Test Orientation Guide for Beta Testers

This guide is intended to help beta testers explore the new features and give a sense of what to expect from the product, and not to be used as a test plan or test suite.

We are most interested in your feedback regarding Bitdefender BETA not only in terms of product defects but also regarding the ease of use and maybe missing functionality that you believe to be important and wish to be added in the future. We strive to build a product that you feel comfortable using, so we appreciate any feedback regarding situations when you feel things could go smoother (not enough information, options that are hard to understand or to use if you need them, any product behavior that you find hard to understand).

1. Installation

Where can I find it?

Well, if you have this document you probably already have the installation kit. If not, check the Bitdefender website for the beta kit.

What does it do?

As a beta tester you should be familiar with this one.

The installation kit is in online format, meaning that it will download the necessary files during setup and this process might take a few minutes, depending on your internet connection speed.

Aside from the obvious, the installation phase is also where the first scan for active malware on the system is performed. If no malware is found you are good to go but otherwise, the disinfection process is triggered.

How can it be tested?

a. One of the simplest tests is the straight forward one. Get the installer, run it and install Bitdefender.
b. Bitdefender detects active malware during installation and removes it. If you encounter problems during this process it would be best to report them.
c. Settings available in the installation wizard are yet another thing to test.
d. The uninstall process is another functionality to test.

Important: For any installation issues like: install failed, download failed, uninstall failed, repair failed or even if a retry is prompted, it's very important to attach the install logs to your feedback. You can find the installation logs, depending on your operating system in these 2 locations:

XP:

*C:\Documens and Settings\All users\Application Data*

Vista/Win7/Win8:

C:\ProgramData

All files that have a ".bin" extension and have a name similar to this "1351070153.bdinstall.bin" should be attached to your feedback.

2. Security Report

Where can I find it?

It's this little button within the main interface top right corner (the highlighted button from the picture below). Well actually, through this button you can access it once it is generated. This report will be generated once a week, but for beta testing purposes the interval of time needed to generate a Security Report is 2 days. There is a way of generating a report faster that will be described in the "How can it be tested" section below.
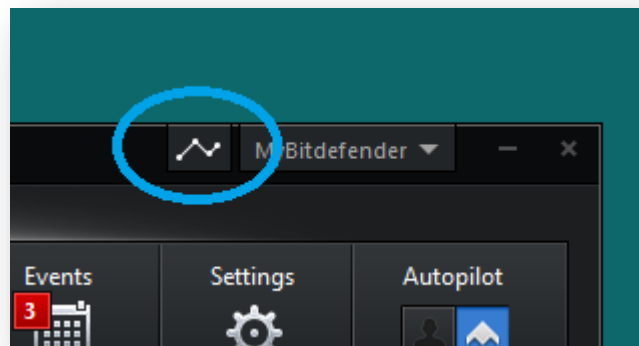

What does it do?

Security Report it's a once a week insight within the activity of your Bitdefender security solution. It also shows you a small set of suggestions for what you could do more in order to achieve a higher level of security.
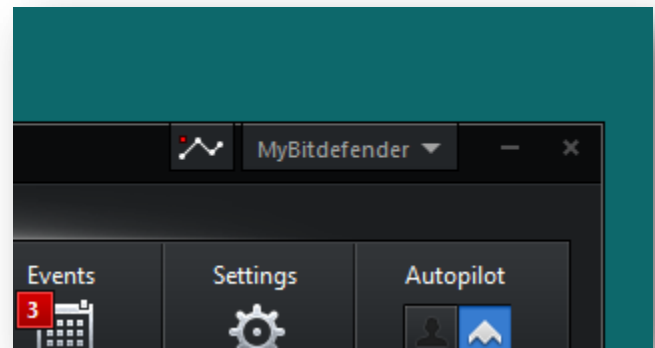
How can it be tested?

First of all, this is a report and the information contained by it is based on activity on your system, so there should be a period of time for data gathering. As stated in the "Where can I find it" section, a 2 days period is necessary (for beta only) to gather the information needed for the report. When the Security Report is generated, a popup message will appear informing you of its availability and also a small change in the user interface will be triggered. This change is shown with the help of the before and after pictures below:

<div align="center">
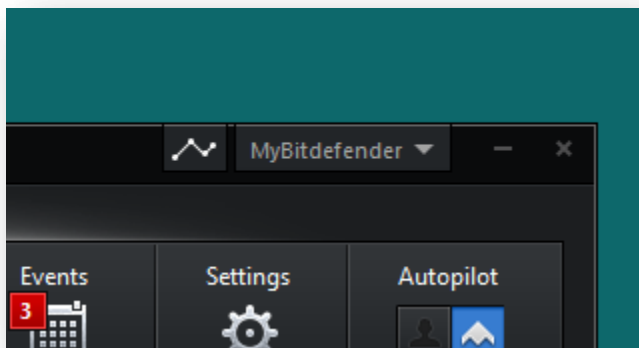
Before - Security Report unavailable   **After - Security Report available**

</div>

Moving on to functionality details, the information gathering process is triggered every hour and a half, or at system shutdown/restart. Knowing this, to forcefully generate a report, what you could do is change your computer's date and time settings to 2-3 days in the future, restart your computer and voila, the little red dot will appear in the main user interface allowing you to open the Security Report.

