turn on **Weekends** and set the time when the bedtime starts and ends.

Note: *If you remove the time limits, your child can use the computer at any time.*



d. **Content Filtering**

You can block access to web sites and pages that contain unsuitable content, keeping your children safe from the many threats of the Internet by limiting the types of content they can view while browsing the web.



Web Content types

You can block access to several content types:

1. **Adult content:** Websites that are aimed at an adult audience with content that is clearly sexual or containing sexual innuendo. For example, sex shop sites or sexually oriented nudity.
2. **Disturbing:** Websites that contain images, explanations, or video games that can be disturbing. This category contains information, images and videos that are disgusting, gruesome or scary, which can potentially disturb younger children.
3. **Drugs:** Websites that promote drug use. For example, sites that provide information on purchasing, growing, or selling any form of these substances.
4. **Gambling:** Websites where people can bet online using real money or some form of credit. For example, online gambling and lottery websites, and blogs and forums that contain information about gambling online or in real life.
5. **Alcohol and tobacco:** Websites that display or promote alcoholic beverages or smoking and tobacco products, including manufacturers such as distilleries, vineyards, and breweries. For example, sites that promote beer festivals and websites of bars and night clubs.
6. **Illegal:** Websites that contain imagery or information that is banned by law.
7. **Illegal downloads:** Unauthorized file sharing or software piracy web sites. For example, sites that provide illegal or questionable access to software, and sites that develop and distribute programs that may compromise networks and systems.
8. **Violence:** Websites that may incite violence or contain gruesome and violent images or videos. For example, sites that contain information on rape, harassment, snuff, bomb, assault, murder, and suicide.
9. **Hate:** Websites that indicate prejudice against a certain religion, race, nationality, gender, age, disability, or sexual orientation. For example, sites that promote damaging humans, animals, or institutions, or contain descriptions or images of physical assaults against any of them.
10. **Weapons:** Websites that contain information, images, or videos of weapons or anything that can be used as a weapon to inflict harm to a human or animal, including organizations that promote these weapons, such as hunting and shooting clubs. This category includes toy weapons such as paintball guns, airguns, and bb guns.
11. **Dating:** Websites that provide a portal for finding romantic or sexual partners. For example, matchmaking sites or mail-order bride sites.
12. **Shopping and auctions:** Websites where people can purchase any products or services, including sites that contain catalogues of items that facilitate online ordering and purchasing and sites that provide information on ordering and buying items online.

13. **Social networks:** Networking portals that connect people in general or with a certain group of people for socialization, business interactions, and so on. For example, sites where you can create a member profile to share your personal and professional interests. This includes social media sites such as Twitter.
14. **Unknown:** Websites that are not categorized. You can use this category to block content that is unknown.

Browsing Internet Safely

Secure browsing helps you use the Internet safely by preventing unintentional access to harmful web sites and adding extra security to your web browser during online banking sessions.

It checks the safety of a web site automatically before you access the site. If the site is rated as suspicious or harmful, the product blocks access to the site. The safety rating of a web site is based on information from several sources, such as F-Secure malware analysts and F-Secure partners.

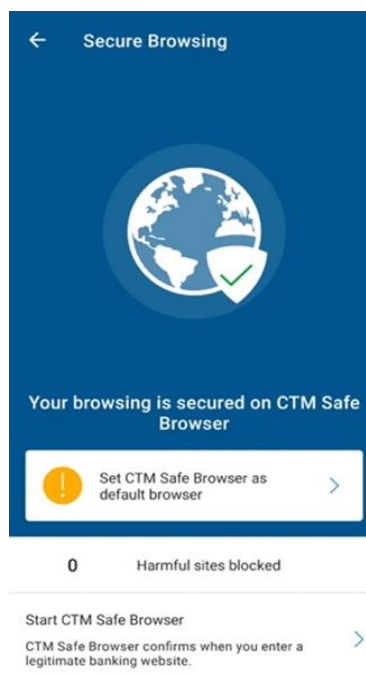
Note: Secure browsing works only with the CTM SAFE browser. Disable Safari and other browsers to prevent your children from using them and protect the product settings with the product password.

CTM SAFE Browser

To properly make use of CTM SAFE and get the most out of the product, set Safe Browser as the default or primary browser on the device. Once Safe browsing is turned on in your app, it automatically starts when you open a supported webpage.

This is particularly important if the device belongs to a child, and you want to protect their online activity. You can consider removing the other browsers from the child's device to ensure that the child cannot access other sites using other browsers.

CTM SAFE Browser



Disabling Safari on children's devices (For iOS Only)

CTM SAFE cannot prevent Safari or other browsers from accessing unsafe sites. We recommend that you disable Safari and other browsers when using the product.

