F-Secure Password Protection

Administrator's Guide

Contents

Chapter

1

Password Protection

Topics:

This documentation provides information on the features of F-Secure Password Protection and how to use them.

1.1 What is F-Secure Password Protection?

F-Secure Password Protection is a password manager app that stores and protects all your passwords.

With Password Protection, all the data is encrypted. The data is stored on both your devices and our servers that are hosted in Finland, Europe, under European data protection laws. The only way to access the data it is with Master Password. Not even F-Secure can access your data.

The password generator in the product creates strong, unique passwords. You only need to set a single, ideally very strong master password, which grants you access to the entire password database. This is the only thing you need to remember.

F-Secure Password Protection allows you to connect devices and synchronize your Password Protection data.

1.1.1 Why you should use different passwords for each service and account

Security experts generally recommend that you use strong, unique passwords for each of your online services and accounts.

Strong passwords that contain several different types of characters are compulsory for some online services - the password that you enter when you sign up is not accepted if it is too short or not complex enough.

However, even if you come up with a highly complex password that is virtually impossible for anyone else to guess, the safety of your account to online services is at risk if you use that same password for each account. For example, if hackers gain access to the login details for one of the services that you use, they can then use that information to access any of your other online accounts where you have used the same password. Using a unique password for each account means that even in the event of a data breach in one of the services you use, your other accounts are not at risk.

1.1.2 What makes a good password

The general recommendation for a good password is that it should be something that is unique, contains a combination of letters, numbers, and special characters, and that it is easy for you to remember but hard for anyone else to guess.

In addition to these general guidelines, there are also several other approaches that improve the safety of your accounts for online services:

- Use different email addresses for different types of online services. This means that if your email account is hacked, it won't put all of your online accounts at risk.
- Avoid using your email address as a username whenever possible. Many services automatically create your account with your email address as a username, but if not, use something else.
- Use generated passwords. When you use a password that is generated by F-Secure Password Protection, there is no memorization system or other clues that can be used to break the password.
- Change your password. It's a good idea to get into a habit of changing your passwords every now and again, but if nothing else, change your password immediately for any service that notifies you of a potential data breach.

What makes a good master password

Choose your master password carefully. To prevent unauthorized access to your data, your password cannot be reset, and you cannot access your password data without your master password.

You cannot use a weak master password with Password Protection. A strong master password should:

- include both lower and uppercase letters,
- include numbers (1, 2, 3) and special characters (.,!;), and
- contain more than 6 characters.

Note: If you select **Remember Master Password**, Password Protection only asks for your Master Password when you lock the app from the menu.

1.1.3 Where your passwords are stored

F-Secure Password Protection stores your passwords on the computer that you use to run the product.

Your passwords are stored in an encrypted format and nobody can access them unless they know your master password and get access to your device.

You can synchronize your passwords across your devices. For security reasons, we do not provide access to the passwords through F-Secure servers. No matter what happens to one of your devices, sync ensures that you will always have access to your passwords on the other devices.

1.1.4 A few words about the security and cryptography in Password Protection

The guiding design principle for F-Secure Password Protection is to respect and protect the anonymity of our users, as well as their sensitive data.

F-Secure Password Protection uses the Advanced Encryption Standard with a key size of 256 bits (AES-256). This algorithm works in the CCM (Counter with CBC-MAC) mode. AES is the recommended standard for modern data encryption.

The master encryption key is derived from your master password using the Password-Based Key Derivation Function 2 (PBKDF2) algorithm specified in Public-Key Cryptography Standards (PKCS) #5; in the PBKDF2 algorithm, we use the Hash-based Message Authentication Code (HMAC) SHA256, random salts, and 20000 iterations. This makes it much more difficult to recover the keys through brute-force or dictionary attacks, even for weaker passwords.

Your master password and the master encryption key are never stored anywhere. The encryption keys exist only when you use the product. However, this also means that there is no way to for F-Secure to recover your password or data for you if you forget the master password. Furthermore, F-Secure does not track you when you synchronize your data across devices.

