



# FortiClient (Linux) - Release Notes

Version 6.2.3

**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](mailto:techdoc@fortinet.com)



December 27, 2019

FortiClient (Linux) 6.2.3 Release Notes

04-623-597453-20191227

# TABLE OF CONTENTS

<b>Introduction</b> .....	<b>4</b>
<b>Installation information</b> .....	<b>5</b>
Installing FortiClient (Linux) .....	5
Installing FortiClient (Linux) using a downloaded installation file .....	5
Installation folder and running processes .....	5
Uninstalling FortiClient (Linux) .....	6
<b>Product integration and support</b> .....	<b>7</b>
<b>Resolved issues</b> .....	<b>8</b>
Endpoint control .....	8
Update .....	8
Other .....	8
<b>Known issues</b> .....	<b>9</b>
Endpoint control .....	9
Malware Protection .....	9
Vulnerability Scan .....	9
GUI .....	10
Update .....	10
Other .....	10
<b>Change log</b> .....	<b>11</b>

# Introduction

FortiClient (Linux) 6.2.3 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) 6.2.3 build 0324.

- [Installation information on page 5](#)
- [Product integration and support on page 7](#)
- [Resolved issues on page 8](#)
- [Known issues on page 9](#)

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 6.2.3 from the machine. If upgrading from FortiClient (Linux) 6.0.4 or a later version, you can directly upgrade to FortiClient (Linux) 6.2.3 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 6.2.3 product integration and support information:

<b>Operating systems</b>	<ul style="list-style-type: none"><li>• Ubuntu 16.04 and later</li><li>• CentOS 7.4 and later</li><li>• Red Hat 7.4 and later</li></ul> All supported with KDE or GNOME
<b>FortiClient EMS</b>	<ul style="list-style-type: none"><li>• 6.2.0 and later</li></ul>
<b>FortiOS</b>	<ul style="list-style-type: none"><li>• 6.2.0 and later</li><li>• 6.0.0 and later</li></ul>
<b>FortiSandbox</b>	<ul style="list-style-type: none"><li>• 3.1.0 and later</li><li>• 3.0.0 and later</li><li>• 2.5.0 and later</li></ul>

# Resolved issues

The following issues have been fixed in version 6.2.3. For inquiries about a particular bug, contact [Customer Service & Support](#).

## Endpoint control

Bug ID	Description
483287	FortiClient (Linux) fails to send antivirus events to EMS.
579291	FortiClient (Linux) sends vulnerability scan results in each KA.
583017	FortiClient (Linux) Red Hat endpoint cannot send software inventory list to EMS.

## Update

Bug ID	Description
593928	FortiClient (Linux) connects to the wrong FortiGuard distribution server (FDS) when the EMS profile is configured to use the legacy U.S. FDS.
588488	GUI update does not trigger update_tls binary.

## Other

Bug ID	Description
597188	Scheduler crashes upon launch on certain Ubuntu 18.04 installations.

### Common Vulnerabilities and Exposures

Bug ID	Description
	FortiClient (Linux) 6.2.3 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>CVE-2019-16155</li></ul>



# Known issues

The following issues have been identified in FortiClient (Linux) 6.2.3. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

## Endpoint control

Bug ID	Description
567858	FortiClient (Linux) should send all IP addresses to EMS.
588494	FortiClient in off-net state fails to switch to default EMS profile after EMS deletes off-net profile in the policy.
601108	FortiClient (Linux) does not automatically register to FortiClient Cloud after user manually disconnects FortiClient (Linux) from FortiClient Cloud.
601407	EMS shows FortiClient (Linux) status as <i>Remote access is not installed</i> .

## Malware Protection

Bug ID	Description
542667	Antivirus (AV) removable device scan does not work.
566687	FortiClient (Linux) AV tab is missing real time protection status.

## Vulnerability Scan

Bug ID	Description
571740	FortiClient (Linux) does not display some scan results.
583025	Vulnerability scan on signature update with automatic patch does not work.

## GUI

Bug ID	Description
577136	Update task shows older version values but reports that it is up-to-date.
593715	FortiClient (Linux) GUI fails to launch in Ubuntu 19, CentOS 8, and Red Hat 8.
595962	FortiClient (Linux) GUI shows vulnerability results page after automatically patching before the scan runs the second time.
601403	FortiClient (Linux) GUI shows connection to EMS at random times when EMS is unreachable.

## Update

Bug ID	Description
582302	FortiClient (Linux) cannot get signature from FortiManager using HTTPS because of failed certificate check.
582747	FortiClient (Linux) always uses port 443 to connect with FortiGuard distribution server (FDS).
601199	FortiClient (Linux) does not try to connect to failover FDS when enabled in EMS.

## Other

Bug ID	Description
586091	Linux logs show up under FortiClient (Linux) ADOM even if it is dually registered to FortiGate and shows the FortiGate serial number.

# Change log

Date	Change Description
2019-12-19	Initial release.
2019-12-27	Updated <a href="#">Introduction on page 4</a> .



**FORTINET**<sup>®</sup>



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.