

# Release Notes

## FortiClient (Linux) 7.2.7



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<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/training-certification>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



December 12, 2024

FortiClient (Linux) 7.2.7 Release Notes

04-727-1099389-20241212

# TABLE OF CONTENTS

<b>Change log</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>5</b>
Licensing .....	5
<b>Special notices</b> .....	<b>6</b>
ZTNA certificates .....	6
Installation of FortiClient fails on Ubuntu 23.10 .....	6
FortiGuard Web Filtering Category v10 Update .....	6
<b>Installation information</b> .....	<b>7</b>
Installing FortiClient (Linux) .....	7
Install FortiClient (Linux) from repo.fortinet.com .....	7
Installing FortiClient (Linux) using a downloaded installation file .....	8
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>
Endpoint control .....	11
GUI .....	11
Quarantine Management .....	11
Remote Access - IPsec VPN .....	11
Remote Access - SSL VPN .....	12
Web Filter and plugin .....	12
<b>Known issues</b> .....	<b>13</b>
New known issues .....	13
Existing known issues .....	13
GUI .....	13
Logs .....	13
Endpoint control .....	14
Remote Access .....	14
Remote Access - SSL VPN .....	14
Web Filter and plugin .....	14
ZTNA connection rules .....	14
<b>Numbering conventions</b> .....	<b>15</b>

# Change log

Date	Change description
2024-12-12	Initial release.

# Introduction

FortiClient (Linux) 7.2.7 is an endpoint product for well-known Linux distributions that provides FortiTelemetry, remote access (IPsec IKEv2 and SSL VPN), zero trust network access, malware protection, web filter, 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) 7.2.7 build 0905.

- [Special notices on page 6](#)
- [What's New in FortiClient \(Linux\) 7.2.7](#)
- [Installation information on page 7](#)
- [Product integration and support on page 10](#)
- [Resolved issues on page 11](#)
- [New known issues on page 13](#)

Review all sections prior to installing FortiClient.

## Licensing

See [Windows, macOS, and Linux endpoint licenses](#).

# Special notices

## ZTNA certificates

Zero trust network access (ZTNA) certificate provisioning requires Trusted Platform Module (TPM) 2.0 on the endpoint with one of the following:

- Maximum of TLS 1.2 in FortiOS
- Maximum of TLS 1.3 in FortiOS if the TPM 2.0 implementation in the endpoint supports RSA PSS signatures

For ZTNA tags for checking certificates, FortiClient (Linux) does not check user certificates and only checks root certificate authority certificates installed on the system. These routes are:

Operating system	Route
Ubuntu	/etc/ssl/certs/ca-certificates.crt
<ul style="list-style-type: none"><li>• CentOS</li><li>• Red Hat</li></ul>	/etc/pki/tls/certs/ca-bundle.crt

## Installation of FortiClient fails on Ubuntu 23.10

FortiClient (Linux) installation fails on Ubuntu 23.10. The workaround is to manually install the following packages on the Linux endpoint before installing FortiClient on Ubuntu 23.10:

```
apt install gconf2-common_3.2.6-8_all.deb  
apt install libgconf-2-4_3.2.6-8_amd64.deb
```

## FortiGuard Web Filtering Category v10 Update

Fortinet has updated its web filtering categories to v10, which includes two new URL categories for AI chat and cryptocurrency websites. To use the new categories, customers must upgrade their Fortinet products to one of the following versions:

- FortiManager - Fixed in 6.0.12, 6.2.9, 6.4.7, 7.0.2, 7.2.0, 7.4.0.
- FortiOS - Fixed in 7.2.8 and 7.4.1.
- FortiClient - Fixed in Windows 7.2.3, macOS 7.2.3, Linux 7.2.3.
- FortiClient EMS - Fixed in 7.2.1.
- FortiMail - Fixed in 7.0.7, 7.2.5, 7.4.1.
- FortiProxy - Fixed in 7.4.1.

Please read the following CSB for more information to caveats on the usage in FortiManager and FortiOS:

<https://support.fortinet.com/Information/Bulletin.aspx>

# 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](#).

FortiClient (Linux) 7.2.7 features are only enabled when connected to EMS 7.2.



