



# **CTM IDP (ID PROTECTION)**

## **User Guide**

(Windows /  
macOS)

March 2022

# Table of contents

<b>Introduction .....</b>	<b>3</b>
<i>System requirements.....</i>	<i>3</i>
<b>Safety Butler Service (Management portal) .....</b>	<b>4</b>
<i>First time login.....</i>	<i>5</i>
<i>Forget password.....</i>	<i>6</i>
<b>Getting started .....</b>	<b>7</b>
<b>Installing CTM IDP onto another device .....</b>	<b>8</b>
<i>Sharing protection with a family or friend.....</i>	<i>9</i>
<i>About Master Password .....</i>	<i>10</i>
<i>Setting up and create Master Password.....</i>	<i>10</i>
<i>About recovery code .....</i>	<i>12</i>
<i>Create and save recovery code .....</i>	<i>13</i>
<b>Using ID Monitoring .....</b>	<b>14</b>
<i>Adding your email address for monitoring.....</i>	<i>14</i>
<i>Changing your contact email address.....</i>	<i>17</i>
<b>Vault (Password Manager).....</b>	<b>18</b>
<i>Save your Password or Credit Card Information.....</i>	<i>18</i>
<i>Connect Devices (Synchronize Vault Data).....</i>	<i>19</i>
<b>Using Autofill.....</b>	<b>19</b>
<i>Autofill and built-in browser password managers.....</i>	<i>20</i>
<b>CTM IDP features per platform.....</b>	<b>21</b>
<i>Contact us.....</i>	<i>21</i>

# Introduction

CTM IDP is an app that prevents you from falling victim to identity theft. Most identity theft incidents originate from cyber criminals exploiting users' weak passwords.

Identity theft happens when someone uses another person's identity or personal information, such as name, social security number, credit card number, or online credentials without permission to commit a crime or fraud. Resolving identity theft is not easy. Once information gets exposed, it can stay out there for years.

With CTM IDP, you can do the following:

- Protect your own and your family's personal information against cyber-crime.
- Improve your security by creating strong and unique passwords, and by synchronizing them across all your devices.
- Receive alerts and guidance on how to respond to an incident when your personal information has been found as part of a data breach or data leak.

At F-Secure, we don't collect any of your personal data or information you enter the product, CTM IDP (a.k.a. ID Protection). User of CTM IDP is anonymous to F-Secure, so we have no way of identifying an individual user's data. We never see any of your information at any stage, and therefore we can't decrypt it or hand it over to a third party. The IDP app servers are owned and operated by F-Secure within the European Union in compliance with Finnish law and applicable to EU rules.

## System requirements

CTM IDP supports computers, smartphones and tablets that are running:

- Android 6.0 or later.
- iOS 13 or later.
- Windows 10 or later (ARM-based tablets are not supported).
- macOS 10.14 (Mojave) or later.

# Safety Butler Service (Management portal)

The Safety Butler Service Management portal is an easy-to-use online service you can use to install CTM IDP 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 IDP from one device to another whenever you choose by sending an email or SMS, and manage your subscription remotely.

The screenshot shows the 'Safety Butler Service' management portal. At the top left is the CTM logo with the text '澳門電訊'. The top right says 'Safety Butler Service'. Below the logo are links for 'CTM SAFE' and 'CTM IDP'. The user is logged in as 'John Doe'. A green checkmark indicates 'Your subscription is valid.' and shows 'Available licenses 1 / 6' with a 'Buy more' button. The main section is titled 'CTM IDP' and features an 'Install CTM IDP' button. Below this, there are sections for users: 'John' with a 'Galaxy S8' device and a 'Release license' link; 'Charlie' with 'Charlie's Windows PC' and a 'Release license' link; 'Aaron' with the message 'This user has not installed CTM IDP yet.'; and 'Baron' with the message 'This user has not installed CTM IDP yet.' The bottom left shows 'by F-Secure' and the bottom right has 'Terms | Privacy'.

Logon [Safety Butler Service](#)

## First time login

1. After receiving the Welcome SMS on your device
2. Enter the phone number registered when applying for the service (**+853 is required**) and the Temp password provided in Welcome SMS.
3. On first time login to the portal, you will be requested to set your own password.
4. Your device is now protected by the Safety Butler service.



