



# FortiClient (Linux) - Release Notes

Version 6.4.2

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



December 21, 2020

FortiClient (Linux) 6.4.2 Release Notes

04-642-663140-20201221

# TABLE OF CONTENTS

<b>Change log</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
<b>What's new in FortiClient (Linux) 6.4.2</b>	<b>6</b>
<b>Installation information</b>	<b>7</b>
Installing FortiClient (Linux)	7
Installing FortiClient (Linux) using a downloaded installation file	7
Install FortiClient (Linux) from repo.fortinet.com	7
Installation folder and running processes	8
Starting FortiClient (Linux)	8
Uninstalling FortiClient (Linux)	9
<b>Product integration and support</b>	<b>10</b>
<b>Resolved issues</b>	<b>11</b>
License	11
Endpoint control	11
GUI	11
Configuration	12
Malware Protection	12
Vulnerability Scan	12
Remote Access	12
Other	13
<b>Known issues</b>	<b>14</b>
Endpoint control	14
Malware Protection	14
Vulnerability Scan	14
Remote Access	15
Settings	15
Logs	15
Other	15

## Change log

Date	Change Description
2020-12-17	Initial release.
2020-12-21	Added <a href="#">Install FortiClient (Linux)</a> from <a href="https://repo.fortinet.com">repo.fortinet.com</a> on page 7.

# Introduction

FortiClient (Linux) 6.4.2 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) 6.4.2 build 0938.

- [Installation information on page 7](#)
- [Product integration and support on page 10](#)
- [Resolved issues on page 11](#)
- [Known issues on page 14](#)

Review all sections prior to installing FortiClient.

# What's new in FortiClient (Linux) 6.4.2

For information about what's new in FortiClient (Linux) 6.4.2, see the [FortiClient & FortiClient EMS New Features](#).

# 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 10](#).



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 6.4.2 from the machine. If upgrading from FortiClient (Linux) 6.0.4 or a later version, you can directly upgrade to FortiClient (Linux) 6.4.2 without first uninstalling the earlier version of FortiClient (Linux).

---

## Installing FortiClient (Linux) using a downloaded installation file

**To install on Red Hat or CentOS 8:**

1. Obtain a FortiClient Linux installation rpm file.
2. In a terminal window, run the following command:  

```
$ sudo dnf install <FortiClient installation rpm file> -y
```

  
<FortiClient installation rpm file> is the full path to the downloaded rpm file.

If running Red Hat 7 or CentOS 7, replace `dnf` with `yum` in the command in step 2.

**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.

## Install FortiClient (Linux) from [repo.fortinet.com](https://repo.fortinet.com)

**To install on Red Hat or CentOS 8:**

1. Add the repository:  

```
sudo dnf config-manager --add-repo https://repo.fortinet.com/repo/6.4/centos/7/os/x86_64/fortinet.repo
```
2. Install FortiClient:  

```
sudo dnf install forticlient
```

### To install on Red Hat or CentOS 7:

1. Add the repository:  

```
sudo yum-config-manager --add-repo https://repo.fortinet.com/repo/6.4/centos/7/os/x86_64/fortinet.repo
```
2. Install FortiClient:  

```
sudo yum install forticlient
```

### To install on Fedora 32:

1. Add the repository:  

```
sudo dnf config-manager --add-repo https://repo.fortinet.com/repo/6.4/centos/7/os/x86_64/fortinet.repo
```
2. Install FortiClient:  

```
sudo dnf install forticlient
```

### To install on Ubuntu:

1. Install the gpg key:  

```
wget -O - https://repo.fortinet.com/repo/6.4/ubuntu/DEB-GPG-KEY | sudo apt-key add -
```
2. Add the following line in `/etc/apt/sources.list`:
  - a. If using Ubuntu 16.04 LTS:  

```
deb [arch=amd64] https://repo.fortinet.com/repo/6.4/ubuntu/ xenial multiverse
```
  - b. If using Ubuntu 18.04 LTS or 20.04:  

```
deb [arch=amd64] https://repo.fortinet.com/repo/6.4/ubuntu/ bionic multiverse
```
3. Update package lists:  

```
sudo apt-get update
```
4. Install FortiClient:  

```
sudo apt install forticlient
```

## Installation folder and running processes

The FortiClient installation folder is `/opt/forticlient`.

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

## Starting FortiClient (Linux)

FortiClient (Linux) runs automatically in the backend after installation.

### To open the FortiClient (Linux) GUI:

1. Do one of the following:
  - a. In the terminal, run the `forticlient` command.
  - b. Open Applications and search for `forticlient`.

After running the FortiClient (Linux) GUI for the first time, you can add it to the favorites menu. By default, the favorites menu is usually on the left-hand side of the screen.



## Uninstalling FortiClient (Linux)

### To uninstall FortiClient from Red Hat or CentOS:

```
$ sudo dnf remove forticlient
```

If running Red Hat 7 or CentOS 7, replace `dnf` with `yum` in the command.

