USER'S GUIDE

Bitdefender® CONSUMER SOLUTIONS

SecurePass

Bitdefender SecurePass

User's Guide

Publication date 20/11/2024

Legal Notice

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from an authorized representative of Bitdefender. The inclusion of brief quotations in reviews may be possible only with the mention of the quoted source. The content can not be modified in any way.

Warning and Disclaimer. This product and its documentation are protected by copyright. The information in this document is provided on an “as is” basis, without warranty. Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This book contains links to third-party Websites that are not under the control of Bitdefender, therefore Bitdefender is not responsible for the content of any linked site. If you access a third-party website listed in this document, you will do so at your own risk. Bitdefender provides these links only as a convenience, and the inclusion of the link does not imply that Bitdefender endorses or accepts any responsibility for the content of the third-party site.

Trademarks. Trademark names may appear in this book. All registered and unregistered trademarks in this document are the sole property of their respective owners, and are respectfully acknowledged.

Table of Contents

About This Guide 1
Purpose and Intended Audience 1
How to Use This Guide 1
Conventions used in This Guide 1
Typographical Conventions 1
Admonitions 2
Request for Comments 2
1. What is Bitdefender SecurePass 3
1.1. SecurePass Trial & Paid versions 3
2. Getting Started 4
2.1. System Requirements 4
2.1.1. Software Requirements 4
2.2. Installation 5
2.2.1. Installing on Windows or macOS 5
2.2.2. Installing on Android 7
2.2.3. Installing on iOS 7
2.3. Setup process 7
3. Importing & Exporting your passwords 9
3.1. Compatibility 9
3.2. Importing into SecurePass 9
3.3. Exporting from SecurePass 11
4. Features Set 12
4.1. Manually Save Passwords 12
4.2. Password Generator 12
4.3. Password Strength Check 13
4.4. Data Organization 14
4.5. Intelligent Autofill 14
4.5.1. Autofill on Android 15
4.5.2. Autofill on iOS 15
4.5.3. Autofill Card Details 16
5. Use as a 2FA Application 17
6. Share Data 18
6.1. Share with Groups 18
6.2. Manage Groups 19
7. Lock Account 20
8. Frequently Asked Questions 21
9. Getting Help 24
9.1. Asking for Help 24
9.2. Online Resources 24

9.2.1. Bitdefender Support Center 24
9.2.2. The Bitdefender Expert Community 25
9.2.3. Bitdefender Cyberpedia 25
9.3. Contact Information 25
9.3.1. Local distributors 26
Glossary 27

ABOUT THIS GUIDE

Purpose and Intended Audience

This guide is intended to all Bitdefender users on all supported operating systems (Windows, macOS, Android, iOS) who have chosen Bitdefender SecurePass as their go-to password management tool. The information presented in this book is suitable not only for computer literates, but it serves as an accessible and friendly guide to everyone.

This guide will help you find out how to make the best of our ultra-secure and feature-rich password manager, by discussing in detail all of its features and functionalities.

We wish you a pleasant and useful lecture.

How to Use This Guide

This guide is organized around several major topics:

Getting Started (page 4)

Get started with Bitdefender SecurePass and the installation process.

Importing & Exporting your passwords (page 9)

Understand how you can import or export passwords in and out of SecurePass.

Features Set (page 12)

Learn how to use Bitdefender SecurePass and all of its features.

Getting Help (page 24)

Where to look and where to ask for help if something unexpected appears.

Conventions used in This Guide

Typographical Conventions

Several text styles are used in this guide for an improved readability. Their aspect and meaning are presented in the table below.

Appearance	Description
`sample syntax`	Syntax samples are printed with monospaced characters.
https://www.bitdefender.com	The URL link is pointing to some external location, on http or ftp servers.
documentation@bitdefender.com	Email addresses are inserted in the text for contact information.
About this Guide (page 1)	This is an internal link, towards some location inside the document.
`filename`	File and directories are printed using monospaced font.
option	All the product options are printed using **bold** characters.
keyword	Important keywords or phrases are highlighted using **bold** characters.

Admonitions

The admonitions are in-text notes, graphically marked, bringing to your attention additional information related to the current paragraph.

Note

The note is just a short observation. Although you can omit it, the notes can provide valuable information, such as specific feature or a link to some related topic.

Important

This requires your attention and is not recommended to skip over it. Usually, it provides non-critical but significant information.

Warning

This is critical information you should treat with increased caution. Nothing bad will happen if you follow the indications. You should read and understand it, because it describes something extremely risky.

Request for Comments

We invite you to help us improve the book. We have tested and verified all of the information to the best of our ability. Please write to tell us about any flaws you find in this book or how you think it could be improved, to help us provide you with the best documentation possible.

Let us know by sending an email to documentation@bitdefender.com. Write all of your documentation-related emails in English so that we can process them efficiently.

1. WHAT IS BITDEFENDER SECUREPASS

Bitdefender SecurePass is a multi-platform service designed to help users store and organize all of their online passwords. It is built with the strongest known cryptographic algorithms for the highest level of safety and digital security. It works as a browser extension and mobile app solution for identity and password management, banking and all other types of sensitive information across devices.

Bitdefender SecurePass can auto-save, auto-fill, automatically generate and manage your passwords - and all other personal, sensitive data - for all websites and online services with the help of a single Master Password, making your overall digital identity much easier to manage.

