



CTM SAFE

User Guide

(Windows / macOS)

March 2022

Table of contents

Introduction	3
<i>System requirements for Microsoft Windows computer</i>	<i>4</i>
<i>System requirements for Apple macOS computer</i>	<i>4</i>
Safety Butler Service (Management portal)	5
<i>First time login.....</i>	<i>6</i>
<i>Forget password.....</i>	<i>7</i>
Getting started to use CTM SAFE.....	8
Installing CTM SAFE onto a different device.....	10
<i>Sharing protection with a family or friend.....</i>	<i>11</i>
<i>Protection status icons.....</i>	<i>13</i>
Making browsing Internet safe for children with Family Rules	14
<i>Adding a new device for children</i>	<i>15</i>
<i>Setting up Family Rules for children.....</i>	<i>17</i>
<i>Web Content types.....</i>	<i>21</i>
Protecting online banking and shopping	23
<i>Checking that browser extensions are in use</i>	<i>24</i>
<i>Enabling browser extension for Safari (For Mac only).....</i>	<i>25</i>
<i>Browsing safely with Safety ratings</i>	<i>26</i>
<i>Returning from or entering a blocked website.....</i>	<i>27</i>
Protecting your device against Virus & Threats	28
<i>Using real-time scanning.....</i>	<i>28</i>
<i>Running a virus scan manually.....</i>	<i>29</i>
Technical Support	32
<i>Using the support tool.....</i>	<i>32</i>
CTM SAFE features per platform	33
<i>Contact us.....</i>	<i>33</i>

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 or the in-app Peoples & Devices view gives you 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 applications on all your devices to protect your security and privacy. CTM 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 the connection when you access an online banking portal.

System requirements for Microsoft Windows computer

Version: CTM SAFE for PC Release 18.2

Operating Systems supported:

- Windows 11.
- Windows 10, Anniversary Update or newer.
- Windows 8.1.
- Windows 7, service pack 1.

Minimum system requirements:

- Processor: 1 gigahertz (GHz) or faster*
- Memory: 1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit)
- Hard disk space: 600 MB available hard disk space
- An internet connection is required to validate your subscription and receive updates. Internet access (ISP) fees might apply.

*ARM- based tablets are not supported.

Supported Browsers:

- Google Chrome.
- Mozilla Firefox.
- Microsoft Edge (Chromium-based).

System requirements for Apple macOS computer

Version: CTM SAFE for Mac Release 18.1

Operating systems supported:

- macOS version 12.0 “Monterey”
- macOS version 11.0 “Big Sur”
- macOS version 10.15 “Catalina” (10.15.5 and higher)

Recommended system requirements:

- Intel processor
- 250 MB of free disk space
- 1 GB or more of memory is recommended
- Internet Connection: An Internet connection is required to validate your subscription and receive updates

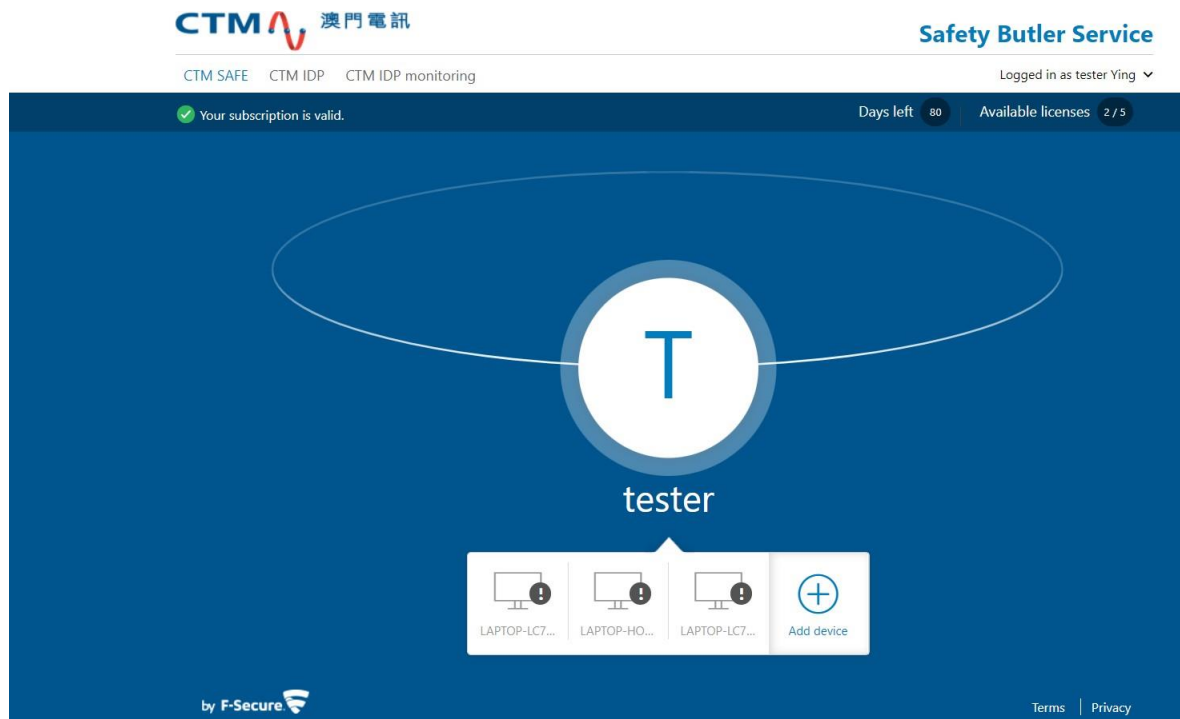
Supported Browsers:

- Google Chrome.
- Mozilla Firefox.
- Safari.