Once you click that button, the dot will disappear. The report will be opened in your default browser if one of these browsers is set as default: Chrome, Firefox, Internet Explorer. Otherwise, Internet Explorer will be used.

A few tests:

    a.   Check that you are notified when a report is available;
    b.   Check that the information contained in the report reflects the activity on your system;
    c.   Check if the report is properly displayed within the supported browsers;
   d.   Check what happens when a supported browser is not installed and you want to see a report.

3. Bitdefender Wallet

Where can I find it?

Mainly this feature can be accessed through the main interface (it's not among the first four panels, so you will have to scroll through the panels to find it) but it's not limited to that. After installation of Bitdefender Total Security Beta, when you open one of the supported browsers (Firefox, Chrome, Internet Explorer) Bitdefender Wallet will introduce itself to you. The Bitdefender Wallet can also be opened from Safepay in order to easily access the credit card details and online banking credentials.
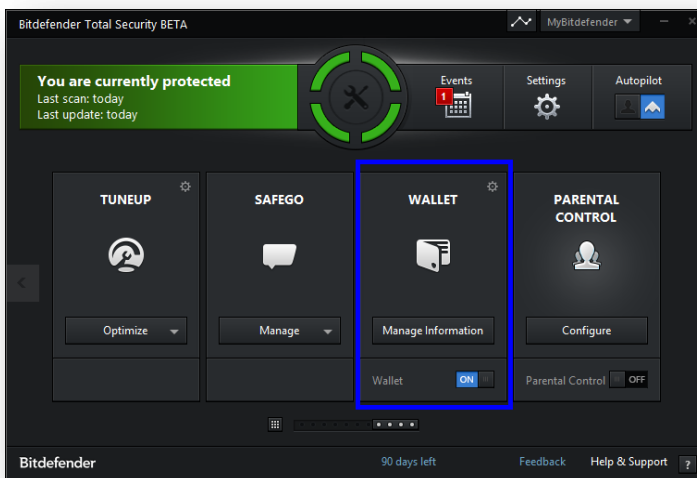
Wallet in main UI
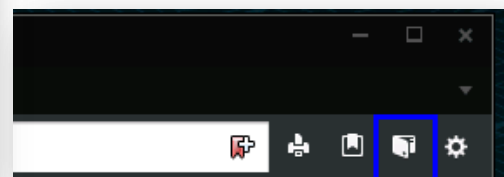
Wallet in Safepay

What does it do?

Bitdefender Wallet is an easy way to store sensitive information like websites logins, emails, passwords and other personal information, in a secure manner, without having to remember any of it while allowing you, and only you access to it.

Before you can use Bitdefender Wallet, a three steps wizard has to be walked through. This wizard will allow you to import a previously created database or start fresh with a new one and will ask a password for your wallet (beware that the password can't be changed and it isn't stored anywhere, so you'd better remember it or else the data stored in your wallet will be out of your reach).

Most of the information is stored and available for you to manually access, except for website logins, like Facebook, Gmail or any other site that asks you for a user and a password. In this case, Bitdefender Wallet will automatically gather your login information and also fill in the credentials when you navigate to a site for which the login information is already stored.

How can it be tested?

The integration with browsers is done by add-ons/browser extensions. This limits the integration to 3 most used browsers: Chrome, Firefox and Internet Explorer. After installation of Bitdefender Total Security Beta, the browser extensions will be ready to be activated and used the first time you will open your browser.

A few tests:

a. After Bitdefender Wallet was configured, make sure the "Save automatically without asking" option is selected from Main User Interface->Wallet settings->Autofill. Open one of the supported browsers, access a web page that has a login form and enter your account on that page (for instance facebook.com). Once the login is completed, check Bitdefender Wallet to see if the login information is stored, as it's supposed to.

b. Access the same web page and check that the information stored in the previous step is automatically filled by Bitdefender Wallet.

c. From the Main User Interface->Wallet Settings, disable the support for a specific browser and check that this setting is correctly handled.

d. Change the settings and verify their effect. Check that there are no unforeseen effects.