### Log in

+85362887050

\*\*\*\*\*

Log in

[Forgot your password?](#)



### Change your password

電話號碼  
+85362887050

Password\*

Show password

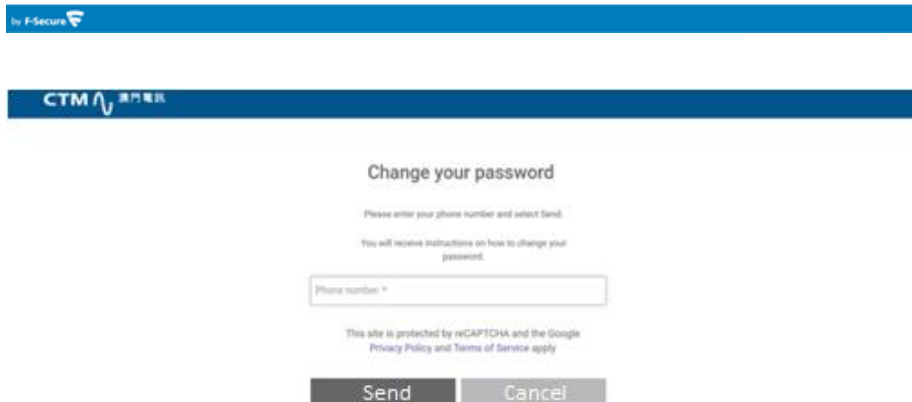
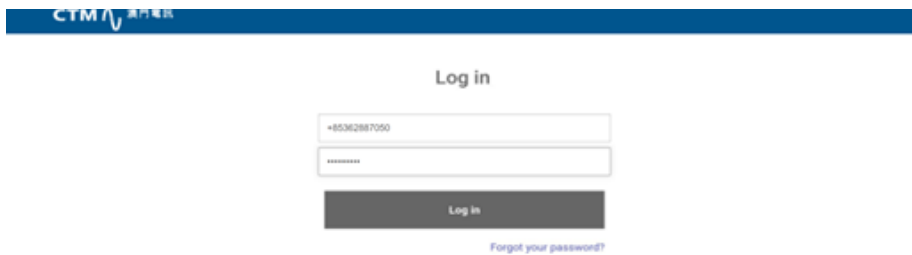
Change Cancel



# Forget password

If you forget 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 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 the SMS received.
4. Set a new password.

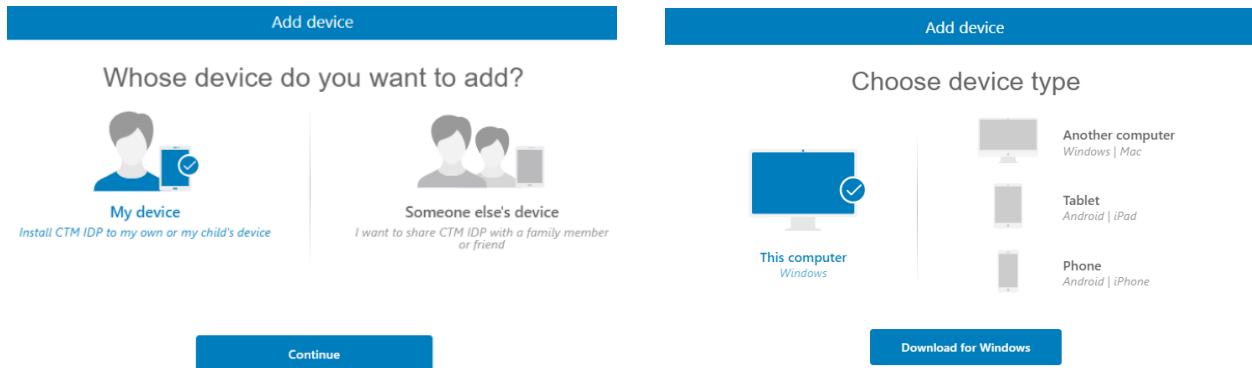


To reset your password, tap the link: <https://accounts-apac.f-secure.com/OneID/portal/ui/password-reset/read-hash?hash=26bc53ca76c14f139a45e1>

# Getting started

You can download and install CTM IDP through the Safety Butler Service. You can also use the Safety Butler Service to send the product to a computer by email or mobile by SMS, making it easy for you to deliver CTM IDP to a device that you want to protect.