You must upgrade EMS to 7.2 before upgrading FortiClient.

---

See [Recommended upgrade path](#) for information on upgrading FortiClient (Linux) 7.2.7.

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

### To install on Red Hat or CentOS:

1. Add the repository:

```
sudo yum-config-manager --add-repo  
https://repo.fortinet.com/repo/forticlient/7.2/centos/8/os/x86_64/fortinet.repo
```

2. Install FortiClient:

```
sudo yum install forticlient
```

### To install on Fedora:

1. Add the repository:

```
sudo dnf config-manager --add-repo  
https://repo.fortinet.com/repo/forticlient/7.2/centos/8/os/x86_64/fortinet.repo
```

2. Install FortiClient:

```
sudo yum install forticlient
```

### To install on Ubuntu 18.04 LTS and 20.04 LTS:

1. Install the gpg key:

```
wget -O - https://repo.fortinet.com/repo/forticlient/7.2/ubuntu/DEB-GPG-KEY | sudo apt-  
key add -
```

2. Add the following line in `/etc/apt/sources.list`:

```
deb [arch=amd64] https://repo.fortinet.com/repo/forticlient/7.2/ubuntu/ /stable  
multiverse
```

**3. Update package lists:**

```
sudo apt-get update
```

**4. Install FortiClient:**

```
sudo apt install forticlient
```

**To install on Ubuntu 22.04 LTS:**

**1. Install the gpg key:**

```
wget -O - https://repo.fortinet.com/repo/forticlient/7.2/debian/DEB-GPG-KEY | gpg --  
dearmor | sudo tee /usr/share/keyrings/repo.fortinet.com.gpg
```

**2. Create /etc/apt/sources.list.d/repo.fortinet.com.list with the following content:**

```
deb [arch=amd64 signed-by=/usr/share/keyrings/repo.fortinet.com.gpg]  
https://repo.fortinet.com/repo/forticlient/7.2/debian/ stable non-free
```

**3. Update package lists:**

```
sudo apt-get update
```

**4. Install FortiClient:**

```
sudo apt install forticlient
```

## 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 (Linux) installation rpm file> -y  
<FortiClient (Linux) 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 (Linux) using the following command:**

```
$ sudo apt-get install <FortiClient (Linux) installation deb file>  
<FortiClient (Linux) installation deb file> is the full path to the downloaded deb file.
```

## 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)

You cannot uninstall FortiClient while it is connected to EMS. Disconnect FortiClient from EMS before uninstalling it.

### 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 7.2.7 product integration and support information:

<b>Operating systems</b>	<ul style="list-style-type: none"><li>• Ubuntu 22.04 and 24.04</li><li>• CentOS Stream 9</li><li>• Red Hat 9 and later</li><li>• Fedora 36 and later</li></ul> All supported with KDE or GNOME
<b>AV engine</b>	<ul style="list-style-type: none"><li>• 6.00287</li></ul>
<b>FortiAnalyzer</b>	<ul style="list-style-type: none"><li>• 7.4.0 and later</li><li>• 7.2.0 and later</li><li>• 7.0.0 and later</li></ul>
<b>FortiAuthenticator</b>	<ul style="list-style-type: none"><li>• 6.5.0 and later</li><li>• 6.4.0 and later</li><li>• 6.3.0 and later</li><li>• 6.2.0 and later</li><li>• 6.1.0 and later</li><li>• 6.0.0 and later</li></ul>
<b>FortiClient EMS</b>	<ul style="list-style-type: none"><li>• 7.2.0 and later</li></ul>
<b>FortiManager</b>	<ul style="list-style-type: none"><li>• 7.4.0 and later</li><li>• 7.2.0 and later</li><li>• 7.0.0 and later</li></ul>
<b>FortiOS</b>	<p>The following FortiOS versions support zero trust network access with FortiClient (Linux) 7.2.7:</p> <ul style="list-style-type: none"><li>• 7.4.0 and later</li><li>• 7.2.0 and later</li><li>• 7.0.6 and later</li></ul> <p>The following FortiOS versions support SSL VPN with FortiClient (Linux) 7.2.7:</p> <ul style="list-style-type: none"><li>• 7.4.0 and later</li><li>• 7.2.0 and later</li><li>• 7.0.0 and later</li><li>• 6.4.0 and later</li></ul>
<b>FortiSandbox</b>	<ul style="list-style-type: none"><li>• 4.4.0 and later</li><li>• 4.2.0 and later</li><li>• 4.0.0 and later</li><li>• 3.2.0 and later</li></ul>

# Resolved issues

The following issues have been fixed in version 7.2.7. For inquiries about a particular bug, contact [Customer Service & Support](#).