Especially when using Safe Browser on children's devices, we recommend disabling Safari, as the app cannot prevent Safari or other browsers from accessing unsafe sites.

These are instructions to disable Safari on iOS 13 or newer. By disabling Safari, you can ensure that your child cannot access unsafe sites using Safari. Disable Safari as follows:

1. Open **Settings**.
2. Go to **Screen Time**.
3. Select **Turn on Screen Time**, if it has not been previously turned on, and then follow the instructions on the screen to enable this.
4. Go to **Content & Privacy Restrictions**, and slide the button to turn it on if it has not previously been turned on.
5. Go to **Allowed Apps**.
6. Find **Safari** in the list of apps and slide the button to turn it off.

Safari is now disabled and will disappear from your favourite apps.

Removing other browsers (For iOS Only)

This topic explains why and how to remove other browsers from iOS devices. By removing all other browsers except Safe Browser, you can maximize your online safety by preventing access to unsafe sites in other browsers.

Especially when using Safe Browser on children's devices, we recommend that you remove all other browsers from your child's iOS device. The SAFE app cannot prevent other browsers from accessing unsafe sites.

To remove other browsers from iOS devices:

1. Press the home button and find the icon of the browser that you want to remove.
2. Press and hold the browser icon. The X symbol will appear in the upper-left corner of the icon.
3. Press X and confirm that you want to remove the browser.

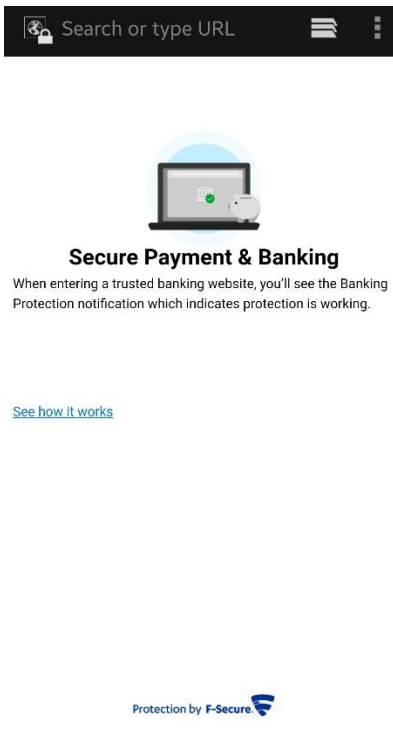
Protecting Online Banking

CTM SAFE Browser protects you against harmful software or sites that may collect and send out the personal details that you enter during an online banking session, including credit card numbers, user account information, and passwords.

When you enter an online banking site, the product will automatically put all other network connections on hold except for the sites you need (and which have been verified as safe by F-Secure). All other connections are restored when your session on the banking site is over. This additional security layer stops harmful software from sending out your private details.

After you have turned on Secure browsing, it automatically protects online banking sessions in the CTM SAFE Browser.

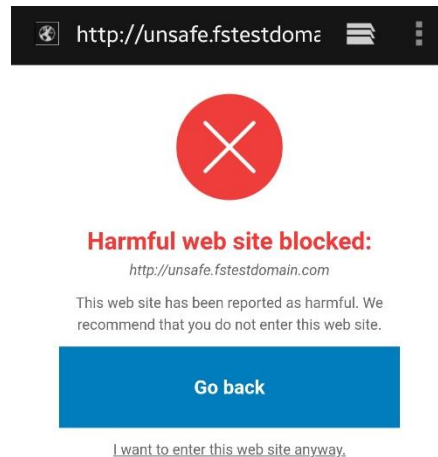
Note: Safe browsing does not protect your online banking session if you use any other browser.



Returning from or entering a blocked website

If you accidentally access a harmful website when using Safe Browser, the app will automatically block access to it and will show a page telling you that the website you have just tried to enter is harmful. There are two things that you can do after this:

1. If you want to return to the original page , select **Go back** on the page.
2. If you know that the site is safe and you still want to enter the site even though Safe Browser has blocked it, follow the **I want to enter this web site anyway** link on the page.