Safety Butler Service (Management portal)

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

Once you have created your Safety Butler account, you can manage your device, view your subscription status, and add your family members to share your Safety Butler Service. You can use the Safety Butler Service 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 conveniently purchase them through the Safety Butler Service.



First time login

1. You will receive a Welcome SMS on your phone
2. Enter the phone number registered when applying for the service (+853 is required) and Temp password provided in Welcome SMS.
3. On first time login to the portal, you will be requested to set your own password.
4. The Safety Butler service can now be used.



Log in

+85362887050

Log in

[Forgot your password?](#)



Change your password

電話號碼
+85362887050

Password*

Show password

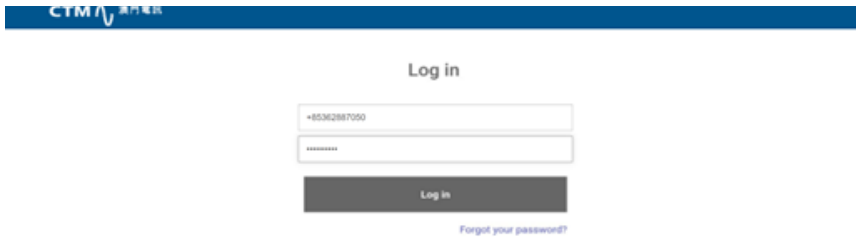
Change Cancel



Forget password

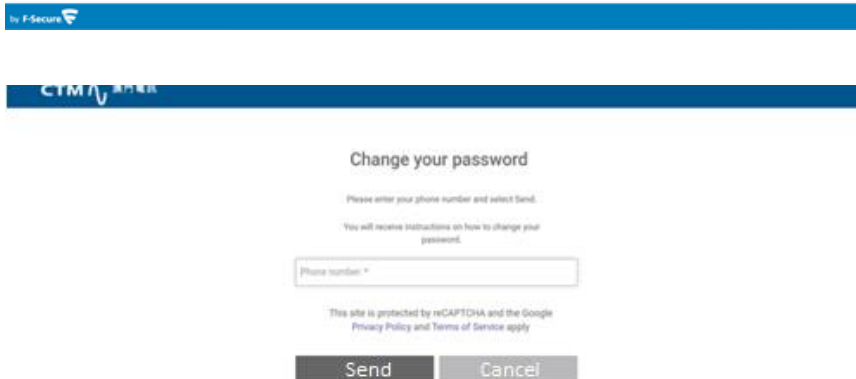
If you forget the account password of the Safety Butler Service, you can create a new password through the process of forget password:

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



The screenshot shows the login page with the following elements:

- Header: CIMV 智慧車
- Title: Log in
- Phone number input field: +85362887050
- Password input field: [Redacted]
- Log in button
- Link: Forget your password?



The screenshot shows the 'Change your password' page with the following elements:

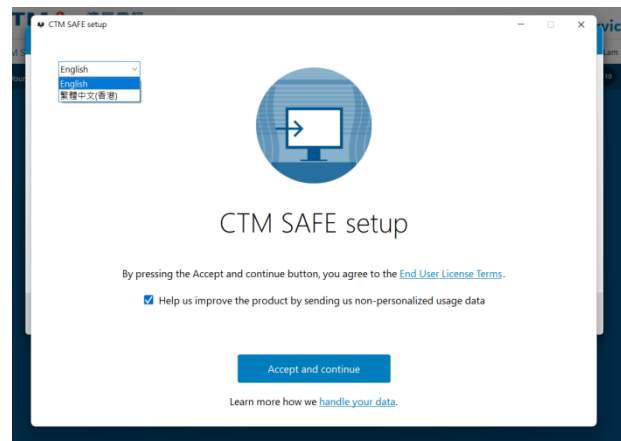
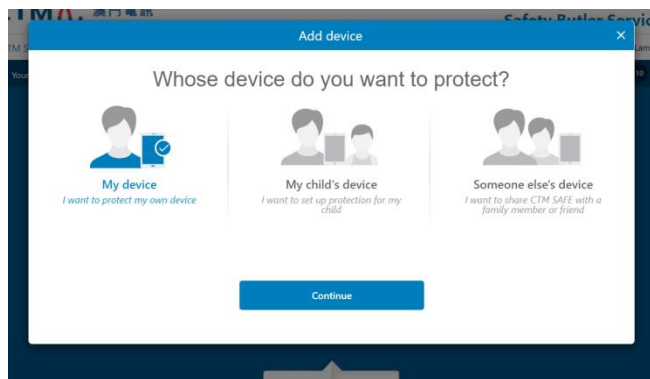
- Header: by F-Secure
- Header: CIMV 智慧車
- Title: Change your password
- Text: Please enter your phone number and select Send.
- Text: You will receive instructions on how to change your password.
- Phone number input field: Phone number *
- Text: This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.
- Buttons: Send, Cancel

To reset your password, tap the link: <https://accounts-apac.f-secure.com/OneID/portal/ui/password-reset/read-hash?hash=26bc53ca76c14f139a45e10ed24275f6>

Getting started to use CTM SAFE

You can download and install CTM SAFE through the Safety Butler Service. You can also send the product to 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 with your mobile number (**+853 is required**) and password.
2. Select **CTM SAFE**, click **Add device**.
Choose whose device you want to add, select **My Device** (if installing to your own devices) and then click **Continue**.
3. Select **This device** to install CTM SAFE on your current device, then select **Downloading for Windows/Mac**
4. Open the downloaded installer and choose the language on the top left corner. Select **Accept and Continue** to download and install CTM SAFE. Your device may need to restart during the process to verify the subscription and install the latest updates.
5. After the installation is complete, open and login to CTM SAFE to activate the product. The product does not protect your device before you activate it.