### To uninstall FortiClient from Ubuntu:

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

# Product integration and support

The following table lists version 6.4.2 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>FortiAnalyzer</b>	<ul style="list-style-type: none"><li>• 6.4.0 and later</li></ul>
<b>FortiClient EMS</b>	<ul style="list-style-type: none"><li>• 6.4.1 and later</li></ul>
<b>FortiManager</b>	<ul style="list-style-type: none"><li>• 6.4.0 and later</li></ul>
<b>FortiOS</b>	<p>The following FortiOS versions support SSL VPN with FortiClient (Linux) 6.4.2:</p> <ul style="list-style-type: none"><li>• 6.4.0 and later</li><li>• 6.2.0 and later</li><li>• 6.0.0 and later</li></ul> <p>The following FortiOS versions support endpoint control and SSL VPN with FortiClient (Linux) 6.4.2:</p> <ul style="list-style-type: none"><li>• 6.2.0 and later</li></ul>
<b>FortiSandbox</b>	<ul style="list-style-type: none"><li>• 3.2.0 and later</li><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 6.4.2. For inquiries about a particular bug, contact [Customer Service & Support](#).

## License

Bug ID	Description
681644	Change FortiClient (Linux) full version VPN expiry days from 3 to 30.

## Endpoint control

Bug ID	Description
648958	EMS fails to match on-fabric detection rule for connected media rule.
654504	FortiAnalyzer shows wrong SIEM information for CentOS 8.2.2004.
666077	FortiClient cannot report the domain it belongs to to EMS.
668065	FortiClient (Linux) loses license on CentOS after disconnecting from VPN.
675702	FortiClient (Linux) in VM fails to send Linux serial number to EMS.

## GUI

Bug ID	Description
650733	SSL VPN authentication radio button defaults to save login if prompt on login is selected.
657762	FortiClient (Linux) does not show disclaimer message when <i>Do Not Warn Invalid Server Certificate</i> is enabled.

## Configuration

Bug ID	Description
648505	Configuration backup does not display error message.

## Malware Protection

Bug ID	Description
612548	FortiClient (Linux) generates antivirus (AV) scan result summary log in the FortiClient /opt/forticlient install directory instead of logs folder.
652585	FortiClient (Linux) causes system hang when compiling if real-time protection is enabled.

## Vulnerability Scan

Bug ID	Description
652644	VCM engine has incorrect permissions and has write permissions for the group user.
656814	FortiClient does not parse vulnerability scan results correctly for Microsoft Office applications.
675044	FortiClient (Linux) fails to get latest vulnerability signature from FortiGuard Distribution Server.

## Remote Access

Bug ID	Description
649706	VPN option <code>prompt_username</code> should be set as false after username is saved.
649717	Always up does not reestablish connection when network is available.
651909	SSL VPN always up fails to work when network interface is turned down then up.
662719	FortiClient (Linux) cannot parse configuration when FortiGate pushes 1000 routes.

## Other

Bug ID	Description
672914	Endpoint control issues affect EMS performance.

## Known issues

The following issues have been identified in FortiClient (Linux) 6.4.2. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

### Endpoint control

Bug ID	Description
646115	Endpoint running process and network statistics information is not visible on EMS.
673119	DHCP IP address on-Fabric detection rule does not work.
675702	EMS does not show Linux device serial number.
676150	Cannot get software inventory from CentOS server.
678357	FortiClient (Linux) does not reflect Red Hat Enterprise Linux OS Zero Trust tag.

### Malware Protection

Bug ID	Description
649641	Real-time protection scan/scan on insertion does not work for removable media.
674410	GUI shows wrong antivirus scan message.

### Vulnerability Scan

Bug ID	Description
677700	CentOS Firefox vulnerability takes long time to patch.
677948	Scan results show no vulnerabilities found, while scan history records vulnerabilities.

## Remote Access

Bug ID	Description
675855	FortiClient (Linux) on Ubuntu does not accept SSL VPN <code>dns-suffix</code> <code>dhcp</code> settings.
677640	SSL VPN autoconnect with or without certificate and with FortiToken enabled does not work.
678647	FortiClient fails to connect to SSL VPN when using SAML authentication with third-party identity provider.
679212	SSL VPN SAML login does not work.
683687	FortiClient fails to auto-connect to FortiSASE VPN.

## Settings

Bug ID	Description
650625	FortiClient (Linux) exports configuration that contains a lot of settings inapplicable for FortiClient (Linux).

## Logs

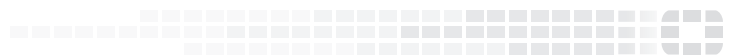
Bug ID	Description
650334	Feature list for log settings is inconsistent between EMS and FortiClient (Linux).
671898	XFS file system does not allow FortiAnalyzer logging.

## Other

Bug ID	Description
582302	FortiClient cannot get signature from FortiManager using HTTPS because of failed certificate check.



**FORTINET®**



Copyright© 2021 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.