1. Login to Safety Butler Service;
2. Select “CTM IDP” from top menu.
3. Choose whose device you want to add, select **My Device** (if installing to your own device) and then click **Continue**.
4. Choose which device to install on

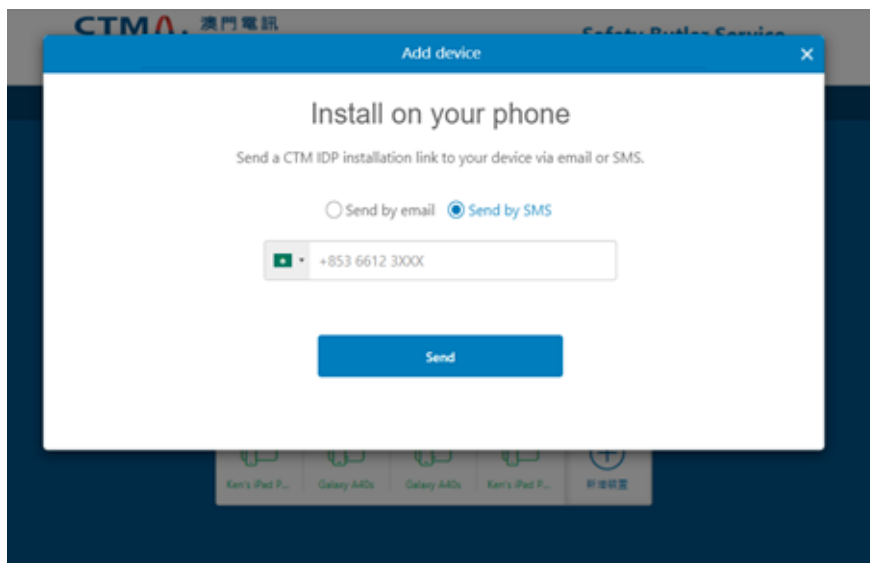
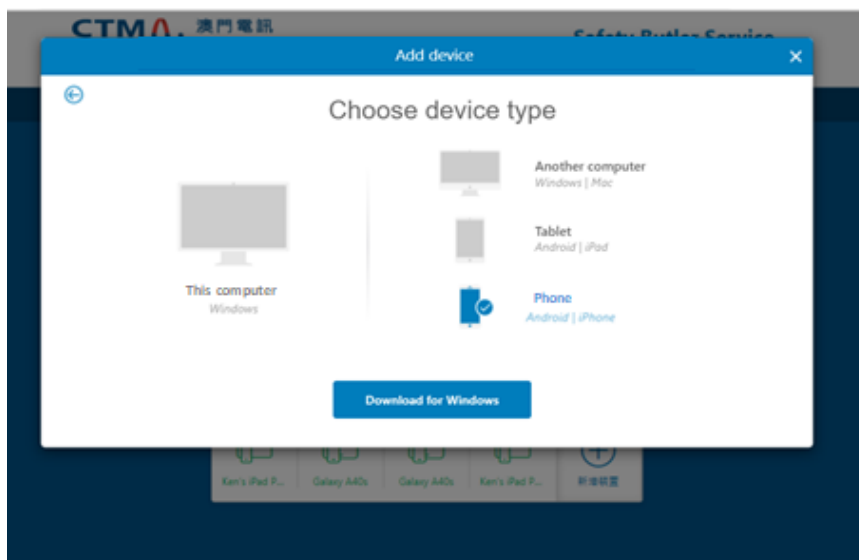


You have now installed CTM IDP on your device, and can start monitoring your email addresses and entering your passwords and other credentials in the app.

**Important:** We strongly recommend that you create a master password recovery code as soon as you have taken IDP into use. The recovery code is the only way for you to regain your CTM IDP master password if you forget it.

