



FortiClient (Linux) - Release Notes

Version 6.2.1

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



July 18, 2019

FortiClient (Linux) 6.2.1 Release Notes

04-621-563659-20190718

TABLE OF CONTENTS

Introduction	4
What's new in FortiClient (Linux) 6.2.1	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
Known issues	10
Change log	11

Introduction

FortiClient (Linux) 6.2.1 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) 6.2.1 build 0272.

- [What's new in FortiClient \(Linux\) 6.2.1 on page 5](#)
- [Installation information on page 6](#)
- [Product integration and support on page 8](#)
- [Resolved issues on page 9](#)
- [Known issues on page 10](#)

Review all sections prior to installing FortiClient.

What's new in FortiClient (Linux) 6.2.1

For information about what's new in FortiClient (Linux) 6.2.1, see the [FortiClient & FortiClient EMS 6.2.1 New Features Guide](#).

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 6.2.1 from the machine. If upgrading from FortiClient (Linux) 6.0.4 or a later version, you can directly upgrade to FortiClient (Linux) 6.2.1 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)

Use the following procedure to uninstall FortiClient (Linux) from Red Hat or CentOS operating systems.

To uninstall FortiClient:

1. In a terminal window, run the following command:

```
$ sudo yum remove forticlient
```

Use the following procedure to uninstall FortiClient (Linux) from Ubuntu operating systems.

To uninstall FortiClient:

1. In a terminal window, run the following command:

```
$ sudo apt-get remove forticlient
```

Product integration and support

The following table lists version 6.2.1 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 6.2.1. For inquiries about a particular bug, contact [Customer Service & Support](#).

Bug ID	Description
547653	AV detects only one (the first) file per scan.
548757	epctrl sometimes crashes randomly after the machine keeps running for some time.
549554	FortiClient GUI shows <i>Dynamic Threat Detection</i> as <i>OFF</i> when EMS has enabled it.
557175	FortiClient GUI does not show FortiSandbox IP address.
557867	FortiTray does not start after fresh install on Ubuntu.
558747	fctsched fills up <i>/var/log/messages</i> with logs.
559898	FortiClient scanunit process randomly crashes after AV engine update.
563187	Problem with logs permissions.
565022	FortiClient performs vulnerability scan on every profile change when EMS has <i>Scan on Registration</i> enabled.

Known issues

The following issues have been identified in FortiClient (Linux) 6.2.1. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

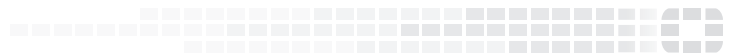
Bug ID	Description
532494	FortiClient sends invalid AVSCANINFO.
547683	FortiClient does not quarantine Eicar file when EMS profile sets <i>Action on Virus Discovery</i> to <i>Quarantine Infected Files</i> .
548517	FortiClient GUI shows host tags as clickable.
548970	FortiClient does not display online/offline status on the avatar page.
549701	FortiClient always displays avatar source as OS.
557082	FortiClient (Linux) scan for file is slow.
562675	User cannot shut down FortiClient from FortiTray in standalone mode on Ubuntu 18.04.
566678	FortiClient does not hide the system tray when EMS profile enables it.
566687	FortiClient AV tab is missing real time protection status.
567858	FortiClient should send all IP addresses to EMS.

Change log

Date	Change Description
2019-07-18	Initial release.



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.