F-SECURE ID PROTECTION (CTM)

END-USER FAQ FOR PARTNERS

January 2022

F-Secure

Table of Contents

1 CTM ID PROTECTION OVERVIEW

CTM ID PROTECTION (or CTM IDP for short) monitors and detects leaked and exposed personal information online and responds quickly to identity theft threats. Designed to protect against today's many forms of identity theft, our app-based solution alerts you immediately when it detects exposed, personal information. Each alert gives you tailored recommendations on how best to deal with the exposed information with clear suggested next steps. CTM IDP also doubles as an easy-to-use password manager, providing you with an effective way to prevent falling victim to identity theft in the first place.

With CTM IDP, you can do the following:

- Protect your own and your family's personal information against cyber crime.
- 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.
- Improve your security by creating strong and unique passwords, and by synchronizing them across all your devices.

Purpose of this document collect some of the typical end user (consumer) questions and answers.

2 FREQUENTLY ASKED QUESTIONS

GENERIC

Q: How do criminals get access to my personal information?

A: Cyber criminals can get access to your personal information many ways e.g. through a data breach in a common online service, malware infection, phishing web site, by following your network traffic, and many other ways.

Q: What is a data breach?

A: A data breach is either an intentional or unintentional exposure of sensitive and confidential personal or financial data to an untrusted environment. A data breach takes place when cyber criminals break into a company or an online service and steal the private information of its customers or users. This information can range from personally identifiable information, such as names, social security numbers and addresses to directly harmful financial information, such as credit card numbers and bank accounts.

INSTALLATION

Q: Which operating systems CTM IDP supports?

A: CTM IDP supports Android, iOS, Windows and Mac. Mobile apps come with the password manager and ID monitoring capabilities. Windows and Mac apps offer password management capabilities.

Q: Does CTM IDP offers monitoring of personal information only on mobile?

A: No. Monitoring actually happens on the server side. Mobile app is used for setting up the monitoring and showing the alerts in case personal information is breached. Mobile apps bring the protection closer to you as the mobile phone is typically always on and somewhere close. It is the easiest way to immediately notify you.

Q: Why do I need to create Master password for CTM IDP?

A: 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. Choose a hard-to-guess master password (or passphrase) that you can remember, as the app or F-Secure cannot reset your master password. The fact that the app cannot reset the master password has been a conscious decision by F-Secure to increase your security and privacy and protect your data.

Q: The app keeps on reminding me of the master password recovery code. Why do I need to create master password recovery code?

A: 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. F-Secure cannot restore any master passwords, as this would mean accessing your master password, which could be a security risk.

Q: Can I use fingerprint or face-recognition for accessing my passwords?

A: Yes. If you want to use fingerprint to unlock the app, select Use fingerprint to unlock next time. Note that before you can use your fingerprint to unlock CTM IDP, 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.

MONITORING

Q: How does CTM IDP know what personal information to monitor?

A: As soon as you have activated the product and created your master password you are asked to add your first email address to Monitored items. A verification email is sent to the email address you added. Monitoring starts after you have clicked the link in the verification email. Already found breach data is shown on the app screen. The first email address is automatically added as the contact email address.

Q: Why do I need to verify the email address before the results are shown?

A: Each added email address is verified for security and privacy reasons. This way no-one else can add your email address in their app and see the list of your breached personal information.

Q: Does CTM IDP monitor all email addresses I have added in Password manager?

A: No. Monitoring is applied only to email address(es) given in Monitoring tab of the application.

Q: CTM IDP found my personal information among the breached data. What do these breach severities mean?

A: F-Secure ranks the data breaches according to severity based on 1) how much of your data has been leaked, 2) how potentially harmful the leak is, and 3) is the leaked data in an easily-readable format or encrypted. There are three severity levels, where
High severity: Breaches of high severity can involve, for example your password or your credit card details in a readable format.
Mid severity: Breaches of mid severity can involve your social security number, your password in a scrambled format or many pieces of low severity personal information breached at the same time.
Low severity: Breaches of low severity involve one of the following pieces of personal information: username, full name, date of birth, phone number, or address.

Q: What information do I get in breach notification?

A: In case your personal information has been found among breaches, a breach notification will notify what personally identifiable information (PII) has been associated with the breach, what the breach was, what company/entity was breached, when the breach happened, and what other PII has been found.

VAULT (PASSWORD MANAGER)

Q: How can I add passwords in Password manager?

A: You can easily store new passwords by pressing plus icon in Password manager tab of the app.

Q: I have used another password manager previously. Can I import my passwords in Password manager?

A: Yes. CTM IDP supports import from many of the commonly used formats.

Q: How can I use the passwords stored in Password manager?

A: You can copy the items manually using your device's clipboard (copy/paste) or by enabling auto-fill functionality. Auto-fill works in most browsers and in apps.

Q: How can I synchronize passwords across all my devices?

A: In order to have a backup copy of your passwords it is recommended that you enable password synchronization. To be able to sync your data across all your devices, you need to connect the devices that have the app installed. Setup happens through Menu > Connect devices. When you enter the menu, a synchronization code is automatically generated, and it is valid for 60 seconds at a time. A new code is generated immediately after the current code expires. Open the app on the device with which you want to sync your app data. Go to Menu > Connect devices, and enter the synchronization code. Select Connect. When prompted, enter the master password that you use on your other device. Once synchronization is successful, select Confirm.

Q: Can F-Secure see my passwords stored in CTM IDP?

A: No. Your master password and the master encryption key are never stored anywhere. The encryption keys exist only when you use the product. When you turn off CTM IDP, the encryption key is destroyed. We have no way of decrypting any information that you have saved in CTM IDP. In addition, anyone using 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. However, this also means that there is no way for F-Secure to recover your password or data for you if you forget the master password.

EXPIRATION

Q: If I cancel CTM IDP subscription, what happens to my stored passwords?

A: Expired subscriptions stops access to ID monitoring and syncing passwords between devices, but passwords themselves remain accessible.

Q: Do I need to uninstall CTM IDP immediately after expiration?

A: No. You can continue to use it as non-synchronizing password manager. Adding new passwords is not very convenient as they will not be synchronized across all your devices.