After the installation is complete, log in to CTM SAFE to activate the product. After activation, your device will be protected.

CTM 澳門電訊

Log in

Phone number

Password

Log in

[Forgot your password?](#)



CTM SAFE

CTM 澳門電訊

Protecting tester Ying
Subscription valid until 2/5/2022

You are protected

Viruses & Threats
Automatic scanning is protecting you in real time.
Scan

Secure Browsing & Banking
Surf carefree, malicious websites are blocked.

People & Devices
Manage everything protected by your CTM SAFE subscription.
Manage

Recent events

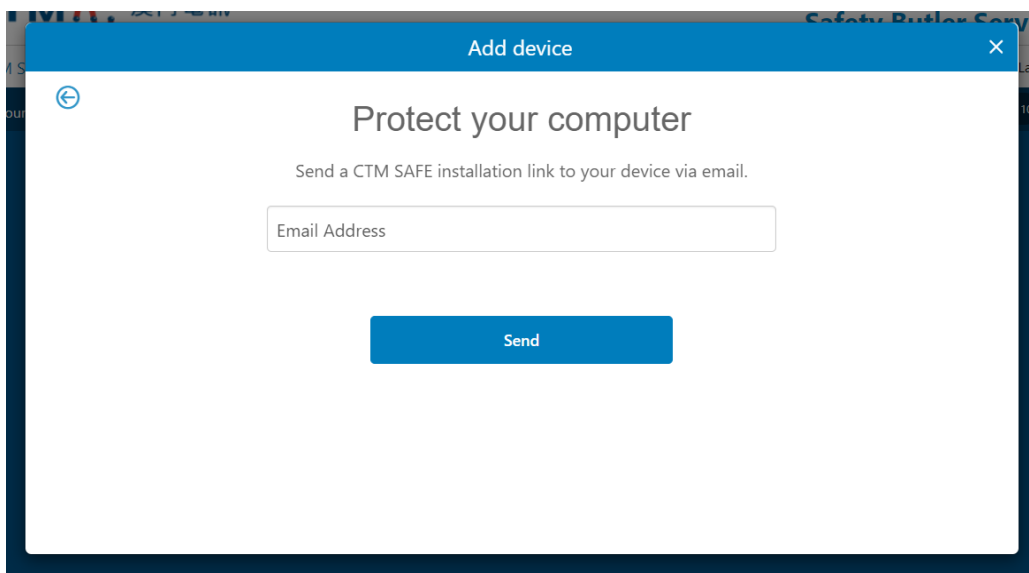
9/2/2022	Subscription is now valid until 5/2/2022
9/2/2022	CTM SAFE was installed

Passwords & Identity
Your subscription also includes CTM IDP.
Install

[View full timeline](#)

Installing CTM SAFE onto a different device

- a. Select the device type, and then press **Continue**
- b. Choose to receive the Welcome SMS through SMS, and then enter the number for the device you would like to install CTM SAFE on
If the device does not have a mobile number, select choose to send the Welcome SMS by email
- c. Select **Send**
- d. Follow the instructions sent in the SMS to install the application



Sharing protection with a family or friend

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 protection with someone else:

1. On CTM SAFE, select **+ ADD DEVICE**.
2. Select **Someone else's device > CONTINUE**.
3. 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.
4. Select **SEND INVITATION**. The user will receive an invitation to join your group
5. This person will receive the invitation email and now has an account that allows 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 that 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.

Protection status icons

The protection status icon shows you the overall status of the product and its features.

Status icon	Status name	Description
	OK	Your computer is protected. Features are turned on and working properly.
	Expired	Your computer is not protected. The subscription has expired.
	Expired and disabled	Your computer is not protected. The subscription has expired, and the product has been disabled.
	Disabled; malfunction	Your computer is not fully or at all protected. The product requires immediate action, for example, a critical feature is turned off or malfunctioning, or updates are very old.
	Disabled	Your computer is not fully protected. The product requires your attention, for example, a security feature such as browsing protection is turned off.
	Updating	The protection is being set up. The product is updating.

Examples of status messages that you may see:

- **Google Chrome browser extension is not in use**
- **Mozilla Firefox browser extension is not in use**
- **Microsoft Edge browser extension is not in use**
- **Your subscription has expired**

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 they usually browse the web with their mobile devices unsupervised.

Many web sites contain material that you might consider inappropriate for your children. They can get 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:

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

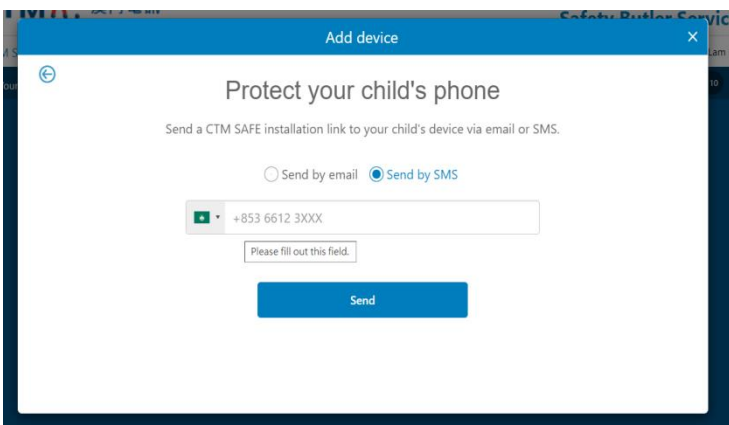
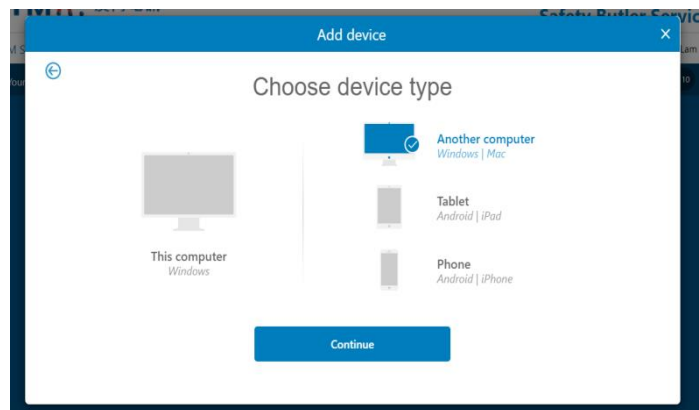
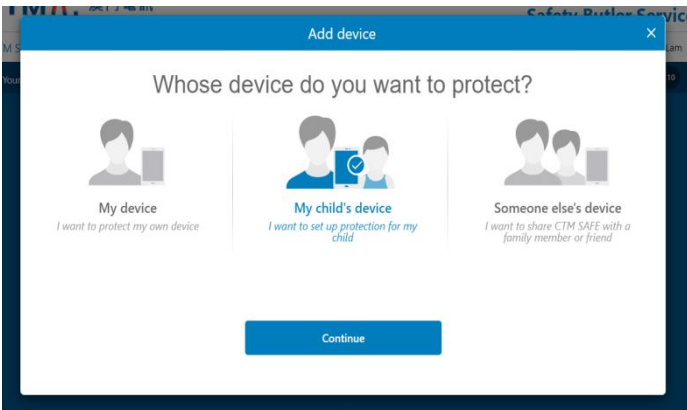
For ease of use, you can manage your child's online activity on your own device. This is a versatile way to make changes and add or remove restrictions on the fly without having your child's device physically with you.

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

Adding a new device for children

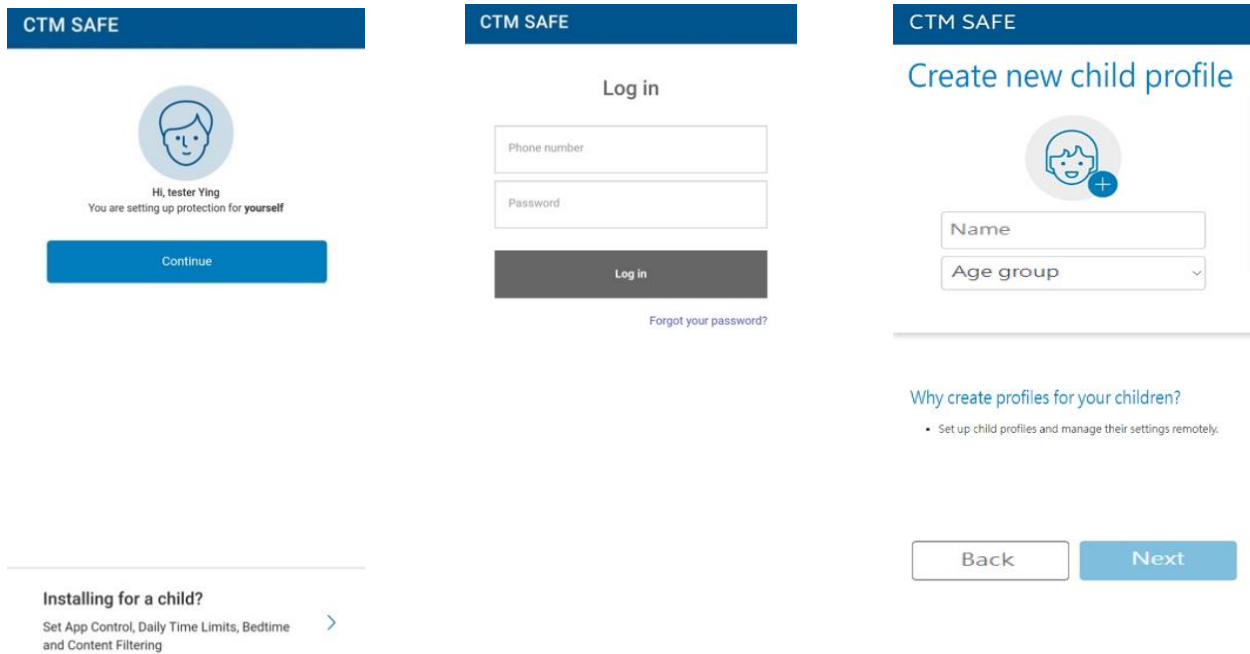
To start using Family Rules, install CTM SAFE on your child's device and set up a child profile. You can set up Family Rules when installing the CTM SAFE app or any time afterwards. Once that's done, you can start protecting your child's online activity.

1. In **CTM SAFE**, click **Add device**.
2. Select **My Child's Device**, and then click **Continue**.
3. Select the device type 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. Select from the existing profiles listed or create a 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.



