



Orientation Guide

for Bitdefender Beta 2018 testers



This guide is intended to help beta testers explore our 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.

Best Practice Rules

A few good practice rules for useful feedback:

1. Use a representative title for your feedback.

Using a representative title will help us greatly in processing your feedback and addressing the issue you are reporting in a subsequent update.

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 in order to obtain the necessary information to reproduce the bug, so it would be best, if possible of course, to add the steps to 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 easier to read, after a while it becomes hard to manage so it's a good practice to file a separate issue for each feedback.



[Update] How to install Bitdefender 2018 BETA

To install Bitdefender Total Security 2018 BETA, go to [Bitdefender Central](#) and login with your existing Bitdefender account or create a new Bitdefender account.

After you successfully log in, click on the “INSTALL BITDEFENDER” button and then click DOWNLOAD. To install the product, just run the software you downloaded.



Webcam Protection

You can find Webcam Protection in Privacy features > Webcam Protection.

Webcam Protection restricts access to your webcam. Only trusted applications will be allowed to grab image, keeping you protected against malware or hackers that might be trying to snoop in on your activities.

Application we know to be clean are automatically allowed access to your webcam whenever they request it. However, untrusted applications are automatically blocked and you are notified immediately.

Webcam protection also allows you to block access to the webcam for all applications, so nobody can snoop on you while you are away from the computer.

How to test this feature?

You can initiate video conference calls on popular conference web apps or native Windows applications. Check to see the browsers or applications you use appear in the Webcam access list as allowed.

- Try blocking one of these applications and initiate a new video conference using it. Bitdefender should notify you that the application was blocked from gaining access to the webcam and the video conference should not work.

If some of the applications you use have weird behaviors when being blocked by Bitdefender or even generate crashes, please send us the feedback.

- Try setting Webcam Protection on verbose mode by enabling notification for allowed applications. Check if you receive the notification whenever you start a video conference.
- Try blocking webcam access to all applications and check whether video calls still work. Do the same thing for browsers and try to start a video conference using a dedicated web application.



Advanced Threat Defense

You can find Advanced Threat Defense in Protection features > Advanced Threat Defense.

The new Advanced Threat Defense technology identifies suspicious processes and actively protects your system from even the most advanced malware.

How to test this feature?

This one should be really hard to test. Just let us know of any crashes or glitches in the UI. Meanwhile, Advanced Threat Defense will keep your computer safe from even the newest malware, including advanced exploits.

[Update] Advanced Threat Defense features a new UI that enables you to view blocked threats on your computer, including advanced attacks like ransomware.

Try adding applications to the whitelist or opening the Advanced Threat Defense screens for threats and ransomware.



[Update] Safe Files for Windows

You can find Safe Files in Protection features > SAFE FILES.

The **Safe Files** feature blocks any unauthorized application access to files in protected folders. By default, Documents, Picture and Desktop are protected. If you have any sync folders on your device, like Dropbox, Google Drive or OneDrive, this will also be automatically protected.

Besides the default protected folders, you can add up to 30 folders of your own.

How to test this feature?

Add and remove different folders in the list. Add up to 30 folders to the list.

Try adding an application to the access list and block its access to protected folders. Open one of the protected files using this application and see what happens.

Allow the same application and open the same file or a different one and see what happens.



[Update] New Bitdefender Firewall UI

You can find Bitdefender Firewall in Protection features > FIREWALL.

Bitdefender Firewall adds an extra layer of protection, by blocking potentially malicious applications that want to connect to the Internet. User personal information stays safe from hackers and data snoops.

The new Firewall has been completely redesigned to improve usability and allow better management of application rules.

How to test this feature?

Here are some guidelines to test the new interface for Bitdefender Firewall:

- Try adding rules to block/allow traffic for specific applications. Those kind of rules should be added to the top of the table rules
- Check that rules are added by default for known applications. Those rules should be added to the bottom of the table rules
- Check that rules order is modified when user changes the known program rules (whitelisted applications by Bitdefender Firewall logic). Rules can be modified either by editing the rule or by changing the access type directly. Modified rules should be at the top of the table
- Try adding conflicting rules with previously created ones
- Try searching for applications by name in search-box.
- Try to reset the rules
- Check to see that the rules are not changed after reboot (especially user created/modified ones)

But we encourage you to use your imagination to discover as many scenarios as possible.



Every other functionality

Just use your imagination and try to break the software.

We thank you again for helping us build better products for you!