FortiClient (Linux) - Release Notes

Version 6.2.6

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

March 10, 2020
FortiClient (Linux) 6.2.6 Release Notes
04-626-611006-20200310

TABLE OF CONTENTS

Change log **4**
Introduction **5**
Installation information **6**
Installing FortiClient (Linux) 6
Installing FortiClient (Linux) using a downloaded installation file 6
Installation folder and running processes 6
Uninstalling FortiClient (Linux) 7
Product integration and support **8**
Resolved issues **9**
GUI 9
Vulnerability Scan 9
Syslog 9
Logs 9
Backend 10
FortiClient Cloud 10
Known issues **11**
Malware Protection 11
Remote Access 11
epctrl 11
FortiManager 11
GUI 12
Update 12

Change log

Date	Change Description
2020-03-10	Initial release.

Introduction

FortiClient (Linux) 6.2.6 is an endpoint product for well-known Linux distributions that provides FortiTelemetry, antivirus, SSL VPN, and Vulnerability Scan features. FortiClient (Linux) can also download and use FortiSandbox signatures.

This document provides a summary of support information and installation instructions for FortiClient (Linux) 6.2.6 build 0356.

- Installation information on page 6
- Product integration and support on page 8
- Resolved issues on page 9
- Known issues on page 11

Review all sections prior to installing FortiClient.

Installation information

Installing FortiClient (Linux)

You can install FortiClient (Linux) on the following operating systems:

- Ubuntu
- CentOS
- Red Hat

For supported versions, see Product integration and support on page 8.

If upgrading from FortiClient (Linux) 6.0.3 or an earlier version using an RPM package, you must first uninstall any version of FortiClient (Linux) earlier than 6.2.6 from the machine.

If upgrading from FortiClient (Linux) 6.0.4 or a later version, you can directly upgrade to FortiClient (Linux) 6.2.6 without first uninstalling the earlier version of FortiClient (Linux).

Installing FortiClient (Linux) using a downloaded installation file

To install on Red Hat or CentOS:

1. Obtain a FortiClient Linux installation rpm file.
2. In a terminal window, run the following command:
   `$ sudo yum install <FortiClient installation rpm file> -y`
   `<FortiClient installation rpm file>` is the full path to the downloaded rpm file.

To install on Ubuntu:

1. Obtain a FortiClient Linux installation deb file.
2. Install FortiClient using the following command:
   `$ sudo apt-get install <FortiClient installation deb file>`
   `<FortiClient installation deb file>` is the full path to the downloaded deb file.

Installation folder and running processes

FortiClient installation folder is `/opt/forticlient`.

In case there are issues, or to report a bug, FortiClient logs are available in `/var/log/forticlient`.

Uninstalling FortiClient (Linux)

To uninstall FortiClient from Red Hat or CentOS:

1. In a terminal window, run the following command:
```
$ sudo yum remove forticlient
```

To uninstall FortiClient from Ubuntu:

1. In a terminal window, run the following command:
```
$ sudo apt-get remove forticlient
```

Product integration and support

The following table lists version 6.2.6 product integration and support information:

Operating systems	• Ubuntu 16.04 and later • CentOS 7.4 and later • Red Hat 7.4 and later All supported with KDE or GNOME
FortiClient EMS	• 6.2.0 and later
FortiOS	• 6.2.0 and later • 6.0.0 and later
FortiSandbox	• 3.1.0 and later • 3.0.0 and later • 2.5.0 and later

Resolved issues

The following issues have been fixed in version 6.2.6. For inquiries about a particular bug, contact Customer Service & Support.

GUI

Bug ID	Description
604509	GUI goes blank when running for a few days.
607479	With EMS disabled, quitting FortiClient (Linux) logs the user out from the Ubuntu 18.04 Desktop session without prompt.

Vulnerability Scan

Bug ID	Description
610150	Update default VCM engine in FortiClient (Linux) to 2.025 or a later version.

Syslog

Bug ID	Description
593683	Redundant system logs fill up syslog.

Logs

Bug ID	Description
601142	FortiClient (Linux) does not generate social media change event if changed from custom to OS or vice-versa.
607390	epctrl sends software inventory to EMS even if there are no updates to software.

Backend

Bug ID	Description
575067	Remove various bash calls from FortiClient (Linux).

FortiClient Cloud

Bug ID	Description
601108	FortiClient (Linux) does not automatically register to FortiClient Cloud after user manually disconnects FortiClient (Linux) from FortiClient Cloud.

Known issues

The following issues have been identified in FortiClient (Linux) 6.2.6. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Malware Protection

Bug ID	Description
542667	AV removable media scan does not work.

Remote Access

Bug ID	Description
615195	VPN fails to establish tunnel when remote is checking the server name extension in SSL VPN client hello message.

epctrl

Bug ID	Description
601401	FortiClient (Linux) should perform on-net/off-net/online/offline calculations.
610458	epctrl fetches software inventory inefficently.

FortiManager

Bug ID	Description
582302	FortiClient (Linux) cannot get signature from FortiManager using HTTPS due to failed certificate check.

GUI

Bug ID	Description
577136	GUI does not reflect update task, showing that it is up-to-date but an older version.
605732	VPN GUI does not refresh properly.

Update

Bug ID	Description
607627	FortiClient (Linux) runs the update task every time the GUI launches.

Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.