Protecting your device against Virus & Threats

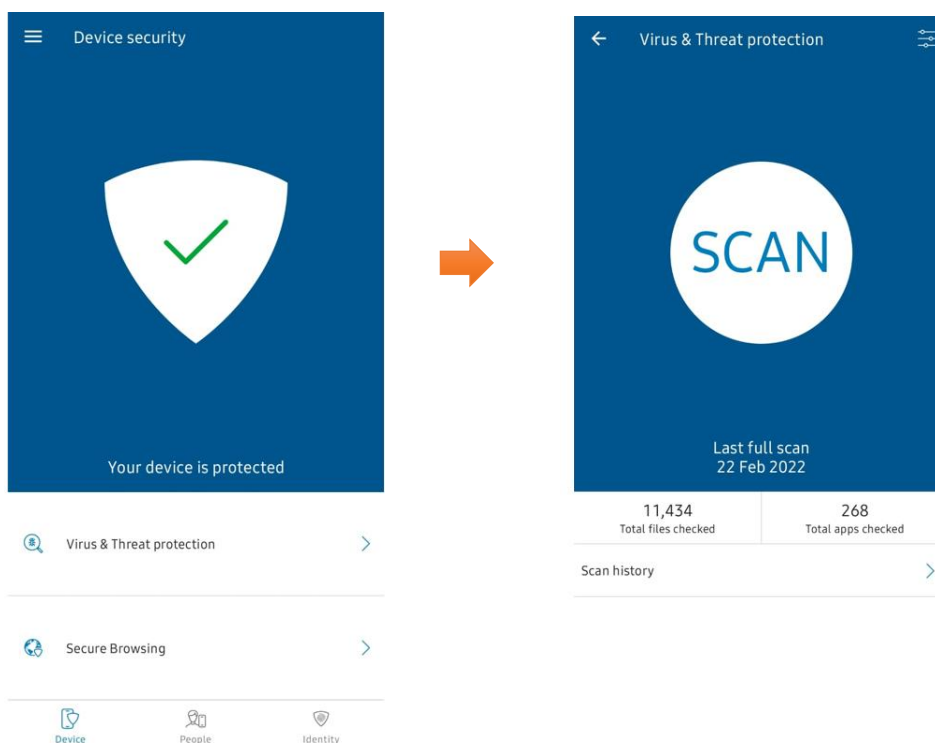
CTM SAFE scans your device for viruses, harmful content, and other threats to your device or your data. When scanning is turned on, the app will scan the device daily automatically. The app will also scan installed programs and inserted memory cards for viruses, spyware, and riskware automatically. You can also manually prompt a scan at any time, or schedule periodic scans.

Scan and remove virus manually (For Android Only)

You can also scan your device for viruses and other malicious code any time you want.

To manually scan files on your device:

1. Open the app and select **Virus & Threat protection**.
2. Select **SCAN**. The scan will start.
3. After the scan is finished, the product will show the following information:
 - Total files checked - the number of the files that were scanned
 - Total apps checked - the number of applications that were scanned
4. Once a scan is complete, you can check the results.



5. If the app detects a file containing a virus or other malicious code during scanning, a notification will appear in the **Virus & Threat protection** view. You may see the following notification, for example:
 - 1 Detection - Potentially unwanted app
 - 1 Infection - Harmful app detected
6. To assess the detected file, open **Scan details** page:
 - a) In **Virus & Threat protection**, select the notification on the main view under **SCAN**.
 - b) To remove the file or files, select **Remove all detections** to remove them from your device simultaneously.
 - c) To see more details, select the notification to check the details of the detection. You may see the following details:
 - App name
 - Package name
 - Problems detected
 - Size
 - d) Select **Remove** to remove the file. The file or files will be removed completely from your device.

You can find descriptions and information on viruses, Trojans, worms, and other forms of unwanted software on the F-Secure web site: [F-Secure Labs: Threat Descriptions](#).

App notifications (For Android Only)

The app will send you notifications about certain app activities, for example, in the following situations:

- When the app is running
- When the app is carrying out a scan
- When a child's time limits are about to come to an end

Some of these notifications are always visible, while others will disappear after a certain period.

By default, the notifications that come from the app are turned on. We recommend keeping these default settings on to ensure the best protection. Important notifications, such as when an installed app is known to be harmful, are shown even if you turn off the notifications.

Technical Support

Here you can find information that can help you solve your technical issues.



Sending logs to support

This topic explains how to send log files to support if requested.

At times, to be able to solve an issue, our technical support may need more detailed information about your device.

To create and send log files to support:

1. Open the app.

- Android, select  > **About**.
- iOS, select  > **HELP** > **About CTM SAFE**.

2. Tap the version number seven times until **SEND LOG** is shown.





3. Select **SEND LOG** and then select your preferred email app.

The message opens in the email app with the recipient field prepopulated and the log(s) attached.

4. Describe the issue in more detail and send the message to our support. An ID number will be provided after the message is sent.

5. You can provide the ID number when contacting customer support.

CTM SAFE features per platform

	 PC	 Mac	 Android	 iOS
Malware Protection	•	•	•	-
Virus Scanning	•	•	•	-
Ransomware Protection	•	-	-	-
Browsing Protection	•	•	•	•
Banking Protection	•	•	•	•
Family Rules - Remote Management	•	•	•	•
Family Rules – Content Filtering	•	•	•	•
Family Rules – Using Time Limitation	•	•	•	•
Family Rules – Application Control	-	-	•	-

Contact us

Should you have any queries, please contact CTM No. 1 Hotline : 1000.