



FortiClient (Linux) - Release Notes

Version 6.2.2

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



November 28, 2019

FortiClient (Linux) 6.2.2 Release Notes

04-622-579770-20191128

TABLE OF CONTENTS

Introduction	4
Installation information	5
Installing FortiClient (Linux)	5
Installing FortiClient (Linux) using a downloaded installation file	5
Installation folder and running processes	5
Uninstalling FortiClient (Linux)	6
Product integration and support	7
Resolved issues	8
Avatar	8
Endpoint Control	8
GUI	8
Other	8
Known issues	10
Endpoint Control	10
Vulnerability Scan	10
Other	10
Change log	11

Introduction

FortiClient (Linux) 6.2.2 is an endpoint product for well-known Linux distributions that provides FortiTelemetry, antivirus (AV), 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) 6.2.2 build 0297.

- [Installation information on page 5](#)
- [Product integration and support on page 7](#)
- [Resolved issues on page 8](#)
- [Known issues on page 10](#)

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 7](#).



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 6.2.2 from the machine. If upgrading from FortiClient (Linux) 6.0.4 or a later version, you can directly upgrade to FortiClient (Linux) 6.2.2 without first uninstalling the earlier version of FortiClient (Linux).

Installing FortiClient (Linux) using a downloaded installation file

Installing 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.

Installing 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 6.2.2 product integration and support information:

Operating systems	<ul style="list-style-type: none">• Ubuntu 16.04 and later• CentOS 7.4 and later• Red Hat 7.4 and later All supported with KDE or GNOME
FortiClient EMS	<ul style="list-style-type: none">• 6.2.0 and later
FortiOS	<ul style="list-style-type: none">• 6.2.0 and later• 6.0.0 and later
FortiSandbox	<ul style="list-style-type: none">• 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 6.2.2. For inquiries about a particular bug, contact [Customer Service & Support](#).

Avatar

Bug ID	Description
0548970	FortiClient does not display online/offline status on the avatar page.
0549701	FortiClient always displays avatar source as OS.

Endpoint Control

Bug ID	Description
0566678	FortiClient does not hide the system tray when EMS profile enables it.
0579104	On CentOS, FortiClient creates multiple enteries on EMS for one client.

GUI

Bug ID	Description
0548517	FortiClient GUI shows host tags as clickable.
0557072	jQuery 1 new CVE disclosed on 2019-04-19 (latest release v3.4.1)
0570297	Security vulnerability from lodash library [CVE-2019-10744]

Other

Bug ID	Description
0544043	FortiClient (Linux) using 1024bit certificate.

Bug ID	Description
0561015	Excluded applications in 'vulnerability compliance check' should not be getting tagged in host tag monitor.
0577629	FortiClient (Linux) checks FDS on an hourly basis, but it doesn't find a newer AV signature even if it's available.
0579750	Privilege escalation in FortiClient (Linux) through <code>fctsched</code> .

Common Vulnerabilities and Exposures

Bug ID	Description
	FortiClient (Linux) 6.2.2 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2019-15711• CVE-2019-16152• CVE-2019-16155• CVE-2019-17652

Known issues

The following issues have been identified in FortiClient (Linux) 6.2.2. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

Endpoint Control

Bug ID	Description
0588494	FortiClient in off-net state failed to switch to default EMS profile after EMS deleted off-net profile in the policy.
0587707	FortiClient cannot connect properly with EMS IP address when FQDN is specified in EMS server settings.

Vulnerability Scan

Bug ID	Description
0586898	VCM auto patch doesn't work when auto scan is enabled on signature update with auto patch option.

Other

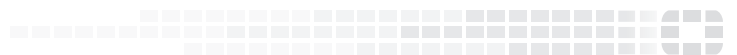
Bug ID	Description
0566687	<i>Antivirus</i> tab is missing realtime protection status.
0566039	Alert user that FortiClient license is expiring because EMS server is unreachable.
0582302	FortiClient cannot get signature from FortiManager using HTTPS because certificate check failed.
0588488	The GUI update doesn't trigger <code>update_tls</code> binary.

Change log

Date	Change Description
2019-10-15	Initial release.
2019-11-28	Updated Common Vulnerabilities and Exposures on page 9.



FORTINET®



Copyright© 2019 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.