# Installing CTM IDP onto another device

5. Choose the correct device type and then click **Continue**
6. Send the Installation link to your device via mobile number.
7. If the device does not have a mobile number, you can choose to send the link via email address.
8. Choose **Send**.
9. Install the application by following the instructions received.



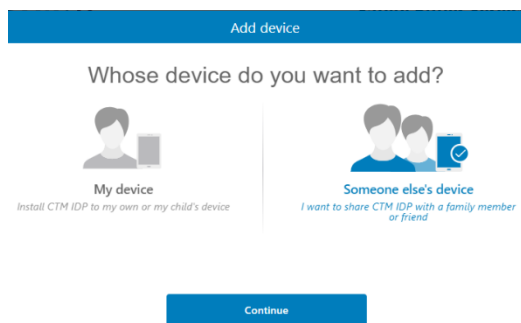


## Sharing protection with a family or friend

When you invite family members or friends to your group, the invited persons get their own user account that allows them to protect their devices using your licenses.

To share protection with someone else:

1. Login to the Safety Butler Service portal with your credentials.
2. On the **CTM IDP** page, select **Install CTM IDP**.
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 mobile number of the user.
5. Select **Send Invitation**. The user will receive an invitation to join your group.



The screenshot shows a blue header with the text 'Add device'. Below it, the title 'Invite a person' is displayed. The question 'Who would you like to invite to your Safety Butler Service group?' is shown. There are three input fields: 'First Name', 'Last Name', and a mobile number field with a dropdown menu showing '+853 6612 3XXX'. A blue 'Send invitation' button and a white 'Cancel' button are at the bottom.

6. After this person will receive an invitation email and will now have an account that 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 that if the person you want to invite to your group has already been added to your group or belongs to another 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.*

## About Master Password

The master password is very important as it gives you access to the app and keeps your password data safe. Once you've installed CTM IDP and you start the application for the first time, the app asks you to create a master password. To increase your security and privacy and protect your data, the app cannot reset the master password.

When CTM IDP is installed and started for the first time, the program will ask you to create a master password. Please create a strong password that you are able to remember, and create a recovery code for the master password.

## Setting up and create Master Password

1. Login to CTM IDP
2. Click on **Get Started**.
3. Select **Create Master Password**. Create a strong master password.
4. Repeat the master password.
5. If you want to use fingerprint to log in to CTM IDP, select Use fingerprint to login. Note that before you can use your fingerprint to log in to the app, you first need to register your fingerprint. Consult the device user manual to find out how to take fingerprint recognition into use in your device.
6. Select **Create**.



Welcome to CTM IDP!

Get started

CTM IDP

CTM 澳門電訊

✔ Congratulations! Your subscription is now active.



### Are you new to CTM IDP?

To get started, please create a Master Password which you will use to access your passwords and personal information.

Create Master Password



### Already have CTM IDP on another device?

Simply connect devices and sync your passwords and personal information.

Connect devices

CTM IDP

CTM 澳門電訊

## Create your Master Password

Your Master Password is used to access all your other passwords and personal information.



Tip: Choose a unique phrase which you can easily remember

Master Password

Repeat Master Password

Create Master Password

### Already have CTM IDP on another device?

Connect devices

## About recovery code

The master password recovery code is a unique and personal code that is the only way of regaining access to the app, should you forget your master password. We cannot restore any master passwords, as this would mean accessing your master password, which could be a security risk. It is strongly encrypted and can only be decrypted on one of your connected devices. This means that it cannot be decrypted on any other user device.