1.1. SecurePass Trial & Paid versions

The Trial version of Bitdefender SecurePass works, by all accounts, identically to the Paid version of the product, but its availability will expire after trial period of 90 days.

Note

Note that the Paid version of the product, whilst it can be purchased as a purely standalone product, unlimited access to SecurePass is included within the Bitdefender Total Security, Bitdefender Premium Security and Bitdefender Ultimate Security subscriptions and their variants.

2. GETTING STARTED

2.1. System Requirements

You may use Bitdefender SecurePass only on devices running the following operating systems:

- **For PC users:**
  - Windows 7 with Service Pack 1
  - Windows 8.1
  - Windows 10
  - Windows 11
- **For macOS users:**
  - macOS 10.14 (Mojave) and later macOS operating systems

  > Note
  >
  > Note that System Performance may be affected on devices that have old generation CPUs.

- **For iOS users:**
  - iOS 11.0 or later iOS operating systems
- **For Android users:**
  - Android 5.1 and later Android operating systems

  > Note
  >
  > - Fingerprint unlock feature is supported on **Android 6.0** and later.
  > - Auto-fill feature is supported on **Android 8.0** and later, compatible with iPhone, iPad and iPod touch.

2.1.1. Software Requirements

To be able to use Bitdefender SecurePass and all its features, your Windows or macOS devices need to meet the following software requirements:

- **Microsoft Edge** (based on Chromium 80 and later)
- **Mozilla Firefox** (version 65 or later)
- **Google Chrome** (version 72 or later)
- **Safari** (version 12 or later)

Note

The **Software Requirements** may be ignored for Android and iOS.

Warning

Failure to meet the System Requirements presented above will result in either the inability of installing Bitdefender SecurePass or the malfunctioning of the product.

2.2. Installation

This chapter will guide you on how to install Bitdefender SecurePass on both the web browsers on your Windows PC and macOS, as well as on your Android or iOS mobile devices.

Important

Prior to the installation process, make sure that you have a valid SecurePass subscription in your Bitdefender Central account so that the browser extension can retrieve its validity from your account.

Active subscriptions are listed in the **My Subscriptions** section within Bitdefender Central.

2.2.1. Installing on Windows or macOS

Unlike most desktop applications and software which need to be installed and set up on these devices, Bitdefender SecurePass comes as a browser extension - also called an add-on - that can be quickly added and enabled to your preferred browser.

The currently supported browsers for the product are the following:

- **Google Chrome**
- **Mozilla Firefox**
- **Microsoft Edge**
- **Safari**

To install Bitdefender SecurePass:

1. After purchasing Bitdefender SecurePass, follow the steps provided in the confirmation e-mail in order to activate your subscription.
2. Log in to Bitdefender Central using your credentials.
   On the left-hand side menu, select **SecurePass**.
3. In the SecurePass panel, select your preferred browser.
4. Install the Browser extension:
   - **Google Chrome:**
     a. Click the **Add to Chrome** button.
     b. In the confirmation box, click **Add extension**.
   - **Mozilla Firefox:**
     a. Click the **Add to Firefox** button.
     b. Click the **Install** button in the upper-right corner of the screen.
   - **Microsoft Edge:**
     a. Click the **Get** button.
     b. Click **Add extension** in the prompt that appears.
   - **Safari:**
     a. The SecurePass installer will download on your macOS device. Double-click the downloaded file and follow on-screen instructions from there.
     b. At the end of the installation process, open the **Safari** browser and select **Preferences** in the top menu bar.
     c. In the Preferences windows, click the **Extensions tab**.
     d. Check the box next to **Bitdefender SecurePass** to enable it.

Once the extension is installed, you can proceed to the Setup process (page 7).

2.2.2. Installing on Android

The easiest method of installing Bitdefender SecurePass for Android phones and tablets is to download the application directly from Google Play, in the following manner:

1. Before anything else, after purchasing, make sure to open the confirmation e-mail you received in order to follow the instructions provided there to activate your SecurePass subscription.
2. Open the Google Play Store on your Android device.
3. In the Google Play Store's search bar, type **Bitdefender SecurePass**, locate and download the application.
4. Once the download is complete, open the app and, if needed, follow the on-screen configuration steps needed to finish the installation process.

The installation on your Android device is now complete. From here, you can proceed to the Setup process (page 7).

2.2.3. Installing on iOS

The easiest method of installing Bitdefender SecurePass for Apple's iOS mobile devices and tablets is to download the application directly from App Store, in the following manner:

1. Before anything else, after purchasing, make sure to open the confirmation e-mail you received in order to follow the instructions provided there to activate your SecurePass subscription.
2. Open the App Store on your iOS device.
3. In the App Store's search bar, type **Bitdefender SecurePass**, locate and download the application.
4. Once the download is complete, open the app and, if needed, follow the on-screen configuration steps needed to finish the installation process.

The installation on your iOS / iPadOS device is now complete! From here, you can proceed to the Setup process (page 7).

2.3. Setup process

To setup Bitdefender SecurePass on your browser/mobile device:

1. After finishing the installation process, open the SecurePass extension/application and log in.

   Use the credentials of the Bitdefender account associated with your SecurePass subscription.

2. You will be prompted to create a **Master Password**.

   > **Important**
   >
   > Note that you will require this Master Password to unlock all the passwords, credit card information and notes saved in Bitdefender SecurePass. This is essentially the key that allows the owner to use this product.