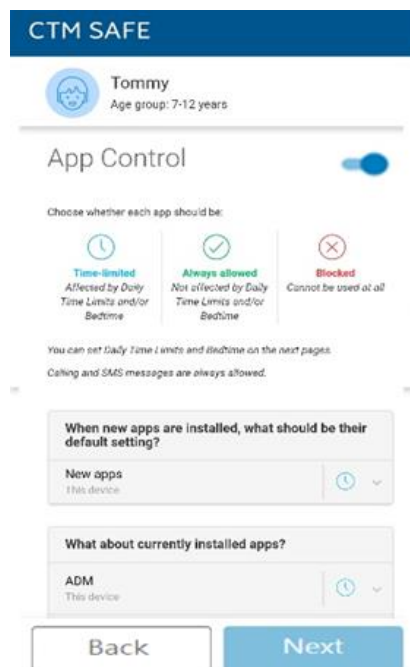
Setting up Family Rules for children

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 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 individually select 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.

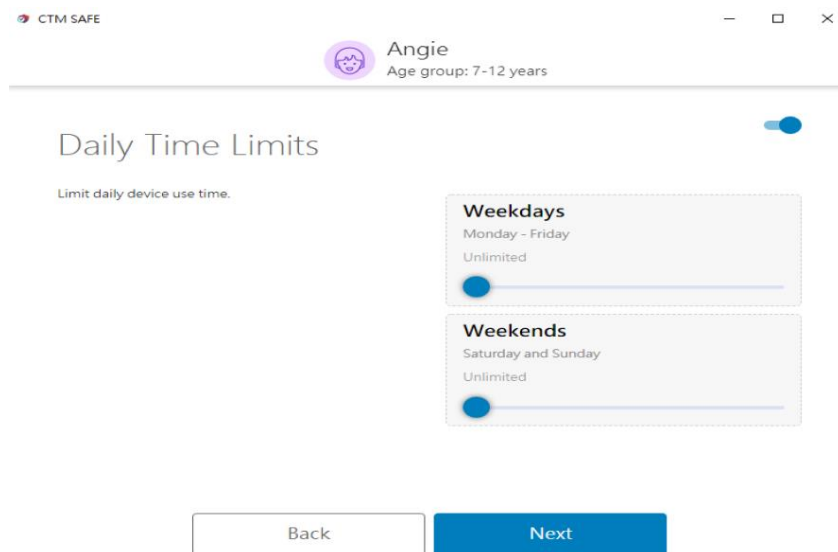


b. **Daily Time Limits**

You can control how long the child is allowed to use the Internet. 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.



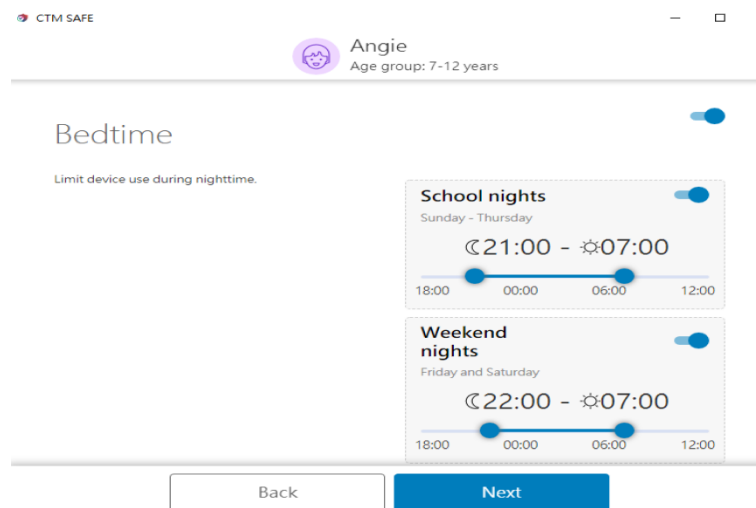
c. Bedtime

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.

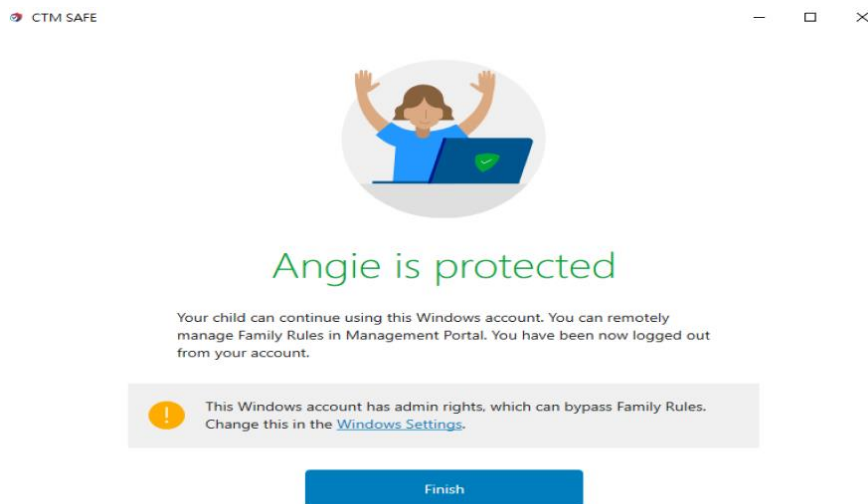
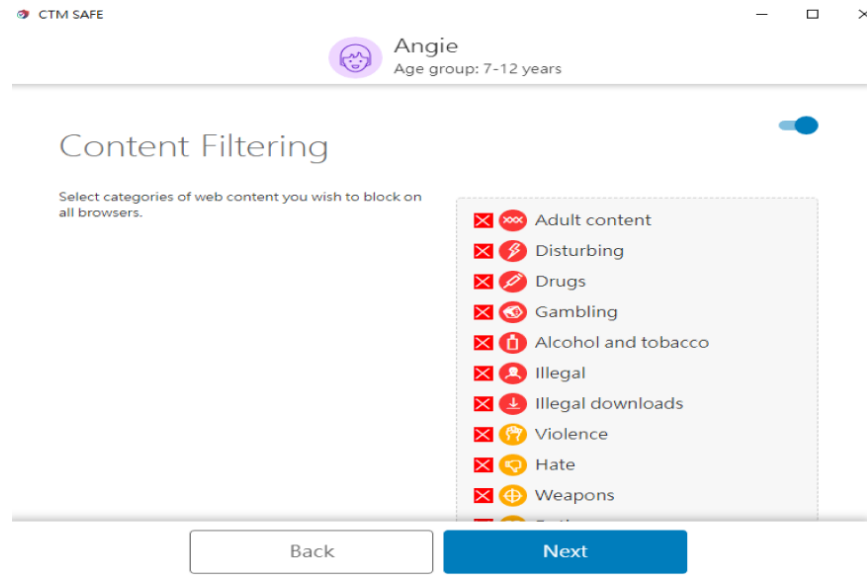
- To set the bedtime on weekdays, turn on **School Nights** and set the time when the bedtime starts and ends.
- To set the bedtime on weekends, turn on **Weekends** and set the time when the bedtime starts and ends.