The F-Secure Password Protection servers are owned and operated by F-Secure within the European Union in compliance with Finnish law and applicable to EU rules.

1.2 Installing F-Secure Password Protection

Instructions on how to install F-Secure Password Protection on your Windows and Mac computers.

1.2.1 Installing Password Protection on Windows computers

Follow these steps install F-Secure Password Protection on a desktop or laptop that runs Windows 7 or newer:

1. In the email that you received, select the Windows button to download the product.

   Note: You received the installation email with the installation key after the company administrator added you as a user to the portal.

   Note: For PSB administrators, who add users to the system, see the instructions in Management Portal - Admin guide.

2. Double-click the downloaded installation package and follow the instructions shown on the screen.
3. When the installation is complete, start F-Secure Password Protection and create your master password.

   Note: We recommend that you create a QR recovery code for your master password. You can use the recovery code to access Password Protection if you forget your master password.

1.2.2 Installing Password Protection on Mac computers

Follow these steps install F-Secure Password Protection on a desktop or laptop that runs Mac OS X 10.7 or newer:

1. In the email that you received, select the Mac button to download the product.

   Note: You received the installation email with the installation key after the company administrator added you as a user to the portal.

   Note: For PSB administrators who add users to the system, see the instructions in Management Portal - Admin guide.

2. When downloading is complete, the application icon and installation folder appear.
3. Drag the application icon on top of the installation folder to start installing Password Protection.
4. When the installation is complete, start F-Secure Password Protection and create your master password.

   Note: We recommend that you create a QR recovery code for your master password. You can use the recovery code to access Password Protection if you forget your master password.

1.2.3 Installing Password Protection on Android devices

Follow these steps install F-Secure Password Protection on an Android device that runs Android 5.0 or newer:

1. In the email that you received, select the **Android** button.

   Note: You received the installation email with the installation key after the company administrator added you as a user to the portal.

   Note: For PSB administrators, who add users to the system, see the instructions in Management Portal - Admin guide.

   You are directed to Google Play Store.
2. Select **Install** to download and install the product.
3. When the installation is complete, start F-Secure Password Protection and create your master password (if the product is installed on the first device) or sync the password with other devices.

   Note: We recommend that you create a QR recovery code for your master password. You can use the recovery code to access Password Protection if you forget your master password.

1.2.4 Installing Password Protection on iOS devices

Follow these steps install F-Secure Password Protection on an iOS device that runs iOS 9.0 or newer:

1. In the email that you received, select the **iOS** button.

   Note: You received the installation email with the installation key after the company administrator added you as a user to the portal.

   Note: For PSB administrators, who add users to the system, see the instructions in Management Portal - Admin guide.

   You are directed to Apple Store.
2. Select **Install** to download and install the product.
3. When the installation is complete, copy the installation key to the app to activate the product.
4. Start F-Secure Password Protection and create your master password (if the product is installed on the first device) or sync the password with other devices.

   Note: We recommend that you create a QR recovery code for your master password. You can use the recovery code to access Password Protection if you forget your master password.

1.2.5 How to create a QR recovery code for your master password

You can create an encrypted QR recovery code, which you can use in case you forget your master password for F-Secure Password Protection.

1. Log in to F-Secure Password Protection.
2. Select **Create Recovery Code** from the menu.
   The QR image is generated automatically.
3. Save the image.
   - On Windows and Mac computers, select where you want to store the image.
4. Print the image or send it to a device where you can print it.

   Note: We recommend that print the image for safekeeping rather than storing the file on your device or computer.
5. Once you have printed the image, delete the file from your device or computer.

1.3 Creating a new password entry

You can save your username, password, and the web address for each of your online services in their own entries.

1. In the product, select ⊕.
2. Enter a title or description for the entry.

Use a title that is easy to find, for example the service name.