   Make sure to enter a strong Master Password without the risk of easily forgetting it.

   Once you decided on a strong and unique Master Password, click **Save & Continue**.

3. Next, you will be provided with a **Recovery Key**.

   > **Warning**
   >
   > Upon creating the Master Password, you will receive a **24-digit recovery key**. Make a note of your recovery key in a safe place and don't lose it. This key is the only way to access your passwords saved in Password Manager in the event that you happen to **forget the Master Password** previously set up for your account.

   - Save the Recovery Key by copying it to your clipboard or downloading it as a PDF file.

     You can press **Close** when done.

4. Once done, select the **Access your Vault** button.

Now that the setup process is complete, you can begin using Bitdefender SecurePass.

3. IMPORTING & EXPORTING YOUR PASSWORDS

Bitdefender SecurePass is built in such a way as to efficiently facilitate communication and data transfer with external sources, platforms and software tools. This is the core reason why the very frequently encountered need of importing or exporting passwords into or out of Bitdefender SecurePass can be satisfied with ease.

3.1. Compatibility

Bitdefender SecurePass can seamlessly transfer data from the following list of applications:

- Bitdefender Password Manager
- Bitdefender Wallet
- Bitdefender SecurePass
- SaferPass
- 1Password
- Kaspersky
- Dashlane
- Chrome browser
- Firefox browser
- Microsoft Edge
- Bitwarden
- LastPass
- KeePass
- RoboForm

This transfer of data between Bitdefender SecurePass and other account management software can be done through the following data formats:

CSV, **JSON**, **XML**, **TXT**, **1pif** and **FSK**.

3.2. Importing into SecurePass

Bitdefender SecurePass allows you to easily import passwords from other password managers and browsers. If you are currently looking to switch to Bitdefender SecurePass from another password managing service, you have most likely stored a considerable amount of credentials such as usernames, passwords, and other login data required for all your accounts.

Now that you have chosen Bitdefender SecurePass, you will be looking to import that saved data into it.

Here is how to import your stored information from other apps and web browsers into Bitdefender SecurePass, **regardless of the operating system** on which you have chosen to install this product:

1. Open Bitdefender SecurePass and go to **Settings**.
   - In browser:
     Click on **Settings** in the top-right corner of the page.
   - In app:
     Tap on the **More** button in the lower-right corner of the screen and, at the top of the list that appears afterwards, tap on **Settings**.
2. In the **Backup & restore** section, select **Import passwords**. The import window will open.
3. Select the name of the password manager or web browser you have used before from the drop-down menu accessible through the **Select file type** field.

   > **Note**
   > If a password was used to encrypt the file, you will be required to enter it in the **Password** field; otherwise, you may leave it blank.

4. Select the **Select file to import** filed.
   Navigate to the location where the exported data belonging to your old password manager has been saved. Choose the file once you find it, and then click **Open**.
5. After selecting the file, select **Import** in the lower-left corner of the import window. The process will begin shortly, accompanied by a progress bar.

Once imported, your passwords will then be accessible on all devices where the Bitdefender SecurePass application or browser extension is installed.

Note

Going back to your password vault in SecurePass, you will notice a folder named **Import**, containing all data from your previous password manager or web browser.

3.3. Exporting from SecurePass

Bitdefender SecurePass allows you to easily export your saved passwords (including account login credentials, secure notes, etc.) into a CSV (comma-separated values) file or an encrypted file if you ever wish to switch to another password manager service, so that your departure from Bitdefender SecurePass will not be a difficult process.

Important

A CSV file is **not** encrypted and contains usernames and passwords in plain text format, meaning your private information can be read by anyone having access to your device and access to any password with which you may choose to protect the file in question. For security reasons, we therefore recommend you follow the instructions below on a trusted device.

Here is how you can export your data from Bitdefender SecurePass:

1. Open Bitdefender SecurePass and go to **Settings**.
   - In browser:
     Click on **Settings** in the top-right corner of the page.
   - In app:
     Tap on the **More** button in the lower-right corner of the screen and, at the top of the list that appears afterwards, tap on **Settings**.
2. In the **Backup & restore** section, select **Export passwords**. The export window will open.
3. Click on **Select file type**. From the drop-down menu, choose to export your data in either a JSON format or a CSV format. You may also enter a password with which to protect the exported file.
   Check the corresponding box if you also want to include shared items.
4. Click **Export** in the lower-left corner of the export window, and save the exported file on your device.

4. FEATURES SET

This chapter will take you through all features and functionalities of Bitdefender SecurePass, explaining their usefulness and how to operate them most efficiently.

4.1. Manually Save Passwords

You can securely store information like passwords, credentials and others, such as credit card information or notes into Bitdefender SecurePass manually, in the following way:

1. Open Bitdefender SecurePass
2. In the **My Vault** tab, press the **+Add item** button.
3. Select the item type you want to add. (account, credit card, identity or note).
4. Fill in the required fields depending on the selected item.
5. After completing all necessary details, save the item in order to add it to your SecurePass vault.

4.2. Password Generator

Bitdefender SecurePass includes a password generation feature that can help with the creation of secure passwords.

To access and use the Password Generator:

1. Open Bitdefender SecurePass and access the **Generate password** tab on the left side of the screen. This will take you to the Password Generator integrated within SecurePass.
2. Customize the password that you are about to generate according to your own needs and preferences.
   - Password Length: Drag the slider to determine any length between 8 to 32 characters.
   - Uppercase / Lowercase letters: Select which - or both - types of letters you want added for the complexity level of your password.
   - Numbers: Checking this box will include numbers in the string of characters that comprises your password.