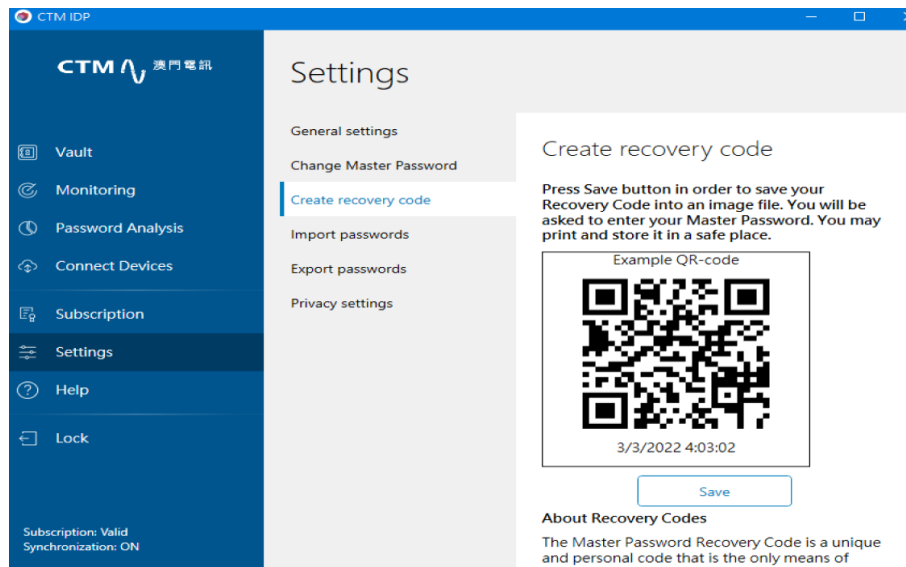
There are a few important things to note about the master password recovery code:

- Every time you change your master password, you need to create a new recovery code.
- You will always need the latest recovery code to regain access to the app.
- If you connect new devices, the app may ask you to create a new master password recovery code. If this is the case, make sure you create a new master password recovery code, as the older code will not work anymore.
- We recommend saving the code as an image and print a copy for safekeeping. The master password recovery code printout should not be stored in the same location as your device.

***Reminder: We strongly recommend that you also create a recovery code for the master password as soon as you have taken CTM IDP into use. It is the only way for you to regain your master password if you forget it.***

## Create and save recovery code

1. On **Menu > Settings**, tap **Create recovery code**.
2. Tap **Save** to save this Recovery Code image and print and store it in a safe place.



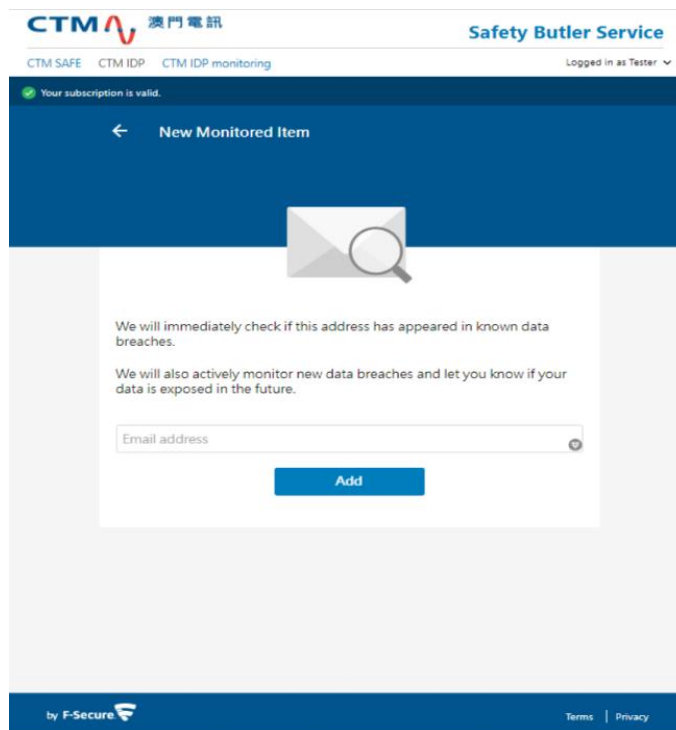
# Using ID Monitoring

With CTM IDP, you can add your email addresses for monitoring and receive guidance on what to do if your personal information has been leaked in a data breach.

The notification email includes information on what personally identifiable information has been associated with the breach; what the breach was; what company or entity was breached; when the breach took place; and other pieces of PII associated with the monitored email address, such as passwords, credit card numbers, street address, and so on.

## Adding your email address for monitoring

1. Select **+ ADD MONITORED ITEM**.
2. In the **New Monitored Item** view, enter your email address
3. Select the **check** icon.