3. Change the icon and background color for the entry. Select  to change the icon, and  to change the color. If you do not select an icon or color, Password Protection randomly selects it for you.
4. Enter a username for the entry.
5. Enter a password for the entry.

   a) Select  if you want Password Protection to generate a new password.
   b) Drag the slider to select the number of characters you want to use.
   c) Select the types of characters you want to use.

   d) Select  to change the current password.
   e) Select **Use this**.
6. Enter a web address for the entry.

   Tip: You can click the color-coded  icon on the Password Protection main view to go directly to the web site stored for the entry.
7. Enter any notes you want to add to the entry.
8. Save your entry.

   - Select **Save**.

1.4 Editing an existing entry

You can change the password or other details for an existing entry, or set it as a favorite so that you can find it more easily.

1. Select the entry that you want to edit.
2. Select  to start editing the entry's details.
3. Change any of the details as necessary.

   Tip: Select  for any of the fields to see hidden content.
4. Save your entry.

1.5 How to recover your master password

If you forget your master password, you can use a QR recovery code that you created earlier to access the app.

Note: You can only regain access to Password Protection with these steps if you have previously created a QR recovery code.

Scan your printed QR recovery code to a file before starting.

1. Start F-Secure Password Protection.
2. Select **Forgot Master Password**.
3. Select **Import Image**.
4. Select the image file or scan the printed image.
   Your master password appears on the screen, and you can log in immediately.
5. Select **Log in**.

1.6 How to import passwords from other password manager apps

You can import your passwords from other password manager apps into F-Secure Password Protection.

F-Secure Password Protection. supports XML file formats from the following apps: 1Password, Dashlane, KeePass2, LastPass, Norton Identity Safe, Password Exporter Firefox plug-in, Password Safe, SecureSafe Password Manager, Sticky Password.

Before you can import the passwords into F-Secure Password Protection, you need to export your data from the other password manager app.

To export your password data in KeePass:

1. Select **Open File** > **Export**.
2. Select **KeePass XML (2.x) format**.
3. Save the file to your computer.

To export your password data in 1Password:

1. Select **Open File** > **Export**.
2. Select **1Password Interchange File (1PIF)**.
3. Save the file to your computer.

To export your password data in Password Safe:

1. Select **Open File** > **Export to** > **XML Format**.
2. Save the file to your computer.

To import the password data into F-Secure Password Protection:

1. In F-Secure Password Protection., go to **Settings** > **Import passwords**.
2. Select **Browse**, then select the file that you exported from the other app.
   Password Protection imports the passwords automatically and tells you how many passwords were imported.

1.7 How to take a backup of your saved passwords

With Password Protection, you can export your saved password data to use as a backup.

1. Select **Export passwords** from the menu.
2. Select **Export**.
3. Choose a name and location for the saved file.
4. Click **OK**.
   Your passwords are exported to the location that you selected.

Note: When you export your Password Protection data, this file is exported into plain text, and therefore can be read more easily by others. If you need to store this file, store it where it cannot be easily accessed or damaged.

1.8 How to sync your passwords between your devices

With F-Secure Password Protection, you can synchronize your passwords to another device.

If you have F-Secure Password Protection on your computer, your Password Protection data is also only stored on that device. The way F-Secure Password Protection has been designed is that syncing devices enables you to have your Password Protection data readily available and always up to date on other devices; this ensures that you have your Password Protection data elsewhere on another device. Therefore, there's no need to worry if a device gets lost, stolen or damaged, your Password Protection data will still be intact on one of your other devices.

Note: If you delete a device from the PSB portal, the Password Protection software remains on the device and the end user can use it. However, the device is not synced any more with the end user's other devices and it does not receive any software updates.

1. Open F-Secure Password Protection.
2. Enter your Master Password when prompted.
3. Go to **Menu** > **Connect devices**.
   An 8-digit sync code is generated. The code is valid for 60 seconds.
4. Open F-Secure Password Protection on the other device that you want to connect with.
5. Go to **Menu** > **Connect devices**, and enter the code that was generated in step 3.
6. Select **Connect**.

7. When prompted, enter the master password for the device that has F-Secure Password Protection installed.
8. When the synchronization is complete, select **OK**, if you are syncing to a desktop.