- Special characters: Add symbols to your password for enhancing the password's complexity.

> **Note**
> Press the **Save settings** button for SecurePass to remember them and always generate passwords based on the settings you saved.

3. Generate a new password by clicking the circular arrow icon located beneath the currently displayed password. Each click generates a new string of characters.
4. Once satisfied with the generated password, you can either copy it to your clipboard or click on the **Save account** button to store it into your vault (by association with other account information).

> **Note**
> You can also quickly generate a password **directly from Sign-Up Forms** by clicking on the Bitdefender SecurePass icon present in the password field of the sign-up page. Clicking on it, you can then choose the **Generate password** option.

4.3. Password Strength Check

Bitdefender SecurePass offers the possibility of evaluating the strength of saved passwords and sensitive data. This is a vital feature in evaluating and assessing any potential vulnerabilities to your data privacy sand security.

To check the strengths of stored passwords:

1. Open Bitdefender SecurePass and, in the mail menu, select the **Security report** tab.
   The Security report tab is broken down in four sections: breached, weak, old, and duplicate.
2. The number of passwords falling into each of the four categories will be shown on the screen.
   Additionally, going through the list of stored passwords, each password will be tagged with the category under which it is located.

In order to understand the meaning behind these security levels, below are some brief details on each of them:

- Breached passwords: If any of your credentials have been part of a data breach, they will be listed under the **breached** section.

> **Note**
> To check if any of your passwords have been compromised and leaked through data breaches, click the **Run security scan** button.

- Weak passwords: SecurePass will identify and flag **weak** passwords stored in your vault based on an internal, locally running algorithm looking at various criteria such as password length, variety of characters, and inclusion of digits or uppercase letters among other factors.
- Old passwords: Passwords that have been saved and unmodified for a longer period than six months will be flagged as **old**.
- Duplicate passwords: Considering that using the same passwords across multiple platforms and accounts presents a big security risk, SecurePass will flag passwords used in more than one place as **duplicate**.

4.4. Data Organization

Within Bitdefender SecurePass, you may organize and therefore more easily manage all of your saved items.

You can categorize your items into specific folders for easy access by following these steps:

1. Open Bitdefender SecurePass and go to **My vault**. Here, tap on the **Add folder** button.
2. Name your folder and tap the **Create** button.
   The new folder will now appear in your vault.

To move items into your created folder:

1. Click on any account you want to move and press the **Edit** button.
2. Press the location shown next to **Save item in** and select the folder name from the drop-down list.
3. Press the **Save Account** button.

The account will now be store in the selected folder.

4.5. Intelligent Autofill

Bitdefender SecurePass allows you to autofill account credentials and information on any Sing-In forms online.

> Note
> As a web browser extension, on either Windows or macOS, the Autofill feature should work seamlessly.

4.5.1. Autofill on Android

To configure SecurePass on Android in order to use Autofill:

1. Open the Bitdefender SecurePass app on your Android device.
2. Tap on the **More** menu button.
3. At the top on the screen, tap on **Settings**.
4. Tap on **Make this your default password manager**
5. Enable Bitdefender SecurePass in the Autofill service list.

> Note
> You can also go to your Android device's settings, in **Passwords & accounts** > **Autofill service** > enable Bitdefender SecurePass.
>
> For Android 11 or earlier versions of the operating system, the settings are: **System** > **Language & Input** > **Advanced**.

6. Tap **OK**.

Once this configuration is done, whenever you tap on a sign-in field, an option called Bitdefender SecurePass will appear on your scree. You can tap it to open the app. Login to SecurePass and your credentials will automatically be filled in.

4.5.2. Autofill on iOS

To configure SecurePass on your iOS device in order to use Autofill:

1. Open the **Setting** app on your iPhone or iPad, and select **General**.
2. Tap on **AutoFill & Passwords**. Ensure the option **AutoFill Passwords and Passkeys** or **AutoFill Passwords** - depending on the iOS version - is turned on.
3. In the **Autofill Form** list, enable the **Bitdefender SecurePass** application.

Once this configuration is done, whenever you tap on a sign-in field, an option called Bitdefender SecurePass will appear on your scree. You can tap it to open the app. Login to SecurePass and your credentials will automatically be filled in.

4.5.3. Autofill Card Details

While SecurePass provides an easily accessible icon for auto-filling login credentials and passwords, the Autofill feature for credit card information works differently:

1. Navigate to the payment or checkout page of the website on which you are looking to use your stored credit card information.
2. Right-click on any blank area of the payment page. This will prompt the contextual menu to appear on your screen.
3. Select Bitdefender SecurePass from the Menu by hovering your cursor over the option. This will open a submenu with further options.
4. Choose the **Autofill credit card info**. This will display a list of any credit cards you have stored in the SecurePass vault.
5. Select the preferred card.

In this way, SecurePass will automatically fill in the payment form fileds with the details of the credit card you chose.

5. USE AS A 2FA APPLICATION

You can always choose to utilize Bitdefender SecurePass as a two-factor authenticator app for any website or platform you want, and manage your 2FA codes alongside your passwords in the following way:

1. Go to the security settings of the website or application where you want to enable the 2FA feature. Typically, you will be presented with a QR code or a verification code during the process.
2. Launch Bitdefender SecurePass, and access the corresponding account you want to configure for 2FA use. Click the **Edit** button.
3. Scroll to the bottom of the account entry page in SecurePass and press on the **Two-factor authentication** option.
4. Scan the QR code or enter the code manually.