Note: *If you remove the time limits, your child will be able to use the computer at any time.*



d. Content Filtering

You can block access to web sites and pages that contain unsuitable content and keep 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.

Protecting online banking and shopping

When Banking Protection is turned on, it automatically detects when you access online banking websites or other sites that contain sensitive information.

Banking Protection adds another layer of security to prevent attackers from interfering with your confidential transactions and protects you against harmful activity when you access your online bank or make transactions online. Banking Protection automatically detects secure connections to online banking websites and blocks any connections that do not go to the intended site. When you are finished using online banking, it will resume other connections.

Banking Protection currently supports the following web browsers:

- Safari (macOS)
- Firefox
- Google Chrome
- Microsoft Edge (Chromium)

Once you close the browser or finish the banking session, you do not have to do anything. **Banking Protection** automatically detects that the banking session is over and closes the **Banking Protection** frame.

By default, Banking Protection is enabled. If it is not enabled, turn on Banking Protection in the following way.

1. On macOS computer:
 1. Select the CTM SAFE icon in the menu bar.
 2. Select **Preferences** from the menu.
 3. Select the **Secure Browsing** tab.
 4. Select the lock icon in the bottom-left corner.

Note: You need administrative rights to change these settings.
 5. Select **Turn on Banking Protection**.
2. On Windows computer:
 1. On the main view, select **Secure Browsing & Banking**.
 2. On the **Secure Browsing & Banking** view, select **Settings**.
 3. Select **Edit settings**.

Note: You need administrative rights to change the settings.
 4. Turn on **Banking Protection**.

Note: *Banking Protection requires browser extensions to be turned on.*

Checking that browser extensions are in use

Browsing protection **requires** browser extensions to be turned on to be able to protect your web browsing, online banking, and shopping, and to show you secure information while you are browsing the internet. Therefore, make sure that browser extensions are turned on.

When you open your browser, it will display a notification about the newly installed extension, and you may need to enable it. If you miss the notification, the main view of the product will show you if the browser extension has not yet been set up. The easiest way to set up the extension for your browser is to select Set up from the notification shown on the product's main view and follow the on-screen instructions.

- If you use **Firefox**, select **Install Firefox extension** under **Browser extensions** and then select **Add**. The extension will be added and enabled for Firefox.
- If you use **Chrome**, select the **Open Chrome Web Store** link under **Browser extensions**. The Browsing Protection by F-Secure page will open in the Chrome Web Store. If the extension has already been installed on Chrome but is disabled, select the **Enable this item** link from the banner on top of the page. If the extension has not been installed yet, select **Add to Chrome > Add extension**. The extension will be added and enabled for Chrome.
- If you use **Microsoft Edge**, select the **Open Edge Add-ons** link under **Browser extensions**. The Browsing Protection by F-Secure page will open in Edge Add-ons. If the extension has already been installed on Microsoft Edge but is disabled, select **Turn on** to enable it. If the extension has not been installed yet, select **Get > Add extension**. The extension will be added and enabled for Microsoft Edge.

"Browsing Protection by F-Secure" added to Microsoft Edge

Another program on your computer added an extension that may change the way Microsoft Edge works.

The extension can:

- Read and change all your data on all websites
- Communicate with cooperating native applications

Turn on extension

Remove extension

Enabling browser extension for Safari (For Mac only)

You must enable the browser extension for Safari to be able to use the browser safely. The product installs the browser extension automatically, and the only thing you need to do is to make sure that the extension is turned on.







To ensure that the browser extension for Safari is turned on:

1. Select the product icon in the menu bar.
2. Select **Preferences** from the menu.
3. Open the **Secure Browsing** tab.
4. Select **Install browser extension**.
The **Browsing protection installation** window opens.
5. From the drop-down, select **Safari** and then **Enable now**.
6. In the **Extensions** dialog, make sure that **Browsing protection** is selected.

You can now use Safari to browse the internet safely.

