

# Release Notes

## FortiClient (Linux) 7.0.11



**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)



January 31, 2024

FortiClient (Linux) 7.0.11 Release Notes

04-7011-983831-20240131

# 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
<b>Installation information</b>	<b>7</b>
Installing FortiClient (Linux)	7
Installing FortiClient (Linux) using a downloaded installation file	7
Installation folder and running processes	8
Starting FortiClient (Linux)	8
Uninstalling FortiClient (Linux)	8
<b>Product integration and support</b>	<b>9</b>
<b>Resolved issues</b>	<b>10</b>
Remote Access	10
Common Vulnerabilities and Exposures	10
<b>Known issues</b>	<b>11</b>
Avatar and social login information	11
GUI	11
Malware Protection and Sandbox	11
License	11
Logs	12
Remote Access	12
Configuration	12
Endpoint Control	13
Endpoint management	13
Vulnerability Scan	13
ZTNA connection rules	13

# Change log

Date	Change description
2024-01-31	Initial release.

# Introduction

FortiClient (Linux) 7.0.11 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) 7.0.11 build 0369.

- [Special notices on page 6](#)
- [What's New in FortiClient \(Linux\) 7.0.11](#)
- [Installation information on page 7](#)
- [Product integration and support on page 9](#)
- [Resolved issues on page 10](#)
- [Known issues on page 11](#)

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 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 9](#).

FortiClient (Linux) 7.0.8 features are only enabled when connected to EMS 7.0 or 7.2.



You must upgrade EMS to 7.0.2 or newer before upgrading FortiClient.

---

See [Recommended upgrade path](#) for information on upgrading FortiClient (Linux) 7.0.11.



FortiClient (Linux) 7.0.11 is not available to install from repo.fortinet.com.

---

## 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 or Debian:

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

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
```

### To uninstall FortiClient from Ubuntu:

```
$ sudo apt-get purge forticlient
```



# Product integration and support

The following table lists version 7.0.11 product integration and support information:

<b>Operating systems</b>	<ul style="list-style-type: none"><li>• Ubuntu 22.04 and later</li><li>• CentOS Stream 9 and later</li><li>• Red Hat 9 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>FortiClient EMS</b>	<ul style="list-style-type: none"><li>• 7.2.0 and later</li><li>• 7.0.0 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) 7.0.11:</p> <ul style="list-style-type: none"><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) 7.0.11:</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><li>• 6.2.0 and later</li></ul>
<b>FortiSandbox</b>	<ul style="list-style-type: none"><li>• 4.2.0 and later</li><li>• 4.0.0 and later</li><li>• 3.2.0 and later</li><li>• 3.1.0 and later</li></ul>

## Resolved issues

The following issues have been fixed in version 7.0.11. For inquiries about a particular bug, contact [Customer Service & Support](#).

## Remote Access

Bug ID	Description
960118	With <prefer_sslvpn_dns>=0, when SSL VPN is up, FortiClient adds dns-suffix to all network interfaces.

## Common Vulnerabilities and Exposures

Bug ID	Description
898817	FortiClient (Linux) 7.0.11 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2023-45590</li></ul>

## Known issues

The following issues have been identified in FortiClient (Linux) 7.0.11. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

### Avatar and social login information

Bug ID	Description
878050	FortiClient (Linux) avatar does not update on FortiGate dashboards and FortiGate cannot show updated information.

### GUI

Bug ID	Description
972930	FortiClient has delay in opening the embedded or external browser after clicking <i>SAML</i> button for VPN connection.

### Malware Protection and Sandbox

Bug ID	Description
888356	User can stop antivirus quick/full scan triggered from EMS.

### License

Bug ID	Description
874676	Endpoint is tagged with existing zero trust network access (ZTNA) host tags for vulnerabilities and antivirus after EMS license is updated from Endpoint Protection Platform to Remote Access.

## Logs

Bug ID	Description
872875	Disabling <i>Client-Based Logging When On-Fabric</i> in EMS does not work for Linux endpoints.
956357	FortiClient (Linux) keeps sending logs to FortiAnalyzer.
979669	User avatar fails to upload to FortiAnalyzer.

## Remote Access

Bug ID	Description
679023	If FortiClient is registered to EMS, EMS and FortiOS should control save-password, always-up and auto-connect.
781762	FortiSASE SSL VPN SAML autoconnect does not work.
782013	FortiSASE SSL VPN SAML always up does not work.
825387	SSL VPN with SAML when fully qualified domain name with DNS round robin is used for load balancing does not work.
851600	FortiClient fails to connect to SSL VPN with FQDN resolving to multiple IP addresses while FortiClient (Linux) could not reach resolved IP address.
871028	When SSL and IPsec VPN profile options are disabled, FortiClient (Linux) can connect to VPN.
876539	FortiClient (Linux) cannot resolve domain name properly using DNS server pushed by SSL VPN in Red Hat 9.
892847	FortiClient always saves SAML credentials. Credentials window is unavailable on subsequent login.
893237	User has no chance to reenter password during autoconnect after identity provider password change.
968070	<code>&lt;disallow_invalid_server_certificate&gt;</code> does not parse correctly in FortiClient (Linux).

## Configuration

Bug ID	Description
730415	FortiClient (Linux) backs up configuration that is missing locally configured ZTNA connection rules.

## Endpoint Control

Bug ID	Description
870938	Quarantined Linux client can connect to VPN via CLI.

## Endpoint management

Bug ID	Description
891264	EMS creates duplicate records for domain-joined Ubuntu endpoints.

## Vulnerability Scan

Bug ID	Description
832731	FortiClient server version <code>forticlient vulscan scan</code> command returns no vulnerabilities.

## ZTNA connection rules

Bug ID	Description
803402	Zero trust network access (ZTNA) certificate is not stored in snap installed Firefox in Ubuntu 22.04.



[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.