   Once this is done, SecurePass will confirm the successful two-factor authentication setup.
5. After this, press the new **View Code** button now visible in the interface. A time-sensitive code is displayed there.
6. Go back to the account where you enabled the 2FA feature and input the code from Bitdefender SecurePass to verify your setup.

After completing this setup process, press the **Save Account** button in SecurePass to finalize the process.

From now on, when singing in on the platform for which you have set up the 2FA feature, you will be prompted to use SecurePass' 2FA codes for the respective account, offering a new layer of security for the account in question.

6. SHARE DATA

Bitdefender SecurePass comes with the possibility of sharing sensitive information securely, such as credentials, passwords or credit card details.

You may use the sharing feature via links:

1. Choose an item stored in your vault.
    - In browser:
      Go to your vault and click on the item you want to share. On the right side, click on the three-dots menu and select **Share link**.
    - In app:
      Go to your vault and tap on the item you want to share. Tap on the link icon and choose the **Generate share link** option.
2. Create the Share link by specifying:
    - The expiration date of the link.
    - The usage limit.
    - Whether or not the link should be password-protected.
3. Once generated, copy the generated link and send it to the intended recipient.

6.1. Share with Groups

Groups are created for the purpose of making data sharing even easier. You can create various groups within Bitdefender SecurePass with other users to securely share sensitive data:

1. Create a Group:
    - Go to **Groups** and press the **Create group** button within the Groups tab.
    - Set a group name and then press the **Create group** button.
2. Add items to Groups:
    - In browser:

    Go to your vault and click on the item you want to share. Click the three-dots menu on the right side of the item and choose **Add to group**.

  - In app:
    Go to your vault and click on the item you want to share. Choose the **Share with group** option.

   Select the group you want to share the item with.

3. Set the access rights (read, write, grant) based on the level of control you want to provide group members with.

4. Press **Save**, then **Done**.

You and group members can review shared items in the group's section.

6.2. Manage Groups

In the **Groups** section of Bitdefender SecurePass you can review all created groups and manage them based on your needs:

- Rename groups.
- Edit members. (invite new members, assign rights to specific members, granting admin or sharing rights, and remove existing members)
- Leave groups.
- Delete groups.

7. LOCK ACCOUNT

Bitdefender SecurePass comes with a **Lock Account** function that instantly locks your account and terminates all active sessions across all devices that have access to it. This feature is especially handy when any suspicions of unauthorized access arise.

To lock your SecurePass account:

1. Open Bitdefender SecurePass.
2. Once in SecurePass:
   - In browser:
     Click on **Settings** in the top-right corner of the page.
   - In the mobile app:
     Tap on the **Secure me** menu button.
3. Press the **Lock Account** button to log out instantly from all devices and terminate ongoing sessions.

8. FREQUENTLY ASKED QUESTIONS

Some common questions about Bitdefender SecurePass tend to reoccur. Here you can learn more about your Bitdefender account, importing passwords, data security protocols, and other related topics.

General questions about Bitdefender SecurePass

What happens when Bitdefender SecurePass expires?

Once your SecurePass subscription expires and is no longer active, you will have a maximum of 90 days to export your passwords. Your passwords will be backed up for another 30 days. During those 90 days, you will only be able to export your data. You cannot continue to use SecurePass. The auto-fill feature will stop working, as well as the ability to generate passwords.

At the end of the 90-day grace period, you have 30 extra days to contact Bitdefender support and request to restore your passwords back to the live database. You will then be able to export your passwords from Bitdefender SecurePass.

Your data will be kept in the live database only until the end of the day it was restored on demand. At midnight the database is erased – and if you have not yet exceeded the 30-day extra period, passwords can be restored again from backup. Raw database data from the backup can be provided upon request to the user, but the database is encrypted and the information cannot be accessed.

What is a Master Password, and why do I have to remember it?

The Master Password is the key that unlocks the door to all the passwords stored in your Bitdefender SecurePass account. The master password must be at least 8 characters long. So create a strong master password, memorize it, and never share it with anyone. To create a strong master password, we recommend you use a combination of uppercase and lowercase letters, numbers, and special characters (like #, $, or @).

Why don't you store my Master Password, and what happens if I forget it?

The reason why we don't store your Master Password on our servers is so that only you can access your account. It's the most secure way. If Bitdefender SecurePass does not recognize your master password, make sure you type it correctly and the Caps Lock key is not active on the keyboard.

If you forget the master password, you can always use the Recovery Key to unlock your SecurePass account. During the sign-up process, Bitdefender SecurePass provides a **recovery key** that can be used to regain access to the account without losing your data.

What is Offline mode?

Offline mode is automatically activated when the Internet connection drops while using Bitdefender SecurePass. If you are already signed in and have entered your master password, Offline mode lets you access your passwords when an Internet connection is out of reach.

How do I uninstall Bitdefender SecurePass?

To uninstall Bitdefender SecurePass:

- On Windows and macOS:
  Remove the SecurePass extension from your web browser. Right-click on the Bitdefender icon and select “Remove”.
- On Android:
  Tap and hold the SecurePass app, then drag it to the top of the screen where it says “Uninstall”.
- On iOS & iPadOS:
  Tap and hold the SecurePass app until all apps on your screen begin wiggling, then tap the X to the top left of the Bitdefender icon.