The screenshot shows the 'New Monitored Item' interface in the CTM IDP system. At the top, there is a header with the CTM logo and '澳門電訊' (CTM), and 'Safety Butler Service' on the right. Below the header, there are navigation links for 'CTM SAFE', 'CTM IDP', and 'CTM IDP monitoring', along with a user status indicator 'Logged in as Tester'. A green notification bar at the top left states 'Your subscription is valid.' The main content area has a blue header with a back arrow and the title 'New Monitored Item'. Below this is a large icon of an envelope with a magnifying glass. The text explains: 'We will immediately check if this address has appeared in known data breaches. We will also actively monitor new data breaches and let you know if your data is exposed in the future.' There is a text input field labeled 'Email address' and a blue 'Add' button below it. The footer includes the 'by F-Secure' logo and links for 'Terms' and 'Privacy'.

The app immediately checks existing data breaches to see if your email address has been mentioned in any of them. If your email address appears in any of the known data breaches, the breaches will be listed in the **Monitoring** view. To be able to see more detailed information about your leaked data and the recommended actions, you will need to first confirm your email address.

4. Open the confirmation email and use the link to confirm that this is your email address.
5. To see the details of your exposed personal information and what you should do, tap on the specific breach listed in the **Monitoring** view.

***Important:*** *To eliminate the risk of your information being misused, we urge you to execute the recommended actions as soon as possible.*

Email subject: Your Personal Data Breach Report

Email subject: CTM IDP email confirmation



## Confirm your email address on CTM IDP

This message was sent to confirm that you are adding the email address "james.bond@gmail.com" in CTM IDP.

CTM IDP is a service which detects if accounts created using this email address have been exposed in online data breaches.

- If you did not request this message, you can ignore it. No personal information linked to this email address will be shared unless you confirmed.

By pressing the Confirm email address button, you agree to the End User License Agreement.

[Confirm email address](#)

Best regards,  
CTM IDP

Please do not reply to this email because we are not monitoring this inbox.

If you are not able to click the confirmation button, go to:

[Link here](#)

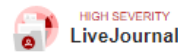
CTM IDP  
<https://www.ctm.net/zh-TW/person/public/T3-010010020040/20221/8f426765239c4ae8a7bfbccae1e3dbf6.html>

© F-Secure Corporation



## Your data has been leaked! Here's what you should do next...

Your personal information have been exposed in a data breach. We found 4 monitored items in this breach.



EMAIL ADDRESS <b>frank.d.smith@outlook.com</b>	PHONE NUMBER <b>*****1234</b>
CREDIT CARD NUMBER <b>*****1234</b>	PASSPORT NUMBER <b>A10000012345678*****</b>

### What should I do now?

Please visit to CTM IDP to see details about your exposed information and recommended actions.

[See breach details](#)

We will continue to monitor the items you have added and will notify you immediately if we find a breach.

Best regards,  
CTM IDP

Please do not reply to this email because we are not monitoring this inbox.

You're receiving this email because labron.james@f-secure.com is assigned as your contact information in CTM IDP. If you wish to receive these emails to another email address, you can change your contact email in the app. ;



## Changing your contact email address

You will receive notifications in your contact email address as soon as any of your monitored email addresses appears in a data breach. The first email address that you add as a monitored item automatically becomes your contact email address.

**Note:** *If you want to change your contact email address, you can do it only through the IDP app on your mobile device.*

To change your contact email address:

