



Bitdefender®

**Bitdefender Endpoint
Security Tools for
Linux**

USER'S GUIDE

Bitdefender Endpoint Security Tools for Linux User's Guide

Publication date 2020.12.07

Copyright© 2020 Bitdefender

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

Preface	iv
1. Purpose and Intended Audience	iv
2. Request for Comments	iv
1. About	1
1.1. Features	1
1.2. Interface	1
2. Scanning for Malware	3
2.1. Scan Options	3
2.2. Quarantine	4
2.3. Events	4
3. Product Status and Updates	6
4. Getting Help	7

Preface

1. Purpose and Intended Audience

This documentation is intended for the end users of **Bitdefender Endpoint Security Tools**, the Security for Endpoints client software installed on computers and servers to protect them against malware and other Internet threats and to enforce user control policies.

The information presented herein should be easy to understand by anyone who is able to work under Linux.

2. Request for Comments

Please write to tell us how you think this guide could be improved and help us provide you with the best documentation possible.

Let us know by sending an e-mail to business-docs@bitdefender.com.

1. ABOUT

Bitdefender Endpoint Security Tools (BEST) is a fully-automated computer security program, managed remotely by your network administrator. Once installed, it protects you against all kinds of malware (such as viruses, spyware and trojans), network attacks, phishing and data theft. It can also be used to enforce your organization's computer and Internet use policies.

1.1. Features

Antimalware protection is the foundation of your security. Bitdefender Endpoint Security Tools protects you in real time and on demand against all sorts of malware, such as viruses, trojans, spyware, adware, etc.

- **On-Demand Scanning** allows detecting and removing malware already residing in the system. You can run scan tasks on specified file and folders.
- **On-Access Scanning** prevents new malware threats from entering the system by scanning local and network files when they are accessed (opened, moved, copied or executed), boot sectors and potentially unwanted applications (PUA).
- **Quarantine** contains the list of quarantined files, their original path, quarantine action time and date and their security status.
- **Scan archives** unpacks and scans inside archives.
- **Bitdefender User Interface Tool (bduitool)** is the interactive interface of Bitdefender Endpoint Security Tools, which allows you to run on-demand scan tasks, and view various information, such as: scan logs, quarantined items, important (security) events, and product version and status.

1.2. Interface

With Bitdefender Endpoint Security Tools command line interface (CLI), you can carry out the following operations:

- Run scan tasks
- View quarantined files, scan logs and events
- Launch updates
- View product settings

To use Bitdefender Endpoint Security Tools, run the following command as **root**:



```
$ sudo /opt/BitDefender/bin/bduitool OPTION [PARAMETERS]
```

The command options are described in the following sections.

2. SCANNING FOR MALWARE

The main objective of Bitdefender Endpoint Security Tools is to keep your computer free of malware. It does that primarily by scanning in real time accessed files, e-mail messages and any new files downloaded or copied to your computer. Besides real-time protection, it also allows running scans to detect and remove malware from your computer.

2.1. Scan Options

Run the `bduitool` command with one of the available scan options:

```
get scanprof [full|quick|custom]
```

Display the scan profile settings for the full, quick or a custom scan.

```
scan -s full|quick|task <taskID>|(custom <path1> <path2> ...)
```

Run a full, quick or custom scan or a previous scan task determined by the task ID. For custom scan, you have to specify a list of paths to be scanned (folders and/or files) where you can also use wildcards.

For example, use:

```
scan -s full to run a full scan.
```

```
scan -s task <taskID> to run the task with the specified task ID.
```

```
scan -s custom /home/user1/folder1 /home/user1/file.txt  
to run a custom scan on the specified file and folders.
```

If using wildcards for custom scans, please keep in mind the following:

```
scan -s custom /dir/*/dir expands a single directory level.
```

```
scan -s custom "/dir/*/dir" expands the full directory tree.
```

```
scan -s custom "/dir/*/dir?" substitutes a single character using  
the question mark (?).
```

```
scan -p
```

Pause all running scan tasks.

```
scan -r
```

Resume all paused scan tasks.

```
scan -q
```

Stop all running or paused scan tasks.

**Note**

The pause, resume or stop commands apply only to scans started from Bitdefender User Interface Tool.

```
get scantasks
```

Display details of all running scan tasks.

```
get scanlog [<taskID>]
```

Display information about the last finished scan task. The command can also display details about the last run of a specific task, if the task ID is mentioned.

```
get scanstatus [<taskID>]
```

Display the status of the scan task with the specified task ID.

2.2. Quarantine

You can display detailed information regarding the quarantined files. Run the `bduioutil` command with one of the available options:

```
get quar [-s <integer_value>]
```

Display a list of quarantined items.

Parameters:

`-s <integer_value>`: Display the specified number of most recent quarantined items.

For example, use:

```
get quar to display all quarantine items.
```

```
get quar -s 10 to display the first 10 items from quarantine.
```

2.3. Events

Bitdefender Endpoint Security Tools keeps a detailed log of events concerning its activity on your computer.

Run the `bduioutil` command with one of the available options:

```
get events [-s <integer value>]
```

Display the list of events that the antimalware module has detected.

Parameters:

`-s <integer value>`: Display the specified number of most recent antimalware events.

`set updatetype <type>`: This parameter sets if the kernel module updates are performed through signature update (default) or product update. The accepted values for `<type>` are *signatures* or *product*.

3. PRODUCT STATUS AND UPDATES

In a world where cyber criminals constantly try to come up with new ways to cause harm, having an up-to-date security program is essential if you are to stay one step ahead of them.

Run the `bduitool` command with one of the available options:

`get ps`

Display information about the product status.

`-v, --version`

Display version information.

`about`

Display information about the product (name, version) and a link to Bitdefender privacy policy.

`update [-p] | [-s] | [-ps]`

Launch an update.

Parameters:

`-s` : Update antimalware signatures.

`-p` : Launch a product update.

`-ps` : Update both signatures and product.



4. GETTING HELP

For any problems or questions concerning Bitdefender Endpoint Security Tools, please contact your network administrator.

For help with the **bdui** command, run it with one of these options:

`-h, --help`

Display this help guide.