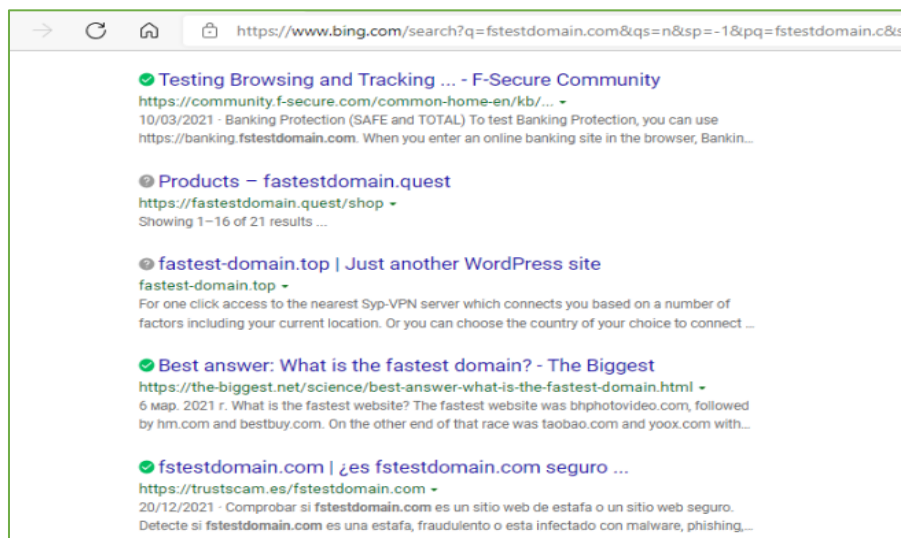
Browsing safely with Safety ratings

Browsing protection shows safety ratings for websites on search engine results. Color-coded icons show the safety rating of the current site. The safety rating of each link on search results is also shown with the same icons:

	The site is safe to the best of our knowledge. We did not find anything suspicious in the web site.
	The site is suspicious, and we recommend that you are careful when you visit this web site. Avoid downloading any files or providing any personal information.
	The site is harmful. We recommend that you avoid visiting this web site.
	We have not analyzed the web site yet or no information is currently available for it.
	The access to this web site is never blocked.
	Administrator has blocked this site and you cannot visit it.

Safety ratings are available on the following search sites:

- Google
- Bing
- Yahoo
- DuckDuckGo

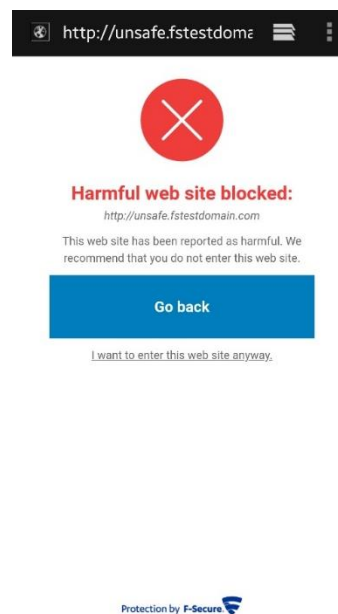
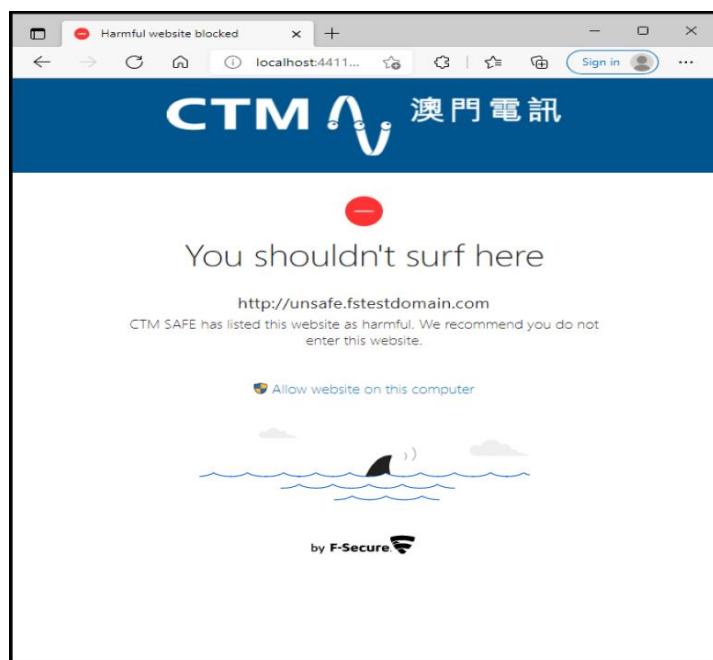


Returning from or entering a blocked website

If you accidentally access a harmful website when using Safe Browser, the app automatically blocks access to it and shows a page telling you that the website you have just tried entering is harmful.

If you still want to enter the website, select **Allow website on this computer > Allow**.

1. Enter your administrator password and select **OK**.
2. The blocked website will open. Also, the product will add the website to the allowed websites list.



Protecting your device against Virus & Threats

The app 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.

CTM SAFE automatically scans your local hard drives, any removable media (such as portable drives or DVDs), and any content that you download. The product also watches your computer for any changes that may suggest that you have harmful files on your computer. When the product detects any dangerous system changes, for example changes in system settings or attempts to change important system processes, its DeepGuard component stops the application from running it as it can be harmful.

Using real-time scanning

Keep real-time scanning turned on to remove harmful files from your computer before they can harm it.

We recommend that you keep Virus protection turned on all the time. You can also scan files manually and set up scheduled scans if you want to make sure that there are no harmful files on your computer or to scan files that you have excluded from the real-time scan.

To make sure that real-time scanning is on (Windows):

1. On the main view of CTM SAFE, select Viruses & Threats.
2. Select "Settings".
3. Select "Edit settings".

Note: You need administrative rights to change the settings.