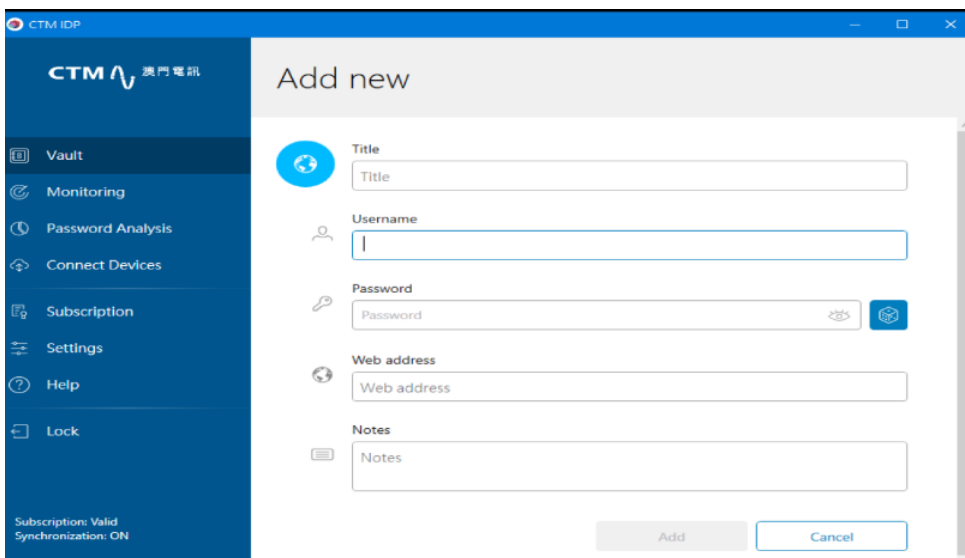
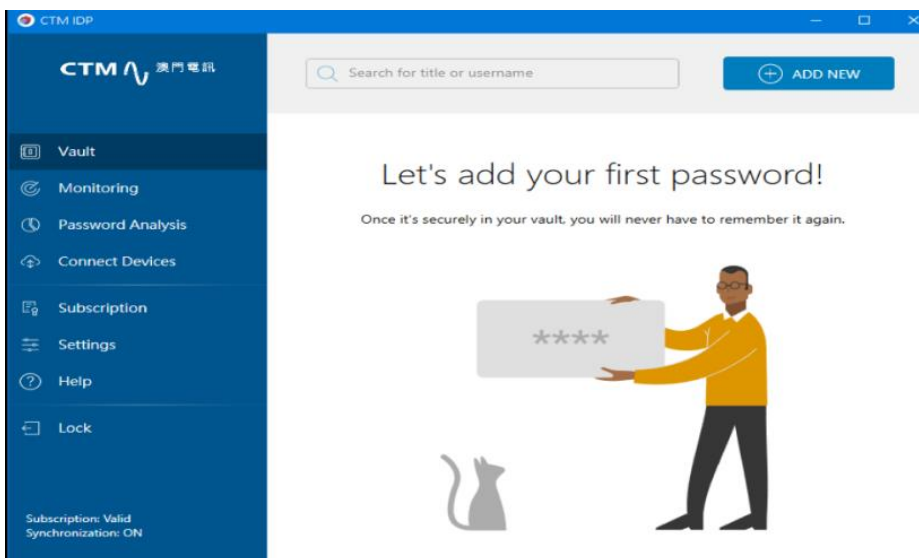
1. Open CTM IDP on your mobile device.
2. Select the top-left main menu and then **Settings**.
3. Under **CONTACT INFORMATION**, select **Email address**.
4. The **Contact information** view will open, listing all the email addresses that you have added for monitoring.
5. Under **CHANGE CONTACT INFORMATION**, select the email address that you want to use as your new contact email. Note that you can use only confirmed email addresses as the contact email address.
6. The **Change contact information?** confirmation dialog will open
7. Select **Assign**.
8. The new email address will now be used.

# Vault (Password Manager)

With CTM IDP, you can create and edit password and payment card entries, let the app generate strong passwords for your online services, and access your password history.

