



# FortiClient (Linux) - Release Notes

Version 6.2.4

**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)



February 06, 2020

FortiClient (Linux) 6.2.4 Release Notes

04-624-597453-20200206

# 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>
GUI .....	8
Remote Access .....	8
FortiAnalyzer .....	8
FortiGuard Distribution Server (FDS) update .....	8
<b>Known issues</b> .....	<b>9</b>
Malware Protection .....	9
Vulnerability Scan .....	9
GUI .....	9
Update .....	9
<b>Change log</b> .....	<b>10</b>

# Introduction

FortiClient (Linux) 6.2.4 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) 6.2.4 build 0340.

- [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 6.2.4 from the machine. If upgrading from FortiClient (Linux) 6.0.4 or a later version, you can directly upgrade to FortiClient (Linux) 6.2.4 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 6.2.4 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 6.2.4. For inquiries about a particular bug, contact [Customer Service & Support](#).

### GUI

Bug ID	Description
606382	<i>FortiClient update completed</i> notification constantly displays.

### Remote Access

Bug ID	Description
601407	EMS incorrectly displays that Remote Access is not installed.
605964	Remote gateway does not support SSL VPN realms.

### FortiAnalyzer

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

### FortiGuard Distribution Server (FDS) update

Bug ID	Description
582747	FortiClient (Linux) uses port 443 to connect to FDS when EMS specifies a different port.



## Known issues

The following issues have been identified in FortiClient (Linux) 6.2.4. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

### Malware Protection

Bug ID	Description
607037	High CPU usage by antivirus (AV) scan on SVN checkout.
542667	AV removable media scan does not work.

### Vulnerability Scan

Bug ID	Description
583025	Vulnerability scan on signature update with automatic patch does not work.

### GUI

Bug ID	Description
604509	GUI goes blank after running for a few days.

### Update

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

# Change log

Date	Change Description
2020-02-06	Initial release.



**FORTINET**<sup>®</sup>



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.