## Endpoint control

Bug ID	Description
1100661	FortiClient (Linux) does not send SNI when connecting to on-premise EMS.

## GUI

Bug ID	Description
1061690	FortiClient (Linux) allows adding an IPsec VPN tunnel.

## Quarantine Management

Bug ID	Description
1071307	Manual quarantine does not work on Debian endpoints with IPv4 enabled.

## Remote Access - IPsec VPN

Bug ID	Description
1061455	FortiClient (Linux) does not support <code>network-id</code> to differentiate multiple IKEv2 certificate-based phase 1 tunnels.

## Remote Access - SSL VPN

Bug ID	Description
1082262	SSL VPN connections fail sometimes.
1099641	Creating SSL VPN tunnel fails when connecting to VPN over Wi-Fi.

## Web Filter and plugin

Bug ID	Description
1067489y	FortiClient generates SSL inspection certificate too frequently.

# Known issues

Known issues are organized into the following categories:

- [New known issues on page 13](#)
- [Existing known issues on page 13](#)

To inquire about a particular bug or to report a bug, contact [Customer Service & Support](#).

## New known issues

No new issues have been identified in version 7.2.7.

## Existing known issues

The following issues have been identified in a previous version of FortiClient (Linux) and remain in FortiClient (Linux) 7.2.7.

### GUI

Bug ID	Description
972930	FortiClient has delay in opening embedded or external browser after clicking <i>SAML</i> button for VPN connection.
1018080	FortiClient (Linux) disables <i>Remote Access</i> tab.
1102058	FortiClient (Linux) does not stop time elapsed counter for connected SSL VPN tunnel when network disruption occurs.
1102566	Toolbar is consistent between Ubuntu and CentOS.

### Logs

Bug ID	Description
872875	Disabling <i>Client-Based Logging When On-Fabric</i> in EMS does not work for Linux endpoints.

## Endpoint control

Bug ID	Description
1031812	User can turn off autoconnect on FortiClient (Linux) when pushed from EMS.

## Remote Access

Bug ID	Description
876539	FortiClient cannot resolve domain name properly using DNS server that SSL VPN pushed in Red Hat 9.
950306	SSL VPN creates two interfaces and routes, causing traffic loss.
1075772	VPN unity features are inconsistent with FortiClient (Windows).

## Remote Access - SSL VPN

Bug ID	Description
1027822	FortiClient fails to connect VPN with <i>Config routing table failed</i> error.
1087901	On Ubuntu 22.04, FortiClient shows 0 bytes while connected to SAML SSL VPN.
1094273	SSL VPN resiliency fails when FortiClient (Linux) cannot reach a gateway after reboot.
1101442	SSL VPN drops during file downloads through the tunnel.
1102801	FortiClient (Linux) using SAML authentication retains credentials.

## Web Filter and plugin

Bug ID	Description
939743	Web Filter does not support IPv6.
977317	FortiClient does not use Web Filter rating URL provided using XML tag on EMS.

## ZTNA connection rules

Bug ID	Description
1094278	Zero trust network access (ZTNA) fails to process when destination rule configured with port range.
1097804	FortiClient (Linux) does not save port range when ZTNA rules are manually created.

# Numbering conventions

Fortinet uses the following version number format:

<First number>.<Second number>.<Third number>.<Fourth number>

Example: 7.2.7.15

- First number = major version
- Second number = minor version
- Third number = maintenance version
- Fourth number = build version

Release Notes pertain to a certain version of the product. Release Notes are revised as needed.



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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 Chief Legal Officer, 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. 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.