Privacy & Security questions about Bitdefender SecurePass

Could Bitdefender employees see my passwords?

Absolutely not. Your privacy is our top priority. This is the main reason why we do not store your master password on our data servers: so that no one has access to your account, not even company employees. Every password and account are highly encrypted with the strongest data security algorithm, and the code we see simply looks like a random string of numbers and letters jumbled together.

What would happen if SecurePass' servers were hacked?

Each password is encrypted locally on your device before it gets anywhere near our servers, so if hackers were to break into our system, they would only get pages of random letters and numbers without your key to decrypt them. This means that you and your account details are always safe with us.

9. GETTING HELP

9.1. Asking for Help

Bitdefender provides its customers with an unparalleled level of fast and accurate support. If you experience any issue or if you have any question about your Bitdefender product, you can use several online resources to find a solution or an answer.

9.2. Online Resources

Several online resources are available to help you solve your Bitdefender-related problems and questions.

- Bitdefender Support Center:
  https://www.bitdefender.com/consumer/support/
- The Bitdefender Expert Community:
  https://community.bitdefender.com/en/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

You can also use your favorite search engine to find out more information about computer security, the Bitdefender products and the company.

9.2.1. Bitdefender Support Center

The Bitdefender Support Center is an online repository of information about the Bitdefender products. It stores, in an easily accessible format, reports on the results of the ongoing technical support and bugfixing activities of the Bitdefender support and development teams, along with more general articles about threat prevention, the management of Bitdefender solutions with detailed explanations, and many other articles.

The Bitdefender Support Center is open to the public and freely searchable. The extensive information it contains is yet another means of providing Bitdefender customers with the technical knowledge and insight they need. All valid requests for information or bug reports coming from Bitdefender clients eventually find their way into the Bitdefender Support Center, as bugfix reports, workaround cheatsheets or informational articles to supplement product helpfiles.

The Bitdefender Support Center is available any time at at the following address: https://www.bitdefender.com/consumer/support/.

9.2.2. The Bitdefender Expert Community

The Expert Community is an environment where Bitdefender users, enthusiasts and fans can engage, exchange ideas, support each other and share their knowledge and solutions. It is also a place of ideation and provides valuable feedback to our development teams. The community members are experienced Bitdefender users happy to help other peers on their own time.

Here you will find meaningful conversations with people that use Bitdefender on their devices. The community offers a true connection with our members and makes your voice heard. It is a place where you are encouraged to participate knowing that your opinion and input are respected and cherished. As a valued provider, we strive to offer an unparalleled level of fast, accurate support and we wish to bring our users closer to us. We have designed our community with this purpose in mind.

You can find our Expert Community webpage here:

https://community.bitdefender.com/en/

9.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia has all the info you need about the latest cyber-threats. This is the place where Bitdefender experts share tips & tricks about how to stay protected from hackers, data breaches, identity theft and social impersonation attempts.

The Bitdefender Cyberpedia webpage can be found here:

https://www.bitdefender.com/cyberpedia/.

9.3. Contact Information

Efficient communication is the key to a successful business. Since 2001 BITDEFENDER has established an unquestionable reputation by constantly striving for better communication so as to exceed the expectations of our clients and partners. Should you have any questions, do not hesitate to contact us directly through our **Bitdefender Support Center:**

https://www.bitdefender.com/consumer/support/

9.3.1. Local distributors

The Bitdefender local distributors are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters.

To find a Bitdefender distributor in your country:

1. Go to https://www.bitdefender.com/partners/partner-locator.html.
2. Choose your country and city using the corresponding options.

GLOSSARY

Activation code

Is a unique key that can be bought from retail and used to activate a specific product or service. An activation code enables the activation of a valid subscription for a certain period of time and number devices and can also be used to extend a subscription with the condition to be generated for the same product or service.

ActiveX

ActiveX is a model for writing programs so that other programs and the operating system can call them. ActiveX technology is used with Microsoft Internet Explorer to make interactive webpages that look and behave like computer programs, rather than static pages. With ActiveX, users can ask or answer questions, use push buttons, and interact in other ways with the webpage. ActiveX controls are often written using Visual Basic. Active X is notable for a complete lack of security controls; computer security experts discourage its use over the internet.

Advanced persistent threat

Advanced persistent threat (APT) exploits vulnerabilities of systems to steal important information to deliver it to the source. Big groups such as organizations, companies, or governments, are targeted by this threat. The objective of an advanced persistent threat is to remain undetected for a long time being able to monitor and gather important information without damaging the targeted machines. The method used to inject the threat into the network is through a PDF file or an Office document that look harmless so that every user can run the files.

Adware

Adware is often combined with a host app that is provided at no charge as long as the user agrees to accept the adware. Because adware apps are usually installed after the user has agreed to a licensing agreement that states the purpose of the app, no offense is committed. However, pop-up advertisements can become an annoyance, and in some cases degrade system performance. Also, the information that some of these apps collect may cause privacy concerns for users who were not fully aware of the terms in the license agreement.

Archive

A disk, tape, or directory that contains files that have been backed up.

A file that contains one or more files in a compressed format.

Backdoor

A hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers.