4. Turn on "Virus Protection".

Running a virus scan manually

You can scan your entire computer to be completely sure that it is free of harmful files or unwanted applications.

The full computer scan scans all internal and external hard drives for viruses, spyware, and potentially unwanted applications. It also checks for items that are possibly hidden by a rootkit. The full computer scan may take a long time to complete. You can also only scan the parts of your system that contain installed applications to find and remove unwanted applications and harmful items on your computer more efficiently.

For Windows, to scan your computer, follow these instructions:

1. Open CTM SAFE and select Viruses and Threats.
2. Select Settings
3. If you wish to change the scan settings, select Change scan settings
4. Select either Quick scan or Full computer scan.
5. If the virus scan finds any harmful items, it shows you the list of harmful items that it detected.
6. Click the detected item to choose how you want to handle the harmful content.

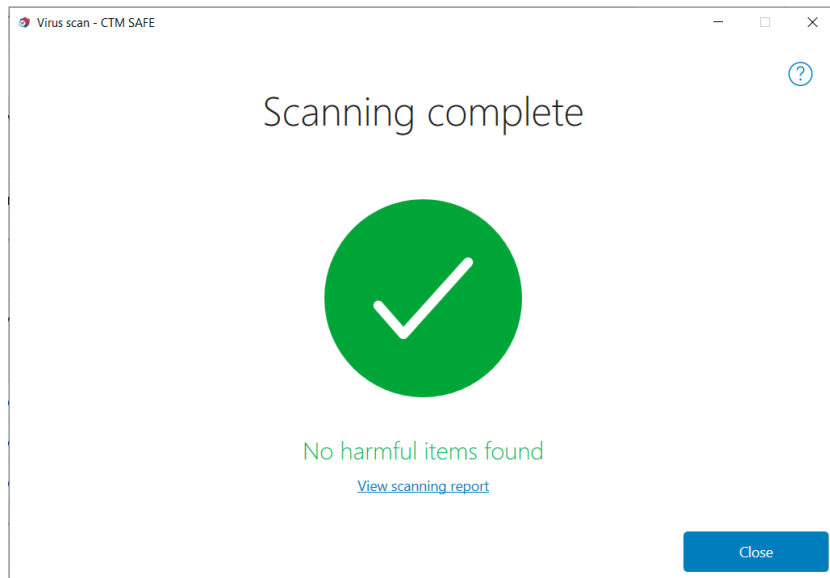
Options	Description
Clean up	Clean the files automatically. Files that cannot be cleaned are quarantined.
Quarantine	Store the files in a safe place where they cannot spread or harm your computer.
Delete	Permanently remove the files from your computer.
Skip	Do nothing for now and leave the files on your computer.
Exclude	Allow the application to run and exclude it from future scans.

Note: Some options are not available for all harmful item types.

7. Select Handle all to start the cleaning process.
8. The virus scan shows the results and the number of harmful items that were cleaned.

Note: The virus scan may require that you restart your computer to complete the cleaning process. If the cleaning requires a computer restart, select Restart to finish cleaning harmful items and restart your computer.

9. You can see the results of the latest virus scan by selecting Open last scanning report.



Scan report - CTM SAFE

Wednesday, 9 February 2022 5:47:19 pm - 5:47:58 pm (UTC+08:00)

Computer name: LAPTOP-LC7CDOU

Scan type: Virus scan

Targets:

- System

Results

- No harmful items found
- Items scanned: 10942

Version information

Scanning engines:

- F-Secure Capricorn: 18.0.824 (2022-02-09)
- F-Secure Hydra: 6.0.425 (2022-02-09)
- F-Secure Lynx: 2.6.4
- F-Secure Online: 18.10.858
- F-Secure USS: 6.0.150 (2020-04-14)
- F-Secure Virgo: 1.3.24 (2022-02-08)
- F-Secure Virgo Detection: 18.10.858

For macOS, to scan your computer, follow these instructions:

You can scan your Home folder or any location that you specify.

You can manually scan files or folders if you suspect that they may contain some malware. To start the manual scan:

1. Click on CTM SAFE icon in the menu bar.
2. Select Choose what to scan.

Tip: Select Scan Home folder to scan all files in your Home folder.

A window opens in which you can select which location to scan.

3. If the product finds any malware during the scan, it will show the name and location of the detected malware and will move the infected file to the Trash automatically.

Tip: Empty the Trash to remove infected files permanently.

4. Click "Virus scan" in the homepage to scan for viruses on your computer.

Technical Support

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





Using the support tool

Before contacting support, run the support tool to collect basic information about hardware, operating system, network configuration and installed software.

- To run the support tool on Windows computer:
 1. Open CTM SAFE from the Windows **Start** menu.
 2. On the main view, select the ☰ menu button.
 3. Select **Help & Support**.
 4. Select **Edit settings**.
Note: You need administrative rights to change the settings
 5. Select **Run support tool**.
 6. Select **Run diagnostics** on the **Support Tool** window.
- To run the support tool on Mac computer:
 1. Go to CTM SAFE folder under **Applications** and run the **Support Tool** application.
 2. Select **Run Diagnostics** on the **Support Tool** window.
 3. Enter the administrator password for your computer.
The support tool will start and display the progress of the data collection.
 4. When the data collection is complete, select where you want to save the resulting **tar.gz** archive and then select **Save**.
The support tool will open a **Finder** window showing the saved file.
Note: You need administrative rights to change the settings

The support tool will start and display the progress of the data collection. When the tool has finished running, it will save the collected data to an archive on your desktop. You can provide the collected data (the diagnostics file) 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