## Save your Password or Credit Card Information

1. Click **Vault**.
2. Click **+ Add**.
3. Select **Password** or **Credit Card**.



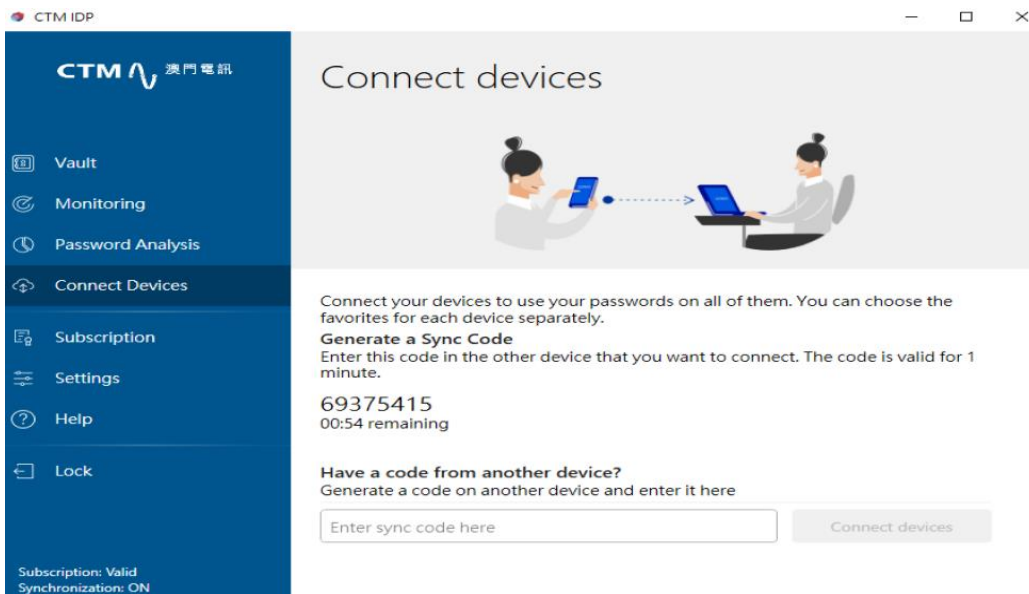
## Connect Devices (Synchronize Vault Data)

You can connect your devices to synchronize your Vault data across all of them. To be able to sync your Vault data across all your devices, you need to connect the devices that have the CTM IDP app installed.

**Warning:** *If you only have the app on one mobile device and you carry out a factory reset, the also reset wipes your Vault data from the device. After this, there is no way to get the data back.*

1. On device A, select **Connect devices** to generate a Sync Code.  
**Note:** *Synchronize passwords will be renewed every 60 seconds.*
2. On device B, select **Connect devices** and enter this sync code and then click **Connect**.
3. When prompted, enter your **master password** that you use on the device in which you generated the sync code.

Your data has now been synchronized between these two devices. If you have more devices to be connected, repeat the above steps with each device. Note that you can generate the synchronization code on any of your connected devices.



# Using Autofill

With the CTM IDP Autofill feature, you can log in to apps and websites without needing to enter usernames and passwords manually.

You need to have the username, password and web address of the service saved in CTM IDP for Autofill to work. When you log in to an app or website with credentials that are saved in CTM IDP, you can have the app enter your username and password automatically.

## Autofill and built-in browser password managers

This topic explains how built-in browser password managers may affect Autofill in CTM IDP.





As most browsers have a built-in password manager, passwords may get saved to the browser automatically. To keep your passwords safe, the best practice is to avoid saving passwords in your browser.

Passwords saved in the browser may also cause issues with Autofill in CTM IDP, as the app is not able to identify the passwords properly for the service that is being logged into.

Before taking Autofill into use in CTM IDP, we therefore recommend the following:

- Turn off the built-in password manager in the browser that you use.
- Make sure that all the passwords stored in the built-in password manager are stored in **Vault** as well. Move your passwords to **Vault** if you have not already done so.
- Once the built-in password manager is turned off, to make sure that none of your passwords remain in the built-in password manager, you may also have to clear the data in the browser.

# CTM IDP features per platform

	 Windows	 macOS	 Android	 iOS
ID Monitoring	-	-	•	•
Breach alerts	• (Email)	• (Email)	• (App/Email)	• (App/Email)
Breach guidance		-	•	•
Secure password storage	•	•	•	•
Password import/export	•	•	-	-
Password generation	•	•	•	•
Password quality analysis	•	•	•	•
Breach guidance	•	•	•	•
Login: Master password	-	-	•	•
Login: Fingerprint/Face	-	-	•	•
Login: QR Recovery Code	•	•	•	•
Password Synchronization	•	•	•	•
System/ app autofill	•	•	•	•
Supported browsers for autofill	Firefox, Chrome	Firefox, Chrome	SAFE Browser, Firefox, Chrome, Opera, Edge	Safari, Chrome

## Contact us

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