Boot sector

A sector at the beginning of each disk that identifies the disk's architecture (sector size, cluster size, and so on). For startup disks, the boot sector also contains a program that loads the operating system.

Boot virus

A threat that infects the boot sector of a fixed or floppy disk. An attempt to boot from a diskette infected with a boot sector virus will cause the threat to become active in memory. Every time you boot your system from that point on, you will have the threat active in memory.

Botnet

The term “botnet” is composed of the words “robot” and “network”. Botnets are internet-connected devices infected with threats and can be used to send spam emails, steal data, remotely control vulnerable devices, or spread spyware, ransomware, and other kinds of threats. Their objective is to infect as many connected devices as possible, such as PCs, servers, mobile or IoT devices belonging to big companies or industries.

Browser

Short for web browser, a software app used to locate and display webpages. Popular browsers include Microsoft Internet Explorer, Mozilla Firefox and Google Chrome. These are graphical browsers, which means that they can display graphics as well as text. In addition, most modern browsers can present multimedia information, including sound and video, though they require plug-ins for some formats.

Brute Force Attack

Password guessing attack used to break into a computer system by entering possible password combinations, mostly starting with the easiest-to-guess password.

Command line

In a command line interface, the user types commands in the space provided directly on the screen using command language.

Cookies

Within the internet industry, cookies are described as small files containing information about individual computers that can be analyzed and used by advertisers to track your online interests and tastes. In this realm, cookie technology is still being developed and the intention is to target ads directly to what you've said your interests are. It's a double-edge sword for many people because on one hand, it's efficient and pertinent as you only see ads about what you're interested in. On the other hand, it involves actually "tracking" and "following" where you go and what you click. Understandably so, there is a debate over privacy and many people feel offended by the notion that they are viewed as a "SKU number" (you know, the bar code on the back of packages that gets scanned at the grocery check-out line). While this viewpoint may be extreme, in some cases it is accurate.

Cyberbullying

When peers or strangers are committing abusive acts against children on purpose to physically hurt them. To damage emotionally, the assaulters are sending mean messages or unflattering photos, thus making their victims isolate from others or feel frustrated.

Dictionary Attack

Password guessing attacks used to break into a computer system by entering a combination of common words to generate potential passwords. The same method is used to guess decryption keys of encrypted messages or documents. Dictionary attacks succeed because many people incline to choose short and single words passwords that are easy to be guessed.

Disk drive

It's a machine that reads data from and writes data onto a disk. A hard disk drive reads and writes hard disks. A floppy drive accesses floppy disks. Disk drives can be either internal (housed within a computer) or external (housed in a separate box that connects to the computer).

Download

To copy data (usually an entire file) from a main source to a peripheral device. The term is often used to describe the process of copying a file from an online service to one's own computer. Downloading can also refer to copying a file from a network file server to a computer on the network.

Email

Electronic mail. A service that sends messages on computers via local or global networks.

Events

An action or occurrence detected by a program. Events can be user actions, such as clicking a mouse button or pressing a key, or system occurrences, such as running out of memory.

Exploits

A way to take advantage of different bugs or vulnerabilities that are present in a computer (software or hardware). Thus, hackers may gain the control of computers or networks.

False positive

Occurs when a scanner identifies a file as infected when in fact it is not.

Filename extension

The portion of a filename, following the final point, which indicates the kind of data stored in the file. Many operating systems use filename extensions, e.g. Unix, VMS, and MS-DOS. They are usually from one to three letters (some sad old OSes support no more than three). Examples include "c" for C source code, "ps" for PostScript, "txt" for arbitrary text.

Heuristic

A rule-based method of identifying new threats. This method of scanning does not rely on specific threat information database. The advantage of the heuristic scan is that it is not fooled by a new variant of an existing threat. However, it might occasionally report suspicious code in normal programs, generating the so-called "false positive".

Honeypot

A decoy computer system set to attract hackers to study the way they act and identify the heretical methods they use to collect system information. Companies and corporations are more interested in implementing and using honeypots to improve their overall state of security.

IP

Internet Protocol - A routable protocol in the TCP/IP protocol suite that is responsible for IP addressing, routing, and the fragmentation and reassembly of IP packets.

Java applet

A Java program which is designed to run only on a webpage. To use an applet on a webpage, you would specify the name of the applet and the size (length and width, in pixels) that the applet can utilize. When the webpage is accessed, the browser downloads the applet from a server and runs it on the user's machine (the client). Applets differ from apps in that they are governed by a strict security protocol.

For example, even though applets run on the client, they cannot read or write data onto the client's machine. Additionally, applets are further restricted so that they can only read and write data from the same domain that they are served from.

Keylogger

A keylogger is an app that logs anything you type. Keyloggers are not malicious in nature. They can be used for legitimate purposes, such as monitoring employees or children activity. However, they are increasingly being used by cyber-criminals for malicious purposes (for example, to collect private data, such as login credentials and social security numbers).

Macro virus

A type of computer threat that is encoded as a macro embedded in a document. Many apps, such as Microsoft Word and Excel, support powerful macro languages. These apps allow you to embed a macro in a document, and have the macro execute each time the document is opened.

Mail client

An email client is an app that enables you to send and receive email.

Memory

Internal storage areas in the computer. The term memory identifies data storage that comes in the form of chips, and the word storage is used for memory that exists on tapes or disks. Every computer comes with a certain amount of physical memory, usually referred to as main memory or RAM.