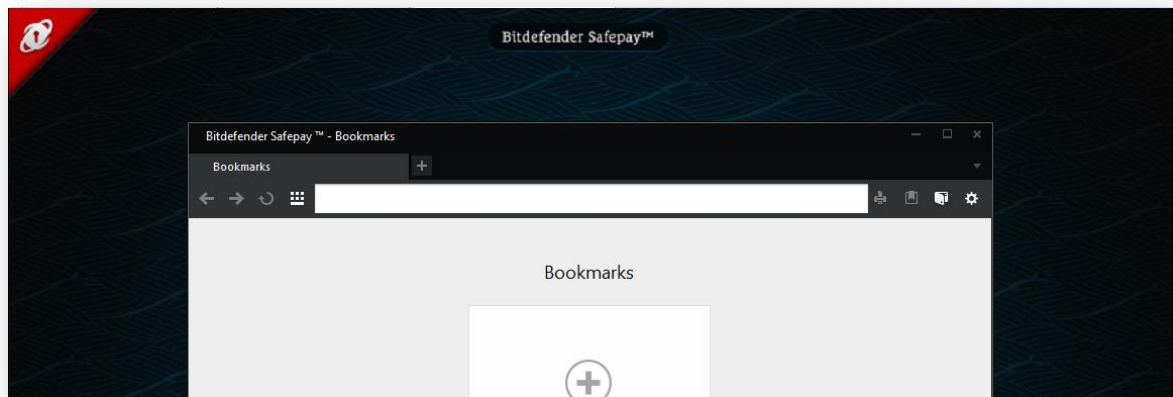e. Add information to your wallet and check how much it can store.

4. Safepay

Where can I find it?

On your desktop as this stylish shortcut:

And this is how it looks:

What does it do?

Using your computer for handling money online is a thing of the present and almost everybody is doing it one way or another by shopping and paying online, managing an online bank account, donating money etc. If a malware infested computer is used to handle money, one can… well lose their money. You could argue that the antivirus will protect your computer for malware, but no matter how good is the detection of an antivirus, another layer of protection is an extremely good way to keep your money in your accounts, especially from the so called zero day malware.

So… what is this extra layer of protection? Safepay is a protected browser running in a secured desktop.

Safepay blocks keyloggers that may steal your credentials for commercial or fraudulent purposes, prevents tempering attempts that other browsers are exposed to and much more.

Safepay can be used as any other browser but is designed having security as first priority. This means you may encounter problems in displaying video content or downloading files because some actions are automatically blocked in order to prevent malware injection and other vulnerabilities.

In this new version of Bitdefender, Safepay is integrated with Bitdefender Wallet (described in the previous point) for an easy way to access your private information stored there.

How can it be tested?

a. First of all, Safepay is not meant to be used as a default browser, but also it should be fairly easy to use. This is why we implemented a mechanism of detecting banks and payment sites, while you browse with your favorite browser, and automatically starting Bitdefender Safepay. Having

this said, the first thing to test is the automatic detection of payment/banking web sites. This test should not be done with only one site and assume that it works but it should be done with as many sites possible, international and local, secured or unsecured and report all sites that do not trigger Safepay.

b. For sites that are not automatically detected, Safepay includes a "Favorite sites" option. Adding a web site as one of your favorite sites will trigger Bitdefender Safepay every time you browse to that web site in another browser, so this is another feature to test. (Note that to disable the automatic trigger of Safepay for a site added as favorite, you need to check the settings menu from Safepay).

c. Check that Safepay detects the usage over an open wifi network and enables the VPN connection.

5. Every other functionality

Where can I find it?
Most of them can be discovered while browsing the interface but not only like that (see the Bitdefender Browser Toolbar)

What does it do?
You will have to find out by yourself. Most of them should be self-explanatory.

How can it be tested?
Just use your imagination and try to break the software.

Important notes

A few good practice rules for useful feedback:

1. Use a representative title for your feedback.

    As your feedback is publicly available to all beta testers, if a feedback title is generic the chance to be found by another beta tester is diminished and duplicate issues will be reported. Also we have to process all of your feedback and you can help us by using a relevant title for the issue.

2. Give as many details as possible.

    One-liner feedback is rarely useful without screenshots, logs, crash dumps or memory dumps. Also, this kind of report will most likely generate a ping pong between you and our team anyway. In order to obtain the necessary information to reproduce the bug it would be best, if possible of course, to add the steps that reproduce the issue (like first do this and then click on that and this issue will arise).

3. Try not to cramp too many issues under one feedback report.

    Having many issues under one feedback, although at first might seem easy to read, after a while it becomes hard to manage.