Non-heuristic

This method of scanning relies on specific threat information database. The advantage of the non-heuristic scan is that it is not fooled by what might seem to be a threat, and does not generate false alarms.

Online predators

Individuals who seek to attract minors or adolescents into conversations on purpose to involve them into illegal sexual activities. Social networks are the ideal place where vulnerable children can easily be hunted and seduced into committing sexual activities, online or face-to-face.

Packed programs

A file in a compression format. Many operating systems and apps contain commands that enable you to pack a file so that it takes up less memory. For example, suppose you have a text file containing ten consecutive space characters. Normally, this would require ten bytes of storage.

However, a program that packs files would replace the space characters by a special space-series character followed by the number of spaces being replaced. In this case, the ten spaces would require only two bytes. This is just one packing technique - there are many more.

Path

The exact directions to a file on a computer. These directions are usually described by means of the hierarchical filing system from the top down.

The route between any two points, such as the communications channel between two computers.

Phishing

The act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The email directs the user to visit a website where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the user's information.

Photon

Photon is an innovative non-intrusive Bitdefender technology, designed to minimize the performance impact of your security solution. By monitoring your PC's activity in the background, it creates usage patterns that help optimize booting and scanning processes.

Polymorphic virus

A threat that changes its form with each file it infects. Since they have no consistent binary pattern, such threats are hard to identify.

Port

An interface on a computer to which you can connect a device. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Externally, personal computers have ports for connecting modems, printers, mice, and other peripheral devices.

In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

Ransomware

Ransomware is a malicious program that tries to make money from users by locking their vulnerable systems. CryptoLocker, CryptoWall, and TeslaWall, are only some variants that hunt personal systems of users.

The infection can be spread by accessing spam emails, downloading email attachments, or installing apps, without letting the user know about what is happening on his system. Daily users and companies are targeted by ransomware hackers.

Report file

A file that lists actions that have occurred. Bitdefender maintains a report file listing the path scanned, the folders, the number of archives and files scanned, how many infected and suspicious files were found.

Rootkit

A rootkit is a set of software tools which offer administrator-level access to a system. The term was first used for the UNIX operating systems and it referred to recompiled tools which provided intruders administrative rights, allowing them to conceal their presence so as not to be seen by the system administrators.

The main role of rootkits is to hide processes, files, logins and logs. They may also intercept data from terminals, network connections or peripherals, if they incorporate the appropriate software.

Rootkits are not malicious in nature. For example, systems and even some apps hide critical files using rootkits. However, they are mostly used to hide threats or to conceal the presence of an intruder into the system. When combined with threats, rootkits pose a great threat to the integrity and the security of a system. They can monitor traffic, create backdoors into the system, alter files and logs and avoid detection.

Script

Another term for macro or batch file, a script is a list of commands that can be executed without user interaction.

Spam

Electronic junk mail or junk newsgroup postings. Generally known as any unsolicited email.

Spyware

Any software that covertly gathers user information through the user's internet connection without his or her knowledge, usually for advertising purposes. Spyware apps are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the internet; however, it should be noted that the majority of shareware and freeware apps do not come with spyware. Once installed, the spyware monitors user activity on the internet and transmits that information in the background to someone else. Spyware can also gather information about email addresses and even passwords and credit card numbers.

Spyware's similarity to a Trojan horse threat is the fact that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's internet connection. Because spyware is using memory and system resources, the apps running in the background can lead to system crashes or general system instability.

Startup items

Any files placed in this folder will open when the computer starts. For example, a startup screen, a sound file to be played when the computer first starts, a reminder calendar, or apps can be startup items. Normally, an alias of a file is placed in this folder rather than the file itself.

Subscription

Purchase agreement that gives the user the right to use a particular product or service on a specific number of devices and for a certain period of time. An expired subscription can be automatically renewed using the information provided by the user at the first purchase.

System tray

Introduced with Windows 95, the system tray is located in the Windows taskbar (usually at the bottom next to the clock) and contains miniature icons for easy access to system functions such as fax, printer, modem, volume, and more. Double click or right-click an icon to view and access the details and controls.

TCP/IP

Transmission Control Protocol/Internet Protocol - A set of networking protocols widely used on the internet that provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic.

Threat

A program or piece of code that is loaded onto your computer without your knowledge and runs against your will. Most threats can also replicate themselves. All computer threats are manmade. A simple threat that can copy itself over and over again is relatively easy to produce. Even such a simple threat is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of threat is one capable of transmitting itself across networks and bypassing security systems.

Threat Information Update

The binary pattern of a threat, used by the security solution to detect and eliminate the threat.

Trojan

A destructive program that masquerades as a benign app. Unlike malicious software programs and worms, Trojans do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse threats is a program that claims to rid your computer of threats but instead introduces threats onto your computer.

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

Update

A new version of a software or hardware product designed to replace an older version of the same product. In addition, the installation routines for updates often check to make sure that an older version is already installed on your computer; if not, you cannot install the update.

Bitdefender has its own update feature that allows you to manually check for updates, or let it automatically update the product.

Virtual Private Network (VPN)

Is a technology that enables a temporary and encrypted direct connection to a certain network over a less secure network. This way, sending and receiving data is secure and encrypted, difficult to be caught by snoopers. A proof of security is the authentication, which can be done only using a username and password.

Worm

A program that propagates itself over a network, reproducing itself as it goes. It cannot attach itself to other programs.